JYU DISSERTATIONS 472

Juhani Rauhala

Time, Money, and Freedom

The Costs of Internet Users' Privacy and Security Concerns

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 472

Juhani Rauhala

Time, Money, and Freedom

The Costs of Internet Users' Privacy and Security Concerns

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi Agora-rakennuksen auditoriossa Aud 1
joulukuun 10. päivänä 2021 kello 10.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium Aud 1 on December 10, 2021 at 10 a.m.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2021

Editors
Timo Männikkö
Faculty of Information Technology, University of Jyväskylä
Timo Hautala
Open Science Centre, University of Jyväskylä

Cover picture illustrators: Yogei Noojin and Rizal Harahap
Cover picture design: Juhani Rauhala

ISBN 978-951-39-8962-0 (PDF)
URN:ISBN:978-951-39-8962-0
ISSN 2489-9003

Permanent link to the online version of this publication: http://urn.fi/URN:ISBN:978-951-39-8962-0

ABSTRACT

Rauhala, Juhani
Time, Money, and Freedom – The Costs of Internet Users′ Privacy and Security Concerns
Jyväskylä: University of Jyväskylä, 2021, 144 p.
(JYU Dissertations
ISSN 2489-9003; 472)
ISBN 978-951-39-8962-0

Internet users with controversial viewpoints may be hesitant to voice their opinions online because they are concerned about consequences that could be inflicted by various entities. Firings, bans from social media, and doxing are some examples of the consequences. Users also have varying opinions about spending money for cybersecurity products and services. Concerns about the risks linked with online free expression may influence such opinions. In addition, some Internet users spend valuable time thinking about and configuring the security settings of their devices. Such time is spent to mitigate the security and privacy risks of the Internet. Some people may be irritated by the amount of time required. Users may be hesitant to express themselves online merely because configuring their devices for a sufficient level of security and privacy is a prerequisite for them, but it takes too much time and effort. Users may, for example, be aware of anonymizing tools and desire to express themselves online, but decide that spending time on anonymity is simply too much effort.

The associations between time spent on personal cybersecurity, the reluctance to express online, and a proclivity to purchase cybersecurity and cyberprivacy solutions do not appear to have been previously studied. The present work investigates the associations. A model is constructed to represent hypotheses, and data was collected using a survey. The model is validated by analyses on the data. The research results show the interrelationships between novel latent factors: 1. time spent by users on their device security and privacy settings, 2. users′ proclivity towards purchasing personal cybersecurity and cyberprivacy solutions, and 3. users′ reluctance to freely express themselves online. Relationships were found between the factors and some demographic and cultural variables. Additional security and privacy issues of smartphones are also considered for their potential impacts on Internet users′ behaviors. Finally, some new terminology is proposed to help understand the societal implications of modern technological advancements.

Keywords: online expression, privacy concerns, security concerns, personal cybersecurity spending, consumer cybersecurity spending, device settings, temporal perceptions, cultural indices, cybercrime, hacking, technology abuse, unorthodox weaponization, technology preterms

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Rauhala, Juhani
Aika, raha ja vapaus – Internetin käyttäjien yksityisyyttä ja turvallisuutta koskevien huolenaiheiden kustannukset
Jyväskylä: University of Jyväskylä, 2021, 144 p.
(JYU Dissertations
ISSN 2489-9003; 472)
ISBN 978-951-39-8962-0

Internetin käyttäjät, joilla on kiistanalaisia näkemyksiä, saattavat olla epäröiviä ilmaista mielipiteitään verkossa, koska he ovat huolissaan seurauksista, joita eri tahot voivat aiheuttaa. Potkut, sosiaalisen median käyttökiellot ja doxing ovat esimerkkejä seurauksista. Käyttäjillä voi myös olla erilaisia käsityksiä siitä, kuinka paljon rahaa heidän tulisi käyttää kyberturvallisuustuotteisiin ja -palveluihin. Huoli online-ilmaisunvapauteen liittyvistä riskeistä voi vaikuttaa siihen. Lisäksi jotkut käyttävät merkittävästi aikaa miettiäkseen ja konfiguroidakseen laitteidensa suojausasetuksia lieventääkseen Internetin turvallisuusriskejä, mikä voi ärsyttää heitä. Käyttäjät voivat epäröidä itsensä ilmaisemista verkossa pelkästään siksi, että laitteiden määrittäminen halutulle suojas- ja yksityisyystasolle vie liikaa aikaa ja vaivaa. Käyttäjät voivat esimerkiksi olla tietoisia anonymisointityökaluista ja haluta ilmaista itseään verkossa, mutta päätyvät siihen, että anonymisointiin kuluva vaiva on liian suuri.

Henkilökohtaiseen kyberturvallisuuteen käytetyn ajan, online-ilmaisun vastahakoisuuden sekä kyberturvallisuus- ja tietosuojaratkaisujen ostamishalukkuuden välisiä yhteyksiä ei näytä olevan aiemmin tutkittu. Tämä työ tutkii näitä yhteyksiä. Työssä on rakennettu hypoteeseja esittävä malli, ja kerätty validointia varten data kyselyllä. Malli validoidaan tietojen analysoinnilla. Tutkimustulokset osoittavat suhteet uusien piilevien rakenteiden välillä: 1. käyttäjien laitteen turvallisuusasetuksiin käyttämä aika, 2. käyttäjien taipumus ostaa henkilökohtaisia kyberturvallisuus- ja tietosuojaratkaisuja ja 3. käyttäjien haluttomuus ilmaista itseään vapaasti verkossa. Tekijöiden ja joidenkin demografisten ja kulttuuristen muuttujien välillä havaittiin tilastollisia riipuvuuksia. Älypuhelimien turva- ja yksityisyyskysymyksiä arvioidaan myös niiden mahdollisten vaikutusten vuoksi Internetin käyttäjien käyttäytymiseen. Lopuksi ehdotetaan uutta terminologiaa, joka auttaa ymmärtämään teknologisen kehityksen yhteiskunnallisia vaikutuksia.

Avainsanat: verkkoilmaisu, ilmaisunvapaus, yksityisyyden suoja, turvallisuusongelmat, henkilökohtaiset kyberturvallisuusmenot, kuluttajien kyberturvallisuusmenot, laiteasetukset, aikakäsitykset, kulttuuriset indeksit, tietoverkkorikollisuus, hakkerointi, teknologian väärinkäyttö, epätavallinen aseistus, psykologian sanastoa, teknologian sanastoa

Author

Juhani Rauhala
Faculty of Information Technology
University of Jyväskylä
Finland
juhani.jr.rauhala@jyu.fi
ORCID 0000-0003-0427-9531

Supervisors

Pasi Tyrväinen
Faculty of Information Technology
University of Jyväskylä
Finland

Nezer Zaidenberg
Faculty of Computer Science
College of Management Academic Studies
Israel

Pekka Neittaanmäki
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers

Rauno Kuusisto
Information Technology Division
Finnish Defence Research Agency
Finland

Simon Trang
Chair of Information Security and Compliance
University of Göttingen
Germany

Opponent

Aggeliki Tsohou
Department of Informatics
Ionian University
Greece

ACKNOWLEDGEMENTS

A doctoral degree is not a be-all and end-all, but many things had to fall into place for me to have the privilege of trying to achieve one. I have received help, inspiration, and encouragement in many forms and from many people over many years, including the years before the beginning of my Ph.D. studies. There are too many people to remember, and I apologize to those I may have overlooked while writing this section.

I would like to express my deepest appreciation to Prof. Pasi Tyrväinen ("it's getting there!") for his scientific guidance, patience, and for allowing me to make mistakes; and to Prof. Pekka Neittaanmäki ("over 120") for his consistent encouragement, help with my dissertation, and for admitting me into the doctoral program. I am also grateful to Prof. Mikko Rönkkö ("make a dummy variable") for his invaluable and solid advice with statistical methods, Prof. Timo Hämäläinen of my follow-up group for his support, Prof. Mikko Siponen ("there's something interesting going on"), Prof. Martti Lehto ("the human aspect"), Dr. Nina Pekkala for much practical advice, Päivi Parikka for the warm welcome to Agora Center, Irawan Nurhas for (among other things) his extensive patience, and Dr. Adrienn Károly for her useful courses on dissertation writing and for her advice on preparing this section. In his role as my supervisor, I wish to extend my sincere thanks to Dr. Nezer Zaidenberg for the important big and small ways that he helped me along. Also helpful to me was the funding that I received from the Agora Center, C.O.M.A.S., and the IT Faculty for my research. I thank Riikka Valkonen for suggesting that I consider applying for a Ph.D. program. A very special thanks is due to all of the survey respondents from around the world. The work of the many editors and anonymous reviewers that reviewed my submitted manuscripts also deserves recognition.

Many thanks to my dissertation pre-examiners Prof. Rauno Kuusisto and Prof. Simon Trang for their thorough reviews of my manuscript, and to scientific editor Dr. Timo Männikkö for his editorial guidance, and to Prof. Tuure Tuunanen. Much gratitude is also due to my defense opponent, Prof. Aggeliki Tsohou. I am also grateful to Timo Hautala of the Open Science Center publishing unit, graduate school coordinator Dr. Sami Kollanus for answering some naïve questions, Dr. Robert Willison for a very insightful discussion on privacy research, Kati Valpe, Marja-Leena Rantalainen for her editing assistance, Prof. Yixin Zhang for her feedback on my journal manuscript, Tiina Lampinen for her kind help with my conference participation, and Dr. Elina Jokinen for cluing me in to new methods to perform writing. I would like to thank Prof. Andrei Costin for his interesting cybersecurity colloquium, and - reaching a bit further back in time – Pertti Saarinen, Kari Ikonen, Reino Talarmo, Kimmo Kinnunen, Lauri Rantaniva for help with my patents, Prof. Sung Hu ("I saw it happen"), Prof. Amid Shahnasser for his always jovial support, Prof. V.V.Krishnan ("Kolmogorov-Smirnov"), Jean Georgakopolous (*long silence*), Phyllis Price, Armando Piccioto ("OK students, boot up the computers!"), and (unfortunately I no longer remember her first name) Ms. Cole ("negativism is a luxury that I can't afford").

I would also like to acknowledge Prof. Rain Ottis ("looks very interesting"), Hilkka Grahn, Dr. Naomi Woods for her course on information security, Dr. Arttu Hakala, Prof. Joon Park ("anytime I can be of help"), Dr. Char Sample, Prof. Tamara Dinev for kindly sharing one of her important research publications with me; Prof. Jun Dai, Prof. Jon Celesia ("that would be cool"), Tiia Puputti ("the audio wasn't clean"), and Lea Hakala. Again reaching a little more into the past, thanks also to Prof. Amir Tabrizi ("you will learn it"), Dr. Mehrdad Nikoonahad ("this is exactly what I didn't want"), Prof. Ken Landon ("so to speak"), Prof. Nouri Shahabi ("I can see that you are tired"), Dr. Patrick Brunelle ("if you can see what I'm indicating"), my very strict typewriting teacher Vernon Bonham ("start over"), David Dansky, Raija-Liisa Ahonen, and Bob Yost for showing how to fight back from adversity.

A special thank you to Tuure, Inca, and Nella for their inspiring ways of looking at the world. Finally, this journey would not have been possible without the support of my family – including Maiju, Martti, Paula, Reijo, and wife Johanna – and friends that believed I could do this (you know who you are).

Jyväskylä 26.11.2021

Juhani Rauhala

LIST OF ABBREVIATIONS

APCO	Antecedents-Privacy Concerns-Outcomes Research Model
BoP	Barrier of Practicality
CVE	Common Vulnerabilities and Exposures
HFI	Human Freedom Index
HFI-EF	HFI Expression Freedom
HFI-PF	HFI Personal Freedom
IDV	Individualism (Hofstede index)
IMSI	International Mobile Subscriber Identity
LoM	Loss of Money
MAS	Masculinity (Hofstede index)
PTS	Personal Technology Space
RtoEx	Reluctance to Express
RtoExC	Reluctance to Express when Consequences Mentioned
RtoExnC	Reluctance to Express when Consequences Not Mentioned
TChS	Think About and/or Change Settings
TMT	Too Much Time
UAI	Uncertainty Avoidance (Hofstede index)

FIGURES

TABLES

CONTENTS

LIST OF PUBLICATIONS

This dissertation is based on the following publications. This dissertation also contains new content that is not included in the publications. Some of the previously unpublished content may be used to prepare additional manuscripts.

PI Juhani Rauhala, Pasi Tyrväinen, Nezer Zaidenberg, Online Expression and Spending on Personal Cybersecurity, 18th European Conference on Cyber Warfare and Security (ECCWS2019), 4-5 July 2019, Coimbra, Portugal, Published by Academic Conferences and Publishing International Limited, Book version ISBN: 978-1-912764-28-0, E-Book ISSN:2048-8610. JUFO ID = 71915.

PII Juhani Rauhala, Pasi Tyrväinen, Nezer Zaidenberg, Does Time Spent on Device Security and Privacy Inhibit Online Expression?, 18th European Conference on Cyber Warfare and Security (ECCWS2019), 4-5 July 2019, Coimbra, Portugal, Published by Academic Conferences and Publishing International Limited, Book version ISBN: 978-1-912764-28-0, E-Book ISSN:2048-8610. JUFO ID = 71915.

PIII Juhani Rauhala, Pasi Tyrväinen, Nezer Zaidenberg, Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime, Encyclopedia of Criminal Activities and the Deep Web, Published by IGI Global, 2020. ISBN: 978-1-522597-15-5, EISBN: 978-1-522597-16-2. JUFO ID = 5478.

PIV Juhani Rauhala, Nezer Zaidenberg, Pasi Tyrväinen, The Effect on Expression Reluctance of Spending Time on Privacy and Security Issues. For submission to the journal Computers and Security. Elsevier. (draft manuscript) 2021. JUFO ID = 53963.

PV Juhani Rauhala, Physical Weaponization of a Smartphone by a Third Party, Cyber Security, Springer, ISBN: 978-3-030-91292-5. Accepted manuscript; to be published December 2021.

PVI Juhani Rauhala, Storage Profiles, Patent No.: US 8,583,689, Date of Patent: Nov. 12, 2013.

PVII Juhani Rauhala, Storage Management, Patent No.: US 8,135,745, Date of Patent: March 13, 2012.

CONTRIBUTION AND ROLE OF THE AUTHOR IN THE ARTICLES

For articles I, II, III and IV I am the main author, and Pasi Tyrväinen and Nezer Zaidenberg are co-authors. Articles I, II, III and IV were done in close collaboration with co-authors Pasi Tyrväinen and Nezer Zaidenberg. Pasi Tyrväinen provided guidance on science, methodology and content, while Nezer Zaidenberg provided guidance mainly on content and style. With the scientific guidance of Pasi Tyrväinen, I designed the survey questionnaires that were used to collect data. Nezer Zaidenberg provided comments and feedback on the survey design. All authors of articles I, II, III and IV participated in data collection. I am the sole author and contributor of article V, and the sole inventor of patents VI and VII.

Articles I - III have been published in Jufo level 1 publications. Article V has been accepted for publication in a Jufo level 1 publication. Article IV is a draft manuscript and is intended for submittal to a journal of Jufo level 2 or 3.

"Ladies and gentlemen…this is a rock."

—Kenneth W. Landon
Professor of Astronomy and Geology

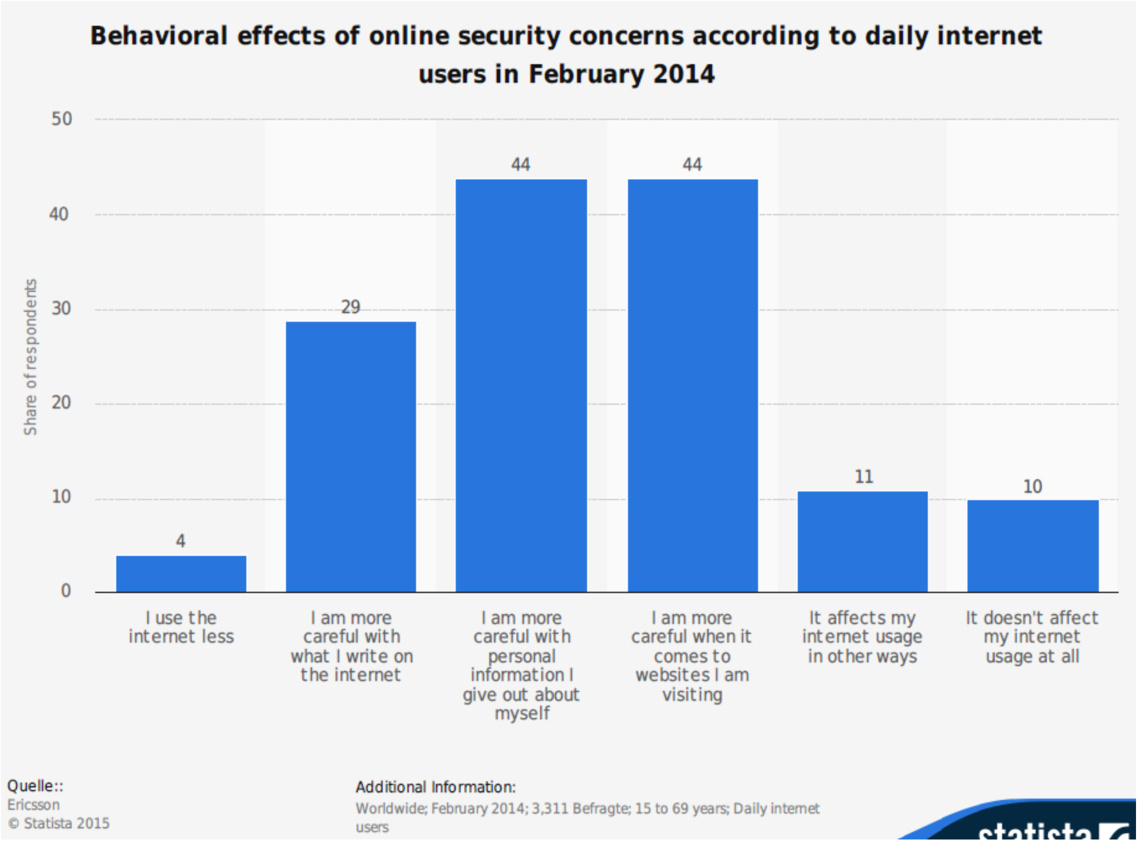
1 INTRODUCTION

Freedom of expression is a widely recognized human right. More recently, it seemed that unrestricted access to the Internet was also becoming recognized as a human right. The Internet is increasingly being used as a forum for both free speech and e-commerce. The security and privacy hazards that come with accessing the Internet are viewed differently by different Internet users. The users also have specific worries and behaviors when it comes to using the internet to express themselves. Users may hold divisive opinions, which they can express in a variety of ways online. Though laws in the jurisdiction of a user may guarantee freedom of speech, controversial opinions or artwork by their natures may not be as well received as favorable or polite comments. The use of the Internet for free speech can be a technique to get around censorship or other barriers to citizens' freedom of expression that may exist in more traditional publication outlets.

The Introduction is divided into the following sections that introduce the topic areas of the dissertation. The topic areas include those presented in the attached articles, supplemental content that includes privacy and security issues that are related to the dissertation theme, and proposed new terminology.

1.1 Motivation

Internet privacy and security concerns cause users to inhibit their Internet usage in various ways (Figure 1).



Behavioral effects of online security concerns according to daily internet users in February 2014

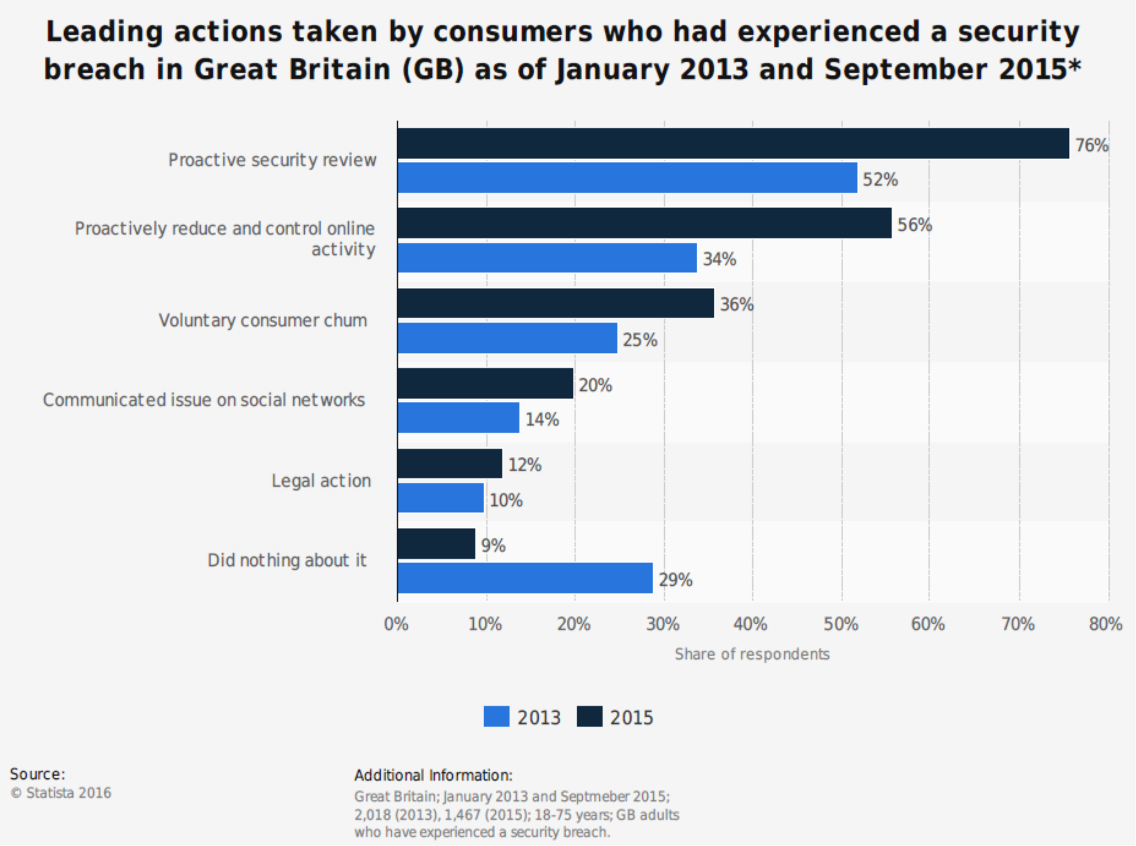
Quelle::
Ericsson
© Statista 2015

Additional Information:
Worldwide; February 2014; 3,311 Befragte; 15 to 69 years; Daily internet users

Figure 1: Behavioral effects of security concerns (Ericsson, 2014)[1]

Users who may have been previously unconcerned about security but have then experienced a data breach have indicated that they take certain actions after the discovery of the breach. The actions include modification and restriction of their own online behaviors (Figure 2). As the chart shows, the tendency of British users to take action has increased in the period from 2013 to 2015.

[1] Figures 1 through 5 are reprinted with permission of Statista



Leading actions taken by consumers who had experienced a security breach in Great Britain (GB) as of January 2013 and September 2015*

Source:
© Statista 2016

Additional Information:
Great Britain; January 2013 and Septmeber 2015; 2,018 (2013), 1,467 (2015); 18-75 years; GB adults who have experienced a security breach.

Figure 2: Actions taken after security breach (Deloitte, 2015)

1.1.1 The importance of free online expression

83% of Internet users worldwide consider online free speech and political expression to be important (CIGI & Ipsos, 2015). Freedom of expression has been designated a universal human right by the United Nations General Assembly (UN General Assembly, 1948). The United Nations has decided that unrestricted access to the Internet is a human right as of 2016. (UN Human Rights Council, 2016). The Internet's ability to serve as a forum for free expression is widely acknowledged. Importantly, political subjects, as well as other topics that are not socially approved, are discussed.

Debates and discussions that occur over online forums and social media, such as Twitter and Facebook, are raising attention to virtually unlimited arrays of topics. Socially controversial topics and political topics are also discussed. The importance of online expression has been recognized for various contexts. In oppressive states, free expression enabled by access to the Internet can be crucial for advancing human rights (Nadi and Firth, 2004).

Internet communication is generally beyond the nation-state’s territorial control, and access to the Internet has been acknowledged as critical to freedom of expression and democratic engagement (Lucchi, 2011). Previous research has shown that using the Internet for free expression can help people avoid censorship and other barriers. Authoritarian regimes have imposed censorship on citizen expressions in traditional publishing media but have more difficulty doing so online (Nadi and Firth 2004). The perceived effectiveness of the Internet against authority or as a tool to provoke insurrection can be evidenced by some governments' restrictions of Internet access in times of protest or upheaval (Cwienk, 2019; Reuters Staff, 2021).

Many states have begun to use legislative or other ways to impose online surveillance on their residents (Ray and Kaushik 2017). According to the findings, the purported justifications for such surveillance, such as the prevention of cyberterrorism or cybercrime, are dubious and out of proportion to the breadth of surveillance sought by the government. Although such surveillance does not directly restrict online expression, it can cause users to be hesitant or concerned. The user may be afraid of being monitored if he or she criticizes the government or its policies in an online forum. Various levels of censorship and limits on online expression are also directly imposed by many states. (Ray and Kaushik 2017).

Booth (2017) has proposed research on the effects of freedom of expression and access to information on the benefits of ICT to national well-being. As of this writing, her research has not been completed. Moreover, her research does not consider the relationship between free online expression and aspects of individual Internet users.

The importance of free online expression is also attested to by the efforts of certain organizations to address possible threats to it. Such threats can even include unanticipated consequences of regulations that are intended to protect privacy, such as the "right to be forgotten" (Stanton, 2014).

Bandyopadhyay (2011) discovered that Internet users' online privacy concerns are influenced by characteristics such as their level of Internet literacy, social awareness, and cultural background. He discovered that one of the possible outcomes of such concerns is a reluctance to utilize the Internet. It is reasonably assumed that this outcome would also limit users' online expressionism.

There are potential consequences for users who make controversial or provocative expressions on the Internet. The consequences can manifest in a variety of ways. The consequences can include a negative reaction from the government (Baroni, 2015; Cooper, 2000; Mony, 2017) or offended individuals (Cassidy, 2017), employers (Jaschik, 2014), or schools (Curtom, 2014). Consequences may also be exacted by vindictive criminal hackers. Cybercrime against individuals has been defined as:

"*Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)*" (Halder & Jaishankar, 2012).

Victims may become a target of doxxing or a target of cybercriminal gangs on the Deep Web. Previous research (Riek & Böhme, 2018) attempted to examine the monetary and non-monetary costs of consumer-facing cybercrime. Scams and financial fraud were among the cybercrime instances examined in the study. Victims of "revenge hacking" and doxxing have suffered terrible consequences (Branigan, 2011; Dascalescu, 2018).

During the 2020 coronavirus pandemic, some whistleblowers and dissidents used the Internet to spread their messages about the crisis.
Those posting unconventional information deemed “fake” were subject to bans of their social media accounts (Gibson 2020; Gandel 2020). A physician was threatened by authorities for posting information online about the spread of the disease (Hegarty 2020). His government declared the information to be false and disruptive to society. An ultra-wealthy tycoon disappeared under questionable circumstances after posting a critical online commentary about the management of the crisis (Tak-ho et al. 2020). Neither wealth nor status necessarily shields users against consequences for their controversial online expressions.
Users may also be concerned about becoming a victim of cyberbullying. Substantial time spent on social media, combined with perceived anonymity, create an environment conducive to cyberbullying (Lowry et al., 2016). Participating in social media is a form of personal expression, and some study on the effects of perceived security threats on users' social media behavior is now underway (Alqubaiti et al., 2016). In the information systems context, researchers have examined neutralization theory. Neutralization theory could apply in a case where a user justifies making an expression that could be considered a violation of law or policy. For example, posting criticism of a king or dictator is illegal in some states (Phelan 2014). In such states, the act is illegal, regardless of whether the criticism is legitimate (e.g., against an unjust decree). The poster neutralizes his illegal criticism as, e.g., resistance to injustice. For example, Siponen and Vance (2010) found that neutralization is an important factor in determining employees’ intention to violate information security policies. The proclivity of cyberbullies to invoke neutralization for their attacks increases with their perceived anonymity (Lowry et al., 2016). This finding would seem to lend credence to a hypothesis that privacy protection (in the form of anonymity) can be a prerequisite to making a controversial expression (in the form of bullying).

1.2 Scope

This research attempts to find the relationships between certain attitudes and behaviors of Internet users. The attitudes and behaviors are defined as six derived latent constructs. Two constructs (which are also combined into a single second-order construct) represent a reluctance to express oneself in the online environment. One of them includes a mentioning of consequences of controversial expression, while the other doesn’t.

Two of the constructs represent the time and effort used for the security and privacy settings of devices. One construct represents the behavior and attitude of users toward purchasing personal cybersecurity products and services. With these six constructs, selected demographic variables, selected cultural indices, selected HFI values and suitable analysis techniques, this research explores the relationships between the constructs and variables and makes a research contribution. It contributes to fields of knowledge about the behavior and attitudes of Internet users.

The various concerns of Internet users may inhibit them from using the Internet for certain tasks. Some concerns pertain to the security of their data. Some users limit their activity due to fears of data breaches or hacking. This dissertation describes novel methods of data profiling and data management that can mitigate some of the risks to users' data from breaches and hacks.

With new technologies comes the potential for the abuse of the technologies. This dissertation includes an exploration of hypothetical methods to physically weaponize a smartphone. Because smartphones are personal devices that are used by billions of users globally, the potential methods of weaponizing them merit preventive investigation.

Terminology science describes special lexemes (or lexical units), which are studied for the meanings and denotions of concepts. Terminology science also engages in the appraisal of existing definitions (Wikipedia Contributors, 2021a). New scientific concepts can be described by types of lexemes called preterms that can be composed of multiple words. (Wikipedia Contributors, 2021a).

ICT is a rapidly evolving field due to the continuous development of new technology and tools, and new emerging research. In the modern computer age, many new technologies have been adopted on a mass scale. Governments, providers of essential services, consumers, and other entities have adopted the technologies. Because ICT has evolved so rapidly (and continues to do so), the terminology for describing concepts related to the field should evolve and be updated as needed. New terminology becomes necessary for the discussion of modern concepts that cannot be succinctly and coherently described in an efficient way using traditional terms of a field. Chapter 5.1 introduces and proposes some new preterms for the current and rapidly evolving field of ICT. The new preterms are intended to address issues that include Internet privacy, information security, and cybersecurity.

1.3 Definitions

In the hypotheses in the article overviews, the following abbreviations are used (PIII):

LoM: Loss of money; personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

RtoEx: Reluctance to express; the reluctance to freely express oneself online or on the Internet.

RtoExC: Reluctance to express due to concerns of possible consequences or safety; the reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.

RtoExnonC: Reluctance to express when users are not reminded of possible consequences or safety issues resulting from the expression.

TChS: Thinking about and changing settings; time considering two aspects of one's ICT device –contemplation of the device's cybersecurity aspects and whether time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

TMT: Too much time; the perception that cybersecurity risk amelioration requires excessive usage of one's time.

This dissertation also proposes the following new preterms:

Adversarial surveillance: *The act of seeking and gathering personal information about an individual for benign or hostile purposes.*

Adversarial detective: *A person or organization that engages in the seeking and gathering of information about an individual for benign or hostile purposes.*

Barrier of practicality: *collectively, those hindrances and obstacles that prevent the immediate and widespread broadcasting or availability of (sensitive or confidential) information.*

Personal technology space: *The expectation of privacy that a person has with their technology; the information that their technology processes, the way that that processed information is used; and the way that their technology is used.*

The following definitions of cyberprivacy and e-stop are discussed in section 5.1.6.

At this time, **cyberprivacy** is tentatively defined as privacy in the context of all connected high-technology. Includes aspects that are encompassed by the common term "Internet privacy."

E-stop is tentatively defined as a cessation of use, adoption or development of a new or emerging technology in order to assess the technology's implications to societal well-being and functioning.

1.4 Outline of thesis

This dissertation consists of the following chapters.

Chapter 1 presents the introduction of the dissertation, including its motivation, scope and outline.

Chapter 2 presents a literature review.

Chapter 3 presents the research framework, including research gaps, research questions, and methods.

Chapter 4 presents an overview of articles PI-PIV, which encompass the central theme of our research. It also presents supplemental findings that are based on an expanded data set.

Chapter 5 presents some supplemental topics that are related to the dissertation theme. Article V and patents VI and VII are presented. Article V describes physical weaponizations of smartphones that, if ever implemented, could cause distress and harm to smartphone users. Patents VI and VII are presented as methods that, if implemented, could alleviate users' concerns about the security of their data.

Chapter 5 also introduces a proposal for the adoption of some new technology preterms. The preterms are intended to enhance the discussion and understanding of the impacts of technology on users' expectations of autonomy and privacy of their data and the online presence of their true 'selves.'

Chapter 6 presents the results of the research. The chapter also discusses some implications for the patents and proposed new preterms.

Chapter 6 is followed by a discussion, conclusion, summary, and appendices.

2 LITERATURE REVIEW

The following sections include an overview of prior research on themes of time, money, and freedom that relate to users' Internet behavior and attitudes.

2.1 Time

Many users spend time making adjustments to the privacy and security settings of their software and devices (Figure 3, Figure 4, Figure 5).

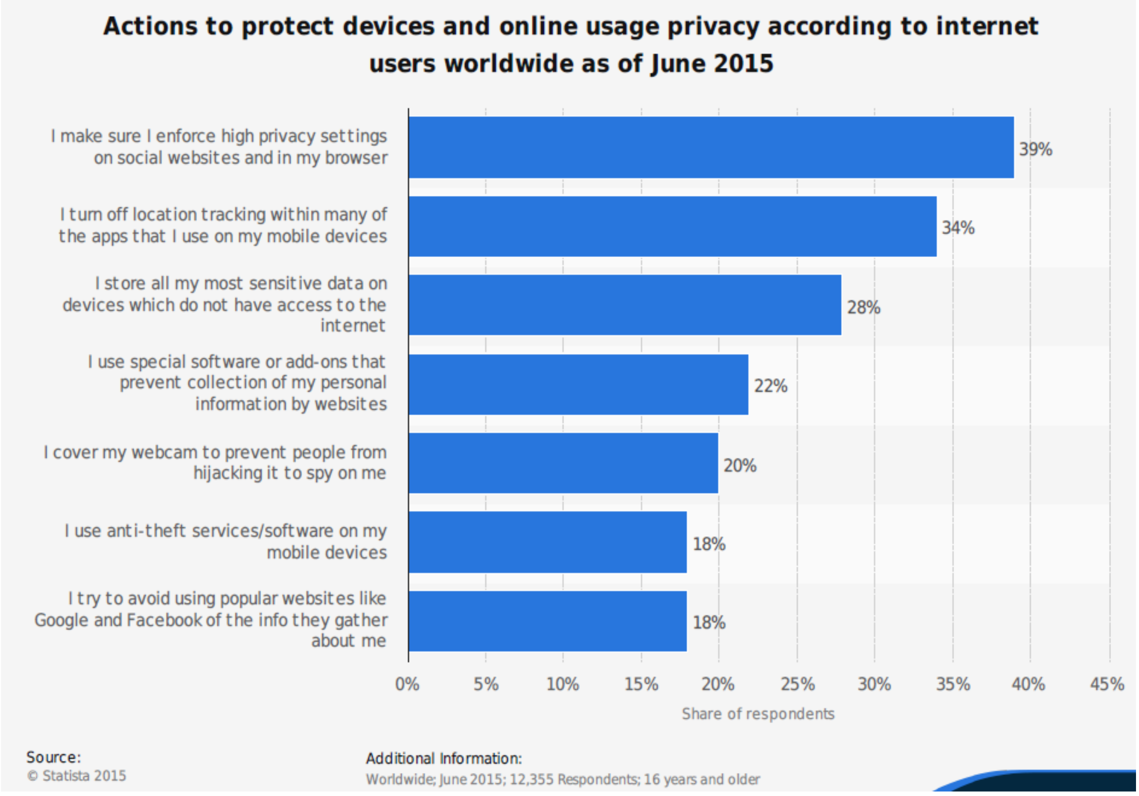


Figure 3: Actions to protect device privacy (CIGI & Ipsos, 2016)

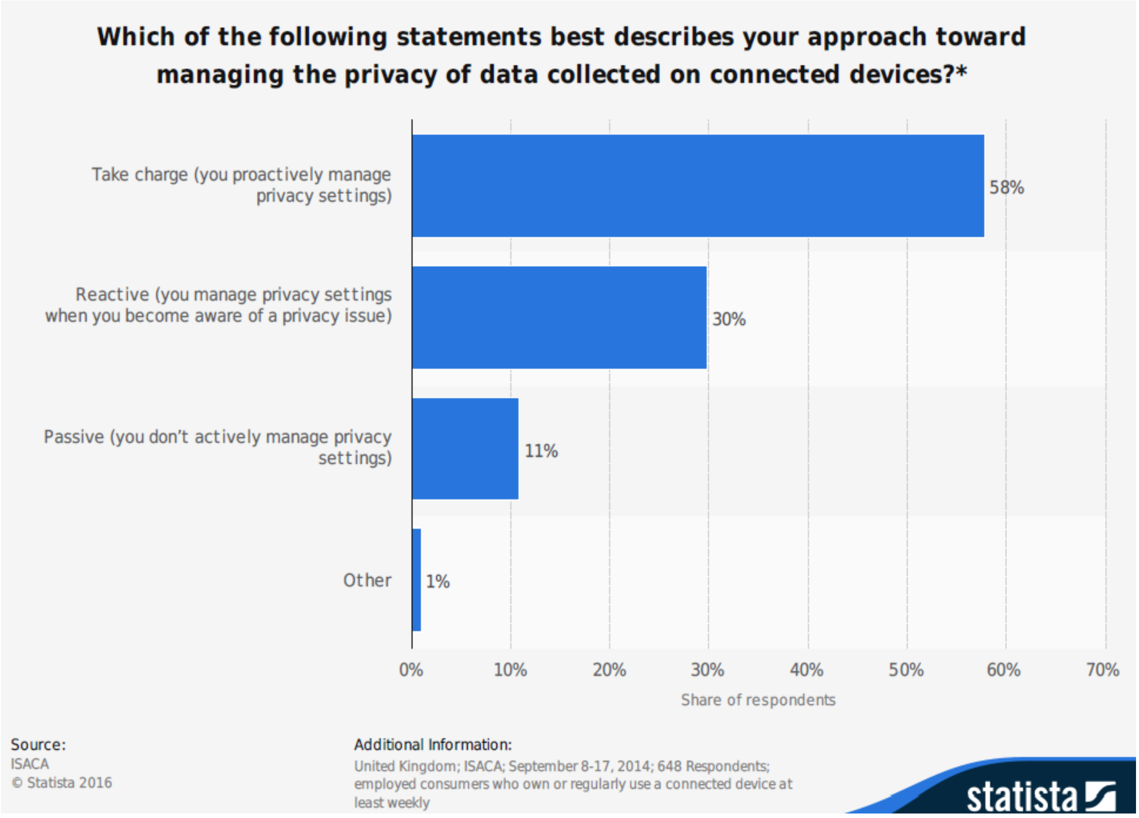


Figure 4: Data privacy management (ISACA, 2014)

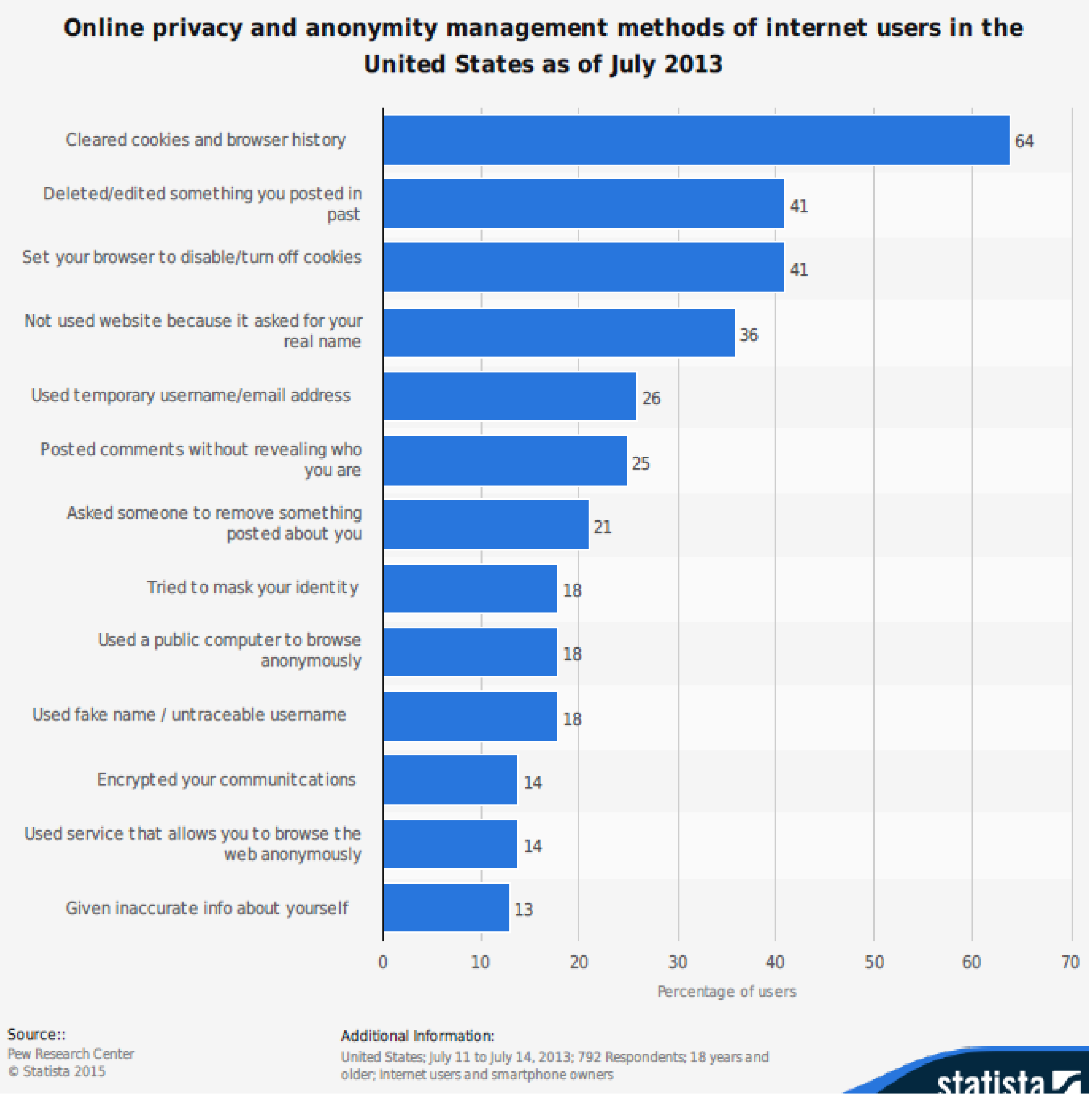


Figure 5: Privacy management of users in the US (Pew Research Center, 2015)

The amount of time Internet users spend on self-protective cybersecurity and privacy-related activities reduces the amount of time they have available for other activities. Spending time connecting to a secure VPN or updating security software, for example, when utilizing open WiFi connectivity in a public location or car, leaves less time for texting and reading social media updates.

Most mouse clicks or screen taps may incur a loading delay when using the Internet. However, the amount of time spent waiting for a security software update process to complete varies. It may occur, e.g., weekly, monthly, or with each session. The frequency is also dependent on such manual updates that the user performs.

Time is quantifiable; however, humans' attitudes or perceptions about the utility or quantity of their expended time are more difficult to measure. Ancona et al. (2001) have described a temporal conceptualization category that they call "actors relating to time." This category includes temporal perceptions and temporal personality. Concerning temporal perceptions concept, the perceptions of

Internet users about the usage of their time may be affected by the "novelty of time" effect, as described by Butler (1995), and by the "time in retrospect" effect (Hicks et al. 1976). The time in retrospect effect could cause a user to overestimate the length of a period of time if it was one in which the user was occupied by activities.

Generally, the excess use of time spent waiting can be merely a perception but may still have negative consequences in terms of user experience or perception of the services for which the waiting is done (Dellaert and Kahn 1999; Business Editors 2002). A study was performed to determine how consumers react when web pages of shopping websites take too much time to load (Anonymous 2010). It found that 70% of respondents reported that they abandon shopping on a site if the site takes more than 10 seconds to load, and 35% said they would not return if the loading delays take "too long."

On the other hand, the tolerance of users to the amount of time spent waiting will vary according to the individual and the context (Katz and Martin 1989). Chatzitheochari and Arber (2012) studied differences in free time between genders for working people in the UK. In all cases, women had the same or less quantity of pure free time as men. Moreover, womens' free time tended to be of lower quality and more subject to interruptions than mens'.

Excessive non-ideal time consumption, therefore, can be said to detract from more desirable activities and may cause a negative perception of offerings associated with waiting. Frustration with excessive time consumption can result in a negative attitude toward, and possibly abandonment of, desirable online content and activities as well. Such activities can include varying forms of expression.

2.2 Money

A generally accepted beneficial use of the Internet is as a platform for commerce, which is continuously increasing (Emarketer.com, 2014). At the same time, spending by consumers and businesses on cybersecurity products and services is also increasing (Morgan, 2017). It is reasonable to expect that users purchase a significant proportion of personal cybersecurity software online. Much of the previous literature on consumer e-commerce has investigated demographic aspects. The remainder of the literature overview on ′money′ overlaps with demographics and is therefore presented in section 2.4.

2.3 Freedom

The importance and consequences of free expression was outlined in the Introduction. Prior research exists on measuring free expression and the innate freedom in different settings. Controversial expressions are those that arouse quarrel or strife or are marked especially by the expression of opposing views (Merriam-Webster n.d.b). As such, they may be interpreted as negative, hostile, or provocative. Controversial expression in an online communications context is affected by certain factors. Such factors include perceived anonymity and familiarity with other online community participants (Luarn and Hsieh 2014). Luarn and Hsieh studied the expression behavior of users in a laboratory-controlled virtual community. The virtual community simulated different online group communications environments. They found that users were more willing to express controversial opinions when their identities were anonymous or when they were familiar with other members of the community. When users in the study were not anonymous, they were more reluctant to express such opinions. This is consistent with Lowry et al.'s (2016) findings insofar as the expressions of cyberbullying can be considered controversial. They also found that there was no effect of anonymity or member familiarity on users' willingness to express non-controversial opinions. Thus, privacy in the form of anonymity can be a prerequisite for a controversial expression in a community where members are unfamiliar.

Online expression may take the form of a hostile communication perceived by a reader to be personally directed at him or her. Jane (2015) has commented on problems with existing research regarding hostile personal communications, or "flaming." Jane states that an inordinate amount of research is predicated on preserving the right of the expressor of hostile communication to make such communications. She argues that more attention should be given to the consequences of the communication in those cases where there the recipient perceives that he or she has been flamed. While my articles' co-authors and I acknowledge that in many cases a controversial expression may be strongly worded or hostile, and may be directed at an individual or organization who may perceive the expression as offensive, we assert that free online expression has intrinsic value and significant societal importance that outweigh the risk of causing offense. Indeed, it can be argued that it is only for offensive or controversial speech that the protections of free speech are intended. We agree with Jane's recommendation but do not address the ethical and legal aspects of controversial expressionism in PI-PIV.

Prior research shows that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications. They found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome.

Liu et al. (2016) applied social exchange theory to examine the perceived risks and rewards of individual users' self-disclosure in social media. The authors found that perceived privacy risk can reduce the willingness of social media users to disclose personal information.

Previous research has looked at the consequences of free expression as well as the advantages of free expression. On a 0-100% or 0-10 scale, users' willingness to share their ideas online has been quantified in terms of a web forum's view/reply ratio (Shen & Liang, 2015) and by asking users how likely they would be to voice their opinions in specific online circumstances (Ho & McLeod, 2008; Stoycheff, 2016). To test willingness to self-censor, Hayes et al. (2005) developed a self-reporting questionnaire consisting of eight five-point Likert questions. The tool's questions, however, are based on a general social context and do not particularly address the self-expression of contentious beliefs on the Internet.

It is of note that Booth (2017) and other researchers utilize the Human Freedom Index (HFI) (Vasquez & Porcnik, 2017). HFI values are nation-specific. Included in the HFI measures are those that measure freedom of expression. Among those measures are "Laws and Regulations that Influence Media Content," "Political Pressures and Controls on Media Content," and "State Control over Internet Access."

2.3.1 Privacy and autonomy

At the core of the desire for privacy is a wish for protection against the misuse of private information (Wacks, 1989). The utility of personal information, at least to online merchants and intelligence agencies, for example, is shown by the fact that they treat it as a commodity. Such information can be used for various purposes, including ones that are not in the users' interests.

A lack of privacy can result in an "*encroachment on moral autonomy*," which is said to interfere with a person's development of their independent moral compass (van den Hoven, 2001). When a person concludes or assumes that they are constantly under surveillance, then the principles that they use are not truly their own. They may become unable to develop their own principles and plans (Benthan 1995, Foucault 1995, Nissenbaum 2010). Privacy violations can result in informational harm, which can cause the victims to become reluctant to engage in socially beneficial activities (Van den Hoven 2001, Nissenbaum 2010).

2.4 Demographics aspects

When considering behaviors pertaining to the privacy and security settings of devices, it is important to review current knowledge of privacy-related behaviors. The scope of this research also includes demographic aspects.

Users' education and age are related to their level of concern about online privacy, according to Sheehan (2002). Hazari and Brown (2013) investigated whether demographic factors influence Internet users' privacy concerns and, as a result, their attitudes toward social networking sites. In contrast to Sheehan's and Regan, Fitzgerald, and Balint's findings, their research revealed no link between age and online privacy concerns. Bandyopadhyay (2011) discovered that Internet users' online privacy concerns are influenced by characteristics such as their level of Internet literacy, social awareness, and cultural background. He discovered that one of the possible outcomes of such concerns is a reluctance to utilize the Internet.

There are also studies that have noted the impact of demographic variables such as nationality and age on Internet behavior. Regan et al. (2013) have evaluated attitudes toward information privacy between age groups categorized by generation. Their analysis revealed a trend where older generations tend to be less concerned than younger ones about wiretapping and data privacy. On the other hand, Tsai et al. (2016) found that users' age, income, and education did not affect their "security intentions" (e.g., the intention to download and update antivirus software, adjust browser settings, etc.). Chen et al. (2010) determined that consumers with different levels of computer expertise have different preferences for attributes of shopping websites.

Two major works that consider the definition and measurement of cultural parameters are those of Hofstede (2001) and House, et al (2004). Hofstede parameters include those that assess Uncertainty Avoidance (UAI) and Individualism (IDV). House et al. parameters have some similarities with House parameters, and include ones for collectivism, uncertainty avoidance, and others. However, House et al. parameters are further sub-divided by their measurement of values (“should be” conditions) and practices (“practices”). In analyzing our results by nationality, we try to apply some of Hofstede's and House et al's parameters. We seek any association between the different values of the appropriate cultural parameters and our new latent variables (described in section 3.3). Another parameter of interest is the Human Freedom Index (HFI). The HFI is an assessment of freedom in selected nations (Vasquez & McMahon, 2020). It is performed by an analysis of 76 different parameters and is published annually. We might expect that some of the new latent variables will vary with selected HFI values.

Cultural similarity (as measured by cultural distance (Hofstede 2001)) has been found by some studies to affect decision-making in various ways. One such way is in the selection of target countries for market expansion by software firms (Jones and Teegen 2001; Rothaermel et al. 2006). However, other research has found that other variables play a more important role in the selections (Ojala and Tyrväinen 2007). Research into culture-based differences in perception of risk for online shopping and other tasks has yielded conflicting results (Sims and Xu 2012). Sims and Xu (2012) found no significant difference between British and Chinese shoppers' perceived risk of online shopping despite those shoppers' differing cultural backgrounds. This conclusion was against their expectations because of results from prior research that showed differences in uncertainty avoidance between the two cultures (Hofstede 1980).

Conflicting results have also been found in the search for differences between genders with respect to privacy concerns. Regan et al. (2013) studied the differences between genders of different generations. They found that for most generations, females are more disapproving of wiretapping than males. The same attitude pattern was seen for a perception that government computer data is a "very serious threat" to privacy. Females are generally more concerned about privacy invasion via electronic means than males (Regan et al. 2013). Sheehan (2002), on the other hand, found no significant differences between genders in terms of the level of privacy concern.

With respect to time, Chatzitheochari and Arber (2012) studied differences in free time between genders for working people in the UK. In their studied cases, women had the same or less quantity of pure free time as men. Moreover, womens' free time tended to be of lower quality and more subject to interruptions than mens'. Burchardt (2010) has examined the relationship between available free time and income for UK residents. The income earned by working was found to be associated with available free time. Generally, as the subjects' earned income increases, their available free time decreases (Burchardt 2010).

2.5 APCO model

An overarching research model has been proposed to enhance the development of privacy research. The model is referred to as the Antecedents - Privacy Concerns - Outcomes (APCO) model (Smith et al. 2011). In the model, antecedents can be defined as influential precursors that help to define the levels of privacy concerns for a selected context. The contextualized privacy concerns are then investigated for their predictiveness of the behavioral outcomes (or "changes of state") under investigation. The ostensible purpose of the model is to help researchers address the many possible antecedents and outcomes that can be identified when conducting privacy research. Interested readers can find more details about the model in the referenced work. Variations of the APCO macro model or models similar to APCO have been applied in other works, e.g., by Benamati et al. (2017), Bandyopadhyay (2009), Sun et al. (2019), Zhang et al. (2013), Dinev et al. (2015), and Ayaburi et al. (2019). Sun et al. (2019) studied information disclosure behaviors (BID) in an e-commerce scenario. The information disclosure behavior that they studied includes mainly the disclosure by users of their own personal information.

3 RESEARCH FRAMEWORK

This section presents the research gaps, research questions, and methodology used to perform the research. It also includes a discussion of challenges that include common method bias.

3.1 Research gaps

Unwanted effects can result from negative expressions (e.g., those that are unpleasant or hostile). Users on the internet may be hesitant to express themselves due to fears of consequences. The time they spend on personal cybersecurity issues may further deter them from expressing themselves in controversial ways.

There seems to be little or no research on e-commerce in terms of consumer purchasing attitudes and behavior for cybersecurity and cyberprivacy products and services. Similarly, there is apparently no prior research on the relationship between expression reluctance and such purchasing. Earlier research has examined personal information disclosure behaviors (BID) in an e-commerce context (Sun et al. 2019). Free online expressionism is similar to personal information disclosure. Free online expressionism, for our study, is rather broadly defined by the wording of the survey that we used to collect data. The questions' wording specifically includes opinions, artwork, messages, writings, and music. In their research, Sun et al. (2019) included pictures and videos within the scope of personal information disclosure. Their study investigated the factors that impact information disclosure so that e-commerce platforms could apply the results to encourage information disclosure by users.

Another similarity between information disclosure and free online expressionism is that online expressionism produces information about users through online activities that can be logged and stored. Like disclosed personal information, such information can thus be indexed and processed. As a result, the contents and metadata produced by users’ free online expressionism could be used to create profiles of individual users.

Personal information that has been disclosed by users online is also commonly used for this purpose. Knowledge of users' true identities is not necessary for such profiling. Depending on the nature of the user-produced content and analyses applied to it, the expressionism could even be used to identify a user from a context where they have attempted to anonymize their identity. The anonymized identity may be an online persona or the user's true identity (see sections 5.1.5.2, 5.1.5.3, and 5.1.5.5 for a discussion of online identities). Anonymization is one way to achieve online privacy for an individual. Anonymization is important for many cases of controversial expressionism. Internet users may wish to anonymize their identities, for example, in countries under the control of authoritarian regimes, or when their expressions are not aligned with the prevailing political climates or political movements of the moment.

Thus, we would expect that a willingness to engage in controversial expressionism will be predicated, for many users, on an expectation of privacy. Technology-wise, this can require satisfactory implementations of privacy. Users may believe that privacy will shield them from the consequences of their controversial viewpoints or other expressions - expressions that they would otherwise not have made. Such expressions may not align with the usage context's socially acceptable norms and customs or with the overall political climate.

Democracy is based on the participation of citizens. If democratic nations strive for healthy democracies with active public participation, then we ought to be interested in those factors that may affect the willingness of users to express themselves online, whether the expressions are frivolous or politically groundbreaking dissents. Users' expressions can include mundane or socially acceptable ones and those controversial ones that freedom of speech laws exist to protect.

However, a lack of perceived privacy may cause users to be reluctant to engage in socially beneficial behavior (Van den Hoven 2001, Nissenbaum 2010). Such behavior could include free online expressionism. Troublingly, in light of Van den Hoven's (2001) assessments, aspects of users' faculties may also be affected. Van den Hoven suggests that a perceived lack of privacy may inhibit the ability of people to develop critical thinking, moral independence, and other traits. There should be a significant need for further research on privacy and the faculties of citizenries that it impacts. Especially of interest are such citizens' faculties that are necessary (or even critical) for effective democratic governance. Policymakers in democracies should benefit from such additional research.

Some may argue that people have a free choice of whether to use the Internet. They may suggest that to avoid being concerned about online privacy risks, users may choose not to use the Internet or connected technologies. Such a choice would hardly be deliberate. The Internet is a permanent and pervasive fixture of modern living. It is an infrastructure for which users have no viable alternative. Thus, users who wish to function in contemporary society do not have an option and must use the Internet with its associated privacy risks. Nissenbaum (2010) and Barrigar et al. (2006) have discussed such 'false choice' arguments. The Internet is here to stay with its online discourse and privacy risks. It merits study for its impacts on users' privacy concerns and the resulting costs.

It is possible that consumers' reservations about the Internet as a forum for free expression are linked to rising Internet use for personal cybersecurity goods and services by those same users.

Previous research has looked at the impact on one's willingness to reveal personal information. Based on past study, it is possible that apprehension about expressing oneself on the Internet is linked to fears about the consequences. The present work directly assesses the reluctance to express controversial viewpoints. It also assesses the reluctance that is caused by concern about consequences. Further, reluctance to express oneself may lead to the purchase and use of cybersecurity as a means to protect oneself in these cases. However, there seems not to be previous results addressing this hypothesis.

This work does not evaluate neutralization tendencies. Our survey's questions about expression do not imply or suggest that any of the expressions, though perhaps controversial, would necessarily be deviant or forbidden by policy or law.

In light of the philosophy of Van den Hoven (2001) and the work of Nissenbaum (2010), we expect that concerns about consequences, especially those that may result from a lack of anonymity, will cause users to be reluctant to freely express themselves online. The perceived lack of privacy may be a generally held belief by the user, or may be situational or dependent on their ability to make necessary adjustments to the pertinent settings on their computer or device.

Users' fears of repercussions may limit their ability to use the Internet for free expression. This restricting effect could be linked to what users believe and how they act when it comes to dealing with security and privacy issues with their devices. The constraining effect could also be linked to users' attitudes toward and perceptions of how much time they spend dealing with security and privacy issues on their devices. However, the association between online expression aspects and the perception of time consumption on security aspects does not appear to have been previously studied. Users may be reluctant to express themselves online simply because securing an acceptable level of security and privacy costs too much time and effort. That is, the users may be aware of the importance and abundance of tools providing online security and privacy and may wish to express themselves online but decide that spending time on such things is just too much effort. Concerns about consequences may not only have an inhibiting effect on users' use of the Internet for expression - it may also correlate with their desire to purchase personal cybersecurity products and anonymizing services.

There does not seem to be existing research on social exchange theory applied to controversial expressions by individual users online. Attempts to measure a reluctance to express on the Internet or to establish the same as a latent factor are lacking in previous research.

The HFI measures of “Laws and Regulations that Influence Media Content” and “Political Pressures and Controls on Media Content” could be useful for this study on the condition that they are applied indirectly. That is to say, for example, that an assumption would be that an average user would feel some reluctance to freely express themselves as a result of the laws and controls. (The relationship of HFI to the scope of this study is considered in section 5.4.) This study addresses reluctance more directly in the survey questions, whereas the subset of HFI measures does not measure reluctance to express. The parameters used for HFI's index do not measure concern regarding the consequences of personal free expression, and neither have they been analyzed for their relationship to Internet users' attitudes and behaviors toward purchasing personal cybersecurity protections.

Previous research (Riek & Böhme, 2018) attempted to examine the monetary and non-monetary costs of consumer-facing cybercrime. Scams and money fraud were among the cybercrime instances examined in the study. The costs in Riek and Bohme's study are not the price of the fear of negative repercussions that may arise from online expression. In the present study's RtoEx and RtoExC factors, the repercussions specified in some of the indicator questions are intentionally vague and nonspecific. They can take many different forms, including, but not limited to, cybercriminal attacks on users.

Based on previous research, it can be hypothesized that the reluctance to express oneself on the Internet may be connected with concerns about the consequences. Further, reluctance to express oneself may lead to the use of cybersecurity as a means to protect oneself in these cases. However, there seems not to be previous results addressing this hypothesis. The relationship between online expression aspects and personal cybersecurity spending seems to be lacking in prior research.

To test willingness to self-censor, Hayes et al. (2005) developed a self-reporting questionnaire consisting of eight five-point Likert questions. The tool's questions, however, address a general social context and do not particularly address the self-expression of contentious beliefs on the Internet. Previous study has not attempted to quantify or establish a reluctance to express on the Internet as a latent factor. The HFI's freedom measures do not account for individual citizens' concerns regarding the consequences of their personal free expression. This work helps to address these gaps.

Smith et al. (2011) have presented gaps in current information privacy research. Such gaps include the need to address relationships between antecedents and privacy concerns and the privacy calculus stream in their model. Benamati et al. (2017) have partially addressed this by examining privacy awareness, age, and gender as antecedents in an applied model. Benamati, Ozdemir, and Smith used a construct of "privacy protecting behaviors" with reference to Facebook. Their construct included scales of behavior for limitations of friending, of posting, and of adjustments to settings that control the revelation of personal information. A rendition of the model is in Figure 6.

We expand prior research by investigating the correlation between perception of time consumption used for addressing device cybersecurity and the willingness to express freely on the Internet. Since unpopular, provocative, or negative expressions can result in unwanted consequences, Internet users may be reluctant to express themselves because of concerns about such consequences. The users may want to express their opinions anonymously. However, the time and effort that they spend on personal cybersecurity issues may further discourage their controversial expressionism. Thus, issues related to device assessment and adjustment may be concerns that relate to a reluctance outcome. Demographics may be antecedents to the concerns. We hypothesize that users are more reluctant to freely express themselves online when they feel that they spend excessive time on their devices' cybersecurity and privacy aspects. We apply the hypotheses and results to the APCO model. This is relevant to the users' participation in online expression contexts that include social media.

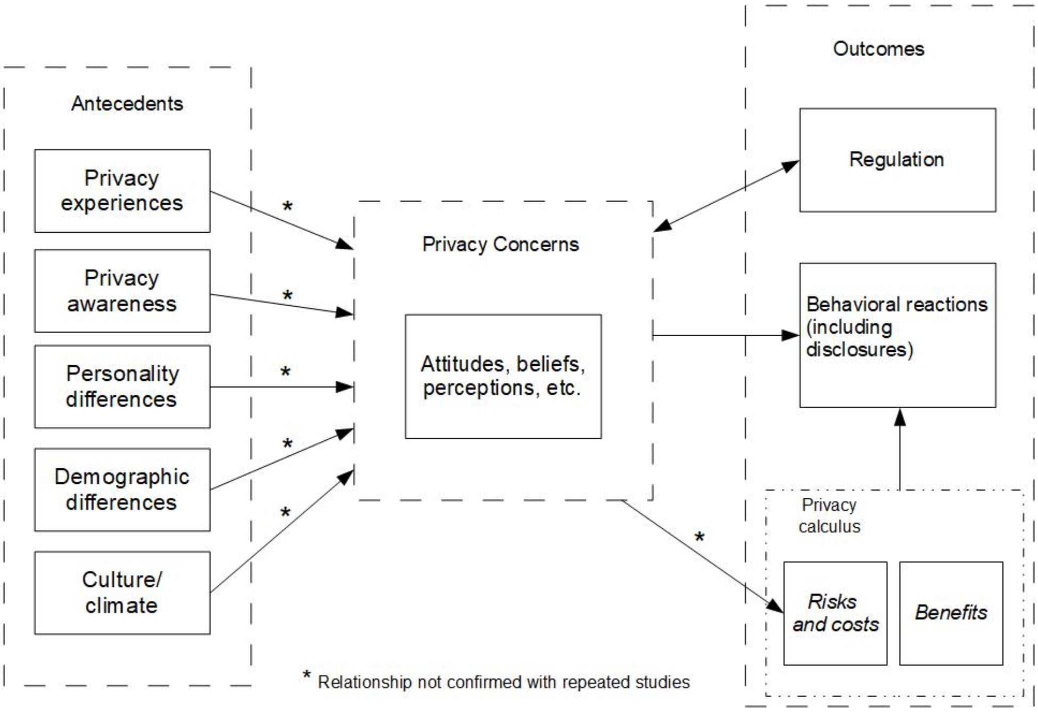


Figure 6: Rendition of Antecedents->Privacy Concerns->Outcomes model (Smith et al. 2011)

3.2 Research questions

The concerns that Internet users have about personal online privacy and security are expected to influence some aspects of the users' behaviors and attitudes. The aspects studied in this research are: users' attitudes toward spending on personal cybersecurity, their attitudes toward controversial online expressionism, and their behavior toward the settings on their device that control privacy and security, as well as their perceptions of such time used for the settings. More briefly, the aspects are their time, money, and freedom.

We want to find out whether users’ concerns affect their spending on products and services that are designed to protect their personal cybersecurity and privacy. Users’ concerns can manifest as a reluctance to use the Internet for free expressionism. This reluctance may have a statistical relationship with users’ personal cybersecurity spending. A relationship may also exist between the time that users spend on their devices’ privacy and security settings, and those users’ free expressionism. We are also interested in the role that some demographic groupings may have in the relationships as antecedents, moderators or mediators.

A goal of our research is the examination of users' reluctance to express themselves online in relation to their attitude and perception regarding time consumption for their devices’ security and privacy aspects. Such aspects include the contemplation, examination, and adjustment of the relevant device settings. Users' reluctance to express online may correlate with their perception of whether addressing the security and privacy issues requires an excessive amount of time. These effects may differ across certain demographic groupings, including cultural groupings. We will attempt to explain such differences.

We are also interested in bringing attention to potential dangers from smartphones, and in methods to reduce some cyber-risks to users’ data files that they store in their smartphones.

The research questions addressed in PI (section 4.1) are as follows:

> RQ 1: Is there a relationship between the money that Internet users spend on privacy and security features for their devices, and those users’ reluctance to controversially express themselves online?
>
> > RQ 1.1: Do users have a different reluctance to controversially express themselves if they are reminded of potential consequences?
> >
> > RQ 1.2: Does the relationship in RQ 1 differ between demographic groupings?

The research questions addressed in PII (section 4.2) are as follows:

> RQ 2: Is there a relationship between the time that Internet users spend on the privacy and security aspects of their devices, and those users’ reluctance to freely express themselves online?
>
> > RQ 2.1: Is there a relationship between the mere contemplation of one’s device’s privacy and security aspects, and the reluctance to controversially express oneself online?
> >
> > RQ 2.2: Are users more reluctant to controversially express themselves if they perceive that it takes excessive (or “too much”) time to deal with the security and privacy settings of their device?

The research questions addressed in PIII (section 4.3) are as follows:

> RQ 3: Is there a relationship between the time that Internet users spend on the privacy and security aspects of their devices, and the users' proclivity to spend money for those same aspects?

The research questions addressed in PIV (section 4.4) are as follows:

> RQ 5: Do some demographic factors influence Internet users' reluctance to express themselves online; whether directly, or indirectly by moderating privacy concerns?
>
> > RQ 5.1: Can additional insight be gained from applying some research results to the Antecedents-Privacy Concerns-Outcomes model?
> >
> > RQ 5.2: If the mere contemplation of device security and privacy settings is interpreted as a manifestation of privacy concerns, then does that impact the reluctance to controversially express oneself?
> >
> > RQ 5.3: Do different demographic groups have different reluctances to freely express themselves online?

The research questions RQ 1 through RQ 5.3 are addressed by the hypotheses in the corresponding sections and articles.

The research questions addressed in PV (section 5.2) are as follows:

> RQ 4: What are some historically unusual physical dangers from smartphones that could be implemented by third parties?
>
> > RQ 4.1: What are the potential physiological impacts of such dangers on users?

Research questions related to the patents PVI and PVII in section 5.4:

> RQ 6: Is there a way to reduce the risk of cyber-hacking or unauthorized access to users’ data files by using a method of profiled storage?
>
> RQ 7: Is there a way to reduce the risk of cyber-hacking or unauthorized access to users′ data files by implementing a method of a continuously maintained pseudo-cache system of distributed storage?

In addition to the article-specific research questions, we pose additional research questions. The additional research questions are for investigating nationality and cultural aspects as they relate to some of the latent constructs that are described in section 3.3.

RQ 8: Do the latent factors RtoEx, TChS, or TMT vary by nationality?

RQ 8.1: Will TMT differ by nationality according to cultural indices.

RQ 8.2: Will RtoEx differ by nationality according to either cultural indices or an HFI value?

RQ 8.3: Will TChS differ by nationality according to either cultural indices or HFI value?

Research questions RQ 8 – RQ 8.3 are addressed by the hypotheses described in section 5.4.

3.3 Latent construct development

To help answer research questions RQ1 – RQ 5.3, this work proposes six latent factors: three corresponding to a reluctance to self-express online (RtoEx, RtoExnonC, RtoExC), one corresponding to a favorable attitude toward purchasing personal cybersecurity and cyberprivacy services and products (LoM), one corresponding to a perception that handling security and privacy aspects of one's device requires an excessive amount of one's time (TMT, from "too much time"), and one corresponding to the performance of checking and changing device privacy and security settings (TChS, from "think about and change settings"). The factors are presented in PIII as follows:

- Reluctance to Express (RtoEx): Reluctance to freely self-express online. The reluctance of expressing can be further divided into two factors based on inclusion or exclusion of consequences of the expression, RtoExC and RtoExnonC, respectively.
- Reluctance to Express when Consequences mentioned (RtoExC): Reluctance to Express due to concerns about possible consequences or safety; The reluctance to freely express oneself online due to concerns about the risk of consequences or safety issues resulting from the expression.
- Reluctance to Express When Consequences Not Mentioned (RtoExnonC): Reluctance to Express when users are not reminded of possible Consequences or safety issues resulting from the expression.
- Too Much Time (TMT): The perception that cybersecurity risk amelioration requires excessive usage of one's time
- Think Change Settings (TChS): Time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether the time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

- Loss of Money (LoM): Personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

Each of the latent variables are derived from sets of indicator questions. The indicator questions were included in a survey, and each consisted of responses along a five-point Likert scale from “strongly agree” to “strongly disagree.”

TMT was derived from five questions that assess the view that too much time has been spent on device security and privacy concerns, as well as the perception that time spent on device security and privacy issues has taken time away from other activities. TChS is a three-question factor that assesses whether the user has thought about and examined (and perhaps adjusted) their device's security and privacy settings. Cumulatively, we suggest the five “too much time” indicator questions imply that the respondent spends time contemplating and actively addressing security and privacy aspects but tends to feel negatively about doing so (“too much time” implies that the amount of time required is excessive and detracts from activities for which the respondent could preferably be using their time). The questions for TMT and TChS are presented in PII.

The study included questions on respondents' spending attitudes and behaviours toward cybersecurity. The questions are presented in PI. Responses to a series of four indicator questions identify the latent variable Loss of Money (LoM). The LoM questions are as follows: two questions to determine whether the respondent has purchased security software to improve his cybersecurity, and two questions to determine the respondent's general attitude regarding cybersecurity purchases. Overall, the LoM indicator questions appear to show a propensity to purchase software goods or services that improve personal cybersecurity.

The research model defines as a latent factor "reluctance to freely express oneself on the Internet" (RtoEx). The factor corresponds to eight scale questions, four of which mention consequences or safety. This factor enables analysis for correlations and the performance of other analyses against other variables or factors. The questions for the RtoEx variable are listed in PI. They ascertain the attitude of respondents toward hypothetical scenarios of their posting of controversial content online. Such content can include provocative opinions or artwork. The question set includes one question to ascertain their attitude toward using electronic methods vs. face-to-face communication when discussing a sensitive topic with a friend. We suggest that the responses to this question set can convey the level of the respondents' reluctance to express themselves using electronic methods, including the Internet.

3.4 Demographic aspects

The statistical relationships between the three latent factors may differ across demographic groupings. Groupings considered in this research are income, level of ICT expertise, age, and gender.

3.5 Quantitative approach and data

This work pursues users' behaviors and attitudes toward cybersecurity spending regardless of how the user may prefer to do such shopping. It does not differentiate users' preferences between shopping at a brick-and-mortar store or online.

PIV uses as a general basis the Antecedents -> Privacy Concerns -> Outcomes (APCO) research model defined by Smith, Dinev, and Xu (2011). Variations of the APCO model or models similar to APCO have been applied in other pertinent works in the field, e.g., by Benamati, Ozdemir, and Smith (2017) and by Bandyopadhyay (2009). Our work may be described by way of comparison to Bandyopadhyay's 2009 framework. In Bandyopadhyay's framework, there are three consequences, or outcomes, of users' privacy concerns: 1. Refusing to provide personal information, 2. Refusing to enter e-commerce transactions, and 3. Refusing to use the Internet. While Bandyopadhyay's framework has implications for online marketers (Bandyopadhyay, 2009), ours presumes implications for individuals' online expression. In our variation of the framework, we specify one outcome - a reluctance to freely express oneself on the Internet. Our RtoEx variable may be considered a variation of both 1. Refusal to provide personal information, and 3. Refusal to use the Internet. In place of "privacy concerns" in Bandyopadhyay's proposed framework, we use "usage or perceived excessive usage of time addressing device privacy and security aspects." With regard to the antecedents, we instead use the demographic factors of ICT expertise, income, and gender as independent variables for a regression analysis between latent factors.

A survey was administered over the Internet in the form of a Web questionnaire to a population composed mainly of university students and working adults. The question items were brainstormed into a pool from which the most appropriate items were selected for the constructs. Multiple items were selected for each construct. The items have different wordings to qualify as separate questions and are non-trivially redundant. We attempted to avoid making the items too lengthy or difficult. The items were designed to measure the same construct within the scale. The indicator questions were designed with a level of specificity to minimize crossover into related constructs, or unpredicted constructs that were not intended to be measured.

Readability analysis was performed on the indicator question sets for each latent variable. The questions for each latent variable were combined into a block for analysis. The RtoEx questions have a 12th (Flesch-Kincaid) or 9th (Dale-Chall) grade readability level. The TMT and TChS questions have a 9th (Flesch-Kincaid) or 12th (Dale-Chall) grade level. Thus, the questions should be readily understood by those respondents with an education equivalent to that of an American high school graduate. The LoM questions have not been analyzed for readability. The differing results between the Flesch-Kincaid and Dale-Chall analyses between our scale sets may show problems in applying either to a scale questions setting. This issue is left for other researchers to investigate.

3.5.1 Sample for supplemental results

Newer analysis results are available for the calculations that were done in PI, PII, and PIII. The newer results are presented in sections 4.1.4, 4.2.4, and 4.3.4, and are derived from a larger data set that was available after the publication of the articles. The set was used for PIV. The newer set contains 265 responses. Descriptive statistics for the sample are shown in Table 1. The newer results from this data are presented in the respective article chapters as additional results. The newer results are presented in the Appendix with some more details than those in the published articles.

Table 1: Sample, N=265

Variable	Percentage
Gender	
Male	57.4
Female	42.6
Age	
15-25	36.6
26-36	32.5
37-44	14.3
45-54	10.2
55-64	4.9
≥65	1.5
Annual income (euros or US dollars)	
≤4,999	27.5
5,000 - 19,999	24.5
20,000 - 39,999	18.9
40,000 - 59,999	11.3
60,000 - 79,999	7.5
80,000 - 99,999	3.4
≥ 100,000	6.8
Nationality	
Finland	49.4
USA	23.8
Israel	19.2
other	7.6
ICT expertise (mean score from scales, 4.5 highest - 1.0 lowest)	
>3.8-4.5	23.0
>3.1-3.8	41.6
>2.4-3.1	30.5
>1.7-2.4	4.8
1.0-1.7	0.8

3.6 Methods

The studies in articles PI through PIV share common methods. A survey was administered to populations that included university students and working adults. The survey was anonymous and contained indicator questions designed to assess the effects on the 'Time, Money, and Freedom' of Internet users. The measured effects pertain to users' concerns about their privacy and security, and of potential consequences of users' controversial expressionism. The survey also included questions to gather some demographic information. The responses were analyzed by factor analysis techniques that included varimax rotation and assessment of communalities and loadings. Reliability analysis was also done by computations of the KMO-Bartlett sphericity test and Cronbach's alpha.

The mean scores of the indicator questions were used for subsequent analyses. The analysis included computations of Pearson and Spearman correlations (as appropriate) and multiple regression analysis. Performance of structural equation modelling was deferred as the sufficiency of the data was debatable.

Correlations between the latent factors and between the latent factors and selected demographic variables were computed. The mediation effects of combinations of latent factors with demographic variables were determined. Further descriptions of the methods are presented in sections x - y and in the attached articles.

The results were presented, compared against the hypotheses that were presented in the articles. Confirmations and rejections of the hypotheses were stated and discussed. Recommendations, including recommendations for future research, are made based on the findings and asserted implications.

PV is a meditation on some limited hypothetical methods to physically weaponize a smartphone. The writing is based on a review of some media reports on capabilities to remotely disable and destroy smartphones, reports and research on the tampering of smartphones by various actors, and the engineering experience of the author. It also discusses the problems and dangers that can result from the counterfeiting of smartphones and smartphone accessories.

The section on new preterms (section 5.1) is presented as a proposal for new terminology to help encompass new concepts. The new concepts relate to personal autonomy over one's data and to data processing that modern developments in connected technology have enabled. The new terminology is intended to help make discussions and understandings of these issues more readily understandable and meaningful.

The patents PVI and PVII are presented as potential methods to reduce some security and privacy risks to users' data that is stored on their connected devices.

3.6.1 Common method bias

A typical challenge in observational studies is making an account for common method bias. We use a multi-trait single method approach. The cross-sectional study was implemented with an Internet web-based survey. The survey was accessed with a URL that was provided to potential respondents. Some sources of common method bias pertinent to our data gathering method include common scale properties, question ambiguity, social desirability in wording, and others. In this work, we attempt to account for common method biases as described in PIV.

The questions for individual factors (traits) in our survey were grouped together. The questions on "time spent" were temporally spaced before the questions on "reluctance to express." We believed that grouping the factor questions together would help the respondent to better ponder the question's topic so that they would be cognitively prepared to answer the subsequent questions about the same factor more accurately. The respondent had the opportunity to ponder the questions without an intermittent clearing of his or her short-term memory by the distraction of new unrelated questions. It was believed that this, in turn, would lead to more accurate, or at least not less accurate, responses to the questions. Research supports the grouping of related survey questions for improved results (Krasnick and Presser 2010), as do companies that specialize in online surveys (Hillmer 2019; SurveyMonkey 2020).

We address the motivational factor with an attempt to improve response accuracy. The survey is voluntary and anonymous, and addresses timely topics that affect most people. The topics include cybersecurity and self-expression online. The university students in Finland (approximately 130 respondents) were invited to take the survey with a notice that doing so would make them eligible to enter a prize drawing. Because the survey was anonymous, there were no individually attributable social consequences of the responses, and consequently, a respondent should not have a desire to provide a socially acceptable response. Moreover, the nature of the questions is such that there is little or no context for "socially acceptable" responses. In these ways, the bias due to motivation factors is mitigated. We also provided an announcement email containing the survey invitation. The email contained a brief introduction to the survey topic.

The first page of the survey was an introductory "welcome page" that contained instructions, a brief description of the questioning style and how the responses would be used, a reminder that the survey was anonymous, and that inexact responses would be acceptable. The page also contained an optional initial free-form text field that allowed respondents to write the first thing that came to their mind upon hearing the phrase "Internet security and privacy." This brief initial ‘brainstorm’ was hoped to have a motivational effect. It was also hoped to have an initial stimulatory but neutral priming effect on the respondents. In psychological terms, the sought effect may be considered positive priming or semantic priming. The respondents would begin filling the survey primed with their initial and unfiltered ‘gut reaction’ to the topic.

During the design and administration of our survey, we attempted to address applicable psychometrics issues as described by DeVellis (2003).

Our design is validated by good internal consistency reliability, as indicated by the values of the reliability parameters presented in the attached papers PI – PIV

4 OVERVIEW OF THE INCLUDED ARTICLES

This section presents an overview of the articles that are related to the central theme of the dissertation.

4.1 Article: Online Expression and Spending on Personal Cybersecurity (PI)

This article explores the LoM and RtoEx constructs.

4.1.1 Research questions

RQ 1: Is there a relationship between the money that Internet users spend on privacy and security features for their devices, and those users' reluctance to controversially express themselves online?

RQ 1.1: Do users have a different reluctance to controversially express themselves if they are reminded of potential consequences?

RQ 1.2: Does the relationship in RQ 1 differ between demographic groupings?

The paper addresses the following hypotheses:

H11: Users' refusal or reluctance to express themselves online (RtoEx) is correlated with their personal cybersecurity spending attitude and behavior (LoM).

H12: The correlation of H11 will vary by certain demographic factors.

4.1.2 Background

This research analyzes whether users are more inclined to spend money on personal cybersecurity if they are reluctant to express themselves online. The researchers consider that it is important to consider the attitudes of users toward free expression on the Internet and possible consequences resulting from users' reluctance to freely express themselves on the Internet. This is relevant to participation in social media and other online expression contexts. The relationship between online expression aspects and personal cybersecurity spending seems to be lacking in prior research.

4.1.3 Findings

In this study, the set of 191 responses was analyzed using SPSS factor analysis tools for the Loss of Money (LoM), Reluctance to Express (RtoEx), Reluctance to Express when Consequences Mentioned (RtoExC) and Reluctance to Express when Consequences Not mentioned (RtoExnonC) factors. The analysis results are in Table 2.

Table 2: Factor analysis Spearman intercorrelations and Cronbach's alphas in PI

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
LoM	.500**	.863**	.639	.871
RtoEx	.198**	.699**	.395	.838
RtoExnonC	.359**	.564**	.457	.764
RtoExC	.292**	.699**	.490	.796

Pearson correlation analysis was performed between LoM and the other three latent factors. The results are in Table 3. H11 is confirmed for all of the RtoEx factors.

Age was not correlated with LoM. A linear regression analysis for LoM was performed using age and the RtoExC factor as independent variables. This showed some correlation (adjusted R squared = .037, p-value = .011). Therefore, H12 is validated for age.

Table 3: Pearson correlations between RtoEx and LoM (two-tailed significances: * to 0.05 level; ** to 0.01 level) in PI

n=191	RtoEx	RtoExnonC (consequences not mentioned)	RtoExC (consequences mentioned)
LoM	.199**	.149*	.201**

The mean response for the LoM scales among all respondents was 2.92. Recalling that the Likert scale was set for 1=strongly agree to 5=strongly disagree, and 3=neither agree nor disagree, the result shows a rather neutral attitude.

The mean response to the RtoEx, RtoExC and RtoExnonC scales for all respondents are shown in Table 4. We see that all the values indicate that respondents tend to be reluctant to express themselves online in controversial ways.

Table 4: Mean responses to the RtoEx, RtoExnonC and RtoEx scales in PI

N=191	RtoEx	RtoExnonC	RtoExC
Mean (1 – 5)	2.73	2.61	2.85

The findings address the research questions as described in section 6.1.

4.1.4 Supplemental findings

A newer analysis was performed using a bigger data set (n=265) that was available after the publication of PI. The sample is described in section 3.5.1. The results are presented below and compared with the results that were presented in PI.

Factor analysis with the bigger data set again confirmed the validity of the three factors. Detailed statistical analysis results for the factor analysis are in Appendix A.

Correlations between the latent factors are shown in Table 5. The resulting correlations values are monotonically consistent with the findings in PI and are not significantly different ($Z \leq -0.282$, $p \geq .778$)[2].

Table 5: Pearson correlations between RtoEx and LoM (two-tailed significances: * to 0.05 level; ** to 0.01 level) with newer data set

n=265	RtoEx	RtoExnonC (consequences not mentioned)	RtoExC (consequences mentioned)
LoM	.175**	.140*	.175**

The mean response for the LoM scales among all respondents was 2.93 and consistent with the original finding of 2.92. Recalling that the Likert scale was set for 1=strongly agree to 5=strongly disagree, and 3=neither agree nor disagree, the result again shows a rather neutral attitude.

The mean responses to the RtoEx, RtoExC and RtoExnonC scales for all respondents are shown in Table 6. We again see that all the values indicate that respondents tend to be reluctant to express themselves online in controversial ways.

Table 6: Mean responses to the RtoEx, RtoExnonC and RtoEx scales with newer data

N=265	RtoEx	RtoExnonC	RtoExC
Mean (1 – 5)	2.72	2.65	2.80

A linear regression analysis for LoM was repeated using age and the RtoExC factor as independent variables. This again showed some moderation (adjusted R squared = .034, p-value = .004). The adjusted R squared value is smaller (.034 vs. .037) but still consistent with the finding in PI.

The model diagram that was used in PI is updated with the newer findings in Figure 7.

[2] Based on significance calculation from https://www.danielsoper.com/statcalc/calculator.aspx?id=104

Appendix A contains detailed results tables for the supplemental findings.

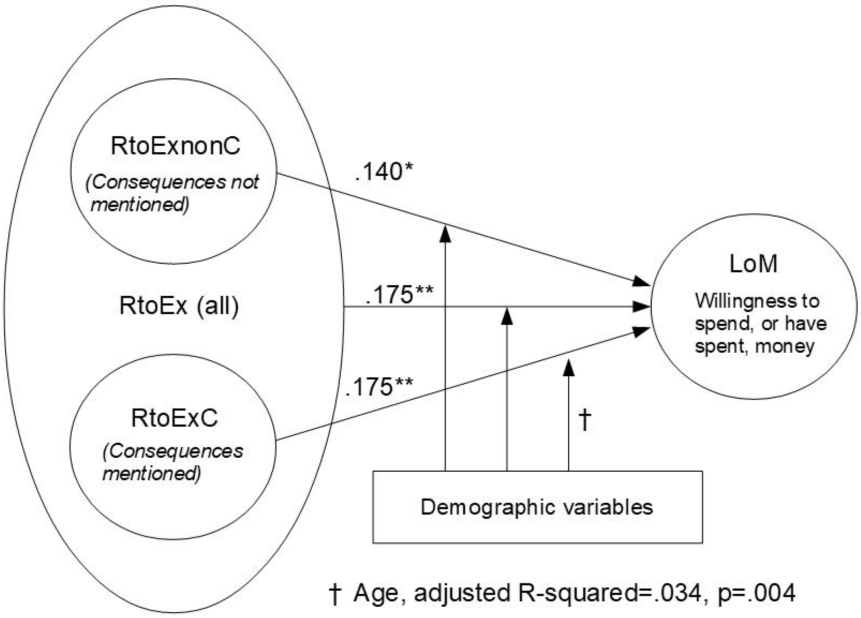

RtoExnonC
(Consequences not mentioned)
RtoEx (all)
RtoExC
(Consequences mentioned)
.140*
.175**
.175**
LoM
Willingness to spend, or have spent, money
†
Demographic variables
† Age, adjusted R-squared=.034, p=.004

Figure 7: Model diagram used in PI, labelled with newer results

4.2 Article: Does Time Spent on Device Security and Privacy Inhibit Online Expression? (PII)

This article explores the RtoEx, TChS, and TMT constructs.[3]

4.2.1 Research questions

RQ 2: Is there a relationship between the time that Internet users spend on the privacy and security aspects of their devices, and those users' reluctance to freely express themselves online?

> RQ 2.1: Is there a relationship between the mere contemplation of one's device's privacy and security aspects, and the reluctance to controversially express oneself online?
>
> RQ 2.2: Are users more reluctant to controversially express themselves if they perceive that it takes excessive (or "too much") time to deal with the security and privacy settings of their device?

[3] Note: PII contains an error in the data analysis. Interpretations of the correlations of other variables with age, and of the effects of age as an independent variable should be inverted. This dissertation uses a corrected analysis.

This study addresses the following hypotheses:

H21: Users' perception that it takes excessive (or "too much") time to deal with the security and privacy settings of their device (TMT) will positively correlate with a reluctance to express (RtoEx).

H22: The contemplation of one's device's privacy and security aspects (TChS) will positively correlate with a reluctance to express (RtoEx).

H23: The correlation of users' perception that it takes excessive (or "too much") time to deal with the security and privacy settings of their device to a reluctance to express (H21) will vary by age, level of ICT expertise, and/or income.

H24: The correlation of the contemplation of one's device's privacy and security aspects to a reluctance to express (H22) will vary by age, level of ICT expertise, and/or income.

4.2.2 Background

We expand prior research by investigating the correlation between perception of time consumption used for addressing device cybersecurity and the willingness to freely express on the Internet. Negative expressions (e.g., unpleasant or aggressive) can result in unwanted consequences. Internet users may be reluctant to express themselves because of concerns about such consequences. The time they spend on personal cybersecurity issues may further discourage their controversial expressionism. We hypothesize that users who feel they spend excessive time on their devices' cybersecurity and privacy aspects are more reluctant to freely express themselves online. This is relevant to the users' participation in social media and other online expression contexts.

4.2.3 Findings

Factor analysis was performed using SPSS 24 to evaluate the validity of the latent variables. The results are in Table 7.

Table 7: Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alphas in PII

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
RtoEx	.199**	.673**	.384	.831
TChS	.314**	.481**	.403	.668
TMT	.223**	.752**	.404	.770

The results in Table 8 show that reluctance to express oneself online correlates positively with a long-perceived time spent on setting device security settings

(.220**) but not significantly with time spent thinking about device security settings. Thus, we can confirm hypothesis H21 and reject hypotheses H22 and H24. Out of the potential moderating variables, we found a correlation between reluctance to express and age (-.225**) but not with other background variables. In a linear regression analysis, the same factors (TMT and age) together reached significant correlation (adjusted R squared = .075, p-value = .000), thus H23 is confirmed for age.

Table 8: Pearson correlations between RtoEx and TMT, TChS, and age in PII. Two-tailed significances: * to 0.05 level, ** to 0.01 level

n=197	Device security/privacy takes "too much time" (TMT)	Spend time thinking about and changing settings (TChS)	Age (15-25, 26-36, 37-44, 45-54, 55-64, or 65+)
RtoEx	.220**	.077	-.225**

The findings address the research questions as described in section 6.3.

Table 9 presents the mean scale responses for - and percentage of - respondents tending to agree with - TMT, TChS, and RtoEx.

Table 9: Mean scale responses, and percentages of respondents who tend to agree or strongly agree with TMT, TChS, and RtoEx in PII

N=197	Overall addressing security and privacy aspects takes too much time (TMT)	Overall spend time thinking about device security and check/change settings (TChS)	Reluctant to express online (RtoEx)
Mean scale response	3.40	2.65	2.74
	27.4%	59.9%	57.4%

4.2.4 Supplemental findings

A newer analysis was performed using a bigger data set (n=265) that was available after the publication of PII. The sample is described in section 3.5.1. The results are presented below and compared with the results that were presented in PII.

Factor analysis with the bigger data set again confirmed the validity of the three factors. Detailed statistical analysis results for the factor analysis are in Appendix B.

Correlations between the latent factors are shown in Table 10. The resulting values are monotonically consistent with the findings in PII and are not significantly different (Z ≤ -0.441, p ≥ .659)[4].

Table 10: Pearson correlations between RtoEx and TMT, TChS, and age with newer data set. Two-tailed significances: * to 0.05 level, ** to 0.01 level

n=265	Device security/privacy takes "too much time" (TMT)	Spend time thinking about and changing settings (TChS)	Age (15-25, 26-36, 37-44, 45-54, 55-64, or 65+)
RtoEx	.238**	.067	-.185**

A linear regression analysis for RtoEx was repeated using age and the TMT factor as independent variables. This again showed some moderation (adjusted R squared = .077, p-value = .000). The adjusted R squared value is larger (.077 vs. .075) and consistent with the finding in PII.

The model diagram that was used in PII is updated with the newer findings in Figure 8.

Table 11 presents the mean scale responses for - and percentage of respondents tending to agree with - TMT, TChS, and RtoEx. The results are consistent with the original findings.

Table 11: Mean scale responses, and percentages of respondents who tend to agree or strongly agree with TMT, TChS, and RtoEx with newer data

N=265	Overall addressing security and privacy aspects takes too much time (TMT)	Overall spend time thinking about device security and check/change settings (TChS)	Reluctant to express online (RtoEx)
Mean scale response	3.36	2.66	2.73
	30.6%	59.6%	57.7%

Appendix B contains detailed results tables for the supplemental findings.

[4] Based on significance calculation from https://www.danielsoper.com/statcalc/calculator.aspx?id=104

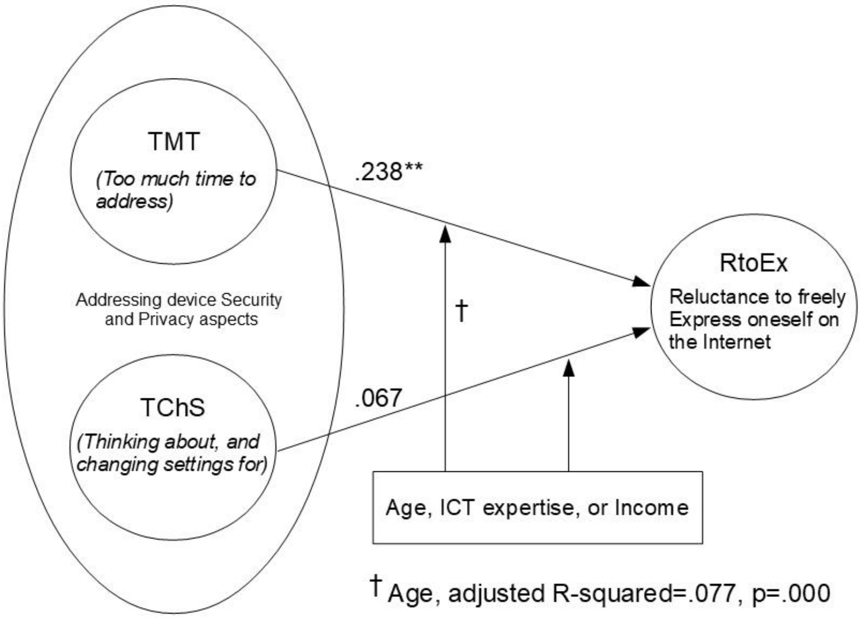

TMT
(Too much time to address)
Addressing device Security and Privacy aspects
TChS
(Thinking about, and changing settings for)
.238**
.067
†
RtoEx
Reluctance to freely Express oneself on the Internet
Age, ICT expertise, or Income
† Age, adjusted R-squared=.077, p=.000

Figure 8: Model diagram used in PII, labelled with newer results

4.3 Article: Online Expression, Personal Cybersecurity Costs, And the Specter Of Cybercrime (PIII)

This article explores the relationship between the LoM and TChS constructs, and discusses issues of cybercrime. [5]

4.3.1 Research questions

RQ 3: Is there a relationship between the time that Internet users spend on the privacy and security aspects of their devices, and their proclivity to spend money for the same aspects?

This study addresses the following hypotheses:

> *H31*: The contemplation of one's device's privacy and security aspects (TChS) will be correlated with a positive attitude toward purchasing personal cybersecurity products and services (LoM).

[5] Note: PIII contains an error in the data analysis. Interpretations of the correlations of other variables with age, and of the effects of age as an independent variable should be inverted. This dissertation uses a corrected analysis.

*H32***:** Users' contemplation of their device's privacy and security aspects (TChS) combined with one or more demographic variables will predict their attitudes and behaviors about personal cybersecurity spending (LoM).

4.3.2 Background

Controversial expression in an online communications context is affected by factors that include perceived anonymity and familiarity with other online community participants (Luarn & Hsieh, 2014). Luarn and Hsieh studied the expression behavior of users in a laboratory-controlled virtual community. The virtual community simulated different online group communications environments. They found that users were more willing to express controversial opinions when their identities were anonymous or when they were familiar with other members of the community. When users in the study were not anonymous, they were more reluctant to express such opinions. They also found that there was no effect of anonymity or member familiarity on users' willingness to express non-controversial opinions.

Prior research has shown that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications. They found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome. Negative expressions (e.g., unpleasant or aggressive) can result in unwanted consequences. Internet users may be reluctant to express themselves because of concerns about such consequences. The time they spend on personal cybersecurity issues may further discourage their controversial expressionism.

Previous research has attempted to address the monetary and non-monetary costs of consumer-facing cybercrime (Riek & Böhme, 2018). The research focused on cybercrime incidents such as scams and payment fraud. The costs in Riek and Bohme's research are not the costs of the fear of consequences that could result from expressing oneself online. The feared consequences in the RtoEx subfactor of this study are unspecified and general. They may occur in varying forms that include cybercriminal attacks against the user.

The authors believe that it is important to consider the attitudes of users toward free expression on the Internet and possible consequences resulting from users' reluctance to freely express themselves on the Internet. Some consequences can manifest in the form of cybercriminal attacks. Such attacks can include hacking of users' devices by taking advantage of software vulnerabilities that enable injections of malware. Cybersecurity and cyberprivacy solutions help to protect users against online threats. There are many free solutions available, but the perceived bona fide worthiness of the solutions is evidenced by users who are willing to pay for them. Thus, an assessment of a willingness to spend money for such solutions should be a robust indicator of whether users believe that there are genuine online threats to themselves that must be mitigated. There seems to be no available research regarding the association between users' proclivity to purchase personal security and privacy solutions and their dedication of time to adjusting their device security and privacy settings. Software developers and cybersecurity software merchants should have an interest in this. If the same users who are spending time on their settings adjustments are also willing to buy security software, design and marketing decisions can benefit from this knowledge. PIII helps to fill this research gap.

4.3.3 Findings

An analysis in SPSS 24 to verify the three latent variables produced the results in Table 12.

Table 12: Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alphas in PIII

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
TChS	.319**	.485**	.407	.673
TMT	.221**	.772**	.405	.766
LoM	.500**	.863**	.639	.871

Analysis of the results (Table 13) for the TChS vs. LoM hypothesis shows a significant correlation; thus, H31 is confirmed. Regression analysis is performed on LoM as the dependent variable against some demographic variables. The analysis shows some correlation with the combination of TChS and age (adjusted R squared = .035, p-value = .013). H32 is therefore valid for age.

Table 13: Pearson correlation between LoM and TChS in PIII. Two-tailed significance: * to 0.05 level.

	n	Spend time thinking about and changing settings (TChS)
LoM	191	.160*

The findings address the research questions as described in section 6.2.

4.3.4 Supplemental findings

A newer analysis was performed using a bigger data set (n=265) that was available after the publication of PIII. The sample is described in section 3.5.1. The results are presented below and compared with the results that were presented in PIII.

Factor analysis with the bigger data set again confirmed the validity of the factors. Detailed statistical analysis results for the factor analysis are in Appendix C.

Analysis of the results (Table 14) for the TChS vs. LoM hypothesis shows a stronger correlation than in PIII (.212** vs. .160*). According to the Z-test the correlations are not significantly different (Z = 0.564, p = .573)[6]. Regression analysis is performed on LoM as the dependent variable against some demographic variables. The analysis shows some correlation with the combination of TChS and ICT expertise and age (adjusted R squared = .070, p-value = .000). H32 is therefore valid for ICT expertise and age. ICT expertise is found to be an additional moderator when analyzing the bigger data set.

Table 14: Pearson correlation between LoM and TChS with the newer data set. Two-tailed significance: ** to .010 level.

	n	Spend time thinking about and changing settings (TChS)
LoM	265	.212**

The model diagram that was used in PIII is updated with the newer findings in Figure 9.

Appendix C contains detailed results tables for the supplemental findings.

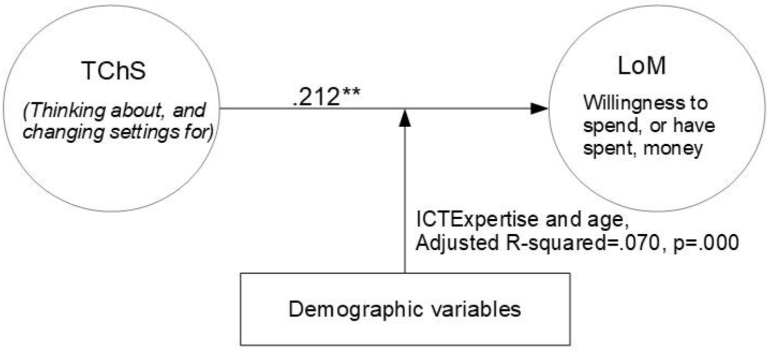

TChS
(Thinking about, and changing settings for)
.212**
LoM
Willingness to spend, or have spent, money
ICTExpertise and age,
Adjusted R-squared=.070, p=.000
Demographic variables

Figure 9: Model diagram used in PIII, labelled with newer results

4.4 Article: The Effect on Expression Reluctance of Spending Time on Privacy and Security Issues (PIV)

This article gives a more in-depth treatment of the TChS, TMT, and RtoEx constructs and applies Smith et al.'s (2011) APCO research model.

[6] Based on significance calculation from https://www.danielsoper.com/statcalc/calculator.aspx?id=104

4.4.1 Research questions

RQ 5: Do some demographic factors influence Internet users′ reluctance to express themselves online; either directly, or indirectly by moderating privacy concerns?

RQ 5.1: Can additional insight be gained from applying some research results to the Antecedents-Privacy Concerns-Outcomes model?

RQ 5.2: If the mere contemplation of device security and privacy settings is interpreted as a manifestation of privacy concerns, then does that impact the reluctance to controversially express oneself?

RQ 5.3: Do different demographic groups have different reluctances to freely express themselves online?

This study addresses the following hypotheses. They are described in detail in PIV:

H51: Users′ perception that it takes excessive (or ″too much″) time to deal with the security and privacy settings of their device (TMT) will positively correlate with a reluctance to express (RtoEx).

H52: The contemplation of one′s device′s privacy and security aspects (TChS) will positively correlate with a reluctance to express (RtoEx).

H53: The contemplation of one′s device′s privacy and security aspects (TChS) will positively correlate with a perception that it takes excessive (or ″too much″) time to deal with the aspects (TMT).

H54a: ICT expertise will positively correlate with users′ contemplation of their devices′ privacy and security aspects (TChS)

H54b: Income will correlate positively with users′ contemplation of their devices′ privacy and security aspects (TChS)

H54c: Gender will correlate with users′ contemplation of their devices′ privacy and security aspects (TChS).

H55a: ICT expertise moderates the correlation between the contemplation of one′s device′s privacy and security aspects and a perception that it takes excessive time to deal with the aspects (H53).

H55b: Income moderates the correlation between the contemplation of one′s device′s privacy and security aspects and a perception that it takes excessive time to deal with the aspects (H53).

H55c: Gender moderates the correlation between the contemplation of one′s device′s privacy and security aspects and a perception that it takes excessive time to deal with the aspects (H53).

H56a: ICT expertise moderates the correlation between the contemplation of one′s device′s privacy and security aspects and a reluctance to express (H52).

H56b: Income moderates the correlation between the contemplation of one's device's privacy and security aspects and a reluctance to express (H52).
H56c: Gender moderates the correlation between the contemplation of one's device's privacy and security aspects and a reluctance to express (H52).
H57a: ICT expertise moderates the correlation between users' perception that it takes excessive time to deal with the security and privacy settings of their device and a reluctance to express (H51).
H57b: Income moderates the correlation between users' perception that it takes excessive time to deal with the security and privacy settings of their device and a reluctance to express (H51).
H57c: Gender moderates the correlation between users' perception that it takes excessive time to deal with the security and privacy settings of their device and a reluctance to express (H51).

4.4.2 Background

Smith et al. (2011) have developed a research model to enhance research related to privacy concerns. The model is called the Antecedents-Privacy Concerns-Outcomes (APCO) model (see Figure 6). As its creators define, the model can represent privacy concerns' mediating or moderating effects on the relationships between antecedents and behavioral outcomes. The model also includes an accounting for the variables or factors used in risk-benefit assessments that the users do.

The model has been applied by other researchers to map numerous variables into the model operationalization. It has been used in works by Benamati et al. (2017), Bandyopadhyay (2009), Sun et al. (2019), Zhang et al. (2013), Dinev et al. (2015), and Ayaburi et al. (2019). Variables that have been applied include "privacy awareness," age, gender, and "privacy protecting behaviors" that include limitations on one's posting in a social media context.

The previous research applications of APCO have helped address some of the research gaps outlined by Smith et al. (2011). This paper addresses some of the gaps by applying variables that include the TChS, TMT, and RtoEx factors to the model.

This paper uses an expanded data set relative to PII to assess relationships between the time (TChS and TMT) and expression reluctance (RtoEx) factors. Moreover, it includes gender as a demographic factor. This study also applies the Antecedents-privacy concerns-outcomes (APCO) model.

4.4.3 Research Task

This section contains a short description of the research task and the bases of some of the hypotheses that are presented in PIV.

4.4.3.1 Hypotheses development

We attempt to ascertain causality using the three baseline criteria of Antonakis et al. (2010), those being (to paraphrase) temporality, correlation, and exclusion of other causes. To establish the necessary temporal relationship between the latent variables, we present that the questions in the survey regarding time usage precede the questions regarding a reluctance to express. Hence, there is an acute temporally ordered reminder to the respondent of time consumption used for settings adjustments, before the questions about online expression. The other argument for the proper temporal relation is that the pragmatic user will initially tend to customize or adjust their PC or connected device features and settings before initially using the device. Our prior investigation (Rauhala et al. 2019a) found that most users check and adjust the security and privacy settings of their devices prior to initial use. In addition, many devices and operating systems, such as Android devices, will initially prompt the user to make choices for their settings during first use. The settings include ones for privacy and security. For example, the user is asked whether to enable location services and given the option to choose a PIN for locking their device.

Moreover, users who are aware of "revenge hacking" (Branigan 2011) may be motivated to make adjustments to their privacy and security settings preventively. Such adjustments would help to protect against revenge hacking. The action may be especially necessary prior to the expression of a controversial or provocative opinion online. Controversial or provocative online expressions have motivated various retaliatory acts. The Internet is often used to commit retaliation. The second criterion is established upon analysis of the data. The third condition is more difficult, as, by nature, any study is limited in the factors and variables that are elicited by data gathering or by analysis. Few behavioral studies can consider or analyze every possible contributing causal factor of an effect. In this work, we may only assert causality to the extent that the analyzed elicited variables and factors have been included in our analysis. Between Antonakis et al.'s criteria and our discretion, we believe there are reasonable grounds to assert that there is some directional causality between the factors discussed. The model as applied to this article is in Figure 10. The numbered hypotheses in Figure 10 are listed and described in detail in PIV.[7]

[7] To help content-flow, these hypotheses are numbered differently in this dissertation.

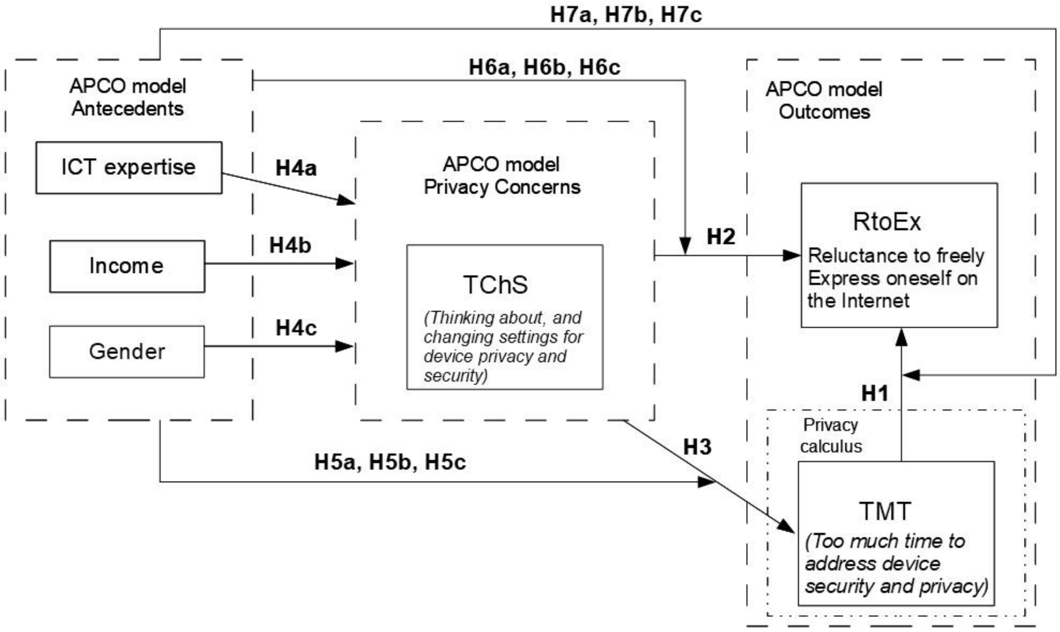

H7a, H7b, H7c
H6a, H6b, H6c
APCO model
Antecedents
ICT expertise
Income
Gender
H4a
H4b
H4c
APCO model
Privacy Concerns
TChS
(Thinking about, and changing settings for device privacy and security)
H2
APCO model
Outcomes
RtoEx
Reluctance to freely Express oneself on the Internet
H1
Privacy
calculus
TMT
(Too much time to address device security and privacy)
H3
H5a, H5b, H5c

Figure 10: Antecedents-Privacy Concerns-Outcomes model for the hypotheses

4.4.4 Findings

The latent extractions and validity calculations on them were performed and confirmed the validity of the latent variables.
We perform a Pearson correlation analysis between the three factors RtoEx, TMT, and TChS using SPSS software. The results in Table 15 show a significant positive correlation between a reluctance to express oneself online and a long-perceived time spent on setting device security settings (.238**). On the other hand, there is no significant correlation between the factors RtoEx and TChS, with TChS representing the usage of time for thinking about device security settings. Hypothesis H51 is thus confirmed, and hypothesis H52 is rejected. A positive correlation of .179**, p=.003 was found for TChS and TMT, thus confirming H53.

Table 15: Pearson correlations between RtoEx and TMT and TChS in PV. Two-tailed significances: * to .050 level, ** to .010 level, *** to .001 level

n=265	Device security/privacy takes “too much time” (TMT)	Spend time thinking about and changing settings (TChS)
RtoEx	.238***	.067

H54a is also confirmed with a weak positive correlation between ICT expertise and TChS (p=.055) (Table 16). H54c is confirmed with a significant correlation between gender (male respondents) and TChS. No significant correlation was found between income and TChS (0.025, p=.684); thus, H54b is rejected.

Table 16: Correlations between independent antecedents and latent variables in PV

Independent variables	TChS	TMT	RtoEx
ICT expertise	.118 (p=.055)	.100	.048
Income	.025	.159**	.101
Gender	.208**	.107	.214***

The moderating effects of the demographic variables for H54a-c were analyzed in a regression analysis on H51. Gender and income moderate H51 (adjusted R-squared .118, p=.000). Thus, H57b and H57c are confirmed, and H57a is rejected. Female respondents and those with higher incomes are more likely to be reluctant to express themselves online if their device privacy and security settings require excessive time to address. Regression was also performed on the antecedents against H52 and H53. Income and gender were found to moderate H52 (adjusted R-squared .072, p=.000). H56b and H56c are confirmed, and H56a is rejected. For regression of the antecedents against H53 (TChs -> TMT) yielded an effect from income. H55b is thus confirmed, and H55a and H55c are rejected. TChS, combined with income, predicted some variance in TMT (adjusted R-squared .049, p=.001). Users with higher income are more likely to decide, upon consideration of their devices' security issues (TChS), that the issues require too much time to address (TMT). Table 16 shows the correlations between the antecedents and the concern factor and outcome factors. The results show a confirmation of H4a and H4c, and rejection of H4b, though income moderated H53 and ICT expertise did not.

Figure 11 presents the results in the applied APCO model. Table 17 presents the percentage of respondents tending to agree with TMT, TChS, and RtoEx. Perhaps strikingly, more than half of all respondents are reluctant to make controversial expressions online, with almost two-thirds of female respondents being reluctant.

Table 17: Percentages of respondents who tend to agree or strongly agree with TMT, TChS, and RtoEx in PV

N=265	Overall addressing security and privacy aspects takes too much time (TMT)	Overall spend time thinking about device security and check/change settings (TChS)	Reluctant to express online (RtoEx)
Overall	30.64	59.6	57.7
Male	32.9	67.8	52.0
Female	27.4	48.7	65.5

Appendix D contains detailed results tables for the findings of the regression analyses.

The findings address the research questions as described in section 6.4.

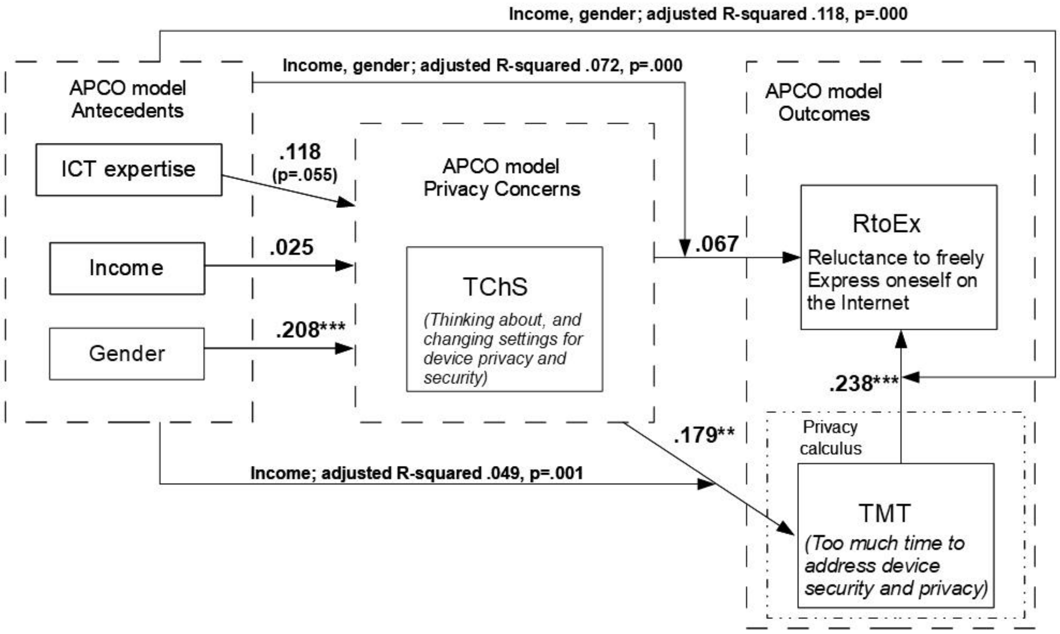

Income, gender; adjusted R-squared .118, p=.000
Income, gender; adjusted R-squared .072, p=.000
APCO model Antecedents
ICT expertise
Income
Gender
.118 (p=.055)
.025
.208***
APCO model Privacy Concerns
TChS
(Thinking about, and changing settings for device privacy and security)
.067
APCO model Outcomes
RtoEx
Reluctance to freely Express oneself on the Internet
.238***
.179**
Privacy calculus
TMT
(Too much time to address device security and privacy)
Income; adjusted R-squared .049, p=.001

Figure 11: Macro model with results

5 SUPPLEMENTAL TOPICS

Some broader technology and privacy issues are considered beyond the main theme of this work. These include the consideration of societal consequences that may result from various cybersecurity threats to individuals.

IT is a rapidly evolving field due to the continuous development of new technology and tools and new emerging research. As such, the terminology for describing concepts related to the field should evolve and be updated as needed. New terminology becomes necessary to for the discussion of modern concepts that cannot be succinctly and coherently described in an efficient way using traditional terms of a field. Section 5.1 introduces and propose some new preterms for the IT field. We hope that the presented preterms will benefit the discussions and understanding of Internet privacy, information security and cybersecurity.

Internet users may be concerned about the security vulnerabilities of their devices or data. The mere loss of use of a smartphone may cause significant stress to users. Such loss can reasonably imply a breach of personal data that may result in, for example, data loss or unauthorized access. Battery-powered connected devices themselves may pose unexpected physical threats. Section x discuss a consideration of these unconventional physical threats. Section 5.3 describes two techniques that may reduce risks to user data and thus help to maintain user confidence in the security of their devices and data.

5.1 New preterms for the modern information technology age

Terminology science describes special lexemes (or lexical units) which are studied for the meanings and for their denotion of concepts, as well as for the appraisal of existing definitions (Wikipedia Contributors, 2021a). New scientific concepts can be described by types of lexemes called preterms that can be composed of multiple words. (Wikipedia Contributors, 2021a).

5.1.1 Surveillance paradigm and tools

Merriam-Webster dictionary defines surveillance as:

> *"close watch kept over someone or something (as by a detective)"*
> (Merriam-Webster, n.d.e)

Post facto surveillance of online content has become commonplace. It is trivial to perform. Information about media and texts that have been uploaded or posted by a user can be searched with search engines. Depending on the user's privacy precautions, online content can be found. The search results can include his social media postings and other freely available information. Freely available information can include that in electronically accessible public databases and in databases made available by data brokers and online data conglomerators. Data conglomerators include the popular services whitepages.com and spokeao.com. Internet search engines such as bing and duckduckgo do not require special credentials (such as a detective's license) for their use.

Real-time monitoring of unsecured IP cameras, or 'live CCTV camera hacking' has become accessible to Internet users (Shankhdhar, 2021). Such cameras include unsecured home IP/WiFi cameras. With the help of an IP camera geolocation service such as https://hacked.camera/map/ and other gleaned information, real-time video surveillance of a 'target' area can be performed by amateur detectives, hacking hobbyists or any user (IPVM Team, 2018; Editorial Staff, 2020).

More targeted and effective real-time surveillance can be carried out using more sophisticated tools such as those available for eavesdropping of cellular network communications. Internatational Mobile Subscriber Identity (IMSI) catcher devices are available from websites such as www.thespyphone.com. (This website's "about" page declares that their customers include "private persons.") The devices are available from online merchants and can intercept and monitor cellular network communications in real-time. As of this writing, the cost of the necessary equipment to eavesdrop on cellular communications (including 4G communications) varies. The cost can range from around $150USD[8] to $7,000USD (Goodin, 2020).

Moreover, an 'SS7' security flaw can be used to gain access to a targets Telegram, WhatssApp, or Facebook accounts (Storm, 2016). This can enable observation and tracking of the target's online activities and location. The flaw can be exploited by non-sophisticated users (Gitogo, 2019).

[8] See https://www.alibaba.com/product-detail/Low-price-4-Port-GoIP-Gateway_1600179099771.html?spm=a2700.galleryofferlist.normal_offer.d_title.578a38c7S0CNWK

5.1.2 Detectives – traditional vs. modern

A detective is defined as:

> "*one employed or engaged in detecting lawbreakers or in getting information that is not readily or publicly accessible.*" (Merriam-Webster, n.d.c).

In the IT age, some professional private detective services have used labels such as Internet detectives (or Internet sleuths)[9], or Internet private investigators (Rostocki, 2021).

Detective-like activities in the modern Internet age encompass the use of new powerful search tools that are not the exclusive domains of nation states or so-called professional detectives. In practice, nearly everyone with Internet access can search for information on any individual. Free services such as mylife.com, spokeo.com, and whitepages.com provide basic information on search targets that have entries in their databases. Some services that offer information that has somewhat higher barriers of practicality and who may charge a fee do not require the customer to provide proof of licensure as a professional detective.[10,11] The uniqueness and speciality of the 'detective' profession has been diluted because of advancements in technology.

Other occupations and professions have met a similar, though more complete demise over time. Occupations such as knockerupper (a person that would manually awaken others at a designated time by knocking), elevator operator (a person designated to operate an elevator's controls for its users), and travel agent no longer exist or have been largely replaced by technological advancements. These examples of obsolete occupations are ones where workers performed tasks and fulfilled roles that were important and necessary in the past. The roles have been rendered obsolete by technological advancements. Customers now perform these services for themselves. The significance and need for the occupations have been eliminated or reduced, as has the distinction of the occupational titles. In many respects, the title of 'detective' has little prestige beyond law enforcement, and little significance beyond legacy licensure formalities for some specialties within the profession.

Sophisticated surveillance equipment such as International Mobile Subscriber Identity (IMSI) catchers is available for purchase online, though sales to consumers in some countries may be restricted. IMSI catchers can be purchased for as little as $150USD.[12] Some merchants such as detectivestore.com only

[9] https://www.internetdetective.net/

[10] See https://www.spokeo.com/purchase?url=%2F

[11] See https://support.whitepages.com/hc/en-us/articles/115012779187-How-do-I-change-my-payment-method-

[12] See https://www.alibaba.com/product-detail/Low-price-4-Port-GoIP-Gateway_1600179099771.html?spm=a2700.galleryofferlist.normal_offer.d_title.578a38c7S0CNWK

permit sales of such powerful devices to authorized institutions,[13] while others such as thespyphone.com apparently permit sales to private persons.[14]

IMSI catchers are able to intercept cellular and data traffic from the target's device. The information contained in the intercepted traffic would reveal the target's associates as well as his plans for meetings and excursions. Unless the target is wily and sophisticated, or communicates with his associates using a form of supplemental encryption, the target's plans for meetings and excursions would be revealed in advance and not post facto. When voice communications and other communications of the target can be intercepted in real-time, the need for traditional detective footwork (such as stakeouts or following) is reduced.

Most Internet users are neither wily nor sophisticated with regards to countering such advanced surveillance. Most Internet users in the United States have performed an online search on themselves (Madden, 2013) or someone else (Madden et al., 2007). The searches can reveal a wide range of information about the target in the form of 'digital footprints' that include names, addresses, phone numbers, photos, posted content, and more (Madden et al., 2007). Thus, the majority of Internet users in the United States have already performed detective-like tasks in search of digital footprints of their targets. Much of the information contained in such data had previously had a high barrier of practicality and would often require the services of a professional detective. Examples of such data would be photographs or opinion letters to newspaper editors. Thanks to the Internet the barrier of practicality for such information is now greatly reduced, and the information (if accessible online) is now available to anyone.

The dictionary defines 'adversary' as:

> "*having or involving antagonistic parties or opposing interests*"
> (Merriam-Webster, n.d.a)

When an adversarial detective seeks and gathers information about an individual the retrieved information is not under the control of that individual. The individual is likely unaware that personal information about him is being sought or collected. Once the personal information has fallen into an additional set of hands, the security and privacy of that information has been reduced. With a wider dissemination of the information, the risk of even wider dissemination (accidental or not) or abuse of that information increases. The availability of the information is being harnessed and potentially exploited without the target's knowledge. Wacks (1989) asserts "*that the core of the preoccupation with the right to privacy is protection against the misuse of personal, sensitive information.*" The individual cannot know whether, or how, the now more-widely disseminated information about him may be exploited in the future. With these assertions in mind, we argue that any Internet search for information about a private person is, by default, adversarial. Even if such a search is authorized by the person, the privacy and

[13] See https://www.detective-store.com/imsi-catcher-for-phone-calls-and-sms-messages-interception-1293.html

[14] See https://www.thespyphone.com/about-us/

security of his personal information that appears in the results is reduced by virtue of the incremental dissemination that has occurred from the search. With rare exception (a possible example would be an election candidate), this is not in the interest of the person whose information is being sought.

5.1.3 New preterms: 'Adversarial surveillance' and 'adversarial detective'

We propose the following new preterms:

Adversarial surveillance: *The act of seeking and gathering personal information about an individual for benign or hostile purposes.*

Adversarial detective: *A person or organization that engages in the seeking and gathering of information about an individual for benign or hostile purposes.*

An example of a benign purpose for data collection in the above contexts would be to populate a seemingly mundane database that nonetheless may have a significant potential to be abused. The signficant potential could result from a low barrier of practicality (* see below) for widespread dissemination of the information, or from the sensitive nature of the collected data (e.g., affiliation with a political ideology whose public favor may significantly change over time.) The risk of widespread dissemination could result from, among other things, poor information security practices of the collecting entity, or uncertain future of the equipment or organization that stores the collected data. Hostile purposes are those intended to bring immediate or future harm to the person. The harm may be direct or indirect, and the purposes can include hacking the persons devices or doxing him.

5.1.4 'Barrier of practicality'

Barrier of practicality: *collectively, those hindrances and obstacles that prevent the immediate and widespread broadcasting or availability of (sensitive or confidential) information.*

The barrier of practicality is to be expressed using a reference scale, numerical or nominal. The scale should have values that indicate the effectiveness of the BoP. The effectiveness should be judged using a range that extends from insignificant, ('low') to significant ('high').

Here are examples of the assessment of scenarios for assigning BoP parameters. In the 1960's, to disseminate unauthorized copies of a sensitive document would require an adversarial detective to physically enter the location of the document, pilfer the document, create mimeograph copies of it, and then distribute those copies manually, or by using a courier service. This 1960's process is rife with risks to the adversarial detective, as well as potentially strenuous requirements of time consumption and physiological energy. It also requires the availability and proper functioning of mechanical devices, acceptable performance of courier services, and so on. It can be said that the barrier of practicality protecting the information of the sensitive document in this case is significant, or 'high.'

Contrast the above scenario with one from modern times. If a sensitive document is stored on a networked computer, an adversarial detective could, due to poor information security practices of the data custodian or with widely available exploits and hacking tools, instantaneously download a perfect replica of the electronic document. He could then immediately make it available for instantaneous download and potential abuse by any number of interested users, anywhere with an Internet connection. In this case, one could say that the barrier of practicality is ′low′. With the use of network identity masking or other tracking obfuscation tools, the adversarial detective can almost eliminate his risk of being caught and identified, unlike in the 1960's where a perpetrator had needed to visit a geographical location and contend with physical obstacles. In the modern case described, there are essentially no obstacles or hindrances to the immediate and widespread availability of the document after it has been pilfered.

There are many other information security and privacy scenarios to which this preterm can be applied. Ideally, the BoP could be used to to reliably compare the privacy risks of different extant situations and hypothetical scenarios. This would require an objective method to quantify the BoP. A method for quantifying the BoP on a case-by-case basis will be developed in future research. A consistent and rigorous method for determining the BoP level would enable a reliable and objective BoP level. This would make the BoP parameter useful for comparing the privacy and information security risks of different situations and contexts.

5.1.5 ′Personal technology space′

Personal technology space: *The expectation of privacy that a person has with their technology; the information that their technology processes, the way that that processed information is used; and the way that their technology is used.*

The new preterm ′personal technology space′ is defined here, in part, in terms of existing concepts of various personal spaces. We have attempted to avoid definitions of the existing accepted concepts that would be excessively general or high-level. Such definitions potentially include an excessive amount of parameters and characteristics that would make differentiation difficult between the various accepted concepts. We have tried to limit the defining characteristics of the existing personal space concepts to only those that are most essential for the respective concepts. This helps with differentiating the existing concepts and with defining the new preterm, ′personal technology space′ using the existing concepts. In the following we will try to define the personal technology space in the context of some existing notions of abstract personal spaces.

PTS includes an expectation of dominion and privacy over the space.

5.1.5.1 Physical space

Proxemics "is the study of human use of space and the effects that population density has on behaviour, communication, and social interaction."

The concept of personal (physical) space has been found to be universal across cultures, though practical personal (physical) distance preferences between cultures vary from around 40cm to 1m (Sorokowska et al., 2017), the concept of personal (physical) space has been found to be universal across cultures (Sorokowska et al., 2017 ; Sommer, 1959)

Invasions of one's physical space have been said to be those that provoke defensive fighting or withdrawal (so called "fight or flight") reactions (Sommer, 1959). Other factors influencing the desire to guard one's personal space include a desire to avoid catching a disease (Park, 2015).

Unlike 'personal space' as applied in the geographical or body-centric contexts, Personal Technology space is not a fixed territorial area nor is it carried around by the person like an abstract spatial bubble.

5.1.5.2 Psychological space or emotional space

When considering so-called 'psychological space', research that exists on the concept has defined it quite broadly. The definition has attributes that include physical territory, objects, self-presentation, social attachments, attitudes, habits, and values into the scope of the concept (Belousova et al., 2015; Bukhanets & Bayer, 2016; Nartova & Bochaver, 2004). This concept of psychological space has some overlap with PTS, but includes factors that PTS does not.

A personal technology space can be considered a form of psychological or emotional space that is intimately tied to a desire for information privacy and dominion over one's true online identity or persona in the cyber realm (as distinct from ″cyber persona″, see section 5.1.5.3).

In a contemplation of the similar-sounding but different cyber persona concept, Jain (2009) has suggested that a user's cyber persona includes information about their contact information, social networks, preferences, and important life events. He does not include aspects of information processing or information handling. For the present purpose, the ′cyber-persona′ may be considered the information and presentation of the user's virtual doppelganger or "parallel online existence" over which the user believes they have, or should have some control. In contrast, the information of PTS is related to the user's true or authentic identity and is generally that which is incidentally collected during ordinary online transactions and activities. PTS includes an expectation of dominion and understanding over the processing and handling of one's data - more so than in one's cyber persona.

5.1.5.3 Cyber persona or online identity

Wikipedia defines ′online identity′ most broadly as ″*a social identity that an Internet user establishes in online communities and websites*″ (Wikipedia, 2021c). The concept of a ′cyber persona′ has been contemplated by Jain (2009) as more of an online consumer profile that is compiled by online providers of products and services. In his definition, the data is apparently collected incidentally to the consumer's activities, and the consumer can even be oblivious to the collection and storage of his information. For example, the seller will store the consumer's purchase information as a normal and expected part of the transaction. Thus, Jain's description does not consider an expectation of sovereignty and control by the user over his cyber persona. The Wikipedia definition for 'online identity' which is also called an 'internet persona' (Wikipedia, 2021c) is similar to the one considered in Rodogno's (2012) work.

Rodogno (2012) has considered more esoteric questions regarding personal online identity. He presents various arguments for differing concepts and motivators of online identity. A definitive description of personal online identity is evasive amongst the literature. We do not deal with the more esoteric questions about what form of online identity(s) the user wishes to present and protect. For our purpose, we assume that there is some personally identifiable information online and subject to processing by his devices over which the user wishes to have sovereignty or ownership, and by definition this is not their cyber persona.

The concept of an online identity is more specifically described by Wikipedia (2021c) as:

"...a social identity that an Internet user establishes in online communities and websites.... (online) *identities are associated with users through authentication, which typically requires registration and logging in. Some websites also use the user's IP address or tracking cookies ..."*

The online identity is malleable and may be an alter-ego or pseudonym. Thus the user's protection of his identity, or of the integrity of his identity is not a core aspect of the online identity. When a user's online identity's reputation is tarnished, the user may replace it with a new online identity. The online identity or cyber-persona is not centered on the user's true identity or 'self' as is PTS.

PTS is more concerned with the user's expectation of privacy and with functions of the devices and technologies that collect, transmit and processes the online identity data. The transmission can be into storage or into subsequent processes that use the data.

5.1.5.4 'Safe space'

In terms of facility, a safe space is commonly described as an area for use or a group of individuals (Yee, 2019). Areas for use can include physical spaces such as a classroom, and groups of persons designated as safe spaces can include traditionally marginalized ones who agree to avoid certain topics while communicating (Ho, 2017). These groups or physical spaces are also called 'emotional safe spaces'. Such spaces are for restricted discussions that exclude specified topics. Indeed, Merriam-Webster (n.d.d) defines safe space as "*a place (as on a college campus) intended to be free of bias, conflict, criticism, or potentially threatening actions, ideas, or conversations.*"

Alternatively, safe spaces have been designated for the purpose of unrestricted and open discussions. During discussions in these spaces, participants are encouraged to take intellectual risks. Topics that may make others feel uncomfortable are allowed to be debated in these spaces (Ho, 2017). Physical spaces may be designated for open discussion of 'uncomfortable' topics, and these spaces may also be referred to as 'academic safe spaces' (Ho, 2017).

For the current purpose, safe spaces are understood to be places or locations (including Internet discussion forums that include social media) intended for interaction that are defined in terms of exclusive topics, or topics that may not be raised or discussed. The topics are determined by the safe space leadership or by a collective decision, thus they are not autonomously controlled by the individual. Though disclosure of personal information and sensitive personal information may occur in safe spaces (and thus may imply an expectation of a privacy agreement with other participants), the individual should not have an expectation of ultimate control of such spaces and thus the safe space paradigm is not applicable to the personal technology space concept. The safe space is not centered on the individual. When choosing to join or utilize a safe space, the user is joining an entity that is mutually agreed with others or already exists. The regulation of the space is collective or performed by a separate leadership.

5.1.5.5 Definition of personal technology space

Personal technology space is a concept whose core aspects overlap with those of other 'space' concepts as shown in Table 18.

Fundamental aspects of modern technology utilization by individuals that are important to PTS include physical access to one's connected devices, remote access to one's devices, control of electronically 'published' personal information, and the expected ability to control and conceal universally public personal information that is made available online by various authorities and organizations. These overlap with the autonomy over one's psychological space, which, by definition, includes an expected possibility to control and conceal universally public personal information that is made available online (the applicable aspects of psychological space are 'protection of personal identity' and 'self-presentation').

A personal technology space is the expectation of privacy that a person has with their technology; the information that their technology processes, the way that that processed information is used; and the way that their technology is used. PTS exists because the underlying technologies required for the privacy expectation exist. The privacy expectation and right has not ceased to exist because of the new technologies, though the technologies have generally made personal privacy more vulnerable. Rather, the fundamental right to privacy and the importance of privacy have remained despite technological advances.

The importance of privacy to a healthy society has been outlined by Nissenbaum (2010) and others.

Table 18: Fundamental aspects that define various 'space' concepts (not all aspects are shown)

Aspect	**Personal technology space (PTS)**	Cyber-persona (or online identity)	Physical space	Psychological space	'Safe space' (author's interpretation from Yee, 2019; Ho, 2017)
Perception or expectation of autonomy or sovereignty.	✓	✓ an "actively constructed presentation" (Wikipedia, 2021c)	✓	✓	
Body and physical distance of body from others. Body-centric abstract bubble.			✓	✓ (Nartova-Bochaver, 2004)	✓ (those with disruptive viewpoints are not allowed into the space.)
Fixed geographical area			✓	✓ ('personal territory', [Nartova-Bochaver, 2004])	✓ (in the case of physical meeting places.)
Physical objects / things	✓ (only connected devices.)			✓	
Social attachments (real or virtual).		always (Jain, 2009), or in some cases. (Wikipedia, 2021c)		✓	maybe (the user may choose a safe space based on his social circle.)
Attitudes				✓	maybe
Self-presentation		✓		✓	maybe (the user may choose a safe space but not necessarily

					express himself while in it.)
Alter-ego / doppelganger / pseudonym presentation		✓ (Wikipedia, 2021c)			
Protection (of integrity) of personal identity	✓			✓	
Habits		✓ only as presented online, or Internet usage habits.)		✓ (Nartova-Bochaver, 2004)	
Values		✓ (to the extent reflected by his online expressionism and electronically recorded or stored preferences.)		✓ (Nartova-Bochaver, 2004)	✓ (user chooses the safe space corresponding to his values.)
Expectation or desire for control over the handling of online personal information or personally created original online content or information.	✓				
Third-party electronically stored personal information, preferences, and life events.		✓ (Jain, 2009). Note: Jain’s definition does not include ’active creation’ of the persona.			

The conceptual positioning of PTS in relation to other personal space concepts is shown in Figure 12.

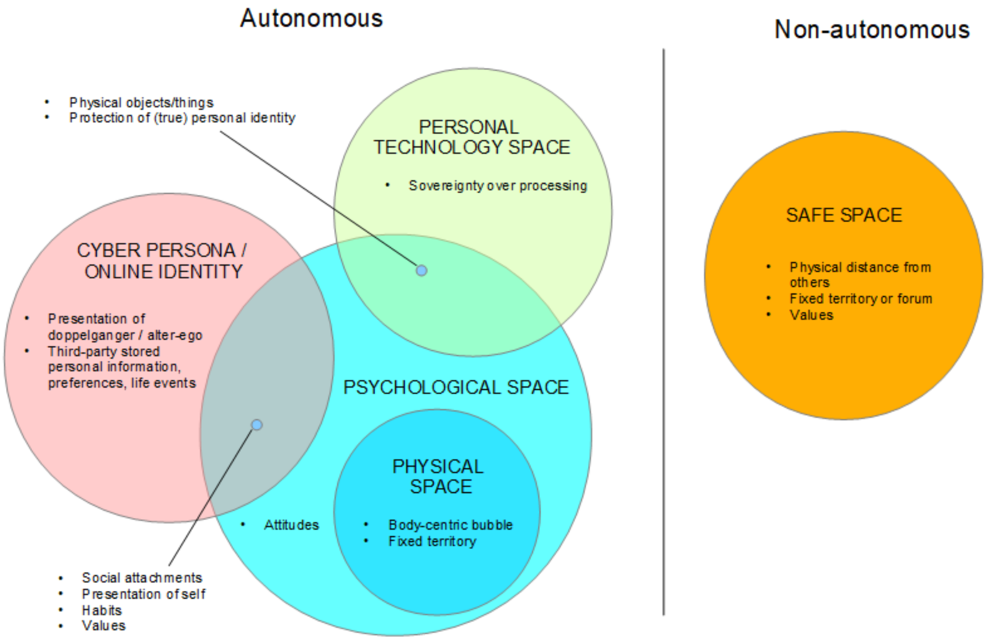

Autonomous
Non-autonomous
Physical objects/things
Protection of (true) personal identity
PERSONAL TECHNOLOGY SPACE
Sovereignty over processing
CYBER PERSONA / ONLINE IDENTITY
Presentation of doppelganger / alter-ego
Third-party stored personal information, preferences, life events
PSYCHOLOGICAL SPACE
PHYSICAL SPACE
Attitudes
Body-centric bubble
Fixed territory
Social attachments
Presentation of self
Habits
Values
SAFE SPACE
Physical distance from others
Fixed territory or forum
Values

Figure 12: PTS amongst other personal space paradigms

5.1.6 Additional terms for future development

We hope that our future work should develop and define at least two more pre-terms. Two such terms are 'cyberprivacy' and 'E-stop'.

5.1.6.1 Cyberprivacy

At this time, cyberprivacy is tentatively defined as privacy in the context of all connected high-technology. Includes aspects that are encompassed by the common term "Internet privacy."

5.1.6.2 E-stop

E-stop is tentatively defined as a cessation of use, adoption or development of a new or emerging technology in order to assess the technology's implications to societal well-being and functioning. The cessation is warranted until an assessment can be made that satisfies a condition where the implications are deemed to be acceptable, or where the negative implications (or detrimental effects) to society (alternatively, to the targeted societal scenario or context) are deemed acceptable in comparison to the benefits of the technology. Potential threats of detrimental effects can be reported from observations or epiphanies that occur during development, reports by users, or CVE (common vulnerabilities and exposures) reports. For the purpose of this pre-term, the well-being and functioning of society is measured in terms of the maintenance and preservation of fundamental human rights. The rights include those of privacy. The ′new or emerging technology′ in the tentative definition above could be, for example, a new software application for a vertical market that has indirect influence over the lives of many, a new type of social media platform, or special-purpose drones that utilize independent AI.

E-stop can be expressed in terms of the familiar traffic light signals. For example, ′red′ can indicate a need for immediate cessation of adaptation of the technology due to a potential detriment that has been discovered that could have a critical detrimental effect; ′yellow′ could indicate that the technology development or adoption can proceed with caution – some detriments are anticipated but are not insurmountable or critical; and ′green′ can mean that the technology development or adoption can proceed as no unacceptable societal detriments are anticipated. A green e-stop condition could exist, for example, after the issues identified in an assessment are addressed and mitigated.

5.2 Potential Dangers from Third-party Technological Abuse of Smartphones

This supplemental topic addresses some ways that smartphones could be weaponized. Smartphones are widely used and thus smartphone safety and their potential to be abused should be continuously assessed.

5.2.1 Article: Physical Weaponization of a Smartphone by a Third Party (PV)

In this article, we describe some hypothetical methods of physically weaponizing smartphones. The methods can induce harm by abuse of the smartphone′s battery or RF transmitter. Some accessories and other features of smartphones could also be weaponized.

5.2.1.1 Research questions

RQ 4: What are some historically unusual physical dangers from smartphones that could be implemented by third parties?

RQ 4.1: What are the potential physiological impacts of such dangers on users?

5.2.1.2 Background, research task and method

In this article, a review of physical dangers from smartphones was performed vicariously. The work included an investigation of reports of a new self-destruct method developed for smartphones, the characteristics and dangers of smartphone batteries, and reports of injuries caused by smartphone malfunctions. The physiological consequences to users of some hypothesized dangers were estimated. Some mitigations and preventive measures for the hypothesized threats are suggested. Finally, a categorical framework and corresponding threat assessment templates are proposed.

5.2.1.3 Findings

Research question 4.1 is not a simple one to answer definitively as the article research is limited to information that is readily available online, and the author not an expert in traumata or explosives. Nonetheless, news reports of injurious incidents reveal the dangers to users that can result from explosions or fires from smartphone batteries. The technological chemistry and physics of smartphone batteries and the recent development of a physical self-destruct function for smartphones could potentially be abused to realize threats of technologically coordinated attacks against smartphone users. Extrapolating from reported incidents and prior research, the physiological dangers of fire, explosion, heating, and loss of device functionality can range from distress to fatality. The specific impacts would depend on the attack manifestation on the user's device.

Research question 4 is answered in the above paragraph. There may be certain potential dangers from modern cellphones and smartphones that are dependent on the technologies in the devices. Third-party implementation implies that the potential attacks are not carried out by an assumed trusted partner in the device purchase or usage scenarios. In the hypothetical scenarios, there could also be potential attackers that are not third parties.

The author assumes that most users have not considered the threats because the threat mechanism may be rather unconventional. Nevertheless, if such hypothetical threats were to be carried out and subsequently publicized, they may have grave effects on users' motivation to use smartphones. The effects may also apply to their motivation to use any mobile or Internet-connected lithium battery-powered device, whether for self-expression or for any other purpose.

5.3 Mitigating cyber risks to users' data files on their smartphones

This section describes an application of two patents from the viewpoint of reducing risks to Internet users' data.

5.3.1 Patent: Storage Profiles (PVI)

This patent describes a method of tagging data files according to usage context or contexts in which they are expected to be needed.

5.3.1.1 Research question

RQ 6: Is there a way to reduce the risk of cyber-hacking or unauthorized access to users' data files by using a method of profiled storage?

The tagging of files or other data items by way of allocated metadata field(s) is intended to ease file categorization and searching. Unfortunately, categorization and tag-searching of files can also be exploited during targeted searches by users that have gained unauthorized access to the storage device. Using tags, an unauthorized user can easily search for specific and potentially high-value files. This is especially problematic when a user stores all of their files on their primary device (typically a mobile device). Regardless of whether the user's files have been tagged, a hack or data breach on the user's device would make all of the user's files vulnerable.

Consider a case where a sensitive data item tagged as "personal" or "classified" is on the user's device during a usage context in which the file is not needed. If a hacker gains access to the file owner's files, the hacker may seek out files with specific metadata tags. By searching for files with specific tags, attackers may seek files that contain information about the user's finances or other personal information. The "personal" or "classified" file would be at risk, even though the user did not need it in the usage situation they were in when the breach occurred.

When a user stores all of their files on their primary device, the files are also at some risk of accidental exposure or distribution whenever the device is used to share content or show file contents to others. By being stored on the device, files that are inappropriate for the current usage scenario may be accidentally exposed or distributed. For example, suppose a hurried presenter seeks a file to display for their colleagues at a meeting. In that case, the presenter may accidentally show a spreadsheet of their household budget or a vacation photo.

One way to help prevent such risks is to load and offload files from the device depending on the expected usage context. This can be achieved by tagging the files or data items according to the usage scenarios for which they are appropriate or needed (see Figure 13:). Then, the user can load only those files that are necessary (based on their tags) from a secondary storage device. The user can also offload files, based on their tags, that are not necessary or appropriate for their current purpose. As a result, fewer files are stored on the user's device at any one time. This storage profiling reduces the overall risks from a hack or data breach of the device. Thus the user may feel more at ease while using their device for online expression or other tasks. Storage profiling also reduces the risk of accidental or inappropriate file exposure or distribution.

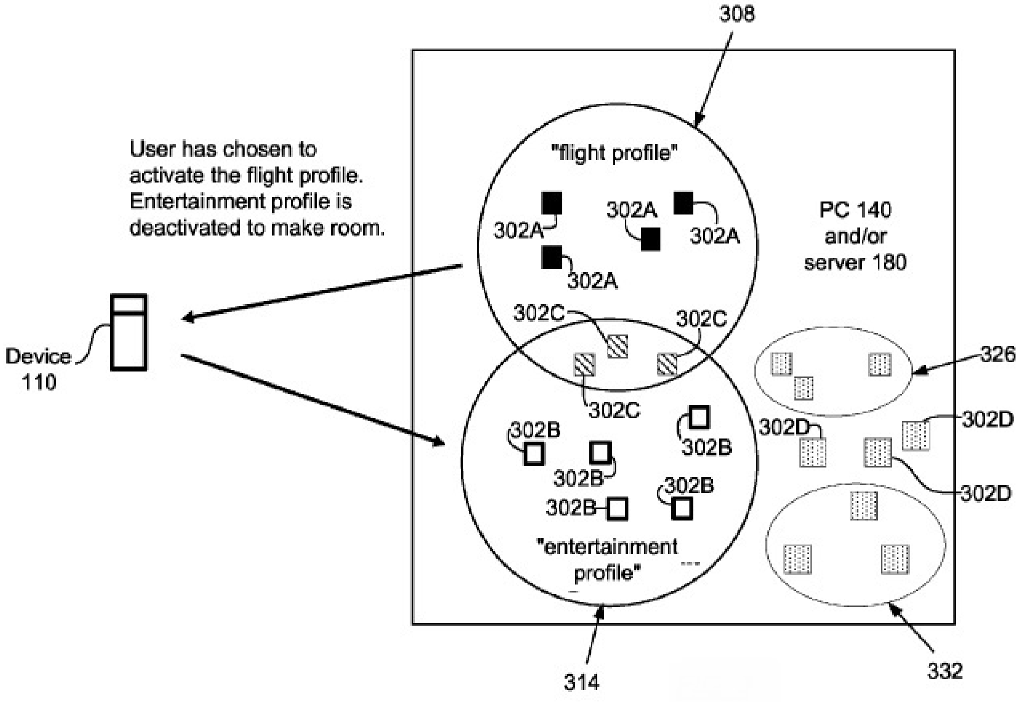


Figure 13: Diagram of profiled storage configuration from PVI. Items labelled 302A are ′flight′ profile objects. 302B items are ′entertainment′ profile objects. 302C items belong to both profiles. Other labellings are described in the patent.

5.3.2 Patent: Storage Management (PVII)

This section describes a system of loading and offloading data files from a users device. The the system is implemented dynamically or on demand, and can result in a reduction in the amount of users data that is most exposed on their primary device. The currently unneeded and offloaded and files can be stored in devices that have better security configurations.

5.3.2.1 Research question

RQ 7: Is there a way to reduce the risk of cyber-hacking or unauthorized access to users′ data files by implementing a method of a continuously maintained pseudo-cache system of distributed storage?

The term "cache" in computer science can refer to any one of various levels of random access memory on a computer or device that is differentiated from the other levels by its data access times and usually also by its capacity. Here, the term "pseudo-cache" refers to a distributed storage system between different storage platforms (on separate machines) that is automatically used ad-hoc in the background, or on user demand.

Combining a pseudo-caching method with the concept in PVI, a configuration can be implemented whereby the offloaded (i.e., currently unneeded) files are stored on machines or devices (e.g., personal server, third-party owned cloud server, etc.) that have more robust security measures than the user's immediately accessible device. The immediately accessible device may be a smartphone or laptop that the user is utilizing with a relatively higher level of activity. The activity can include actions that use the files that have been uploaded to his device that are necessary for the current usage context. The files are ones that the files' owner expects may be needed for the scenario, whether for configuration of other software, editing, sharing, or any other purpose where storage on the immediately accessible device enables the most efficacious method for fulfilling the current need. By having only those files necessary for the current purpose on his or her device, and currently unneeded files on a more secure storage platform, the user can reduce the overall risk exposure for the totality of his or her files. The offloading and downloading concepts of the profiled objects are illustrated in Figure 14. Because of the reduced risk, the user may feel more confident about freely using his or her device for expression and other purposes while connected to the Internet.

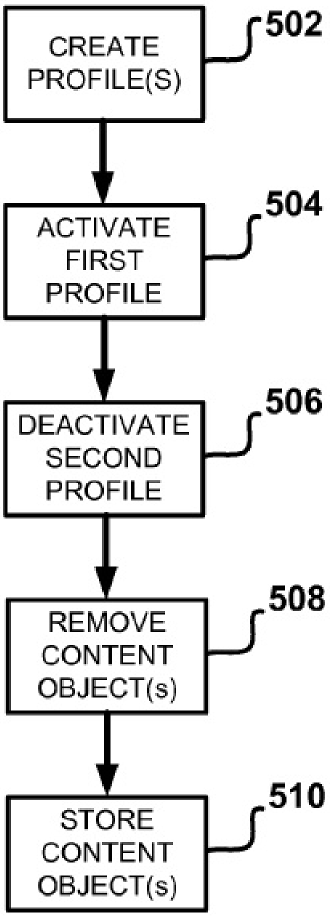


Figure 14: Diagram of process flow from PVII. After the profiles are created (502), the objects associated with a profile can be collectively transferred onto (510) and off (508) of the user's primary device using a system of prioritized storage devices. Further descriptions of the labelling and details of the process are in the patent.

5.4 RtoEx, TChS and TMT by Nationality

In this section we present hypotheses to address research questions RQ 8 through RQ 8.3 from section 3.2.

We study the relationship between three latent factors and cultural indices and the Human Freedom Index

It may be argued that TMT may more readily manifest from an impatient personality. Impatience is more associated with masculinity (Turner 2016) and assertiveness is associated with masculinity (Thomas 2001). Thus it would be conceivable that TMT value may be associated with Hofstede's Masculinity (MAS) (Hofstede, 1984) or House et al's Assertiveness Practices (House, 2004) indices.

H81: TMT will differ by nationality according to select cultural indices.

Uncertainty avoidance, by definition, relates to a willingness to take risks (Hofstede 1980, p.171). We might expect that respondents from cultures with a lower UAI would be less reluctant to express themselves. Similarly, respondents from cultures that place a higher value on individualism may be less reluctant to express themselves. We expect that RtoEx will differ by nationality in accordance with cultural parameters IDV, UAI, and House et al.'s parameters of Societal Institutional Collectivism Practices and Societal In-Group Collectivism Practices. House et al's two Globe parameters of Uncertainty Avoid Practices (UAP) and Uncertainty Avoidance Should Be (UAS) are also expected to vary with RtoEx. These last two House et al. parameters are correlated (p<.01) with Hofstede's UAI index (House et al. 2004, p.140). The HFI "expression and information" index is described by Vasquez & Porcnik (2017). Of the various HFI indices, this parameter seems pertinent to RtoEx as it purports to partly indicate expression freedom in a country. Thus, we may also expect that differentiation of RtoEx by nationality will occur in line with the nationalities' HFI "expression and information" (HFI-EF) values.

> *H82*: RtoEx will differ by nationality according to select cultural indices or HFI-EF value.

Because TChS is a preventive self-protective act, we may expect TChS to correlate with UAI. Index values from the HFI supercategory of Personal Freedom (PF) may also be suitable to compare with nationality-based TChS values. The HFI-PF is derived from the HFI-EF subcategory and additional parameters (Vasquez & Porcnik, 2017). The additional parameters include "Association, Assembly, and Civil Society" and "Rule of Law." If an HFI-PF value of a nation is low, we may expect the respondents to be more self-protective in ways that include the adjustment of their devices' security and privacy settings (TChS).

> *H83*: TChS will differ by nationality according to UAI or HFI-PF value.

6 RESULTS

The results in this section are presented mainly as answers to the research questions. Detailed results can be seen in sections 4, 5, 6.5 through 6.7, and in the Appendix.

6.1 Money and freedom

The findings in PI show that users who tend to be reluctant to express themselves online also tend to have a positive attitude toward spending money for personal cybersecurity protections.

Research question 1.1 is answered in the affirmative. There is a greater correlation between the LoM factor and RtoExC than there is between LoM and RtoExnonC. Internet users who are concerned about potential consequences for their controversial expressions are more inclined to spend money on cybersecurity and privacy products and services.

Research question 1.2 is answered in the affirmative for age. Older Internet users who are concerned about potential consequences for their controversial online expressions are more inclined to buy cybersecurity products and services than younger users (see footnote 5).

Thus, research question 1 may be answered in the affirmative when the question is slightly modified to consider both the behavior of spending and the attitude toward spending as encompassed by the indicator questions for RtoEx. There exists a relationship between the purchasing activity of Internet users toward privacy and security features for their devices and their attitudes toward such spending; and those users' reluctance to controversially express themselves online.

6.2 Money and time

Research question 3 is answered in the affirmative. There is a relationship between the time that Internet users spend on the privacy and security aspects of their devices, and their tendency to spend money on personal cybersecurity.

6.3 Time and freedom

The findings in PII show that users who believe that addressing their device security and privacy issues requires excessive time will be more reluctant to express themselves online.

Research question 2.1 is answered in the negative. We found no relationship between the mere contemplation of one's device's privacy and security aspects, and the reluctance to controversially express oneself online.

Research question 2.2 is answered in the affirmative. Our findings suggest that users are more reluctant to controversially express themselves if they perceive that it takes excessive (or "too much") time to deal with the security and privacy settings of their device.

Research question 2 is answered with a conditional affirmative. There is a relationship between the time that Internet users spend on the privacy and security aspects of their devices, and those users' reluctance to freely express themselves online when users perceive that the time is excessive. The mere application of time to addressing the security and privacy aspects of their devices, in itself and regardless of the objective quantity of the time, is not associated with a reluctance to express online.

6.4 A.P.C.O. model application

Research question 5.1 is answered with a cautious yes. Mapping of the latent constructs, selected demographic antecedents, and associations was done in good faith but may be problematic with varying interpretations of the parameters of this study and of the original APCO model taxonomy. In line with the results from PII, TChS (the "privacy concern" parameter) by itself doesn't affect the RtoEx outcome. However, when regression analysis is performed with the income and gender antecedents, we find that those antecedents play a significant role in moderating the TChs->RtoEx relation. Income was found to moderate the TChS->TMT (TMT being the "privacy calculus") relation. It can be said that those users with higher incomes who contemplate their device security and privacy settings (TChS) are more likely to conclude that such contemplation, and resulting corresponding adjustments, are too time-consuming (TMT), and may subsequently be more reluctant to controversially express themselves online (RtoEx outcome).

Research question 5.2 is answered in the above paragraph. The privacy concern variable of TChS does not itself affect the RtoEx outcome. Only by way of the income and gender moderators does it have an effect on the RtoEx outcome.

Research question 5.3 is answered in the affirmative. Table 12 shows that female respondents are more likely to be reluctant to express themselves online (65.5%) than male respondents (52.0%).

6.5 Demographic variables and their moderation effects

Results are presented with respect to demographic variables. Table 19 shows the demographic variables that were studied in the articles.

Table 19: Demographic factors whose moderating effects were evaluated in the articles

Article	Income	ICT expertise	Age	Gender
PI			x	
PII	x	x	x	
PIII	x	x	x	
PIV	x	x		x

6.5.1 Results from regression analyses

In PI, age was found to moderate RtoExC->LoM (adjusted R^2 =.037, p=.011). With the larger data set described in section 3.5.1, the effect was consistent with the earlier finding (adjusted R^2 =.034, p=.004).

In PII, age was found to moderate TMT->RtoEx (adjusted R^2 =.075, p=.000). Using the larger data set, the identical regression analysis (limited to inclusion of age only) showed a consistent result (adjusted R^2 =.077, p=.000).

In PIV a regression analysis that included multiple demographic factors was performed on all combinations of the latent factors RtoEx, TChS and TMT. Income and gender moderated TMT->RtoEx (adjusted R^2 =.118, p=.000). Income and gender also moderated TChS->RtoEx (adjusted R^2=.072, p=.000). Only income moderated TChS->TMT (adjusted R^2=.049, p=.001).

In PIII, age was found to moderate TChS->LoM (adjusted R^2=.035, p=.013). With the larger data set, ICT expertise and age together moderated the relationship (adjusted R^2=.070, p=.000).

6.5.2 Correlations with the latent variables

In PI, age was not significantly correlated with LoM. However, the variables were correlated in a supplemental analysis (ρ -.135, p=.028, see Appendix A). In PII, age was found to correlate with RtoEx (ρ=-.225, p≤.010). The supplemental finding was consistent with this result (ρ=-.185, p≤.010) and a Z-test showed that the two results did not significantly differ. In PII, age was also correlated with TMT (ρ=-.169, p=.018), but was not correlated in the supplemental analysis (see section 4.2.4). In PIV, ICT expertise was found to marginally correlate with TChS (ρ=.118, p=.055). Income was found to correlate with TMT (ρ=.159, p≤.010). Correlations were also found between gender and TChS (ρ=.208, p≤.010) and gender and RtoEx (ρ=.214, p≤.001). The correlation analyses results are shown in Table 20.

Table 20: Pearson correlatios of demographic variables with the latent factors (n.s. = not significant, n.a. = not evaluated)

Independent variables	LoM	TChS	TMT	RtoEx
Age	n.s., p>.050 [15]	n.a.	-.169* [16]	-.185**
ICT expertise	n.a.	.118 (p=.055)	n.s., p>.050	n.s., p>.050
Income	n.a.	n.s., p>.050	.159**	n.s., p>.050
Gender	n.a.	.208**	n.s., p>.050	.214***

6.6 Summary table of results

Table 21 (PIV) shows the results of this research in the context of current established knowledge. The results are based on the n=265 dataset that was used in PIV and that is described in section 4.4. PIV and the summary table do not include analysis results of LoM effects.

[15] ρ -.135*, p=.028 in supplemental analysis.

[16] n.s., p>.050 in supplemental analysis.

Table 21: Table of results in relation to previous research (PIV, from which hypothesis labels are keyed)

Hypotheses /observations	Confirmed /rejected	Description	Corroborates, or consistent with	Contradicts, or inconsistent with
H1	***	TMT will positively correlate with RtoEx.	N.A.	N.A.
H2	rejected	TChS will positively correlate with RtoEx.	N.A.	N.A.
H3	**	TChS will positively correlate with TMT	N.A.	N.A.
H4a	(p=.055)	ICT expertise will positively correlate with TChS	Chen, et al. (2010)	Sheehan (2002)
H4b	rejected	Income will positively correlate with TChS	Tsai, et al. (2016) Zhang, et al. (2013)	-
H4c	*** (males)	Gender will correlate with TChS	European Commission (2019) Girl Scout Research Institute (2019)	Sheehan (2002)
H5a	rejected	ICT expertise moderates H3.	N.A.	N.A.
H5b	*	Income moderates H3.	N.A.	N.A.
H5c	rejected	Gender moderates H3	N.A.	N.A.
Observation 1	*	TChS moderates H2	N.A.	N.A.
H6a	rejected	ICT expertise moderates H2	N.A.	N.A.
H6b	**	Income moderates H2	N.A.	N.A.
H6c	***	Gender moderates H2	N.A.	N.A.
Observation 2	rejected	TChS moderates H1	N.A.	N.A.
H7a	rejected	ICT expertise moderates H1	N.A.	N.A.
H7b	*	Income moderates H1	N.A.	N.A.
H7c	***	Gender moderates H1	N.A.	N.A.
Observation 3	rejected	ICT expertise is correlated with RtoEx	-	Sun, et al. (2019)
Observation 4	***	Gender is correlated with RtoEx	Beaussart and Kaufman (2013)	-
Observation 5	**	Income is correlated with TMT	Burchardt (2010)	-

*** = confirmed to three-star significance p ≤ .001, ** = confirmed to two-star significance p ≤ .010, * = confirmed to one-star significance p ≤ .050.

6.7 Nationality and cultural effects

In PIII, no significant effects of nationality were found on the TChS to LoM relationship. However, the data set in PIII was skewed to a single nationality and relatively small.

In this section, we present some additional results and propose answers to the hypotheses of section 5.4 and the research questions 8 through 8.3 of section 3.2. We briefly explore differences between nationalities for their RtoEx, TChS, and TMT values. We also investigate relationships between three of the latent factors (RtoEx, TChS and TMT) and selected Hofstede, House et al., and HFI indices. The analysis is done with a data set of n=306 that consists exclusively of Finns (43%), Americans (22%), Brazilians (19%), and Israelis (17%).[17]

Because of the different sample sizes for the nationalities, perform tests for variances. We compare using the Tukey-Kramer and Kruskall-Wallis tests as appropriate to find the differences in latent factor means between the nationalities.

We perform the Tukey-Kramer HSD calculation to find the differences between the means of TMT for the nationalities (Table 22).

Recall the formulation of the five-step scale questions as 1=strongly agree to 5=strongly disagree. The results show that respondents of Brazilian nationality disagree less strongly than Finns about TMT. The same might also be said of Americans (p=.079) and Israelis (p=.081) with respect to Finns.

For TChS, marginally significant differences were found between Israelis and both Finns and Americans. Finns and Americans might tend to agree more strongly with TChS than Israelis.

For the RtoEx case, we employ Kruskal-Wallis (K-W) test due to unequal variances. The K-W gives a significance of .575, and thus RtoEx between nationalities is not significantly different. H82 is rejected.

Research question 8.2 is answered with a negative as a result of the rejection of H82. Research question 8 is answered in the affirmative for TMT and TChS only.

Table 22: Tukey-Kramer HSD results, including marginal differences, n=306

Factor	Finland	USA	Brazil	Israel	Sig.
TMT	3.501		3.186		.040
TMT	3.501	3.233			.079
TMT	3.501			3.208	.081
TChS	2.606			2.974	.071
TChS		2.567		2.974	.079

[17] This is an expansion of the data set that was used in PIV. These analyses and results may be later included in PIV or compiled as part of a separate manuscript.

6.7.1.1 Latent factor vs. cultural and HFI indices

We analyze the values of the categorized latent factor of TMT for correlation with selected Hofstede and House indices. The indices of interest are Hofstede's Masculinity (MAS) and House et al's Assertiveness Practices. The compared values are in Table 23. Results of the correlation analyses are in Table 24.

Table 23: Hofstede and House et al. parameters for comparison to TMT

Latent factor or Cultural index	Finland	USA	Brazil	Israel
TMT	3.501	3.233	3.186	3.208
MAS	26	62	49	47
Assertiveness-Practices	3.81	4.55	4.20	4.23

Table 24: Pearson correlations, Two-tailed significance ** to .010 level

N=306	MAS	Assertiveness-Practices
TMT	-.173**	-.165**

The results in Table 24 show a strong correlation between TMT and Hofstede's MAS index as well as House et al.'s Assertiveness-Practices index. H81 is confirmed for MAS and Assertiveness-Practices.

Research question RQ 8.1 is thus answered in the affirmative.

We also analyze the values of the categorized latent factor of TChS for correlation with the Hofstede's UAI and the HFI-PF value. The compared values are in Table 25. Results of the correlation analysis are in Table 26.

Table 25: Hofstede and HFI parameters for analysis against TChS

Latent factor or Cultural index	Finland	USA	Brazil	Israel
TChS	2.606	2.567	2.725	2.974
UAI	59	46	76	81
HFI-PF	9.21	8.66	7.1	7.26

Table 26: Spearman (monotonic) correlations

N=306	UAI	HFI-PF
TChS	.131*	-.088
Sig.	.022	.123

Based on the results in Table 26, we may infer that respondents from cultures of higher UAI will be less likely to adjust their device security settings (TChS). We had expected the inverse to be true. One way that this may be explained is as follows: when users change default settings, it may create a situation of uncertainty if the users are not sure about the ramifications of the adjustments. Therefore, to avoid such uncertainty, they will not endeavour to change the settings. Contrary to our expectations, no significant correlation was found between TChS and HFI-PF. H83 is confirmed for UAI and rejected for HFI-PF.

We answer RQ 8.3 with our finding that the tendency of users to adjust their devices' security and privacy settings (TChS) is inverse to their cultures' UAI value.

Future research can further investigate the influence of nationality and cultural aspects in the presented research models. Hofstede, House et al., and HFI parameters can be used for the investigations.

6.8 New terminology

A literature review and assessment of psychological and physical person-centered space concepts has found that current terminology has deficiencies. The current terminology is insufficient to express personal space concepts that have evolved with the development of powerful new technologies. The technologies are highly connected and contain user-created content with low BoPs for distribution. The content can include highly personal content, personally identifiable information and controversial expressionism.

New lexical preterms are introduced to address this terminology gap. The terms, defined in sections 5.1.3 - 5.1.5 are:

- adversarial surveillance
- adversarial detective
- Barrier of Practicality (BoP)
- Personal Technology Space (PTS)

In addition, two more terms are proposed that should be developed during additional research. These terms, defined in section 5.1.6 are:

- cyberprivacy
- E-stop

6.9 PV - potential physical weaponization of smartphones

Research question 4.1 is not a simple one to answer definitively as the article research is limited to information that is readily available online, and the author not an expert in traumata or explosives. Nonetheless, news reports of injurious incidents reveal the dangers to users that can result from explosions or fires from smartphone batteries. The technological chemistry and physics of smartphone batteries and the recent development of a physical self-destruct function for smartphones could potentially be abused to realize threats of technologically coordinated attacks against smartphone users. Extrapolating from reported incidents and prior research, the physiological dangers of fire, explosion, heating, and loss of device functionality can range from distress to fatality. The specific impacts would depend on the attack manifestation on the user's device.

Research question 4 is answered in the above paragraph. There may be certain potential dangers from modern cellphones and smartphones that are dependent on the technologies in the devices. Third-party implementation implies that the potential attacks are not carried out by an assumed trusted partner in the device purchase or usage scenarios. In the hypothetical scenarios, there could also be potential attackers that are not third parties.

The author assumes that most users have not considered the threats because the threat mechanism may be rather unconventional. Nevertheless, if such hypothetical threats were to be carried out and subsequently publicized, they may have grave effects on users' motivation to use smartphones. The effects may also apply to their motivation to use any mobile or Internet-connected lithium battery-powered device, whether for self-expression or for any other purpose.

6.10 Patents PVI and PVII

RQ6 is answered in the affirmative. One way to help prevent the risks from unauthorized access to files is to load and offload files from the device depending on the expected usage context. This can be achieved by tagging the files or data items according to the usage scenarios for which they are appropriate or needed. Then, the user can load only those files that are necessary (based on their tags) from a secondary storage device. The user can also offload files, based on their tags, that are not necessary or appropriate for their current purpose. As a result, fewer files are stored on the user's device at any one time. This storage profiling reduces the overall risks from a hack or data breach of the device. Thus the user may feel more at ease while using their device for online expression or other tasks. Storage profiling also reduces the risk of accidental or inappropriate file exposure or distribution.

RQ7 is also answered in the affirmative. By combining a pseudo-caching method with the concept in PVI, a configuration can be implemented whereby the offloaded (i.e., currently unneeded) files are stored on machines or devices (e.g., personal server, third-party owned cloud server, etc.) that have more robust security measures than the user's immediately accessible device. The immediately accessible device may be a smartphone or laptop that the user is utilizing with a relatively higher level of activity. The activity can include actions that use the files that have been uploaded to his device that are necessary for the current usage context. The files are ones that the files' owner expects may be needed for the scenario, whether for configuration of other software, editing, sharing, or any other purpose where storage on the immediately accessible device enables the most efficacious method for fulfilling the current need. By having only those files necessary for the current purpose on his or her device, and currently unneeded files on a more secure storage platform, the user can reduce the overall risk exposure for the totality of his or her files. Because of the reduced risk, the user may feel more confident about freely using his or her device for expression and other purposes while connected to the Internet.

LIMITATIONS

This study does not examine the effect of time management on the perspective of the person who is waiting. Such time management could include the users' own management of their time while they wait for a security software update. Another example would be the management of the waiting time by a software vendor. The vendor's software could display some content on the user's display during an update (Hanyang et al., 2015). This study also does not account for distortions in the response data caused by time-in-retrospect or "novelty of time" effects. However, the effects of the distortions are believed to be insignificant. This is because users' attitudes and behaviors tend to be guided by their perceptions and not by objective reality.

The indicators for the TMT construct have limitations. Ideally, the respondents to the TMT questions would have had first-hand experience in, at a minimum, checking the settings of their devices. Some users may not have ever checked the security and privacy settings of any of their devices. For these respondents, the validity of the TMT indicator data may be problematic. Such users may have responded according to an attitude that they imagined they would have in case they were to check the settings. Alternatively, such users may not have checked settings due to an unfounded prejudicial attitude that such a task is not worthy of one's time, and thus tended to agree with TMT (such a response would accurately convey the perspective, but would not necessarily be helpful if or when the research results are applied). Such users may have also responded by selecting the most neutral Likert option, "neither agree nor disagree." The response decisions and bases for them for this group of users are not known. The quantity of such respondents is not known, though based on mean responses to the TChS indicators it is estimated to be no more than 14% of the sample.

We have assumed that the "intratemporal preferences" of our survey respondents are time-consistent. Our study does not differentiate the respondents according to their time-preference-dependent behavior choices (e.g., as in O'Donaghue and Rabin, 2000). Future research could categorize survey respondents according to the O'Donaghue and Rabin behavior framework to gain insight into the online expression reluctance and the privacy and security settings behaviors of Internet users.

This study did not take into account any of the available free and open-source personal cybersecurity technologies and tools. Tor browser, ClamAV, and free VPN services are examples of such products. Some survey respondents may have given negative responses to the LoM questions because they believe they can achieve adequate personal cybersecurity without spending money.

We have suggested that the survey data from our sample can be inferred to a target population of Internet users of any age who live in western-style democratic societies. However, there is coverage error due to the relatively small sample size.

During statistical analyses of the ordinal Likert response data, we have made an assumption of equal intervals for most calculations (Spearman correlation computations being an exception). Our results may vary to some degree if there are differences in perceived interval significances by respondents, between individual respondents, or by respondent groups.

There may be some common method bias in the responses. Despite attempting to mitigate implicit theory bias by forbidding the review of earlier than the displayed questions and answers, questions of predicted constructs were often grouped together on the visible page of the survey. The user may have read all of the visible questions before answering them, thus raising the possibility of implicit theory bias.

The survey was administered in English. This could be a limitation because English is not the native language of most of the respondents. However, such respondents were mainly students of college or university level or had already completed their higher education. A readability analysis of the scale questions showed a readability level that ranged from 9th to 12th grade. Many respondents were not native English speakers, so some task factors bias or ability factor bias may be present. These biases may apply for respondents who, for example, are not native English speakers and who study a field in which English is not prevalent in the literature.

With regard to the income variable moderation on the TMT construct, we have assumed that the variable is mainly representative of annual income earned through labor. We have not accounted for other sources of income, such as those from investments or gambling. Income from investments or other passive sources does not necessarily require reciprocal time expenditures from users. Gambling income may vary widely with a user's time involvement, as may passive income. Moreover, unlike the time used for the labor income and passive income scenarios, the time spent on gambling may easily result in a very small income, loss of income that was procured from other sources, or debt.

Some Hofstede and House et al. indices were used in this dissertation (sections 5.4 and 6.7). Global migration, intranational demographic changes, and cultural evolutions have occurred since the development of the indices. These may have adversely affected the current validity or values of the indices.

In section 5.3, we do not address secondary dangers that result from users focusing their attention on their smartphones, e.g., while walking or driving. Nor do we address the dangers that result from various frauds from hacked smartphones, such as privacy threats, information security threats, financial loss, or identity theft. We also do not address harms that may directly result from (appealing) smartphone functionality (designed into the device) that may cause detriments to health or lifestyle. The popular media routinely deals with most of these issues in the context of privacy and information security risks or of health effects. For example, articles claiming to deal with "dangers" or "physical hazards" of the smartphone do not usually present issues inherent in the technologies in the devices. Instead, the issues relate to and result from their usage (Shmerling, 2020; UCI, 2019). Injuries resulting from repetitious movements such as "thumb arthritis", weight gain, neck issues, and concerns over normal radiofrequency (RF) emissions from the device are also discussed on some websites, such as Catron (2018) and Davis (2018). We also do not address informational weaponization, such as an attack on the user with software, messaging, or signaling designed to manipulate the user. Such attacks may be e.g., media files, software, or signaling that produces overt or subliminal messaging, suggestive advertising or search results, fake news, and so on. We do not go into technical or technological detail.

Moreover, section 5.3 does not address dangers or threats resulting from inferior quality or faulty devices, whether or not such devices are counterfeit. We do not address smartphone abuses such as the rigging of a smartphone to trigger an explosion (e.g., a separate roadside bomb to which the phone has been connected). Such activity has been perpetrated in, among other places, zones of war or conflict and in civilian populations by terrorists (Officer, 2006).

Chapter 5.3 also does not address threats from accidental or inadvertent causes, such as mistaken inputs and commands to the UI, software bugs, or incidental radio interference. As the article title implies, this article does not address threats resulting from the abuse of the smartphone by its primary user. We also do not address the usage of the smartphone as a handheld blunt instrument or projectile.

In section 5.1.2, we do not consider or address certain detective specialties, such as criminal detective, insurance claim investigator, due diligence investigator, and so on. My intent is to utilize the fundamental definition and concept of the work that is generally understood to be common to all detectives.

DISCUSSION

For behaviors and attitudes toward personal cybersecurity spending (LoM) and attitudes toward making controversial expressions online (RtoEx), the results showed a significant correlation. This confirms H11. The result was also confirmed in the supplemental findings. Some users who are reluctant to freely express controversial viewpoints online not only deprive themselves of making the online expressions; they also divert some of their purchasing power toward personal cybersecurity. Whether RtoEx has a causal role in the spending diversion has not been established.

With regard to the correlation between LoM and RtoExnonC or RtoExC, the strongest correlation was between LoM and RtoExC. This may be expected because the respondent who is concerned about safety or consequences can have more motivation to protect their device than a respondent who is reluctant to express themselves for reasons not related to safety or consequences. When the correlation between LoM and RtoExnonC is examined, a correlation is seen there as well, though not as significant as between LoM and RtoExC. Internet users who are not as concerned about safety issues or consequences of freely expressing controversial topics online do still have concerns about personal cybersecurity for other reasons. These users have a favorable attitude toward purchasing, or have purchased, cybersecurity products and services to a lesser extent than users who are concerned about consequences or safety issues of controversial online expression.

Age was not found to be correlated with LoM in PI, but in the analysis with the expanded data set, a correlation was found. Older users have a greater proclivity to purchase personal cybersecurity products and services. This difference in findings may be explained by the makeup of respondents in the expanded data set. Many of the respondents in the expanded set are MTurk workers. MTurk workers are younger and more educated than the average working adult but have lower incomes (Pew Research Center, 2016). Thus more of the MTurk respondents of any age, having more education and being conscientious about their income, may be more knowledgable about free cybersecurity and privacy tools that are available. This can reduce the need or motivation to buy such tools.

In PII and PIV, one research goal was to determine the correlations between the factors as well as the correlations between the factors TChS and TMT and the demographic factors. The factor correlations between TChS, RtoEx, and TMT were determined, as were the correlations between the antecedents (in PIV) and TChS. We found that RtoEx and TMT are positively correlated, which is consistent with the result in PII. Linear regression was also performed on the privacy concern factor TChS and the TMT outcome factor against the RtoEx outcome. The analysis showed that TChS does not moderate TMT against RtoEx.

Regression was also performed on the antecedents against H53 (TChs -> TMT). We noted an effect from income. TChS, combined with income, predicted some variance in TMT.

In PII, there was a correlation of RtoEx with age. The result was confirmed in the supplemental analysis. Older users are more reluctant to make controversial expressions online (see footnote 3). This result seems inconsistent with Regan, Fitzgerald, and Balint's (2013) findings that older users tend to be less concerned about anonymity and privacy. In the analysis for PII (not presented in the paper), age was correlated with TMT – older users tend to believe that adjusting security and privacy settings take excessive time. However, no such correlation was determined in the supplemental findings. The expanded data set contained many responses from MTurk workers, who use their computers as working tools for income, and tend to have higher educations than average working adults. As a result, it may be easier for them to learn and to adjust their device settings. In addition, because their computers or devices are tools for income (by virtue of their using MTurk), they have a financial interest in securing their device. Thus, for them, the time needed to adjust settings for security and privacy is not seen as wasteful or excessive.

Age was found to moderate TMT against RtoEx. In PII, it was found that older users are more reluctant to express themselves online, as are those who consider the time that they use for device security and privacy to be excessive.

Researchers (Smith et al., 2011; Bandyopadhyay, 2011) have proposed variations of the APCO model to improve privacy research. Smith et al. (2011) identified gaps in the research based on their review of existing privacy research and its common modeling. Since then, some research has been performed that addresses some of the gaps (Benamati et al., 2017; Zhang et al., 2013; Sun et al., 2019). Our work contributes to the understanding of privacy research by showing relationships between the antecedents of income, ICT expertise, and gender; and TChS, TMT calculus, and RtoEx outcome. The privacy concern in our application of the model is represented by the latent construct of "thinking about and possibly adjusting security and privacy settings," TChS. We found that income antecedent has a moderating effect on the TChS -TMT correlation. Upon TChS, those users with higher incomes are more likely to experience TMT. Despite our expectations, no such moderating effect was found from ICT expertise. ICT expertise was positively correlated with TChS but did not moderate the relationship between TChS and TMT (H53). We observed that income and gender moderates H51. Women and those with higher incomes are more likely to be reluctant to express themselves online if their device privacy and security settings require excessive time to address. H57b and H57c are confirmed. ICT expertise did not moderate H51, so H57a is rejected.

In PIII, six latent factors were proposed and defined: RtoEx, RtoExC, and RtoExnonC, which correspond to a reluctance to self-express online; TMT, which corresponds to a perception that handling the security and privacy aspects of one's device requires an excessive amount of one's time; TChS, which corresponds to time spent considering device cybersecurity and privacy settings; and LoM, which corresponds to personal cybersecurity spending. These factors were established by analysis in PI and PII. In PIII, TChS and LoM were derived using a factor analysis of responses to some indicator items.

TChS and LoM were found to be significantly correlated in a study of two latent variables, confirming hypothesis H31. There was no significant correlation between the two factors and the three most common nationalities of survey respondents. This result may be due to the relatively small number of non-Finnish respondents in the data set.

Age and TChS were found to be significant predictors of LoM in a regression study. As a result, the age moderation in Hypothesis H32 is correct. Older people who are concerned about the privacy and security settings on their devices are more likely to spend money on personal security or are more inclined to do so (see footnote 5).

A newer expanded data set of n=265 was used for re-analysis of data in articles PI, PII, and PIII. The results from the original and newer data sets were compared. For comparison, the data sets are assumed to be independent. This can be considered a boundary condition for the Z significance test. The Z-score tests showed that the correlation results from the two data sets did not significantly differ. Most of the re-analyzed regression results were also consistent. In PIII, the original regression analysis showed age to be a moderator of the TChS->LoM relation. With the larger data set, age and ICT expertise both moderated the relation (see sections 5.3.3 and 5.3.4).

An explanation for this difference in PIII may be that the newer data set contained responses that were obtained using MTurk. Many MTurk respondents may use their devices and the Internet in earnest as tools to earn income. They do this in addition to (or instead of) using them for recreation, research or play. The additional respondents may have a higher level of ICT expertise (as they have dedicated their efforts to use their devices and the Internet to earn income with MTurk). MTurk workers have lower incomes than average working adults, and possibly higher ICT expertise as well, due to their MTurk activities. A lower income would cause a reduced ability to make purchases. Thus, their responses may have resulted in the additional ICT expertise variable to the original regression on LoM of TChS and age.

Our findings are in agreement with Tsai et al.'s (2016) findings in that income was not correlated with TChS. TChS is our defined manifestation of "privacy concern." We did find that ICT expertise was weakly correlated with TChS. Users with more ICT expertise are more likely to TChS. This may be unsurprising in light of the work by Chen et al. (2010), who found that users' preferences for the attributes of shopping websites vary with their levels of computer expertise. Gender was also significantly correlated with TChS, thus confirming H54c. Male users are more likely to contemplate and subsequently adjust their device security and privacy settings. This finding has congruency with the statistical data reported by the European Commission (2019) and with the research of the Girl Scout Research Institute (2019). They found that females are underrepresented in ICT studies (European Commission 2019) and that girls are less confident in their ICT skills than boys (Girl Scout Research Institute 2019). On the other hand, we might have expected that female respondents would be more willing to change settings if only they had the necessary skills and the confidence in their skills.

This expectation could be inferred based on findings from Regan et al. (2013) and Beaussart and Kaufman (2013).

We found that ICT expertise is weakly correlated with TChS. Sheehan (2002), on the other hand, did not find a significant relationship between the intensity of computer usage and privacy concerns. One explanation could be the increase in cyber security awareness in consumers since the time of Sheehan's study.

Gender, in combination with income, was found to moderate H51, confirming H57b and H57c. The H51 moderation effects of gender and income may be explained by the findings of Chatzitheochari and Arber (2012), Burchardt (2010), and Beaussart and Kaufman (2013). Income and gender also moderated H2, confirming H6b and H6c. This is consistent with findings from Nugent et al. (2016), who reported that individuals (across major religions) with higher incomes tend to have more interest in engaging in political activity and a greater belief in the importance of free speech. The European Commission (2019) and Girl Scout Research Institute (2019) have reported on the ICT education and confidence disparity between genders. Regan et al. (2013) and Beaussart and Kaufman (2013) have reported on the privacy concerns and sensitive disclosure tendencies of females, respectively. Lower ability and confidence to address ICT device settings and a greater concern about privacy are consistent with our findings.

Zhang et al. (2013) applied the APCO model using CFIP (concern for information privacy) as a proxy for privacy concern. They found that income is not correlated with CFIP in a mobile-commerce context. Our result (income is not found to correlate with TChS) may be consistent with Zhang's finding that income is not correlated with CFIP. We have asserted that TChS corresponds to users' privacy concerns for the purpose of applying the APCO model.

In other previous research applying the APCO model (Sun et al. 2019), mutual online expressions with other social media users over a popular topic (i.e., "hot topic interactivity") has been modeled as an antecedent - agnostic of the controversy of the topic. Sun et al. found that the number of times online shopping per month (this can be construed as "more time spent on the Internet") had a positive impact on information disclosure behavior (BID). In Sun et al.'s work, BID includes posting personal photos and personal income information. This subset of BID information is sensitive but not necessarily controversial. Insofar as RtoEx has a negative correspondence with Sun's BID, and monthly frequency of online shopping can correspond with ICT expertise (our survey's questions for the ICT expertise construct included a question on the number of years using ICTs and on how many hours a day one uses the Internet), our results differed from Sun et al.'s.

Our earlier work showed a correlation of age to RtoEx (Rauhala et al. 2019b). Sun et al. (2019), on the other hand, found no significant relationship between age and information disclosure. We found no significant correlation of Income and ICT expertise to RtoEx. We have found age to be correlated with TMT but not with TChS (Rauhala et al. 2019a). This can be considered agreement with Benamati et al. (2017), who found only a marginal correlation between age and CFIP (concern about information privacy). Our prior work found that age also moderates the relationship between TMT and RtoEx (Rauhala et al. 2019a). In this study that uses an expanded data set, income was also found to be correlated with TMT, and ICT expertise was found to be weakly correlated with TChS. We have considered the temporal time-in-retrospect and "novelty of time" effects of user perceptions, but such effects are believed to be insignificant to our work. We have shown correlations and effects of the demographic variables income, ICT expertise, and gender on an applied APCO model. It should be noted that Benamati et al. (2017) included both limitations of making posts and of making adjustments to Facebook settings into a single construct. In the present paper, we have differentiated and separated out adjustment settings into our TChS construct. The scale for posting limitations has been encompassed by the RtoEx construct.

The excessive time that was spent by one user may be more or less than the excessive time reported by another user. Moreover, with subjective survey questions such as hours, there may even be cases where one respondent's acceptable amount of time may be more than an amount that is considered "too much" by another respondent. However, what is most crucial for TChS is that an amount of time was indeed used for thinking and changing settings, and for TMT that the time spent on security and privacy aspects is judged to be excessive. We assume that a reported excessive (or "too much") time in all cases will be more than an amount of time that the user has deemed as acceptable.

Our results suggest a causal relationship between TMT and RtoEx. Using Antonakis et al.'s (2010) criteria (temporality, correlation, and exclusion of other causes), we assert a temporal relationship by the order of our survey questions and the predecession of users' initial device usage by configuration actions (Rauhala et al. 2019a). We should also expect that users should be reluctant to make controversial expressions without cybersecurity protections or privacy protections (e.g., anonymity). Liu et al. (2016) found that users prefer that certain trust conditions should be fulfilled prior to self-disclosure of sensitive personal information. All other possible causes of RtoEx cannot be excluded, but an attitude of TMT implies that the security and privacy settings cannot be accomplished because of insufficient time. Therefore, it is reasonable that RtoEx should follow. TChS was not correlated with RtoEx.

Though there was no correlation between income and TChS, it did moderate the relationship between TChS and TMT (H53). A positive correlation was found between TMT and RtoEx (H51): users who experience TMT are also more likely to experience RtoEx.

With respect to nationalities, we had expected RtoEx to vary by nationality. This expectation was based on differences between cultural index values for parameters of two widely used and well-known cultural indices. Differences between HFI index values for the four analyzed nations had also implied that RtoEx should vary accordingly. Surprisingly, RtoEx did not significantly differ between the respondents of the nationalities. This would suggest that the Internet is indeed a 'great equalizer.' It seems that the Internet is a truly global expression platform for Internet users - not only 'global' in the sense of worldwide availability - but also in the culturally- and nationality-agnostic sense. Users do not necessarily perceive inhibitions to their free expressionism that have been associated with their own culture or nationality. Such inhibitions were implied by cultural index values studied by Hofstede and House et al. many years ago. The annually updated national HFI values are also disjointed from our RtoEx results.

Nationality-based TMT values were correlated with Hofstede's MAS and House et al.'s Assertiveness Practices indices in an expected way. Respondents from nationalities of higher MAS and Assertiveness Practices values felt relatively more TMT.

TChS values were not correlated with UAI in the way that we had expected. Instead of users' actions to TChS in order to avoid cybersecurity and cyberprivacy risks during device usage, users of higher UAI showed reduced TChS. It is hypothesized that this indicates that such users may want to avoid risking "messing up" their device by making adjustments for which the effects are not understood. No association between TChS and HFI-PF was found. It appears UAI is associated with TChS. The political conditions (as defined by HFI-PF) of the nation corresponding to the users' nationality did not have bearing on TChS. Nationality and culture appear to influence TChS through their UAI (uncertainty avoidance).

There are some steps that governments and industry could take to improve Internet users' perceptions of online safety. Nation-states that respect free online expression as a fundamental right for their citizens may choose to create and implement cybersecurity strategies and regulations that improve their citizens' perceptions of the level of online safety. In this way, their citizens may perceive a reduced need to spend time addressing their device settings or their cybersecurity software, and thus an improved opportunity to express themselves online or to perform other preferred tasks. The personal cybersecurity products and services industry could design device security and privacy safeguards to be easier to understand and adjust, and to automate more functions to the background of device or software UIs. Thus, device security and privacy aspects would (ideally) be less time-consuming for consumers to address. However, there may not be clear economic motivations for the cybersecurity industry to modify its consumer products and services in such a manner.

The perceived need for extra personal cybersecurity solutions may be reduced if default security and privacy settings were improved. This would allow users to devote more time and money to other tasks and transactions. Users should be able to trust that their electronics have adequate privacy and security protection right out of the box. Users' trust in the protection of their privacy and security is positively associated with their online purchase intentions, according to previous research (Chen & Barnes, 2007).

Governments should guarantee the framework and conditions for free expression by their citizens with online regulatory safeguards that reflect traditional safeguards in traditional communications media, in order to encourage open and robust political debate. This could allow Internet users to feel more free to spend their money and time on personal interests rather than worrying about their online privacy and security. Users may spend more time expressing themselves and researching offerings if they have less reason to be concerned about being victims of cybercrime.

However, national legislative and regulatory conditions that promote free expression are not necessarily enough. Among the contributions of this research is a novel way to assess a reluctance to express oneself online; the latent variable RtoEx. Previously research has mainly evaluated a willingness to disclose information, or a willingness to express oneself, not a reluctance. The Human Freedom Index (HFI) has a shortcoming in the assessment that is used for indexing.

The criteria used for assessment do not include any measurement of the beliefs or opinions of the residents of the evaluated nations with respect to their nation's level of freedom. The laws or regulations of a nation, especially with respect to freedom of speech, may "look good on paper," but authorities may be selective with the laws that they enforce. Laws or policies do not necessarily result in the marketplace of ideas or open political dialog that they are supposed to enable. The measurement of expression reluctance within citizens of a nation can help to increase the accuracy of assessments of human freedom in the nation. Such a measurement may arguably be even more important than the nation's official laws and policies. Legislated freedom of speech has little meaning if, for whatever reason, the people are afraid to exercise that freedom.

Nissenbaum (2010) compiled and summarized many detrimental impacts that a lack of privacy may cause to individuals and society. In the interest of addressing such impacts, national indices that assess the levels of privacy intrusions or de facto surveillance by governments, akin to the HFI, should be developed.

Recently so-called "cancel culture" has introduced a new set of potential consequences to anyone who wishes to express a controversial opinion. If an individual, group, or website expresses content that is deemed unacceptable, consequences may be imposed against them by other users or by 'big tech' companies such as Google (EU Times 2020, Ryan 2018) and Twitter (Gibson 2020). Such consequences have been known to include account banning, so-called shadow-banning, and distortion of search results to reduce the Internet visibility of the purportedly offending party. Future research can investigate factors relating to the cancel culture phenomenon and how they interrelate.

Future research on this topic can address differences between additional demographic groupings in their attitudes and behaviors as defined by the presented and other related latent constructs. Such groupings could include those by political leaning, occupation, and education level. The attitudes and behaviors of Internet users who have been victims of malware, hacking or other forms of cybercrime should also be investigated. Some research on this has already been done by Xin et al. (2021).

In the interest of promoting the evolution of the Internet as a global democratizing force, empirical research should determine those demographic groupings that are most concerned, most reluctant to express, and least savvy with information and communication technologies. Mitigations for the online privacy and security concerns of the most affected groupings could then be investigated.

Future research can assess the measurable amounts of time that various security software updates or security updates take to complete. This information can be applicable when performing research about users who prefer to update their software manually. Users who manually update can be distinct from users who choose to configure their security software to update automatically, i.e., as background processes.

Internet users' hesitation to freely communicate their views and opinions online could be explained using applied social exchange theory. Further research might look into the elements that prevent individuals from expressing controversial ideas online, as well as the conditions that encourage them to do so. This research can also be extended by investigating whether users’ reluctance to express themselves online is variable with specific topics.

Certain demographic variables can be investigated in relation to personal cybersecurity spending and any aversion to expressing oneself online. Users could also be surveyed to see how concerned they are about being targeted by cybercriminals as a result of their online actions. In the future, analysis for geographical region clustering and other clusterings could be performed based on available survey data. Future work in this research is also expected to include applied structural equation modeling (SEM).

A smartphone is usually associated with a single user. Technology to cause the self-destruction of a smartphone has been developed and demonstrated. Smartphones contain batteries with significant potential energy that could be triggered to ignite or explode. The fire or explosion can damage the smartphone’s functionality or injure (or possibly kill) the user. The potential exists for the technology to be weaponized to attack a smartphone user. Even with no fire or explosion, the loss of functionality of the smartphone can cause significant distress to the user. The range of potential methods, triggers, and culprits that could cause such attacks should be proactively researched. These issues could be studied and discussed in, for example, think tanks, working groups, or research projects.

The implementation of the patents described in PVI and PVII, or similar mechanisms, could be part of a strategy to help Internet users feel less reluctant to use the Internet in certain situations. The reluctance to express online or the expressing of sensitive information has been shown to be restricted by concerns about consequences or to have certain pre-requisites. The individual obstacles for disclosing sensitive information or expressing controversial viewpoints could be partly mitigated with devices and software that are more secure and whose privacy settings are easily understood. The perceived reduced risk that can be achieved with data security mechanisms could lower the threshold for users to more freely avail themselves of the communications and transaction opportunities on the Internet.

We proposed some new preterms for the benefit of the research fields of cybersecurity and cyberprivacy. As technology has advanced at a rapid pace, so has the adaptation of new technologies for many purposes and for many facets of society. Technological advancements are often pursued for humanity's benefit and are usually seen as 'good.' The computer age and Internet age have seen a fervor and eagerness by individuals and organizations to adopt new technologies. We believe that the fervor and eagerness of technology adaptation should be tempered with sober assessments of its implications to human well-being. The new preterms can help the discussions and understandings of the implications. The discussions and assessments should address implications to the intended usage context and to larger society.

Future studies should investigate the effects of the studied factors on other e-commerce besides the purchasing of cybersecurity and cyberprivacy solutions.

SUMMARY

The research that forms this dissertation is intended to try to find the costs, to individuals and to society, of Internet users' cyberprivacy and cybersecurity concerns. It aims to help define those costs in terms of losses of time, money, and freedom.

The costs of time were measured by first determining two time-related latent constructs from analyzed survey data. The constructs are TChS (Think about and change settings) and TMT (Too much time). The relationships of the two constructs to other pertinent constructs and variables were then analyzed. The cost is ultimately determined by the intereffects of the two constructs with the other two higher-level categories of costs in this research, namely "loss of money" and "loss of freedom." In PII, the relationship between time and loss of freedom was found. The loss of freedom was found to be related to a perception that addressing the privacy and security settings on one's device requires excessive time.

The cost in money was, similar to the method for time, measured by first determining a construct that describes a proclivity toward buying software and services that protect personal cybersecurity and cyberprivacy. The construct is derived from survey data and is denoted LoM for "loss of money." The relationship between this construct and users' concerns was analyzed by seeking the relationships between it and the expression reluctance (or "loss of freedom") constructs. There is a relationship between LoM and users' reluctance to express themselves on the Internet. This relationship was found in PI.

The cost to users in terms of "loss of freedom" was again assessed by first finding the appropriate construct from survey data. The construct is called RtoEx, for "reluctance to express." This is arguably the most important for the research purpose. The construct can be further (perhaps tenuously) subdivided into two, namely RtoExC and RtoExnonC. These subdivided constructs represent the level of reluctance when the survey respondent is reminded of potential consequences for controversial expression, or not, respectively. The top-level construct of RtoEx was mainly used in the research. The relationship between reluctance to express (RtoEx) and loss of money (LoM) was performed in PI. The relationship between reluctance to express (RtoEx) and contemplate and adjust settings (TChS) and too much time (TMT) was investigated in PII, and an association between RtoEx and TMT was found.

In PIII, the relationships between too much time (TMT), contemplate and adjust settings (TChS), and loss of money (LoM) were studied. A positive association between TChS and LoM was found.

Thus the interrelationships between the constructs can convey the situation in a more realistic way than attempts at simple quantitative presentations of the costs. During this research and its analyses, it became evident that the determination and quantification of such costs as they directly result from users' cyberprivacy and cybersecurity concerns is not straightforward.

In article PIV, the antecedents-privacy concerns-outcomes (APCO) model was applied to analysis results that were obtained from a newer data set. The

antecedents were evaluated for their effects using the model. The privacy calculus, defined as too much time (TMT), was found to be moderated by gender for the expression reluctance (RtoEx) outcome. Thinking about and changing settings (TChS) by itself was not correlated with expression reluctance (RtoEx), but a regression showed that gender and income moderate it to RtoEx. The privacy concern, defined as addressing device settings TChS, was correlated with a perception that the activity requires too much of one's time, TMT. Moreover, income moderated the correlation.

Demographically, males were found to be more likely to think about and change their device security settings (TChS) than females. Females were more likely to feel reluctance to express their controversial viewpoints (RtoEx) than males. No correlation was found between gender and too much time (TMT). Income was found to correlate with TMT. A weak correlation was found between ICT expertise and the contemplation and adjustment of settings (TChS).

Table 21 (PIV) shows the results of this research in the context of current established knowledge. The results are based on the n=265 dataset that was used in PIV, and are described in section 6.6.

The comparisons of the factors based on nationality suggest that the usage of the Internet for controversial expressionism is not influenced by users' national cultures. However, users' perceptions or feelings about the amount of time and effort required to perform certain tasks with the technologies (e.g., TMT) appear to be influenced by users' cultures. Our findings also suggest that users' cultures influence their proclivity to perform tasks that are ancillary to Internet usage. An example of such a task is the adjustment of device or software settings for personal preference (TChS).

Modern technology has brought benefits and risks. Users may avoid technology-based risks by avoiding using the technology. The risks may result from many types of players that utilize different means to harm or attack the users in a wide range of scenarios. The risks may come from the online expression of opinions that are taken as offensive (and thus provoke some form of retaliation). The risks may also affect everyone indirectly by way of reduced willingness by users to participate in online social and political dialogs. Smartphones could also be physically weaponized, thus enabling a new means for bad actors to target a single user.

Users may be more willing to use their devices if their data are less vulnerable to breaches and damage. If users' data can be distributed between storage platforms such that only the minimum required data is stored on their most vulnerable device, then the remainder of their data is safer. As a result, the risks of data breaches and privacy invasion are reduced, and, from this viewpoint, the most vulnerable device is safer to use.

Human vocabularies have evolved throughout history. New words and terms appear, and others become obsolete. New preterms become necessary in the social dialog to help discuss and understand novel developments in technology and their resulting wider implications. We have proposed the new preterms "personal technology space" (PTS), "barrier of practicality" (BoP), "adversarial surveillance," "adversarial detective," "cyberprivacy," and "E-stop." We hope that they could benefit the discussion and understanding of the implications of any new or pervasive technology.

Free online expression has natural intrinsic value. Free online expression is also a way to circumvent traditional communication restrictions and censorship that may be imposed by authoritarian regimes on traditional publishing media. It is hoped that this work will help stakeholders find ways to mitigate the costs of time, money, and freedom to Internet users that result from their security and privacy concerns. When such costs are mitigated, the full societal benefits of the global connected Internet can be better and more fully realized in practice. The improved realization can be brought about if fewer users are reluctant to express themselves in online discussions and debates. Such reluctance can be reduced if the users have their desired levels of privacy and device security.

SUMMARY IN FINNISH

Tämän väitöskirjan muodostavan tutkimuksen tarkoituksena on löytää Internetin käyttäjien tietoturva- ja kyberturvallisuusongelmien kustannukset yksilöille ja yhteiskunnalle. Sen tarkoituksena on auttaa määrittelemään nämä kustannukset ajan, rahan ja vapauden menetyksinä.

Ajan kustannukset mitattiin määrittämällä ensin kaksi aikasidonnaista piilevää rakennetta analysoiduista tutkimustiedoista. Rakenteet ovat TChS (Ajattele ja muuta asetuksia) ja TMT (Liian paljon aikaa). Kahden rakenteen suhteet muihin asiaankuuluviin rakenteisiin ja muuttujiin analysoitiin seuraavaksi. Kustannukset määräytyvät viime kädessä näiden kahden rakenteen yhteisvaikutuksesta tämän tutkimuksen kahden muun korkeamman tason rakenteen kanssa, nimittäin "rahan menetys" ja "(ilmaisun-)vapauden menetys". PII:ssä havaittiin ajan ja vapauden menetyksen välinen suhde. Vapauden menetyksen havaittiin liittyvän käsitykseen siitä, että laitteen yksityisyys- ja suojausasetusten käsittely vaatii liikaa aikaa.

Rahallinen kustannus mitattiin ajan kustannusta mittaavan menetelmän tapaan määrittämällä ensin rakenne, joka kuvaa taipumusta ostaa ohjelmistoja ja palveluita, jotka suojaavat henkilökohtaista kyberturvallisuutta ja yksityisyyttä. Rakenne on johdettu kyselytiedoista, ja sitä kutsutaan LoM:ksi "rahan menetys". Tämän rakenteen ja käyttäjien huolenaiheiden välistä suhdetta analysoitiin etsimällä sen ja "ilmaisunvapauden menetys" -rakenteiden välisiä suhteita. LoM:n ja käyttäjien haluttomuuden ilmaista itseään Internetissä -rakenteen välillä löydettiin suhde. Tämä suhde löytyi julkaisussa PI.

Käyttäjien "vapauden menetyksen" kustannuksia arvioitiin uudelleen etsimällä ensin soveltuva käsiterakenne tutkimustiedoista. Rakennetta kutsutaan RtoEx:iksi "haluttomuudesta ilmaista". Tämä on epäilemättä tärkein tutkimuksen kannalta. Rakenne voidaan jakaa edelleen (ehkä heikosti) kahteen osaan, nimittäin RtoExC ja RtoExnonC. Nämä jaetut rakenteet edustavat vastahakoisuuden tasoa, kun kyselyn vastaajaa joko muistutetaan mahdollisista seurauksista kiistanalaiselle ilmaisulle tai ei muistuteta. Tutkimuksessa käytettiin pääasiassa ilmaisuhaluttomuuden RtoEx:n ylimmän tason rakennetta. Ilmaisuhaluttomuuden RtoEx:n ja rahan menetyksen LoM:n välinen suhde toteutettiin julkaisussa PI. Ilmaisuhaluttomuuden RtoEx:n ja asetuksien ajattelun ja mahdollisen muutoksen TChS:n ja liian paljon ajan TMT:n välistä suhdetta tutkittiin PII:ssa jolloin havaittiin yhteys ilmaisuhaluttomuuden RtoEx:n ja liikaisen ajan TMT:n välillä.

PIII:ssa tutkittiin liikaisen ajan TMT:n, asetuksien ajattelun ja muutoksen TChS:n ja rahan menetyksen LoM:n välisiä suhteita. TChS:n ja LoM:n välillä havaittiin positiivinen yhteys.

Rakenteiden väliset suhteet voivat siten välittää tilanteen realistisemmin kuin yritykset yksinkertaisiin määrällisiin esityksiin kustannuksista. Tämän tutkimuksen ja sen analyysien aikana kävi ilmi, että sellaisten kustannusten määrittäminen ja kvantifiointi, jotka johtuvat suoraan käyttäjien tietoturvasta ja kyberturvallisuusongelmista, ei ole suoraviivaista.

Artikkelissa PIV aiemmasta kirjallisuudesta löytyvää APCO-mallia sovellettiin analyysituloksiin, jotka saatiin uudemmasta tietojoukosta. Edellisten vaikutukset arvioitiin mallin avulla. Yksityisyyslaskennan (”privacy calculus”), joka on mallissa määritelty TMT:ksi (liiaksi ajaksi), havaittiin olevan sukupuolen mukaan moderoitu RtoEx-tuloksen kannalta. Ajan kustannus (TChS) itsessään ei korreloinut ilmaisuhaluttomuuden RtoEx:n kanssa, mutta regressio osoitti, että sukupuoli ja tulot hillitsevät sen vaikutusta ilmaisuhaluttomuuteen (RtoEx). Huoli yksityisyyden suojasta, joka mallissa määritellään TChS:ksi, korreloi liikaisen ajan TMT:n kanssa. Lisäksi tulot hillitsivät korrelaatiota.

Demografisesti miehillä todettiin olevan todennäköisemmin taipumus ajatella ja muuttaa asetuksia (TChS) kuin naisilla. Naiset tunsivat todennäköisemmin haluttomuus ilmaista kiistanalaisia näkemyksiänsä (RtoEx) kuin miehet. Korrelaatiota ei havaittu sukupuolen ja liiallisen ajan käsityksen TMT:n välilla. Tulojen todettiin korreloivan liikaisen ajan TMT:n kanssa. ICT-osaamisen ja asetuksistaan ajattelun ja niiden muutosten (TChS:n) välillä havaittiin heikko korrelaatio.

Taulukko 21 (PIV) esittää tämän tutkimuksen tulokset tämänhetkisen vakiintuneen tutkimustiedon yhteydessä. Tulokset perustuvat 265 henkilön aineistoon, jota käytettiin PIV:ssä ja joka on kuvattu kohdassa 4.4.

Kansalaisuuteen perustuvien tekijöiden vertailut viittaavat siihen, että käyttäjien kansalliset kulttuurit eivät vaikuta Internetin käyttöön kiistanalaiseen ekspressionismiin. Käyttäjien kulttuurit vaikuttavat kuitenkin vaikuttavan käyttäjien käsityksiin tai tunteisiin tiettyjen tehtävien suorittamiseen tarvittavasta ajasta ja vaivasta (TMT). Tuloksemme viittaavat myös siihen, että käyttäjien kulttuurit vaikuttavat heidän taipumukseensa suorittaa tehtäviä, jotka liittyvät Internetin käyttöön. Esimerkki tällaisesta tehtävästä on laitteen tai ohjelmiston asetusten säätäminen henkilökohtaisten mieltymysten mukaan (TChS).

Nykyaikainen tekniikka on tuonut hyötyjä ja riskejä. Käyttäjät voivat välttää tekniikkaan perustuvia riskejä välttämällä tekniikan käyttöä. Riskit voivat johtua monenlaisista toimijoista, jotka käyttävät erilaisia keinoja vahingoittaakseen tai hyökätäkseen käyttäjiin monenlaisissa tilanteissa. Riskit voivat aiheutua sellaisten mielipiteiden ilmaisemisesta verkossa, joita pidetään loukkaavina (ja jotka siten aiheuttavat jonkinlaisen kostotoimenpiteen). Riskit voivat myös vaikuttaa kaikkiin epäsuorasti, koska käyttäjät eivät halua osallistua sosiaalisiin ja poliittisiin online verkkovuoropuheluihin. Älypuhelimet voitaisiin myös aseistaa fyysisesti, jolloin huonot toimijat voisivat kohdistaa uuden keinon yhdelle käyttäjälle.

Käyttäjät voivat olla halukkaampia käyttämään laitteitaan, jos heidän tietonsa ovat vähemmän alttiita tietovuodoille ja vaurioille. Jos käyttäjien tiedot voidaan jakaa tallennusalustojen välillä siten, että vain vähimmäistiedot tallennetaan heidän haavoittuvimpaan laitteeseensa, loput heidän tiedoistaan ovat turvallisempia. Tämän seurauksena tietorikkomusten ja yksityisyyden loukkaamisen riskit pienenevät, ja tältä kannalta haavoittuvin laite on turvallisempi käyttää.

Ihmisten kielet ovat kehittyneet historian aikana. Uusia sanoja ja termejä ilmestyy ja toiset vanhenevat. Sosiaalisessa vuoropuhelussa tarvitaan uusia alustoja, joiden avulla voidaan keskustella ja ymmärtää tekniikan uutta kehitystä ja sen laajempaa vaikutusta. Olemme ehdottaneet uusia käsitteitä "henkilökohtainen teknologiatila" (PTS), "käytännöllisyyden este" (BoP), "vastustajavalvonta", "vastustaja etsivä", "kyberyksityisyys" ja "E-stop". Toivomme, että niistä olisi hyötyä keskustelussa ja ymmärryksessä minkä tahansa uuden tai yleisen tekniikan vaikutuksista.

Ilmaisunvapaus verkossa on luontainen arvo. Vapaa ilmaisu verkossa on myös keino kiertää perinteiset viestintärajoitukset ja sensuuri, jotka autoritaariset hallitukset voivat asettaa perinteisille julkaisuvälineille. Toivotaan, että tämä työ auttaa sidosryhmiä löytämään keinoja lieventää Internetin käyttäjille aiheutuvia ajan, rahan ja vapauden kustannuksia, jotka aiheutuvat heidän turvallisuus- ja yksityisyyskysymyksistään. Kun tällaisia kustannuksia pienennetään, maailmanlaajuisen Internetin kaikki yhteiskunnalliset hyödyt voidaan saavuttaa paremmin ja täydellisemmin myös käytännössä. Parempi toteutuminen voidaan saada aikaan, jos entistä harvempi käyttäjiä on haluton ilmaisemaan itseään verkkokeskusteluissa ja väittelyissä. Tällaista haluttomuutta voidaan vähentää, jos käyttäjillä on heidän haluamansa yksityisyyden ja laitteen suojauksen taso.

REFERENCES

Alqubaiti, Z., Li, L., & He, J. (2016). The Paradox of Social Media Security: Users' Perceptions versus Behaviors. *Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16*, 29–34. https://doi.org/10.1145/2978178.2978187

Ancona, D. G., Okhuysen, G. A., & Perlow, L. A. (2001). Taking Time to Integrate Temporal Research. *Academy of Management Review*, *26*(4), 512–529. https://doi.org/10.5465/amr.2001.5393887

Anonymous. (2010, January). KEEPING ONLINE CUSTOMERS. *Dealerscope*, *52*(1), 26. Accessed 22 January 2020

Ayaburi, E. W., Wairimu, J., & Andoh-Baidoo, F. K. (2019). Antecedents and Outcome of Deficient Self-Regulation in Unknown Wireless Networks Use Context: An Exploratory Study. *Information Systems Frontiers*, *21*(6), 1213–1229. https://doi.org/10.1007/s10796-019-09942-w

Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. *Journal of Business & Economics Research (JBER)*, *7*(3). https://doi.org/10.19030/jber.v7i3.2269

Baroni, D. (2015, July 3). New Zealand Government To Punish Online Trolls With Prison Time. *Reaxxion.Com*. http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time

Barrigar, J., Burkell, j, & Kerr, I. (2006). Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information. *Canadian Business Law Journal*, *44*, 54.

Belousova, A. K., Mozgovaya, N. N., Barsukova, O. V., Vyshkvyrkina, M. A., Kryschenko, E. P., Mochalova, Yu. A., Pavlova, T. V., & Tushnova, Yu. A. (2015). The Scope of Values and Limits of the Personal Psychological Space of Students-Emigrants. *Mediterranean Journal of Social Sciences*, *6*(4), 379–382. https://doi.org/10.5901/mjss.2015.v6n4s3p379

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents – Privacy Concerns – Outcomes model. *Journal of Information Science*, *43*(5), 583–600. https://doi.org/10.1177/0165551516653590

Bentham, J. (1995). *The Panopticon Writings*. Verso.

Booth, R. E. (2017). The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations. *Proceedings of the 23nd Americas Conference on Information Systems.*

Branigan, S. (2011, July 31). Revenge Hacking. *Trends in High Tech Security*. https://sbranigan.wordpress.com/2011/07/31/revenge-hacking/ Accessed 17 May 2019

Bukhanets, A. O. & Bayer, O. O. (2016). THE RELATION OF ADOLESCENTS' SOVEREIGNTY OF PSYCHOLOGICAL SPACE WITH COPING STRATEGIES AND INTRAPERSONAL CONFLICTS. *Vìsnik Dnìpropetrovs'kogo Unìversitetu: Serìâ Psihologìâ,*

22(9/1), .https://doi.org/10.15421/101605 (Translated from Ukrainian by Google translate, 2021.)

Business editors. (2002, July 31). New Study Says Poor Web Site Performance Can Cost Millions in Wasted Marketing Money; Study Cites High Level of Frustration & Abandonment for Popular Sites. *Business Wire*, 1.

Butler, R. (1995). Time in organizations: Its Experience, . Explanations and Effects. *Organization Studies*, *16*(6), 925–950. https://doi.org/10.1177/017084069501600601

Cassidy, P. (2017, November 3). Man petrol bombed homes in revenge for Facebook post. *STV News*. https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/ Accessed 22 January 2020

Chatzitheochari, S., & Arber, S. (2012). Class, gender and time poverty: A time-use analysis of British workers' free time resources: Class, gender and time poverty. *The British Journal of Sociology*, *63*(3), 451–471. https://doi.org/10.1111/j.1468-4446.2012.01419.x

Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research*, *63*(9–10), 1007–1014. https://doi.org/10.1016/j.jbusres.2009.01.023

CIGI & Ipsos. (2015). Share of global internet users who find online free speech and political expression important as of November 2014, by country. In *Statista*.

CIGI & Ipsos. (2016). Protective actions taken by internet users worldwide over the past year as of February 2015 [Graph]. In *Statista*. Retrieved 2016, from https://www.statista.com/statistics/463380/protection-of-devices-and-internet-privacy-worldwide/

Cooper, A. K. (2000, July 12). China: Government punishes Internet journalists. *Committee to Protect Journalists*. https://cpj.org/2000/07/china-government-punishes-internet-journalists.php Accessed 10 February 2018

Curtom, G. (2014, April 24). Students punished for expressing free speech on Twitter. *The Cougar*. http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/ Accessed 10 February 2018

Cwienk, J. (2019, December 19). India's Modi isn't alone in blocking internet amid protests. *DW.Com*. https://www.dw.com/en/indias-modi-isnt-alone-in-blocking-internet-amid-protests/a-51743937 Accessed 12 May 2021

Dascalescu, A. (2018, January 3). Doxxing Can Ruin Your life. Here's How (You Can Avoid It). *Heimdal Security*. https://heimdalsecurity.com/blog/doxxing/#doxxingswatting Accessed 17 May 2019

Dellaert, B. G. C., & Kahn, B. E. (1999). How tolerable is delay?: Consumers' evaluations of internet web sites after waiting. *Journal of Interactive Marketing*, *13*(1), 41–54. https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<41::AID-DIR4>3.0.CO;2-S

Deloitte. (November 1, 2015). Leading actions taken by consumers who had experienced a security breach in Great Britain (GB) as of January 2013 and

September 2015 [Graph]. In *Statista*. Retrieved September 25, 2021, from https://www.statista.com/statistics/497160/actions-taken-by-consumers-after-a-security-breach-in-great-britain-gb/

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Emarketer.com. (2014). Worldwide Ecommerce Sales to Increase Nearly 20% in 2014—EMarketer. *Emarketer.Com*. https://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039 Accessed 24 January 2019

Ericsson. (February 21, 2014). Behavioral effects of online security concerns according to daily internet users in February 2014 [Graph]. In *Statista*. Retrieved September 25, 2021, from https://www.statista.com/statistics/293872/online-security-concerns-effects-on-internet-usage/

EU Times. (2020, September 2). Google caught Censoring Search Results that criticize Black Lives Matter. *The European Union Times*. https://www.eutimes.net/2020/09/google-caught-censoring-search-results-that-criticize-black-lives-matter/ Accessed 22 April 2021

Foucault, M. (1995). *Discipline & Punish: The Birth of the Prison*. Vintage Books.

Gandel, S. (2020, January 29). Facebook struggles to stem spread of coronavirus misinformation. *CBS News*. https://www.cbsnews.com/news/facebook-coronavirus-posts-spread-misinformation-on-deadly-outbreak/. Accessed 17 April 2020

Gibson, K. (2020, February 3). Twitter bans Zero Hedge after it posts coronavirus conspiracy theory. *CBS News*. https://www.cbsnews.com/news/twitter-bans-zero-hedge-coronavirus-conspiracy-theory/. Accessed 17 April 2020

Gitogo, G. (2019, February 13). How to Hack Whatsapp, Facebook, Telegram Using SS7 Flaw. *Mobipicker*. https://www.mobipicker.com/hack-whatsapp-facebook-telegram-using-ss7-flaw/#:~:text=Hackers%20exploit%20the%20SS7%20flaw%20by%20making%20the,secret%20code%20will%20be%20sent%20to%20your%20phone.

Halder, D., & Jaishankar, K. (2012). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations*. IGI Global. https://doi.org/10.4018/978-1-60960-830-9

Hayes, A. F. (2005). Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research. *International Journal of Public Opinion Research*, *17*(3), 298–323. https://doi.org/10.1093/ijpor/edh073

Hayes, A. F., Glynn, C. J., & Shanahan, J. (2005). Validating the Willingness to Self-Censor Scale: Individual Differences in the Effect of the Climate of Opinion on Opinion Expression. *International Journal of Public Opinion Research*, *17*(4), 443–455. https://doi.org/10.1093/ijpor/edh072

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. https://doi.org/10.1080/15536548.2013.10845689

Hegarty, S. (2020, February 6). The Chinese doctor who tried to warn others about coronavirus. *BBC News*. https://www.bbc.com/news/world-asia-china-51364382. Accessed 17 April 2020

Hicks, R. E., Miller, G. W., & Kinsbourne, M. (1976). Prospective and Retrospective Judgments of Time as a Function of Amount of Information Processed. *The American Journal of Psychology*, *89*(4), 719. https://doi.org/10.2307/1421469

Ho, K. (2017). Tackling the Term: What is a Safe Space? *Harvard Political Review*. https://harvardpolitics.com/what-is-a-safe-space/

Ho, S. S., & McLeod, D. M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. *Communication Research*, *35*(2), 190–207. https://doi.org/10.1177/0093650207313159

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values* (1st ed.). Sage Publications.

Hofstede, G. H. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations* (2nd ed). Sage Publications.

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (Eds.). (2004). *Culture, leadership, and organizations: The GLOBE study of 62 societies*. Sage Publications.

ISACA. (October 29, 2014). Which of the following statements best describes your approach toward managing the privacy of data collected on connected devices? [Graph]. In *Statista*. Retrieved September 25, 2021, from https://www.statista.com/statistics/374232/managing-data-privacy-on-connected-devices-uk/

Jain, R. (2009, March 8). Cyber Persona. *Ramesh Jain*. Retrieved June 29, 2021, from https://ngs.ics.uci.edu/cyber-persona/

Jane, E. A. (2015). Flaming? What flaming? The pitfalls and potentials of researching online hostility. *Ethics and Information Technology*, *17*(1), 65–87. https://doi.org/10.1007/s10676-015-9362-0

Jaschik, S. (2014, September 15). Interview with professor fired by West Bank university who compares himself to Steven Salaita. *Inside Higher Ed*. Washington, D.C. https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita Accessed 22 January 2020

Jones, G. K., & Teegen, H. J. (2001). Global R&D activity of U.S. MNCs: Does national culture affect investment decisions. *Multinational Business Review*, *9*(2), 1–7.

Katz, K. L., & Martin, B. R. (1989). *Improving customer satisfaction through the management of perceptions of waiting* [Massachusetts Institute of Technology]. http://hdl.handle.net/1721.1/37703

Kwon, O., Kim, C., & Kim, G. (2013). Factors affecting the intensity of emotional expressions in mobile communications. *Online Information Review*, *37*(1), 114–131. https://doi.org/10.1108/14684521311311667

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management*, *53*(1), 53–63. https://doi.org/10.1016/j.im.2015.08.006

Luarn, P., & Hsieh, A.-Y. (2014). Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities. *Online Information Review*, *38*(7), 881–895. https://doi.org/10.1108/OIR-03-2014-0076

Lucchi, N. (2011). Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, *19*(3), 645–678.

Madden, M. (2013). *Majority of online Americans 'Google themselves'* (Pew Research Center). Pew Research Center. https://www.pewresearch.org/fact-tank/2013/09/27/majority-of-online-americans-google-themselves/ Accessed 30 June 2021

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). *Digital Footprints* (Pew Research Center). Pew Research Center. https://www.pewresearch.org/internet/2007/12/16/digital-footprints/ Accessed 30 June 2021

Merriam-Webster. (n.d.a). Adversary. In *Merrian-Webster.com dictionary*. https://www.merriam-webster.com/dictionary/adversary

Merriam-Webster. (n.d.b). Controversy. In *Merriam-Webster.com dictionary*. https://www.merriam-webster.com/dictionary/controversy. Accessed 24 April 2020

Merriam-Webster. (n.d.c). Detective. In *Merrian-Webster.com dictionary*. https://www.merriam-webster.com/dictionary/detective

Merriam-Webster. (n.d.d). Safe space. In *Merriam-Webster.com dictionary*. Retrieved July 24, 2021, from https://www.merriam-webster.com/dictionary/safe%20space

Merriam-Webster. (n.d.e). Surveillance. In *Merrian-Webster.com dictionary*. Retrieved July 24, 2021, from https://www.merriam-webster.com/dictionary/surveillance

Morgan, S. (2017). The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more. *Cybersecurity Ventures*. https://cybersecurityventures.com/cybersecurity-market-report/ Accessed 24 January 2019

Nadi, Y., & Firth, L. (2004). The Internet Implication in Expanding Individual Freedom in Authoritarian States. *ACIS 2004 Proceedings*. ACIS 2004.

Nartova-Bochaver, S. (2004). THE QUESTIONNAIRE "SOVEREIGNTY OF THE PSYCHOLOGICAL SPACE" —THE NEW INVENTORY OF THE DIAGNOSTICS OF THE PERSONALITY. *Psychological Journal*, *25*(5), 77–89. (Translated from Russian by Google translate, 2021.)

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

Pew Research Center. (2015). Online privacy and anonymity management methods of internet users in the United States as of July 2013 [Graph]. In *Statista*. Retrieved 2015, from https://www.statista.com/statistics/219428/online-privacy-and-anonymity-strategies-of-us-internet-users/

Pew Research Center. (2016). *Research in the Crowdsourcing Age, a Case Study*. Pew Research Center. Retrieved September 2021, from https://www.pewresearch.org/internet/2016/07/11/turkers-in-this-canvassing-young-well-educated-and-frequent-users/

Phelan, J. (2014, March 24). This is how these 12 countries will punish you for insulting their heads of state. *GlobalPost / PRI*. https://www.pri.org/stories/2014-03-12/how-these-12-countries-will-punish-you-insulting-their-heads-state Accessed 9 September 2019

Rauhala, J., Tyrväinen, P., & Zaidenberg, N. (2019a). Does Time Spent on Device Security and Privacy Inhibit Online Expression? *PROCEEDINGS OF THE 18TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY*, 394–402. Presented at the 18TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY, S.l.: ACPIL.

Rauhala, J., Tyrväinen, P., & Zaidenberg, N. (2019b). Online Expression and Spending on Personal Cybersecurity. *PROCEEDINGS OF THE 18TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY*, 387–393. Presented at the 18TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY, S.l.: ACPIL.

Rauhala, J. (2013). *STORAGE MANAGEMENT OF PROFILES IN MOBILE DEVICES* (U.S. Patent and Trademark Office Patent No. 8,583,689).

Rauhala, J. (2012). *STORAGE MANAGEMENT* (U.S. Patent and Trademark Office Patent No. 8,135,745).

Ray, A., & Kaushik, A. (2017). State transgression on electronic expression: Is it for real? *Information and Computer Security*, 00–00. https://doi.org/10.1108/ICS-03-2016-0024

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, *26*(1–2), 81–99. https://doi.org/10.1080/13511610.2013.747650

Reuters Staff. (2021, April 2). Myanmar junta cuts internet, protesters say they will not surrender. *Reuters*. https://www.reuters.com/article/us-myanmar-politics-idUSKBN2BP06T Accessed 12 May 2021

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates†. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy004

Rostocki, A. (2021). Internet Private Investigator. *Private Investigator*. https://www.private-investigator-info.org/internet-private-investigator.html Accessed 29 June 2021

Rothaermel, F. T., Kotha, S., & Steensma, H. K. (2006). International Market Entry by U.S. Internet Firms: An Empirical Analysis of Country Risk, National Culture, and Market Size. *Journal of Management*, 32(1), 56–82. https://doi.org/10.1177/0149206305277793

Ryan, D. (2018, August 15). Five examples that show internet censorship is as much a threat to the left as the right. *RT.Com*. https://www.rt.com/news/436058-censorship-left-right-facebook-google/ Accessed 22 April 2021

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), 21–32. https://doi.org/10.1080/01972240252818207

Shen, F., & Liang, H. (2015). Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, 27(1), 111–124. https://doi.org/10.1093/ijpor/edu012

Sims, J., & Xu, L. (2012). Perceived Risk of Online Shopping: Differences Between the UK and China. *UK Academy for Information Systems Conference Proceedings*, *25*.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 34(3), 487. https://doi.org/10.2307/25750688

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Stanton, L. (2014, August 18). EFFECT OF "RIGHT TO BE FORGOTTEN" ON FREE EXPRESSION SPARKS DEBATE. *Cybersecurity Policy Report*. New York.

Storm, D. (2016, April 18). Hackers only need your phone number to eavesdrop on calls, read texts, track you. *Computerworld*. https://www.computerworld.com/article/3058020/hackers-only-need-your-phone-number-to-eavesdrop-on-calls-read-texts-track-you.html Accessed 30 June 2021

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*, 93(2), 296–311. https://doi.org/10.1177/1077699016630255

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce. *Sustainability*, *11*(12), 3311. https://doi.org/10.3390/su11123311

Tak-ho, F., Siu-fung, L., Qiao, Q., & Mudie, L. (2020, March 13). Property Tycoon “Cannon” Ren Incommunicado After Critical Article Appears. *Radio Free Asia*. https://www.rfa.org/english/news/china/tycoon-incommunicado-03132020155224.html Accessed 17 April 2020

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

UN General Assembly. (1948). Universal Declaration of Human Rights. Paris. https://www.un.org/en/universal-declaration-human-rights/index.html

UN Human Rights Council. (2016). Resolution on the promotion, protection and enjoyment of human rights on the Internet. Geneva. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Van den Hoven, J. (2001). Privacy and the Varieties of Informational Wrongdoing. In *Readings in Cyberethics*. Jones and Bartlett.

Vasquez, I., & Porcnik, T. (2017). *The Human Freedom Index 2017: A Global Measurement of Personal, Civil, and Economic Freedom*. Cato Institute, Fraser Institute, and the Friedrich Naumann Foundation for Freedom.

Wacks, R. (1989). *Personal information: Privacy and the law*. Clarendon Press ; Oxford University Press.

Wikipedia Contributors. (2021a). Terminology. In *Wikipedia*. Retrieved June 29, 2021, from https://en.wikipedia.org/wiki/Terminology#Science

Wikipedia Contributors. (2021b). Proxemics. In *Wikipedia*. Retrieved June 29, 2021, from https://en.wikipedia.org/wiki/Personal_space

Wikipedia Contributors. (2021c). Online identity. In *Wikipedia*. Retrieved June 29, 2021, from https://en.wikipedia.org/wiki/Online_identity

Xin, T., Siponen, M., & Chen, S. (2021). Understanding the inward emotion-focused coping strategies of individual users in response to mobile malware threats. *Behaviour & Information Technology*, 1–25. https://doi.org/10.1080/0144929X.2021.1954242

Yee, M. (2019, June 3). Why ‘Safe Spaces’ Are Important for Mental Health—Especially on College Campuses. *Healthline*. https://www.healthline.com/health/mental-health/safe-spaces-college?c=755587367053#1

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile Commerce and Consumer Privacy Concerns. *Journal of Computer Information Systems*, 53(4), 31–38. https://doi.org/10.1080/08874417.2013.11645648

APPENDICES

Appendix A – Supplementary results tables for PI - RtoEx vs. LoM

Table 27: Correlations between extracted factors and demographic variables for newer data for PI

Correlations

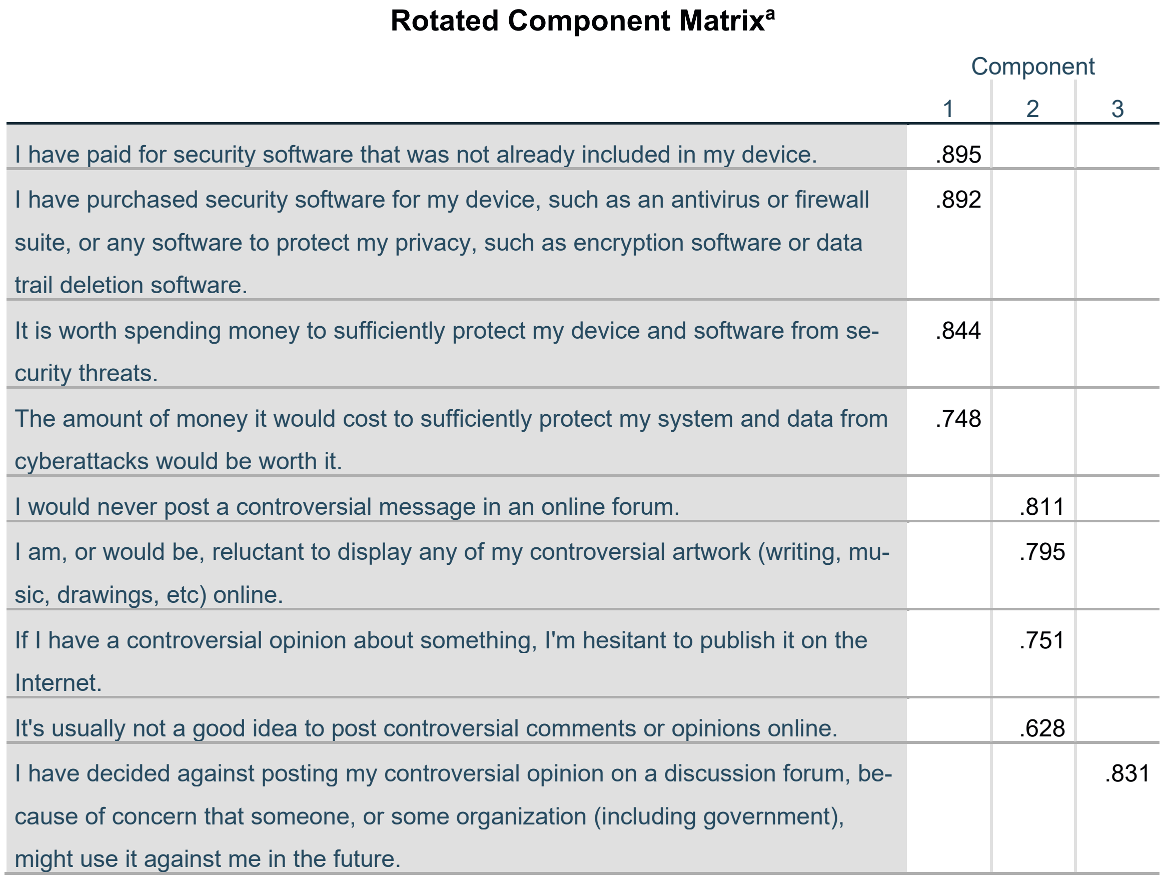
		What is your age?	Please indicate your annual income (euros):	LoM AVG	RtoEx AVG	RtoExnonC AVG	RtoExC AVG	ICTExp AVG
What is your age?	Pearson Correlation	1	.435**	-.135*	-.185**	-.131*	-.199**	.097
	Sig. (2-tailed)		.000	.028	.003	.033	.001	.114
Please indicate your annual income (euros):	Pearson Correlation	.435**	1	-.047	-.101	-.025	-.155*	.246**
	Sig. (2-tailed)	.000		.445	.100	.687	.011	.000
LoM AVG	Pearson Correlation	-.135*	-.047	1	.175**	.140*	.175**	.079
	Sig. (2-tailed)	.028	.445		.004	.023	.004	.203
RtoEx AVG	Pearson Correlation	-.185**	-.101	.175**	1	.895**	.902**	-.048
	Sig. (2-tailed)	.003	.100	.004		.000	.000	.437
RtoExnonC AVG	Pearson Correlation	-.131*	-.025	.140*	.895**	1	.615**	-.043
	Sig. (2-tailed)	.033	.687	.023	.000		.000	.489
RtoExC AVG	Pearson Correlation	-.199**	-.155*	.175**	.902**	.615**	1	-.043
	Sig. (2-tailed)	.001	.011	.004	.000	.000		.481
ICTExp AVG	Pearson Correlation	.097	.246**	.079	-.048	-.043	-.043	1
	Sig. (2-tailed)	.114	.000	.203	.437	.489	.481	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

[Factor analysis reporting -]

Table 28: Rotated component matrix for newer data for PI



Rotated Component Matrix[a]

	Component		
	1	2	3
I have paid for security software that was not already included in my device.	.895		
I have purchased security software for my device, such as an antivirus or firewall suite, or any software to protect my privacy, such as encryption software or data trail deletion software.	.892		
It is worth spending money to sufficiently protect my device and software from security threats.	.844		
The amount of money it would cost to sufficiently protect my system and data from cyberattacks would be worth it.	.748		
I would never post a controversial message in an online forum.		.811	
I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc) online.		.795	
If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.		.751	
It's usually not a good idea to post controversial comments or opinions online.		.628	
I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.			.831

I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.			.803
When discussing something with a good friend, I feel more safe to express controversial opinions face to face, than by electronic communication.			.645
I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.		.475	.629

Extraction Method: Principal Component Analysis.

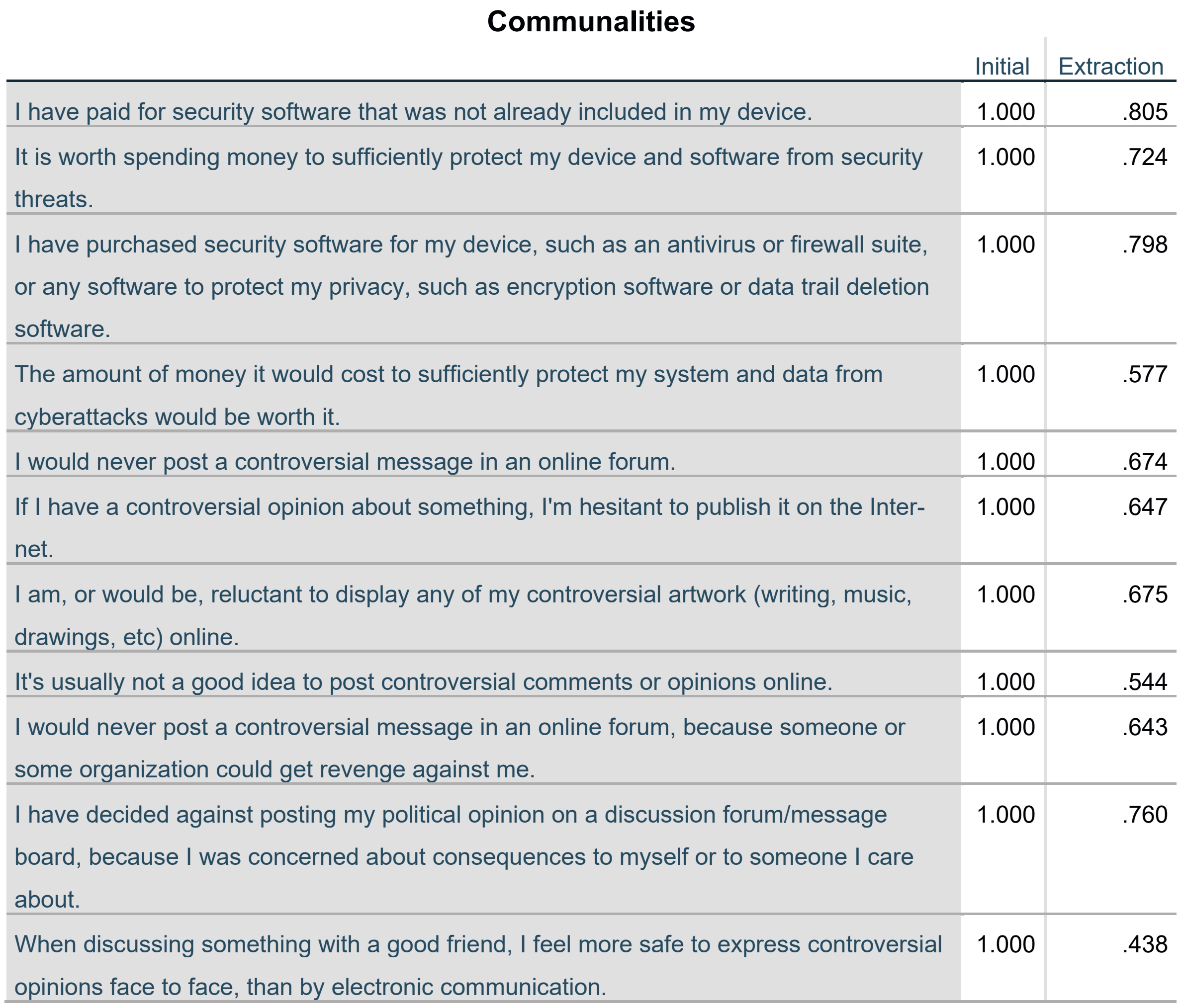
Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 4 iterations.

Table 29: Eigenvalues for newer data for PI

	Initial Eigenvalues		
Component	Total	% of Variance	Cumulative %
1	4.369	36.406	36.406
2	2.670	22.248	58.655
3	1.010	8.415	67.069

Table 30: Communalities for newer data for PI



Communalities

	Initial	Extraction
I have paid for security software that was not already included in my device.	1.000	.805
It is worth spending money to sufficiently protect my device and software from security threats.	1.000	.724
I have purchased security software for my device, such as an antivirus or firewall suite, or any software to protect my privacy, such as encryption software or data trail deletion software.	1.000	.798
The amount of money it would cost to sufficiently protect my system and data from cyberattacks would be worth it.	1.000	.577
I would never post a controversial message in an online forum.	1.000	.674
If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.	1.000	.647
I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc) online.	1.000	.675
It's usually not a good idea to post controversial comments or opinions online.	1.000	.544
I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.	1.000	.643
I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.	1.000	.760
When discussing something with a good friend, I feel more safe to express controversial opinions face to face, than by electronic communication.	1.000	.438

I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.	1.000	.763

Extraction Method: Principal Component Analysis.

[Multiple regression reporting]

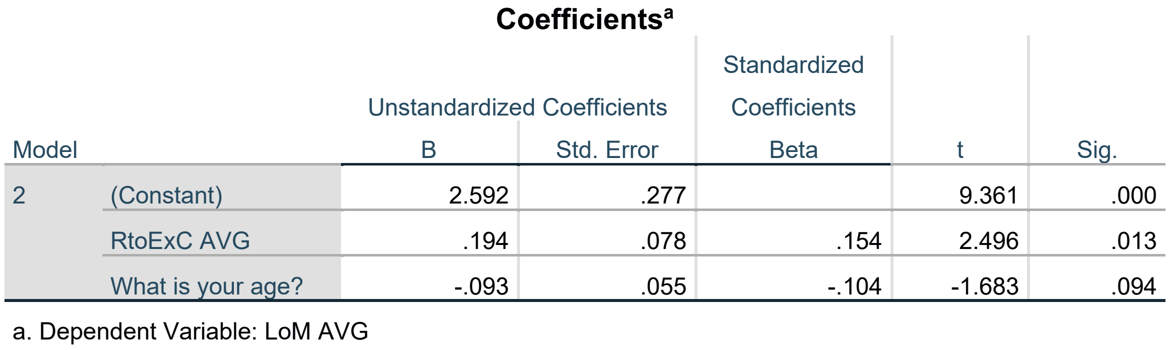
Table 31: Regression model for newer data for PI

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.206[a]	.042	.031	1.10059
2	.202[b]	.041	.034	1.09938

Predictors: (Constant), What is your age?, RtoExnonC AVG, RtoExC AVG[a]

Predictors: (Constant), What is your age?, RtoExC AVG[b]

Table 32: Regression coefficients for newer data for PI



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
2	(Constant)	2.592	.277		9.361	.000
	RtoExC AVG	.194	.078	.154	2.496	.013
	What is your age?	-.093	.055	-.104	-1.683	.094

a. Dependent Variable: LoM AVG

Appendix B – Supplementary results tables for PII - Time and RtoEx

Table 33: Correlations between extracted factors and demographic variables for newer data for PII

Correlations

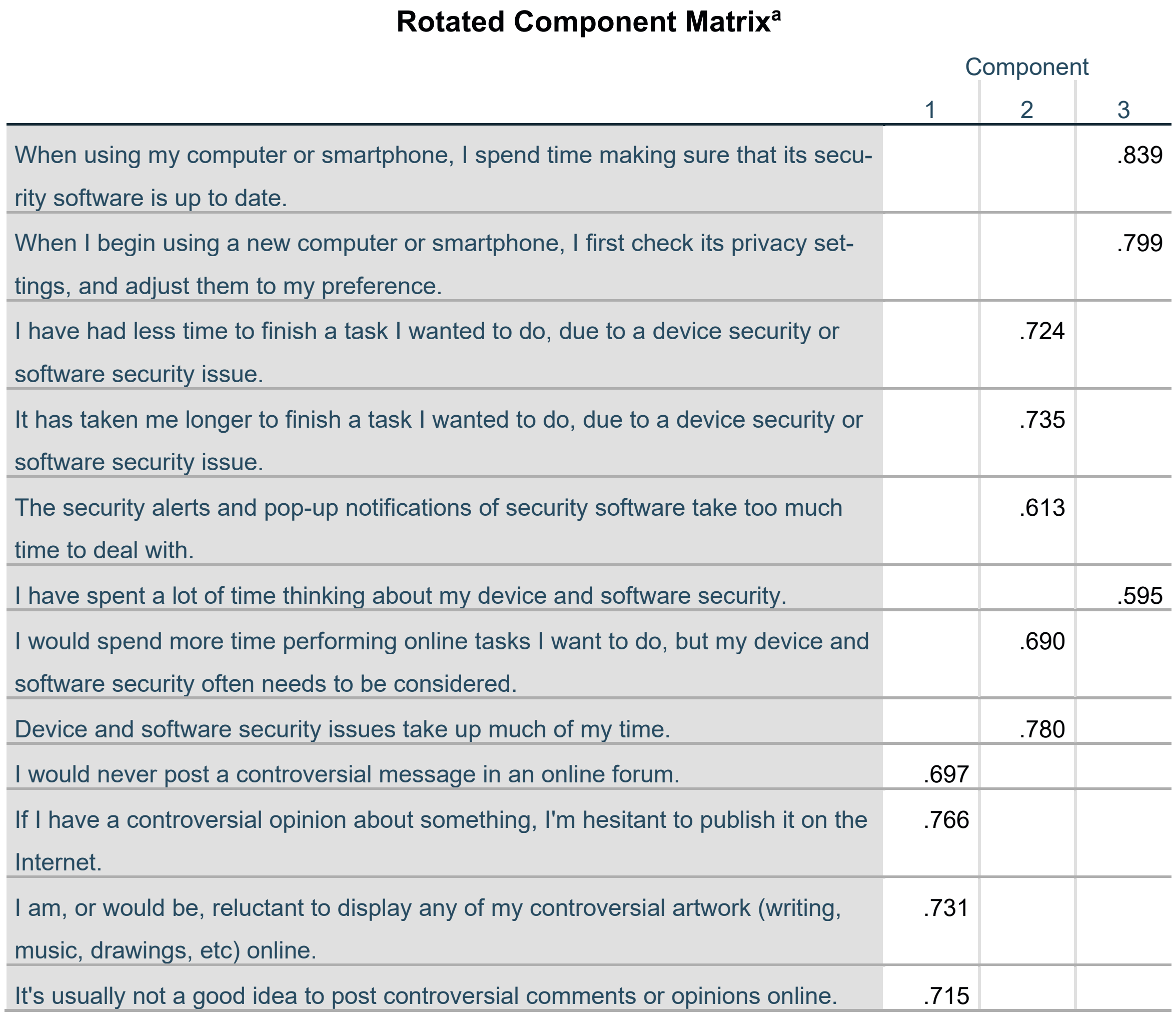
		TChS AVG	TMT AVG	RtoEx AVG	ICTExp AVG	What is your age?	Please indicate your gender	Please indicate your annual income (euros):
TChS AVG	Pearson Correlation	1	.179**	.067	-.118	.052	.208**	-.025
	Sig. (2-tailed)		.003	.276	.055	.396	.001	.684
TMT AVG	Pearson Correlation	.179**	1	.238**	-.100	-.083	.107	-.159**
	Sig. (2-tailed)	.003		.000	.105	.180	.083	.010
RtoEx AVG	Pearson Correlation	.067	.238**	1	-.048	-.185**	-.214**	-.101
	Sig. (2-tailed)	.276	.000		.437	.003	.000	.100
ICTExp AVG	Pearson Correlation	-.118	-.100	-.048	1	.097	-.152*	.246**
	Sig. (2-tailed)	.055	.105	.437		.114	.013	.000
What is your age?	Pearson Correlation	.052	-.083	-.185**	.097	1	-.014	.435**
	Sig. (2-tailed)	.396	.180	.003	.114		.819	.000
Please indicate your gender	Pearson Correlation	.208**	.107	-.214**	-.152*	-.014	1	-.220**
	Sig. (2-tailed)	.001	.083	.000	.013	.819		.000
Please indicate your annual income (euros):	Pearson Correlation	-.025	-.159**	-.101	.246**	.435**	-.220**	1
	Sig. (2-tailed)	.684	.010	.100	.000	.000	.000	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

[Factor analysis reporting -]

Table 34: Rotated component matrix for newer data for PII



Rotated Component Matrix[a]

	Component		
	1	2	3
When using my computer or smartphone, I spend time making sure that its security software is up to date.			.839
When I begin using a new computer or smartphone, I first check its privacy settings, and adjust them to my preference.			.799
I have had less time to finish a task I wanted to do, due to a device security or software security issue.		.724	
It has taken me longer to finish a task I wanted to do, due to a device security or software security issue.		.735	
The security alerts and pop-up notifications of security software take too much time to deal with.		.613	
I have spent a lot of time thinking about my device and software security.			.595
I would spend more time performing online tasks I want to do, but my device and software security often needs to be considered.		.690	
Device and software security issues take up much of my time.		.780	
I would never post a controversial message in an online forum.	.697		
If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.	.766		
I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc) online.	.731		
It's usually not a good idea to post controversial comments or opinions online.	.715		

I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.	.772		
I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.	.759		
When discussing something with a good friend, I feel more safe to express controversial opinions face to face, than by electronic communication.	.492		
I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.	.710		

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 4 iterations.

Table 35: Communalities for newer data for PII

Communalities

	Initial	Extraction
When using my computer or smartphone, I spend time making sure that its security software is up to date.	1.000	.715
When I begin using a new computer or smartphone, I first check its privacy settings, and adjust them to my preference.	1.000	.640
I have had less time to finish a task I wanted to do, due to a device security or software security issue.	1.000	.573
It has taken me longer to finish a task I wanted to do, due to a device security or software security issue.	1.000	.602
The security alerts and pop-up notifications of security software take too much time to deal with.	1.000	.503
I have spent a lot of time thinking about my device and software security.	1.000	.429

I would spend more time performing online tasks I want to do, but my device and software security often needs to be considered.	1.000	.489
Device and software security issues take up much of my time.	1.000	.623
I would never post a controversial message in an online forum.	1.000	.497
If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.	1.000	.594
I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc) online.	1.000	.543
It's usually not a good idea to post controversial comments or opinions online.	1.000	.524
I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.	1.000	.616

I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.	1.000	.630
When discussing something with a good friend, I feel more safe to express controversial opinions face to face, than by electronic communication.	1.000	.269
I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.	1.000	.586

Extraction Method: Principal Component Analysis.

[Multiple regression reporting]

Table 36: Regression model for newer data for PII

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.293[a]	.086	.068	.760527
2	.293[b]	.086	.072	.759086
3	.292[c]	.086	.075	.757659
4	.290[d]	.084	.077	.756759

Predictors: (Constant), TMT AVG, What is your age?, ICTExp AVG, TChS AVG, Please indicate your annual income (euros):[a]

Predictors: (Constant), TMT AVG, What is your age?, TChS AVG, Please indicate your annual income (euros):[b]

Predictors: (Constant), TMT AVG, What is your age?, TChS AVG[c]

Predictors: (Constant), TMT AVG, What is your age?[d]

Table 37: Regression coefficients for newer data for PII

		Unstandardized Coefficients		Standardized Co-efficients		
Model		B	Std. Error	Beta	t	Sig.
4	(Constant)	2.164	.235		9.206	.000
	What is your age?	-.104	.037	-.166	-2.798	.006
	TMT AVG	.236	.062	.225	3.789	.000

Appendix C – Supplementary results tables for PIII - Time and LoM

Table 38: Correlations between extracted factors and demographic variables for newer data for PIII

Correlations

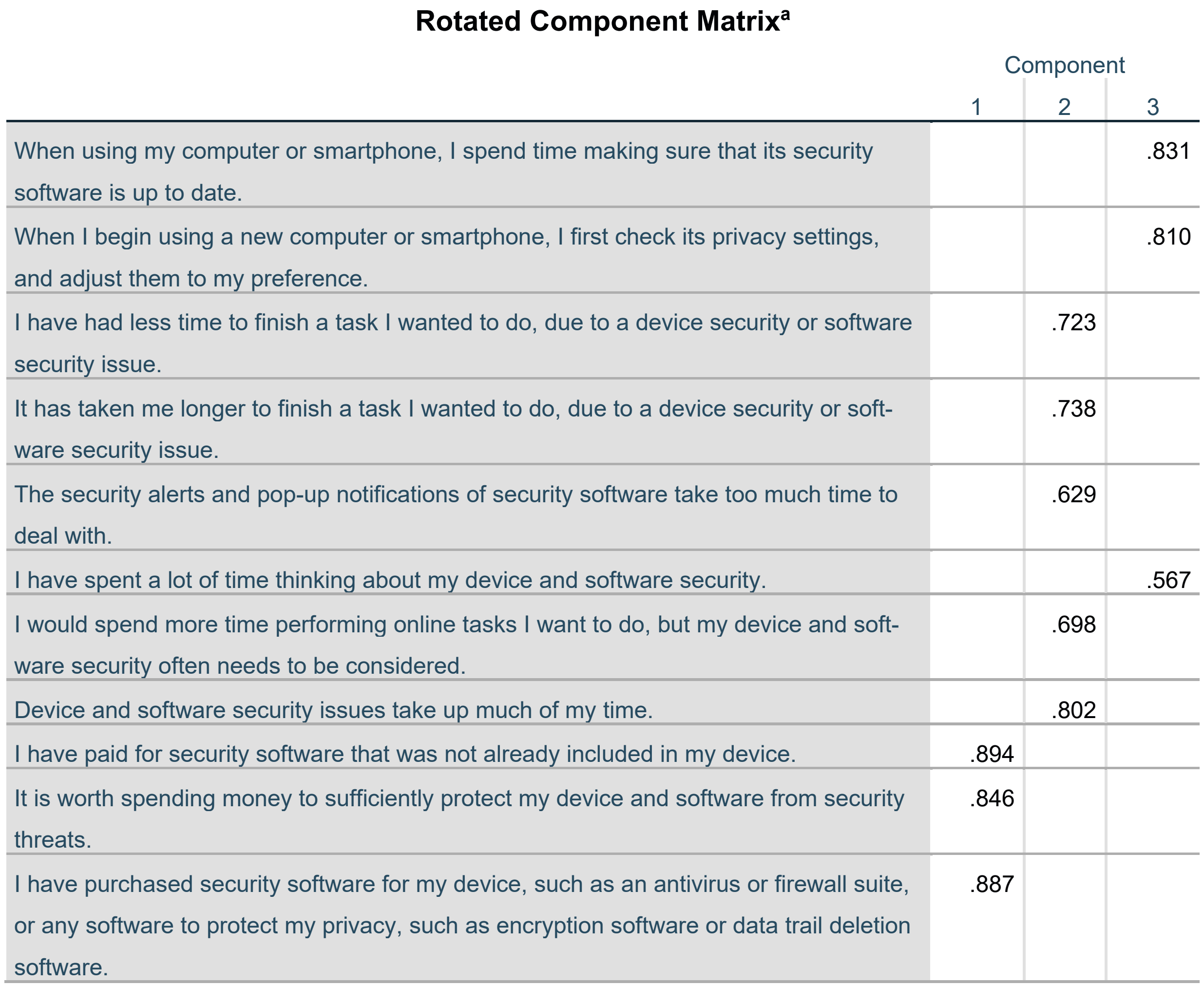
		What is your age?	Please indicate your annual income (euros):	TChS AVG	TMT AVG	LoM AVG	ICTExp AVG
What is your age?	Pearson Correlation	1	.435**	.052	-.083	-.135*	.097
	Sig. (2-tailed)		.000	.396	.180	.028	.114
Please indicate your annual income (euros):	Pearson Correlation	.435**	1	-.025	-.159**	-.047	.246**
	Sig. (2-tailed)	.000		.684	.010	.445	.000
TChS AVG	Pearson Correlation	.052	-.025	1	.179**	.212**	-.118
	Sig. (2-tailed)	.396	.684		.003	.001	.055
TMT AVG	Pearson Correlation	-.083	-.159**	.179**	1	.029	-.100
	Sig. (2-tailed)	.180	.010	.003		.633	.105
LoM AVG	Pearson Correlation	-.135*	-.047	.212**	.029	1	.079
	Sig. (2-tailed)	.028	.445	.001	.633		.203
ICTExp AVG	Pearson Correlation	.097	.246**	-.118	-.100	.079	1
	Sig. (2-tailed)	.114	.000	.055	.105	.203	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

[Factor analysis reporting -]

Table 39: Rotated component matrix for newer data for PIII



Rotated Component Matrix[a]

	Component		
	1	2	3
When using my computer or smartphone, I spend time making sure that its security software is up to date.			.831
When I begin using a new computer or smartphone, I first check its privacy settings, and adjust them to my preference.			.810
I have had less time to finish a task I wanted to do, due to a device security or software security issue.		.723	
It has taken me longer to finish a task I wanted to do, due to a device security or software security issue.		.738	
The security alerts and pop-up notifications of security software take too much time to deal with.		.629	
I have spent a lot of time thinking about my device and software security.			.567
I would spend more time performing online tasks I want to do, but my device and software security often needs to be considered.		.698	
Device and software security issues take up much of my time.		.802	
I have paid for security software that was not already included in my device.	.894		
It is worth spending money to sufficiently protect my device and software from security threats.	.846		
I have purchased security software for my device, such as an antivirus or firewall suite, or any software to protect my privacy, such as encryption software or data trail deletion software.	.887		

The amount of money it would cost to sufficiently protect my system and data from cyberattacks would be worth it.	.750		

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 4 iterations.

Table 40: Eigenvalues for newer data for PIII

	Initial Eigenvalues		
Component	Total	% of Variance	Cumulative %
1	3.254	27.120	27.120
2	2.667	22.221	49.341
3	1.635	13.628	62.969

Table 41: Communalities for newer data for PIII

Communalities

	Initial	Extraction
When using my computer or smartphone, I spend time making sure that its security software is up to date.	1.000	.717
When I begin using a new computer or smartphone, I first check its privacy settings, and adjust them to my preference.	1.000	.658
I have had less time to finish a task I wanted to do, due to a device security or software security issue.	1.000	.578

It has taken me longer to finish a task I wanted to do, due to a device security or software security issue.	1.000	.614
The security alerts and pop-up notifications of security software take too much time to deal with.	1.000	.517
I have spent a lot of time thinking about my device and software security.	1.000	.421
I would spend more time performing online tasks I want to do, but my device and software security often needs to be considered.	1.000	.503
Device and software security issues take up much of my time.	1.000	.647
I have paid for security software that was not already included in my device.	1.000	.804
It is worth spending money to sufficiently protect my device and software from security threats.	1.000	.722
I have purchased security software for my device, such as an antivirus or firewall suite, or any software to protect my privacy, such as encryption software or data trail deletion software.	1.000	.793
The amount of money it would cost to sufficiently protect my system and data from cyberattacks would be worth it.	1.000	.581

Extraction Method: Principal Component Analysis.

[Multiple regression reporting -]

Table 42: Regression model for newer data for PIII

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.285[a]	.081	.063	1.08241
2	.285[b]	.081	.067	1.08034
3	.284[c]	.081	.070	1.07838

Predictors: (Constant), Please indicate your annual income (euros):, TChS AVG, TMT AVG, ICTExp AVG, What is your age?[a]

Predictors: (Constant), TChS AVG, TMT AVG, ICTExp AVG, What is your age?[b]

Predictors: (Constant), TChS AVG, ICTExp AVG, What is your age?[c]

Table 43: Regression coefficients for newer data for PIII

	Unstandardized Coefficients		Standardized Co-efficients		
	B	Std. Error	Beta	t	Sig.
(Constant)	1.713	.452		3.790	.000
TChS AVG	.287	.073	.235	3.921	.000
ICTExp AVG	.228	.113	.122	2.026	.044
What is your age?	-.142	.053	-.159	-2.657	.008

Appendix D –Results tables for PV – Time, RtoEx and and the A.P.C.O. model

[Factor analysis reporting -]

[Correlations]

[Multiple regression reporting]

H5

Table 44: Regression model for TMT as dependent variable

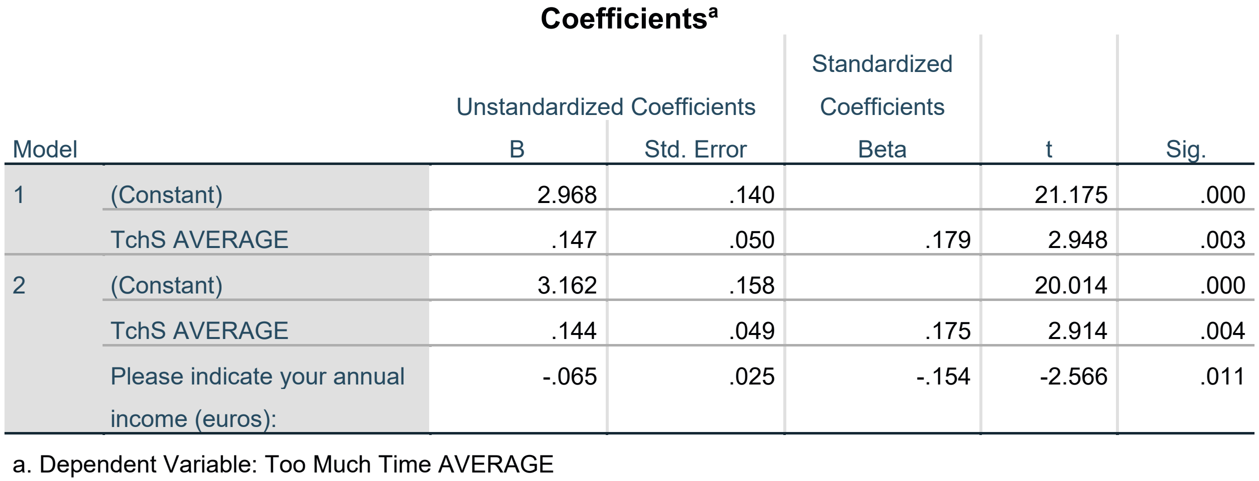
Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.179[a]	.032	.028	.741
2	.236[b]	.056	.049	.733

a. Predictors: (Constant), TchS AVERAGE

b. Predictors: (Constant), TchS AVERAGE, Please indicate your annual income (euros):

Table 45: Regression coefficients for TMT as dependent variable



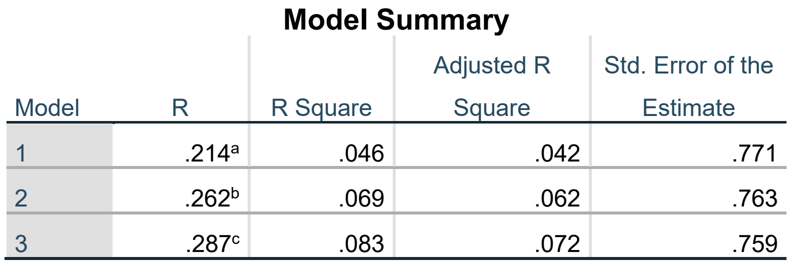
Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.968	.140		21.175	.000
	TchS AVERAGE	.147	.050	.179	2.948	.003
2	(Constant)	3.162	.158		20.014	.000
	TchS AVERAGE	.144	.049	.175	2.914	.004
	Please indicate your annual income (euros):	-.065	.025	-.154	-2.566	.011

a. Dependent Variable: Too Much Time AVERAGE

H6

Table 46: Regression model for RtoEx as dependent variable



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.214[a]	.046	.042	.771
2	.262[b]	.069	.062	.763
3	.287[c]	.083	.072	.759

a. Predictors: (Constant), Please indicate your gender

b. Predictors: (Constant), Please indicate your gender, Please indicate your annual income (euros):

c. Predictors: (Constant), Please indicate your gender, Please indicate your annual income (euros):, TchS AVERAGE

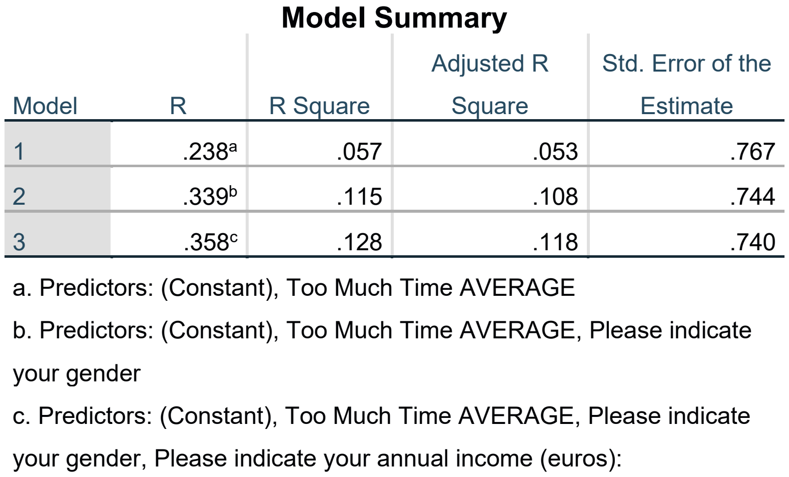
Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
1	(Constant)	3.211	.145		22.209	.000
	Please indicate your gender	-.340	.096	-.214	-3.546	.000
2	(Constant)	3.486	.179		19.463	.000
	Please indicate your gender	-.394	.097	-.248	-4.057	.000
	Please indicate your annual income (euros):	-.069	.027	-.156	-2.552	.011
3	(Constant)	3.273	.208		15.709	.000
	Please indicate your gender	-.435	.099	-.273	-4.401	.000
	Please indicate your annual income (euros):	-.070	.027	-.159	-2.608	.010
	TchS AVERAGE	.103	.052	.120	1.979	.049

a. Dependent Variable: RtoEx AVERAGE

H7

Table 47: Regression model for TMT->RtoEx with RtoEx as dependent variable



Model Summary

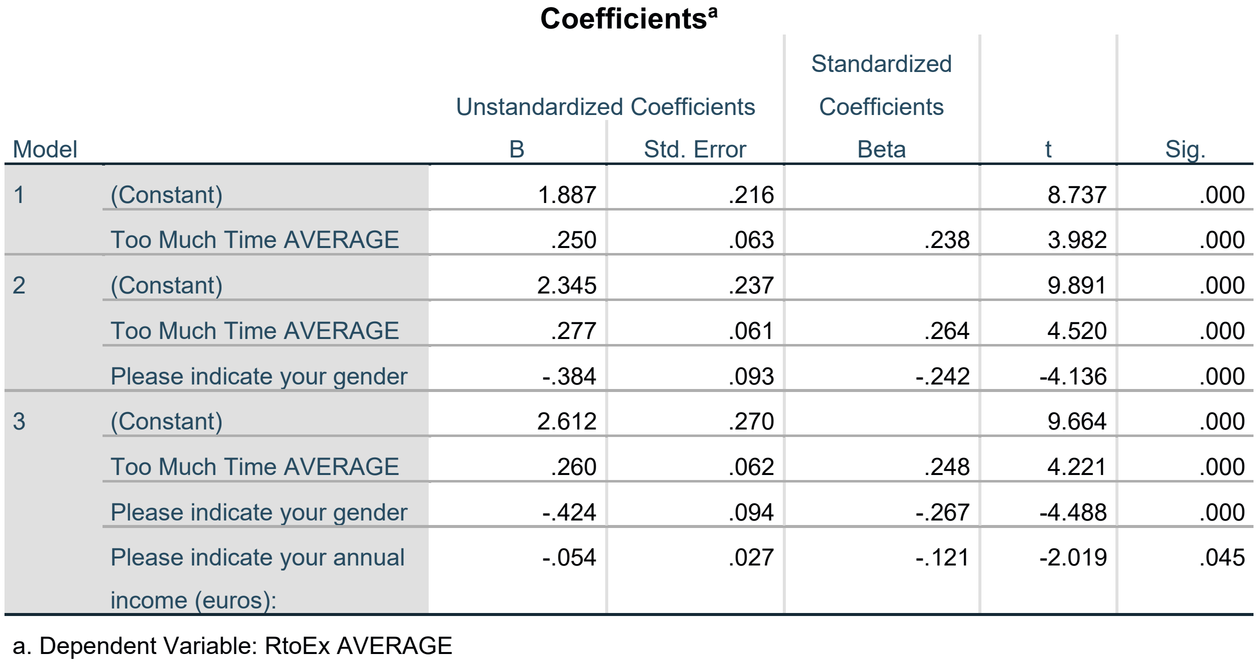
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.238[a]	.057	.053	.767
2	.339[b]	.115	.108	.744
3	.358[c]	.128	.118	.740

a. Predictors: (Constant), Too Much Time AVERAGE

b. Predictors: (Constant), Too Much Time AVERAGE, Please indicate your gender

c. Predictors: (Constant), Too Much Time AVERAGE, Please indicate your gender, Please indicate your annual income (euros):

Table 48: Regression coefficients for TMT->RtoEx with RtoEx as dependent variable



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.887	.216		8.737	.000
	Too Much Time AVERAGE	.250	.063	.238	3.982	.000
2	(Constant)	2.345	.237		9.891	.000
	Too Much Time AVERAGE	.277	.061	.264	4.520	.000
	Please indicate your gender	-.384	.093	-.242	-4.136	.000
3	(Constant)	2.612	.270		9.664	.000
	Too Much Time AVERAGE	.260	.062	.248	4.221	.000
	Please indicate your gender	-.424	.094	-.267	-4.488	.000
	Please indicate your annual income (euros):	-.054	.027	-.121	-2.019	.045

a. Dependent Variable: RtoEx AVERAGE

ORIGINAL PAPERS

P I

ONLINE EXPRESSION AND SPENDING ON PERSONAL CYBERSECURITY

by

Juhani Rauhala, Pasi Tyrväinen & Nezer Zaidenberg 2019

ECCWS 2019: Proceedings of the 18th European Conference on
Cyber Warfare and Security

Reproduced with kind permission by Academic Conferences
and Publishing International Limited.

Online Expression and Spending on Personal Cybersecurity

Juhani Rauhala[1], Pasi Tyrväinen[1] and Nezer Zaidenberg[2]
[1]University of Jyväskylä, Finland
[2]College of Management Academic Studies, Rishon LeZion, Israel
juhani.jr.rauhala@jyu.fi
pasi.tyrvainen@jyu.fi
scipio@scipio.org

Abstract: The Internet is used increasingly as a platform both for free expression and e-commerce. Internet users have a variety of attitudes towards the security and privacy risks involved with using the Internet; and distinct concerns and behaviors with regard to expressing themselves online. Users may have controversial viewpoints that they may express online in various ways. Controversial viewpoints or artwork by their nature may not be as well received as positive or polite expressions. In the online environment, users with controversial viewpoints may be reluctant to express the viewpoints due to concern about possible consequences resulting from the expressions. Consequences may be imposed by individuals, groups, organizations, businesses, or nation-states. Examples of such consequences include firings, removal of forum posting privileges ("banning"), violent attacks, online stalking, and doxing. Users may also have different attitudes towards personal spending of money for cybersecurity products and services. Factors such as concern about the risks associated with free expression online may impact their attitudes towards spending for personal cybersecurity. We perform a factor analysis on survey data. Our goal is to establish variables for expression reluctance, and attitude towards personal cybersecurity purchasing. The positive attitude toward spending on personal cybersecurity, as a factor, includes reported activity of purchasing cybersecurity products or services, and an overall generally positive attitude toward the purchasing of such products or services. We propose a research model that enables an analysis of the relationship between the reluctance to make controversial expressions online and a positive attitude toward spending money on personal cybersecurity products and services. We perform a correlation analysis between the factors. Results indicate that there is a correlation between users' reluctance to express controversial messages online, and a positive attitude towards spending money on personal cybersecurity. Future work will include additional analyses, including the effects of various demographic factors.

Keywords: online expression reluctance, personal cybersecurity spending, privacy concerns, online spending, risk avoidance

1. Introduction

One generally accepted beneficial use of the Internet is as a platform for commerce, which is continuously increasing (Emarketer.com, 2014). At the same time, spending by consumers and businesses on cybersecurity products and services is also increasing (Morgan, 2017). It is reasonable to expect that a significant proportion of personal cybersecurity software is being purchased online. Another commonly accepted benefit of the Internet is that it serves as a platform for free expression. Debate and discussions occur over online forums and social media such as Twitter and Facebook. These discussions are raising attention to a virtually unlimited array of topics. Importantly, political topics are also discussed as well as other topics without socially accepted *savoir-faire*. In oppressive nation-states, the free expression enabled by access to the Internet can be particularly important for increasing the possibilities for improved human rights (Nadi and Firth, 2004). However, there are potential adverse consequences for users making controversial or provocative expressions on the Internet including from governments (Baroni, 2015; Cooper, 2000; Mony, 2017), offended individuals (Cassidy, 2017), employers (Jaschik, 2014), and schools (Curtom, 2014). Concern about such consequences may not only have an inhibiting effect on users' use of the Internet for expression but it may also correlate with their desire to purchase personal cybersecurity products and anonymizing services. These effects may differ across certain demographic groupings. It is possible that misgivings of users about the Internet as a platform for free expression may correlate with increased Internet utilization by those same users for commerce in personal cybersecurity products and services. This study explores this somewhat paradoxical relationship given that the Internet is seen as an overall good for humanity.

This paper first presents an overview of previous related research, followed by a description of the research model. It then establishes two general latent factors. The first corresponds to a reluctance to self-express online. The second factor corresponds to a positive predilection toward personal spending to enhance personal cybersecurity. The correlation between these factors is then analyzed. The results are presented and discussed, followed by a conclusion and a description of future research goals.

2. Background

Booth (2017) has raised some attention to the issue of freedom of expression. Her work examines the relationships between laws and norms governing free expression, and the benefits of ICT on national well-being. As of the time of this writing, Booth's research is not yet complete; moreover, the research does not consider the expression of free speech on aspects of individual users. It is of note that Booth and other researchers utilize the Human Freedom Index (HFI) (Vasquez and Porcnik, 2017). Included in the HFI measures are those that measure freedom of expression. Among those measures are "Laws and Regulations that Influence Media Content," "Political Pressures and Controls on Media Content," and "State Control over Internet Access." The measures of Laws and Regulations that Influence Media Content and Political Pressures and Controls on Media Content could be useful for this study on the condition that they be applied indirectly. That is to say, for example, that an assumption would be that an average user would feel some reluctance to freely express themselves as a result of the laws and controls. This study addresses reluctance more directly in the survey questions, whereas the subset of HFI measures does not measure reluctance to express. The HFI's "expression freedom" measures have not been examined for their relationship to personal cybersecurity spending. In particular, they do not measure concern regarding the consequences of personal free expression and neither have they been analyzed for their relationship to Internet users' attitudes and behaviors toward purchasing personal cybersecurity protections. Other research has established that usage of the Internet for free expression can be a way of circumventing censorship or other hindrances preventing citizens' free expression in more traditional publishing methods, especially in authoritarian regimes (Nadi and Firth, 2014).

There are also studies observing the impact of demographic factors on Internet users' behavior relevant to this study. Research into culture-based differences in the perception of risk in online shopping and other tasks has yielded conflicting results. For example, Sims and Xu (2012) found no significant difference between UK and Chinese shoppers' perceived risk of online shopping despite those shoppers' differing cultural backgrounds. This was against expectations based on the results of prior similar research. However, Chen, Hsu, and Lin (2010) have studied consumers with different levels of computer expertise. They determined that consumers' preferences of attributes of shopping websites differ according to their levels of expertise. Sheehan (2002) found that users' education and age correlate with their level of concern about online privacy. Regan, FitzGerald, and Balint (2014) evaluated attitudes toward information privacy between age groups (specifically generations). Their analysis revealed a trend where younger generations tend to be more concerned than older ones about wiretapping and data privacy. Hazari and Brown (2013) studied whether demographic variables can affect Internet users' privacy concerns and, thus, their attitudes toward using social networking sites. In contrast to the results from Sheehan and from Regan, Fitzgerald, and Balint, their research found that age was not correlated with online privacy concerns. Bandyopadhyay (2011) found that factors such as level of Internet literacy, social awareness, and cultural background affect Internet users' online privacy concerns. He found that among the possible consequences of such concerns is an unwillingness to use the Internet. Liu et al (2016) applied social exchange theory to examine perceived risks and rewards of individual users' self-disclosure in social media. The authors found that perceived privacy risk can reduce the willingness of social media users to disclose personal information. There does not seem to be existing research on social exchange theory applied to controversial expression by individual users online. This study directly assesses the reluctance to express controversial viewpoints. It also assesses the reluctance that is caused by concern about consequences. Previous work has examined the effect on willingness to disclose information about oneself. Based on previous research, it can be hypothesized that the reluctance to express oneself on the Internet may be connected with concerns about the consequences. Further, reluctance to express oneself may lead to the use of cybersecurity as a means to protect oneself in these cases. However, there seems not to be previous results addressing this hypothesis.

This research analyzes whether users are more inclined to spend money on personal cybersecurity if they are reluctant to express themselves online. The researchers consider that it is important to consider the attitudes of users toward free expression on the Internet and possible consequences resulting from users' reluctance to freely express themselves on the Internet. This is relevant to participation in social media and other online expression contexts. The relationship between online expression aspects and personal cybersecurity spending seems to be lacking in prior research.

3. Research model

Based on the research questions raised in the previous section, this study analyzes the correlation between individuals' personal cybersecurity spending (referred to as "Loss of Money," LoM) and their reluctance to express themselves online (RtoEx). The reluctance of expressing is further divided into two factors based on inclusion or exclusion of consequences of the expression, RtoExC and RtoExnonC, respectively. The research model is presented in Figure 1. The hypotheses are as follows.

3.1 Hypotheses

H1: Users' refusal or reluctance to express themselves online (RtoEx) is correlated with their personal cybersecurity spending attitude and behavior (LoM).

H2: The correlation of H1 will vary by certain demographic factors.

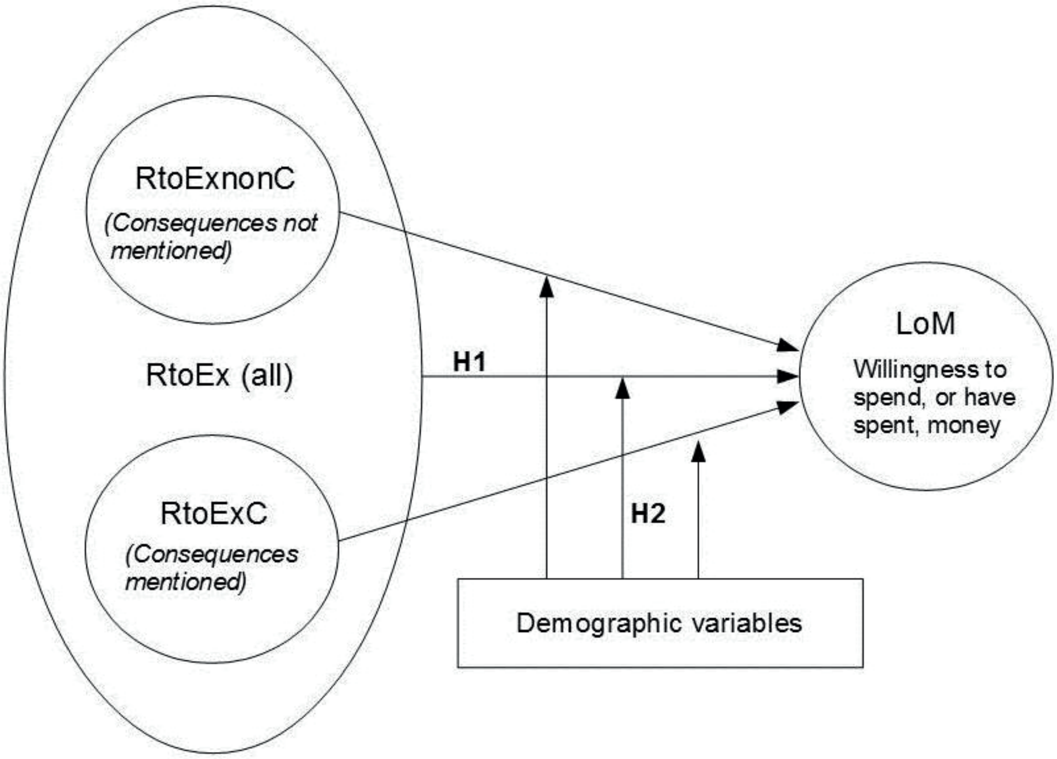


Figure 1: Latent variables RtoEx and LoM, and the independent demographic variables

4. Method

4.1 Operationalizing the model

Latent variables Loss of Money (LoM) and Reluctance to Express (RtoEx) are introduced. Each latent variable is defined by responses to respective sets of indicator questions. LoM is defined by four indicator questions and RtoEx by eight indicator questions. The questions for LoM are designed as follows: two questions to ascertain whether the respondent/subject has actually made a purchase for the purpose of enhancing his cybersecurity and two questions to ascertain the general attitude of the respondent toward security software purchases. Cumulatively, it is suggested the LoM indicator questions indicate the willingness to buy software products or services that enhance personal cybersecurity.

The questions for the RtoEx variable are designed as follows: the questions ascertain the attitude of the respondent toward theoretical scenarios of his/her posting controversial opinions or artwork online, including one question to ascertain his/her attitude toward using electronic methods vs. face-to-face communication for discussion of a sensitive topic with a friend. It is suggested that this set of RtoEx indicator questions can convey the level of the respondent's reluctance to openly communicate using electronic methods, or the Internet.

For data gathering, a survey was administered over the Web to a population composed mainly of university students and working adults. The survey included questions on respondents' behaviors and attitudes regarding personal spending on cybersecurity, and on their attitude toward posting or discussing controversial subjects online (Appendix). The questions were answered using a five-point Likert scale, ranging from "strongly agree" to "strongly disagree." The survey produced 191 useful responses. Responses by nationality include Finland (131 responses), USA (28 responses), and Israel (14 responses). The age groups of respondents are given in Table 1. The average age was approximately 31 years.

Table 1: Respondents by age group

n	15-25	26-36	37-44	45-54	55-64	65+
191	84	53	20	20	6	3

5. Results

5.1 Correlations between indicator questions for each latent variable

Because the response data to the indicator questions consist of Likert rankings to ordered categories, a Spearman correlation analysis is used. The results show a high correlation among responses to the four LoM indicator questions (Appendix, Table 4). The lowest correlation is .500 and the highest .863, all with two-star significance at the 0.01 level (two-tailed). Cronbach's alpha for the LoM questions is .871. The results also show a high correlation among responses to the eight RtoE indicator questions (Appendix, Table 5). The lowest correlation is .198 and the highest .699, all with two-star significance at the 0.01 level (two-tailed). Cronbach's alpha for the RtoEx questions is .838. For the four RtoExnonC questions, Cronbach's alpha is .764. For the four RtoExC questions, Cronbach's alpha is .796. Because the indicator questions for each latent variable (component) have high intercorrelation, the mean scores of the responses were computed and utilized for analysis. The Cronbach's alpha values are acceptable for good internal consistency within the sets of indicator questions (Table 2).

Table 2: Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor, mean correlations, and Cronbach's alpha

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
LoM	.500**	.863**	.639	.871
RtoEx	.198**	.699**	.395	.838
RtoExnonC	.359**	.564**	.457	.764
RtoExC	.292**	.699**	.490	.796

5.2 Correlations between latent variables

Pearson correlation analysis is performed on LoM as the dependent variable and RtoEx, RtoExnonC, and RtoExC as the independent variables. For all respondents, there is a correlation of .199** between RtoEx and LoM (Table 3). This correlation increases to .201** when respondents were presented with a consequences or safety issue in the survey question. For responses to RtoEx questions without a mention of consequences or safety, the correlation decreases to .149*. It might be expected that respondents who are reluctant to express themselves due to a concern about resulting consequences would have a more positive attitude toward spending money on their personal cybersecurity. There is a significant correlation between LoM and RtoExC. The correlation between LoM and RtoExnonC is weaker. Age was not correlated with LoM. A linear regression analysis for LoM was performed using age and the RtoExC factor as independent variables. This showed some correlation (adjusted R squared = .037, p-value = .011). Therefore, H2 is validated for age.

Table 3: Pearson correlations between RtoEx and LoM (two-tailed significances: * to 0.05 level; ** to 0.01 level)

n=191	RtoEx	RtoExnonC (consequences not mentioned)	RtoExC (consequences mentioned)
LoM	.199**	.149*	.201**

6. Discussion

For behaviors and attitudes toward personal cybersecurity spending (LoM), and attitudes toward making controversial expressions online (RtoEx), the results showed significant correlation. This confirms H1. Some users who are reluctant to freely express controversial viewpoints online not only deprive themselves of making the online expressions, but they also divert some of their purchasing power toward personal cybersecurity. Whether RtoEx has a causal role in the spending diversion has not been established.

With regard to correlation between LoM and RtoExnonC or RtoExC, the strongest correlation was between LoM and RtoExC. This may be expected because the respondent who is concerned about safety or consequences can have more motivation to protect their device than a respondent who is reluctant to express themselves for reasons not related to safety or consequences. When the correlation between LoM and RtoExnonC is examined, a correlation is seen there as well, though not as significant as between LoM and RtoExC. Internet users who are not as concerned about safety issues or consequences of freely expressing controversial topics online do still have concerns about personal cybersecurity for other reasons. These users have a favorable attitude toward purchasing, or have purchased, cybersecurity products and services to a lesser extent than users who are concerned about consequences or safety issues of controversial online expression.

7. Limitations of the study

The survey was administered in English. Thus, the accuracy of the results may be tainted by limitations in non-native English speakers' understanding of the survey questions. There were no survey questions to assess the English language competence of the respondents. The nationality of individual respondents could be indirectly used to gauge the reliability of individual responses; e.g., if a respondent indicates that their nationality is of a country whose official languages do not include English. In this case, inconsistency between responses of a question category may be at least partially explained by a possible non- or misunderstanding of the questions. In this study, it is generally assumed that all respondents have a sufficient understanding of all the survey questions. This assumption is supported by the fact that the respondents who are not native English speakers are, for the most part, university students or academic professionals.

This study did not consider free and open source personal cybersecurity products and tools that are available. Such tools include Tor browser, ClamAV, and free VPN services. Some respondents may have responded negatively to the survey questions regarding spending because they believe that they can achieve sufficient personal cybersecurity without spending money doing so.

8. Conclusion

This research demonstrated a significant correlation between Internet users' reluctance to controversially express themselves online and a positive proclivity toward personal cybersecurity spending. The correlation was even stronger for those users concerned about safety issues and consequences that could result from controversial online expression. It may be inferred that these concerned users are more actively making purchases of cybersecurity products and services. While sales of cybersecurity products and services are good for the cybersecurity industry, they also indicate the real cybersecurity concerns of Internet users. Many Internet users go online, but are then reluctant to freely express themselves, spending their time and money to alleviate perceived cybersecurity risks. This scenario is not the ideal or optimal use of the Internet by society. Future research can investigate methods to encourage free expression online and reduce the perceived risks of such free expression. An extension of this research can be to explore on which topics users are less inclined to express their opinions online.

From the viewpoint of encouraging open and robust political discourse, governments should ensure the framework and conditions for free expression by their citizens with online regulatory safeguards that correspond to the traditional safeguards in traditional communications media. This could help Internet users feel freer to spend money for personal interests instead of diverting spending due to concerns about their online privacy and security.

The HFI may be enhanced by the inclusion of a measure to assess citizens' reluctance to express legal, but controversial, viewpoints online. Citizens may be reluctant to express such viewpoints despite states' official policies allowing free expression. The concern about consequences resulting from such expression may not necessarily align with states' official policies and the possibility of state-imposed consequences does not necessarily align with states' official policies. The current HFI does not account for citizens' concerns and perceptions of these issues.

Applied social exchange theory could be expanded to account for Internet users' reluctance to freely express their thoughts and opinions online. Further research could explore the factors that inhibit users from expressing controversial viewpoints and factors that encourage such expression online.

In future, the correlation between the studied factors and additional demographic factors will be analyzed as well as a regression analysis of these factors against them. This research will continue to determine the effects of some independent variables (e.g., income and ICT expertise) on hypothesis H1. The work will explore the relationship of certain demographic variables to personal cybersecurity spending and to any reluctance to express oneself online. Subject to available survey data, analysis for geographical region clustering and other clustering may be performed.

Appendix 1

Table 4: Survey questions comprising the Loss of Money (LoM) component

Loss of Money (LoM) (has spent money, or positive attitude toward spending)
1. I have paid for security software that was not already included in my device.
2. It is worth spending money to sufficiently protect my device and software from security threats.
3. I have purchased security software for my device, such as an antivirus or firewall suite, or any software to protect my privacy, such as encryption software or data trail deletion software.
4. The amount of money it would cost to sufficiently protect my system and data from cyberattacks would be worth it.

Table 5: Survey questions comprising the Reluctance to Express (RtoEx, RtoExnonC, RtoExC) component

Reluctance to Express (RtoEx) (Reluctance to Express, with or without mention of consequences)
1. I would never post a controversial message in an online forum.
2. If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.
3. I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc.) online.
4. It's usually not a good idea to post controversial comments or opinions online.
5 I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.
6. I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.
7. When discussing something with a good friend, I feel more safe to express controversial opinions face-to-face than by electronic communication.
8. I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.

References

Bandyopadhyay, S. (2011) 'Antecedents And Consequences Of Consumers Online Privacy Concerns', *Journal of Business & Economics Research (JBER)*, 7(3). doi: 10.19030/jber.v7i3.2269.

Baroni, D. (2015) 'New Zealand Government To Punish Online Trolls With Prison Time', *Reaxxion.com*, 3 July. Available at: http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time (Accessed: 24 January 2019).

Booth, R. E. (2017) 'The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations.', in *Proceedings of the 23nd Americas Conference on Information Systems*.

Cassidy, P. (2017) 'Man petrol bombed homes in revenge for Facebook post', *STV News*, 3 November. Available at: https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/ (Accessed: 24 January 2019).

Chen, Y.-H., Hsu, I.-C. and Lin, C.-C. (2010) 'Website attributes that increase consumer purchase intention: A conjoint analysis', *Journal of Business Research*, 63(9–10), pp. 1007–1014. doi: 10.1016/j.jbusres.2009.01.023.

Cooper, A. K. (2000) 'China: Government punishes Internet journalists', *Committee to Protect Journalists*, 12 July. Available at: https://cpj.org/2000/07/china-government-punishes-internet-journalists.php.

Curtom, G. (2014) 'Students punished for expressing free speech on Twitter', *The Cougar*, 24 April. Available at: http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/ (Accessed: 24 January 2019).

Emarketer.com (2014) 'Worldwide Ecommerce Sales to Increase Nearly 20% in 2014 - eMarketer', *Emarketer.com*. Available at: https://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039 (Accessed: 24 January 2019).

Hazari, S. and Brown, C. (2013) 'An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites', *Journal of Information Privacy and Security*, 9(4), pp. 31–51. doi: 10.1080/15536548.2013.10845689.

Jaschik, S. (2014) 'Interview with professor fired by West Bank university who compares himself to Steven Salaita', *Inside Higher Ed*, 15 September. Available at: https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita (Accessed: 24 January 2019).

Liu, Z. *et al.* (2016) 'Self-disclosure in Chinese micro-blogging: A social exchange theory perspective', *Information & Management*, 53(1), pp. 53–63. doi: 10.1016/j.im.2015.08.006.

Mony, S. (2017) 'Cambodian Netizens Face New Risks as Government Tightens Online Controls', *VOA*, 11 November. Available at: https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html (Accessed: 24 January 2019).

Morgan, S. (2017) 'The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more.', *Cybersecurity Ventures*. Available at: https://cybersecurityventures.com/cybersecurity-market-report/ (Accessed: 24 January 2019).

Nadi, Y. and Firth, L. (2004) 'The Internet Implication in Expanding Individual Freedom in Authoritarian States', in *ACIS 2004 Proceedings*. *ACIS 2004* (94).

Regan, P. M., FitzGerald, G. and Balint, P. (2013) 'Generational views of information privacy?', *Innovation: The European Journal of Social Science Research*, 26(1–2), pp. 81–99. doi: 10.1080/13511610.2013.747650.

Sheehan, K. B. (2002) 'Toward a Typology of Internet Users and Online Privacy Concerns', *The Information Society*, 18(1), pp. 21–32. doi: 10.1080/01972240252818207.

Sims, J. and Xu, L. (2012) 'Perceived Risk of Online Shopping: Differences Between the UK and China', in *UK Academy for Information Systems Conference Proceedings*.

Vasquez, I. and Porcnik, T. (2017) *The Human Freedom Index 2017: A Global Measurement of Personal, Civil, and Economic Freedom*. Washington, D.C.: Cato Institute, Fraser Institute, and the Friedrich Naumann Foundation for Freedom.

P II

DOES TIME SPENT ON DEVICE SECURITY AND PRIVACY INHIBIT ONLINE EXPRESSION?

by

Juhani Rauhala, Pasi Tyrväinen & Nezer Zaidenberg 2019

ECCWS 2019 : Proceedings of the 18th European Conference on
Cyber Warfare and Security

Does Time Spent on Device Security and Privacy Inhibit Online Expression?

Juhani Rauhala[1], Pasi Tyrväinen[1] and Nezer Zaidenberg[2]
[1]University of Jyväskylä, Finland
[2]College of Management Academic Studies, Rishon LeZion, Israel
juhani.jr.rauhala@jyu.fi
pasi.tyrvainen@jyu.fi
scipio@scipio.org

Abstract: Freedom of expression is a recognized human right. More recently, the UN has resolved that unrestricted access to the Internet is also a human right. A commonly accepted benefit of the Internet is that it serves as a platform for free expression. Usage of the Internet for free expression can be a way of circumventing censorship or other hindrances that prevent citizens' freedom of expression in more traditional publishing media. However, the Internet has unique security and privacy risks that may affect users' attitudes toward expressing themselves online. In the online environment, users with controversial viewpoints may be reluctant to express the viewpoints due to concern about possible consequences resulting from the expressions. Consequences may be imposed by individuals, groups, organizations, businesses, or nation-states. In order to mitigate the security and privacy risks of the Internet, some Internet users spend valuable time thinking about and configuring the security settings of their devices. Some users may have a negative attitude toward such time expenditure. Users may be reluctant to express themselves online simply because it costs too much time and effort for proper configuration for anonymity. That is, the users may be aware of the importance and abundance of tools providing anonymity and may wish to express themselves online but decide spending time on anonymity is just too much effort. The association of time spent on personal cybersecurity with the reluctance to express online does not appear to have been studied in prior research. The purpose of this paper is to explore the effects of these issues on users' reluctance to express themselves online. We constructed a model to represent our hypotheses and collected data using a survey. We then validated the model by performing factor and correlation analyses on the collected data. The results of this research show that the attitude of users toward time expenditure on device security aspects correlates with users' reluctance to express themselves online.

Keywords: device security, time consumption, online expression, device settings, frustration

1. Introduction

Freedom of expression has been declared a universal human right (UN General Assembly, 1948). As of 2016, the United Nations has resolved that unrestricted access to the Internet is also a human right (UN Human Rights Council, 2016). A commonly accepted benefit of the Internet is that it serves as a platform for free expression. However, there are potential consequences for users who make controversial or provocative expressions over the Internet from other users and organizations participating in or following the communication (Baroni, 2015; Cassidy, 2017; Jaschik, 2014).

Users' concerns about such consequences may have an inhibiting effect on their usage of the Internet for free expression. This inhibiting effect may correlate with what users believe and how users behave with respect to addressing security and privacy issues of their devices. The inhibiting effect may also correlate with users' attitude toward and perception of the time they spend addressing their devices' security and privacy issues. However, the association between online expression aspects and the perception of time consumption on security aspects is lacking in prior research. Users may be reluctant to express themselves online simply because it costs too much time and effort for proper configuration for anonymity. That is, the users may be aware of the importance and abundance of tools providing anonymity and may wish to express themselves online but decide spending time on anonymity is just too much effort.

This leads to the main goal of this research; that is, to examine users' reluctance to express themselves in relation to their attitudes and perceptions regarding the time and effort they invest on security, i.e., the time spent on security aspects. This is relevant to participation in social media and other online expression contexts. To achieve the research goal, we establish three latent factors: one corresponding to a reluctance to self-express online, one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount ("too much") of one's time, and one for time considering device cybersecurity and privacy settings aspects. We then analyze the correlation among these factors and the correlation between these factors and related demographic factors. We also perform a linear regression of one latent factor against the others and against a demographic factor.

2. Background

The emerging research of Booth (2017) has raised attention to the issue of freedom of expression and the laws and norms thereof in terms of their relationship to the benefits of ICT on national well-being. At present, Booth has not yet completed her research; moreover, the research will not consider the relationship between the expression of free speech on aspects of the individual user. Internet communication is largely beyond the territorial control of the nation-state and access to the Internet has been recognized as important to the freedom of expression and to participation in a democracy (Lucchi, 2011). Previous research has established that usage of the Internet for free expression can be a way of circumventing censorship or other hindrances that prevent citizens' freedom of expression in more traditional publishing media, especially in authoritarian regimes (Nadi and Firth, 2004).

Debate and discussions that occur over online forums and social media, such as Twitter and Facebook, are raising attention to a virtually unlimited array of topics. Importantly, socially controversial topics and political topics are also discussed. Certain organizations consider and evaluate various threats to the freedom of expression online (Stanton, 2014). In oppressive states, free expression enabled by access to the Internet can be particularly important for advancing human rights (Nadi and Firth, 2004). However, there are potential consequences for users who make controversial or provocative expressions on the Internet, including a negative reaction from the government (Baroni, 2015; Cooper, 2000; Mony, 2017) and offended individuals (Cassidy, 2017), employers (Jaschik, 2014), and schools (Curtom, 2014). Participating in social media is a form of individual expression and there is some research-in-progress on the effects of perceived security threats on user's social media behaviour (Alqubaiti, Li, and He, 2016).

The time that Internet users spend on performing self-protective cybersecurity and privacy-related tasks detracts from the amount of time users have available for other preferred activities. For example, when using open WiFi connectivity in a public space or vehicle, spending time connecting to a secure VPN or updating the security software will leave less time for messaging and for checking social media updates. The excess use of time spent waiting can be merely a perception but may still have negative consequences in terms of user experience or perception of the services for which the waiting is done (Dellaert and Kahn, 1999). Another study has been performed to determine how consumers react when web pages of shopping websites take too much time to load (Anonymous, 2010). It found that 70% of respondents reported that they abandon shopping on a site if the site takes more than 10 seconds to load and 35% said they would not return if the loading delays take “too long.” On the other hand, the tolerance of users to the amount of time spent waiting will vary according to the individual and the context (Katz and Martin, 1989). During Internet usage, a loading delay may be experienced with most mouse-clicks or screen taps. However, the need to spend time waiting for a security software update process to complete occurs relatively infrequently, e.g. weekly or monthly.

Excessive non-ideal time consumption, therefore, can be said to detract from more desirable activities and may cause a negative perception of offerings associated with waiting. Frustration with excessive time consumption can result in a negative attitude toward, and possibly abandonment of, desirable online content and activities.

There are also studies observing the impact of demographic factors, such as nationality and age, on Internet behaviour that are relevant to this study. Regan, FitzGerald, and Balint (2013) have evaluated attitudes toward information privacy between age groups (specifically generations). Their analysis revealed a trend where younger generations tend to be more concerned than older ones about wiretapping and data privacy. Chen, Hsu, and Lin (2010) determined that consumers with different levels of computer expertise have different preferences for attributes of shopping websites. Research into culture-based differences in perception of risk for online shopping and other tasks has yielded conflicting results (Sims and Xu, 2012). Sims and Xu (2012) found no significant difference between UK and Chinese shoppers' perceived risk of online shopping despite those shoppers' differing cultural backgrounds. This conclusion was against their expectations and the contradicted results from prior research that showed differences in risk-aversion between the two cultures (Hofstede, 1980).

Controversial expression in an online communications context is affected by other factors. Such factors include perceived anonymity and familiarity with other online community participants (Luarn and Hsieh, 2014). Luarn and Hsieh studied the expression behaviour of users in a laboratory-controlled virtual community. The virtual community simulated different online group communications environments. They found that users were more willing to express controversial opinions when their identities were anonymous or when they were familiar with other members of the community. When users in the study were not anonymous, they were more reluctant to express such opinions. They also found that there was no effect of anonymity or member familiarity on users' willingness to express non-controversial opinions.

Prior research has shown that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications and found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome.

We expand prior research by investigating the correlation between perception of time consumption used for addressing device cybersecurity and the willingness to freely express on the Internet. Negative expressions (e.g., unpleasant or aggressive) can result in unwanted consequences. Internet users may be reluctant to express themselves because of concerns about such consequences. The time they spend on personal cybersecurity issues may further discourage their controversial expressionism. We hypothesize that users who feel they spend excessive time on their devices' cybersecurity and privacy aspects are more reluctant to freely express themselves online. This is relevant to the users' participation in social media and other online expression contexts.

3. Research model

It is important to consider users' attitudes toward free expression on the Internet and the possible consequences of reluctance to freely express. A key goal of our research is the examination of users' reluctance to express themselves in this context in relation to their attitude and perception regarding time consumption for their devices' security and privacy aspects. Previous research has considered implications on free expression and the benefits of free expression. Willingness to express opinions online has been measured in terms of a web forum's view/reply ratio (Shen and Liang, 2015) and by asking users how likely they would be to express their opinions in specified online scenarios using a 0-100% or 0-10 scale (Ho and McLeod, 2008; Stoycheff, 2016). Hayes et al. (2005) established a self-reporting tool consisting of eight five-point Likert questions to measure willingness to self-censor. However, the tool's questions pertain to a general social context and not specifically to self-expression of controversial opinions on the Internet. Attempts to measure a reluctance to express on the Internet or to establish the same as a latent factor seem to be lacking in previous research. Therefore, our research model defines as a latent factor "reluctance to freely express oneself on the Internet," (RtoEx) for analyzing responses to a set of indicator questions asked in a survey. This factor enables analysis for correlations and the performance of other analyses against other variables or factors.

Time per se is easily quantifiable; however, customers' or Internet users' attitudes or perceptions about the quantity or utility of their time usage are more difficult to define. Prior research has considered the consequences of excessive wait times on customers' attitudes. Prior research has also considered the consequences on Internet users of excessive time spent on the Internet. There seems to be no previous research to consider a user's attitudes and perceptions toward their time usage dedicated to the security and privacy aspects of their Internet device. Our model introduces two latent factors to address this gap: one to measure the belief that addressing device security and privacy aspects negatively impacts one's experience (or takes "too much time") and one to measure whether the user has thought about the security and privacy aspects of his/her device and has checked (and optionally changed) its security and privacy settings. These factors are established by responses to indicator questions that were implemented in a survey. We denote these factors TMT (from "too much time") and TChS (from Thinking about and Changing Settings), respectively. TMT and TChS enable easier analysis for research that seeks to analyze or study the concepts in relation to other variables.

When users contemplate, check, or adjust their device's security and privacy settings out of a sense of obligation instead of preference, the user may experience the corresponding time expenditure negatively. The user may think "this takes too much time" or even "this is a waste of time." We expect that this related cognizance of cybersecurity and privacy risks will be reflected by their attitude toward freely expressing themselves online and on their willingness to do so. We want to see if the resultant frustration from a personal experience-based belief or perception that cybersecurity threat amelioration requires excessive personal investment of time, may inhibit the willingness to freely express oneself on the Internet.

Conversely, users' reluctance to express online may correlate with their belief of whether addressing security and privacy issues requires an excessive amount of time. These effects may differ across certain demographic groupings, including cultural groupings. We will attempt to explain such differences. It is possible that misgivings in users about the Internet as a platform for free expression may correlate with the belief (or perception) of these same users regarding the need for excessive time to address security and privacy aspects. Such aspects include the contemplation, examination, and adjustment of the relevant device settings.

This paper uses as a general basis the Antecedents -> Privacy Concerns -> Outcomes (APCO) research model defined by Smith, Dinev, and Xu (2011). Variations of the APCO model or models similar to APCO have been applied in other pertinent works in the field, e.g., by Benamati, Ozdemir, and Smith (2017), and by Bandyopadhyay (2009). Our work may be described by way of comparison to Bandyopadhyay's 2009 framework. In Bandyopadhyay's framework there are three consequences, or outcomes, of users' privacy concerns: 1. Refusing to provide personal information, 2. Refusing to enter e-commerce transactions, and 3. Refusing to use the Internet. While Bandyopadhyay's framework has implications for online marketers (Bandyopadhyay, 2009), ours presumes implications for individuals' online expression. In our variation of the framework, we specify one outcome - a reluctance to freely express oneself on the Internet. In place of "privacy conerns" in Bandyopadhyay's proposed framework, we use "usage or perceived excessive usage of time addressing device privacy and security aspects." With regard to the antecedents in Bandyopadhyay's model, we instead propose to use the demographic factors of age, ICT expertise and income as independent variables for a regression analysis between latent factors.

We establish three latent factors: one corresponding to a reluctance to self-express online (RtoEx), one corresponding to a belief that handling security and privacy aspects of one’s device requires an excessive amount of one’s time (TMT, from “too much time”), and one corresponding to the performance of checking and changing device privacy and security settings (TChS, from “think about and change settings”). We then analyze the correlation among these factors and the correlation between these factors and the related demographic factors. We also plan to examine the effects of demographic factors on the correlation between the two latent factors. The demographic factors include age, income, ICT experience, and nationality.

We have established three factors pertinent to the model:

Reluctance to Express (RtoEx): reluctance to freely self-express online

Too Much Time (TMT): belief that cybersecurity risk amelioration requires excessive usage of one’s time

Think Change Settings (TChS): time considering two aspects of one’s ICT device – contemplation of the device’s cybersecurity aspects and whether time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

The hypotheses are (Figure 1):

H1: TMT will positively correlate with RtoEx.

H2: TChS will positively correlate with RtoEx.

H3: H1 will vary by age, level of ICT expertise, and/or income.

H4: H2 will vary by age, level of ICT expertise, and/or income.

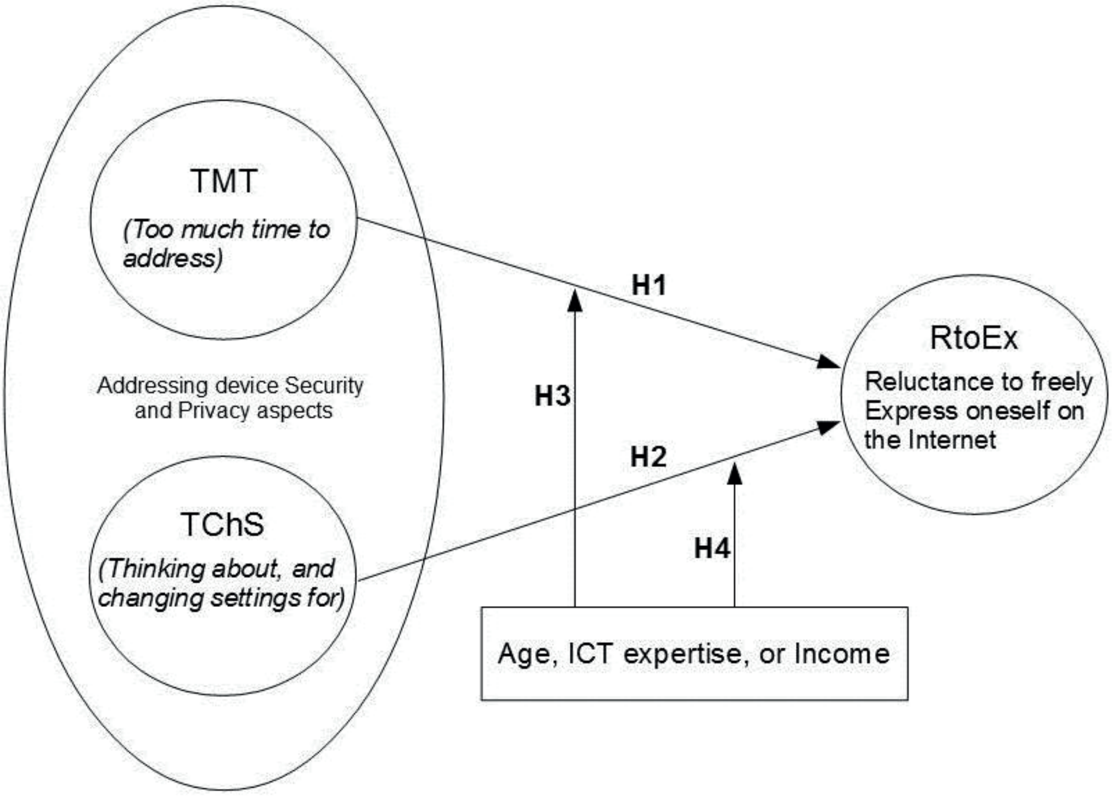

TMT
(Too much time to address)
Addressing device Security and Privacy aspects
TChS
(Thinking about, and changing settings for)
H1
H3
H2
H4
RtoEx
Reluctance to freely Express oneself on the Internet
Age, ICT expertise, or Income

Figure 1: Latent variables TMT, TChS, and RtoEx; and the independent variables

3.1 Latent factors and their indicators

In this study, we defined sets of indicator questions from which each of the latent variables was derived. The indicator questions were included in the survey, and each consisted of responses along a five-point Likert scale from "strongly agree" to "strongly disagree." The questions for TMT were as follows: five questions to assess the perception that excessive time has been spent addressing device security and privacy issues, and a belief that time spent on device security and privacy aspects has detracted from time intended for other tasks. TChS is established with three questions to assess whether the user has contemplated and checked (and perhaps adjusted) their device's security and privacy settings. Cumulatively, we suggest the five "too much time" indicator questions imply that the respondent spends time contemplating and actively addressing security and privacy aspects but tends to feel negatively about doing so ("too much time" implies that the amount of time required is excessive and detracts from activities for which the respondent could preferably be using their time).

The questions for the RtoEx variable were designed as follows: the questions ascertain the attitude of the respondent toward theoretical scenarios of their posting controversial opinions or artwork online, including one question to ascertain their attitude toward using electronic methods vs. face-to-face communication for discussion of a sensitive topic with a friend. We suggest that this set of RtoE indicator questions can convey the level of the respondent's reluctance to openly communicate using electronic methods including the Internet.
For data gathering, a survey was administered over the Web to a population composed mainly of university students and working adults. 197 responses have been obtained, of which 131 are from Finnish nationals.

We use an Exploratory Factor Analysis with direct oblimin rotation to extract latent components from a set of survey questions. The set pertains to TMT, TChS, and RtoEx. The results for TMT and TChS confirm two components. Review of the corresponding survey questions indicates that the TMT and TChS responses are differentiated by the mention of security issues detracting time from preferred tasks, or by a belief that addressing security issues takes too much of one's time (Appendix, Table 5). Thus, we use three latent factors: RtoEx, TMT, and TChS. We performed a Spearman correlation analysis on the indicator question responses corresponding to RtoEx (eight questions), TMT (five questions), and TChS (three questions). Within all three groups of latent variables, we found that the responses have a high correlation. For the RtoEx questions (Appendix, Table 4), we found the lowest correlation to be .199, and the highest .673, both two-star significant at the .01 level (two-tailed). For the TMT questions (Appendix, Table 5), the lowest two-tailed correlation was .223 (two-star) and the highest was .752 (two-star). For TChS (Appendix, Table 5), the lowest two-tailed correlation was .314 and the highest .481, both two-star significant. Based on these correlations and on the factor analysis results, we used the means of the responses for each question set. The representative values of latent factors were calculated as averages of responses to the indicator statements. We used SPSS statistical software to calculate Pearson correlations between the three latent variables as well as the Cronbach's alphas (Table 1). The Cronbach's alpha values show an acceptable reliability between the latent variables' indicators.

Table 1: Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alpha

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
RtoEx	.199**	.673**	.384	.831
TChS	.314**	.481**	.403	.668
TMT	.223**	.752**	.404	.770

4. Results

The results in Table 2 show that reluctance to express oneself online correlates positively with a long-perceived time spent on setting device security settings (.220**) but not significantly with time spent thinking about device security settings. Thus, we can confirm hypothesis H1 and reject hypothesis H2. Out of the potential moderating variables, we found direct negative correlation between reluctance to express and age (-.225**) but not with other background variables. In a linear regression analysis, the same factors (TMT and age) together reached significant correlation (adjusted R squared = .075, p-value = .000), thus H3 is confirmed for age. Other factors added did not reach significant correlations. Analysis of moderating effects of other demographic variables for H3 will be elaborated in forthcoming research. Table 3 presents the percentage of respondents tending to agree with TMT, TChS, and RtoEx.

Table 2: Pearson correlations between RtoEx and TMT, TChS, and age. Two-tailed significances: * to 0.05 level, ** to 0.01 level

n=197	Device security/privacy takes "too much time" (TMT)	Spend time thinking about and changing settings (TChS)	Age (15-25, 26-36, 37-44, 45-54, 55-64, or 65+)
RtoEx	.220**	.077	-.225**

Table 3: Percentages of respondents who tend to agree or strongly agree with TMT, TChS, and RtoEx

Overall addressing security and privacy aspects takes too much time (TMT)	Overall spend time thinking about device security and check/change settings (TChS)	Reluctant to express online (RtoEx)
27.4%	59.9%	57.4%

5. Summary, discussion, and conclusion

In this study, our first goal was to establish three latent factors; one corresponding to a reluctance to self-express online, RtoEx; one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount of one's time, TMT; and one for time considering device cybersecurity and privacy settings aspects, TChS. Based on the factor analysis of the responses to the indicator statements, this was established.

Our second goal was to analyze the correlation between these factors and the correlation between these factors and the related demographic factors. With respect to the 197 responses from our initial survey, the factor correlations were determined as was the correlation between the reluctance to express and age. We found that RtoEx is positively correlated with TMT. The correlation of RtoEx with age is consistent with Regan, Fitzgerald, and Balint's (2013) findings that older users tend to be less concerned about anonymity and privacy. A linear regression was also performed with the age moderator. We found that older users are less reluctant to express themselves online, and are less likely to consider the time that they use for device security and privacy to be excessive.

Our work has not confirmed a causal relationship between TChS or TMT, and RtoEx. Nonetheless, there are some steps that governments and industry could take to improve Internet users' perceptions of online safety. Nation-states that respect free online expression as a fundamental right for their citizens may choose to create and implement cybersecurity strategies and regulations that improve their citizens' perceptions of the level of online safety. In this way, their citizens may perceive a reduced need to spend time addressing their device settings or their cybersecurity software, and thus an improved opportunity to express themselves online or to perform other preferred tasks. The personal cybersecurity products and services industry could design device security and privacy safeguards to be easier to understand and adjust, and to automate more functions to the background of device or software UIs. Thus, device security and privacy aspects would (ideally) be less time-consuming for consumers to address. However, there may not be clear economic motivations for the cybersecurity industry to modify their consumer products and services in such a manner.

This paper reports results while further analysis is still to be done. We looked into the impact of age on the reluctance to express online, but we have not yet done the full analysis of other moderating demographic factors that can have an impact on it. That is left for further analysis.

In our analysis, we also observe differences between nationalities in the responses. One direction to search for potential explanation is cultural differences (Hofstede, 1980). However, with the current number of responses from non-Finnish respondents, we cannot evaluate this alternative without collecting further data. Other potential sources of explanation include the variation of national social media cultures as well as variations in attitudes and actions of enterprises and public institutions on and to individuals expressing non-controversial opinions online. An extension of this research can be to explore topics about which users are less inclined to express their opinion online.

In addition to the relatively low quantity of responses from non-Finnish nationals, this survey has other limitations. The survey was implemented only in English. English is not the native language of most respondents. Our study also does not examine how, in the case of waiting, the management of time affects the perspective of the person waiting. Examples of such cases could be the users' management of the time spent waiting for a security software update to install; or the content displayed on screen by the software during the update (Hanyang, et al., 2015).

Appendix 1

Table 4: Survey questions to indicate level of reluctance to express (RtoEx)

1. I would never post a controversial message in an online forum.
2. If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.
3. I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc.) online.
4. It's usually not a good idea to post controversial comments or opinions online.
5 I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.
6. I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.
7. When discussing something with a good friend, I feel more safe to express controversial opinions face to face, than by electronic communication.
8. I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.

Table 5: Survey questions to indicate that the user contemplates device security aspects (TChS), and perception or belief that dealing with them requires too much of one's time (TMT)

1. When using my computer or smartphone, I spend time making sure that its security software is up to date. (TChS)
2. When I begin using a new computer or smartphone, I first check its privacy settings, and adjust them to my preference. (TChS)
3. I have had less time to finish a task I wanted to do, due to a device security or software security issue. (TMT)
4. It has taken me longer to finish a task I wanted to do, due to a device security or software security issue. (TMT)
5. The security alerts and pop-up notifications of security software take too much time to deal with. (TMT)
6. I have spent a lot of time thinking about my device and software security. (TChS)
7. I would spend more time performing online tasks I want to do, but my device and software security often needs to be considered. (TMT)
8. Device and software security issues take up much of my time. (TMT)

References

Alqubaiti, Z., Li, L. and He, J. (2016) 'The Paradox of Social Media Security: Users' Perceptions versus Behaviors', in *Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16*. *the 5th Annual Conference*, Boston, Massachusetts, USA: ACM Press, pp. 29–34. doi: 10.1145/2978178.2978187.

Anonymous (2010) 'KEEPING ONLINE CUSTOMERS', *Dealerscope*, January, p. 26.

Baroni, D. (2015) 'New Zealand Government To Punish Online Trolls With Prison Time', *Reaxxion.com*, 3 July. Available at: http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time (Accessed: 24 January 2019).

Booth, R. E. (2017) 'The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations.', in *Proceedings of the 23nd Americas Conference on Information Systems*.

Bandyopadhyay, S. (2009) 'Antecedents And Consequences Of Consumers Online Privacy Concerns', *Journal of Business & Economics Research (JBER)*, 7(3). doi: 10.19030/jber.v7i3.2269.

Benamati, J. H., Ozdemir, Z. D. and Smith, H. J. (2017) 'An empirical test of an Antecedents – Privacy Concerns – Outcomes model', *Journal of Information Science*, 43(5), pp. 583–600. doi: 10.1177/0165551516653590.

Cassidy, P. (2017) 'Man petrol bombed homes in revenge for Facebook post', *STV News*, 3 November. Available at: https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/ (Accessed: 24 January 2019).

Chen, Y.-H., Hsu, I.-C. and Lin, C.-C. (2010) 'Website attributes that increase consumer purchase intention: A conjoint analysis', *Journal of Business Research*, 63(9–10), pp. 1007–1014. doi: 10.1016/j.jbusres.2009.01.023.

Cooper, A. K. (2000) 'China: Government punishes Internet journalists', *Committee to Protect Journalists*, 12 July. Available at: https://cpj.org/2000/07/china-government-punishes-internet-journalists.php (Accessed: 24 January 2019).

Curtom, G. (2014) 'Students punished for expressing free speech on Twitter', *The Cougar*, 24 April. Available at: http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/ (Accessed: 24 January 2019).

Dellaert, B. G. C. and Kahn, B. E. (1999) 'How tolerable is delay?: Consumers' evaluations of internet web sites after waiting', *Journal of Interactive Marketing*, 13(1), pp. 41–54. doi: 10.1002/(SICI)1520-6653(199924)13:1<41::AID-DIR4>3.0.CO;2-S.

Hayes, A. F. (2005) 'Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research', *International Journal of Public Opinion Research*, 17(3), pp. 298–323. doi: 10.1093/ijpor/edh073.

Ho, S. S. and McLeod, D. M. (2008) 'Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication', *Communication Research*, 35(2), pp. 190–207. doi: 10.1177/0093650207313159.

Hofstede, G. (1980) *Culture's Consequences: International Differences in Work-Related Values*. 1st edn. Beverly Hills: Sage Publications.

Jaschik, S. (2014) 'Interview with professor fired by West Bank university who compares himself to Steven Salaita', *Inside Higher Ed*, 15 September. Available at: https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita (Accessed: 24 January 2019).

Katz, K. L. and Martin, B. R. (1989) *Improving customer satisfaction through the management of perceptions of waiting*. Massachusetts Institute of Technology. Available at: http://hdl.handle.net/1721.1/37703 (Accessed: 24 January 2019).

Kwon, O., Kim, C. and Kim, G. (2013) 'Factors affecting the intensity of emotional expressions in mobile communications', *Online Information Review*. Edited by K. Chang Lee, 37(1), pp. 114–131. doi: 10.1108/14684521311311667.

Luarn, P. and Hsieh, A.-Y. (2014) 'Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities', *Online Information Review*, 38(7), pp. 881–895. doi: 10.1108/OIR-03-2014-0076.

Lucchi, N. (2011) ‘Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression’, *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, 19(3), pp. 645–678.

Mony, S. (2017) ‘Cambodian Netizens Face New Risks as Government Tightens Online Controls’, *VOA*, 11 November. Available at: https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html (Accessed: 24 January 2019).

Nadi, Y. and Firth, L. (2004) ‘The Internet Implication in Expanding Individual Freedom in Authoritarian States’, in *ACIS 2004 Proceedings*. *ACIS 2004* (94).

Regan, P. M., FitzGerald, G. and Balint, P. (2013) ‘Generational views of information privacy?’, *Innovation: The European Journal of Social Science Research*, 26(1–2), pp. 81–99. doi: 10.1080/13511610.2013.747650.

Shen, F. and Liang, H. (2015) ‘Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies’, *International Journal of Public Opinion Research*, 27(1), pp. 111–124. doi: 10.1093/ijpor/edu012.

Sims, J. and Xu, L. (2012) ‘Perceived Risk of Online Shopping: Differences Between the UK and China’, in *UK Academy for Information Systems Conference Proceedings*.

Smith, Dinev and Xu (2011) ‘Information Privacy Research: An Interdisciplinary Review’, *MIS Quarterly*, 35(4), p. 989. doi: 10.2307/41409970.

Stanton, L. (2014) ‘EFFECT OF “RIGHT TO BE FORGOTTEN” ON FREE EXPRESSION SPARKS DEBATE’, *Cybersecurity Policy Report*, 18 August.

Stoycheff, E. (2016) ‘Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring’, *Journalism & Mass Communication Quarterly*, 93(2), pp. 296–311. doi: 10.1177/1077699016630255.

UN General Assembly (1948) *Universal Declaration of Human Rights*. Paris (217 A). Available at: https://www.un.org/en/universal-declaration-human-rights/index.html (Accessed: 24 January 2019).

UN Human Rights Council (2016) *Resolution on the promotion, protection and enjoyment of human rights on the Internet*. Geneva (A /HRC/ 3 2 /L . 20). Available at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (Accessed: 24 January 2019).

P III

ONLINE EXPRESSION, PERSONAL CYBERSECURITY COSTS, AND THE SPECTER OF CYBERCRIME

by

Juhani Rauhala, Pasi Tyrväinen & Nezer Zaidenberg 2019

Encyclopedia of Criminal Activities and the Deep Web

https://doi.org/10.4018/978-1-5225-9715-5.ch067

Online Expression, Personal Cybersecurity Costs, and the Specter of Cybercrime

Juhani Rauhala
University of Jyväskylä, Finland

Pasi Tyrväinen
https://orcid.org/0000-0001-7716-3244
University of Jyväskylä, Finland

Nezer Zaidenberg
College of Management Academic Studies, Israel

INTRODUCTION

The UN General Assembly has declared freedom of expression to be a universal human right (UN General Assembly, 1948). As of 2016, the United Nations has resolved that unrestricted access to the Internet is also a human right (UN Human Rights Council, 2016). A commonly accepted benefit of the Internet is that it serves as a platform for free expression. Importantly, political topics are also discussed as well as other topics without socially accepted savoir faire. However, there are potential consequences for users who make controversial or provocative expressions over the Internet from other users and organizations participating in or following the communication (Baroni, 2015; Cassidy, 2017; Jaschik, 2014). Such consequences may also be in the form of illegal doxing or hacking attacks by cybercriminals.

Users' concerns about such consequences may have an inhibiting effect on their Internet usage for free expression. This inhibiting effect may correlate with what users believe and how users behave concerning addressing security and privacy issues of their devices. The inhibiting effect may also correlate with users' attitude toward and perception of the time they spend addressing their devices' security and privacy issues. However, the association between online expression aspects and the perception of time consumption on security aspects is lacking in prior research. Users may be reluctant to express themselves online simply because anonymity costs too much time and effort. That is, the users may be aware of the importance and abundance of tools providing anonymity and may wish to express themselves online but decide that spending time on anonymity is just too much effort. Concern about such consequences may not only have an inhibiting effect on users' use of the Internet for expression but it may also correlate with their desire to purchase personal cybersecurity products and anonymizing services.

Another generally accepted beneficial use of the Internet is as a platform for commerce, which is continuously increasing (Emarketer.com, 2014). At the same time, spending by consumers and businesses on cybersecurity products and services is also increasing (Morgan, 2017). It is reasonable to expect that users purchase a significant proportion of personal cybersecurity software online. It is possible that misgivings of users about the Internet as a platform for free expression may correlate with increased Internet utilization by those same users for commerce in personal cybersecurity products and services. This article explores this somewhat paradoxical relationship given that the Internet is seen as an overall good for humanity. It leads to a focus of this chapter; that is, to the consideration of users' reluctance

DOI: 10.4018/978-1-5225-9715-5.ch067

to express themselves in relation to their attitudes and perceptions regarding the time and money they invest in security. This is relevant to participation in social media and other online expression contexts.

To facilitate research and discussion on this topic, six latent factors are elucidated: three corresponding to a reluctance to self-express online, one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount ("too much") of one's time, and one for time considering device cybersecurity and privacy settings aspects. The sixth factor corresponds to a positive predilection toward personal spending to enhance personal cybersecurity. The correlation among two of these factors is then analyzed. A linear regression of one latent factor against the other and against a demographic factor is also performed.

This chapter presents an overview of related research, followed by a description of a proposed research model. It then establishes the general latent factors. Some results are presented and discussed, followed by a description of future research suggestions, and a conclusion.

BACKGROUND

Previous research has considered implications on free expression and the benefits of free expression. Willingness to express opinions online has been measured in terms of a web forum's view/reply ratio (Shen & Liang, 2015) and by asking users how likely they would be to express their opinions in specified online scenarios using a 0-100% or 0-10 scale (Ho & McLeod, 2008; Stoycheff, 2016). Hayes et al. (2005) established a self-reporting tool consisting of eight five-point Likert questions to measure willingness to self-censor. However, the tool's questions pertain to a general social context and not specifically to self-expression of controversial opinions on the Internet. Attempts to measure a reluctance to express on the Internet or to establish the same as a latent factor are lacking in previous research.

The emerging research of Booth (2017) has raised attention to the issue of freedom of expression and the laws and norms thereof in terms of their relationship to the benefits of ICT on national well-being. However, her research does not consider the relationship between the expression of free speech on aspects of the individual user. Internet communication is largely beyond the territorial control of the nation-state and access to the Internet has been recognized as important to the freedom of expression and to participation in a democracy (Lucchi, 2011). Previous research has established that usage of the Internet for free expression can be a way of circumventing censorship or other hindrances that prevent citizens' freedom of expression in more traditional publishing media, especially in authoritarian regimes (Nadi & Firth, 2004).

Prior research has shown that many states have begun imposing online surveillance upon their citizens by way of legislative acts or other means (Ray & Kaushik, 2017). The research suggests that the ostensible justifications for such surveillance, such as cyberterrorism or cybercrime, are questionable and disproportional to the scope of the surveillance desired by the state. Such surveillance does not directly restrict online expression but it can create hesitation or concern in the user. The user may hesitate to criticize the state or its policies in an online forum due to fear of being surveilled. Many states also impose varying levels of censorship and controls on online expression (Ray & Kaushik, 2017).

Debate and discussions that occur over online forums and social media, such as Twitter and Facebook, are raising the attention to a virtually unlimited array of topics. Importantly, socially controversial topics and political topics are also discussed. Certain organizations consider and evaluate the various threats to the freedom of expression online (Stanton, 2014). In oppressive states, free expression enabled by access to the Internet can be particularly important for advancing human rights (Nadi & Firth, 2004).

However, there are potential consequences for users who make controversial or provocative expressions on the Internet, including a negative reaction from the government (Baroni, 2015; Cooper, 2000; Mony, 2017) and offended individuals (Cassidy, 2017), employers (Jaschik, 2014), and schools (Curtom, 2014). Consequences may also be exacted by vindictive criminal hackers. Cybercrime against individuals has been defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)" (Halder & Jaishankar, 2012). Victims may become a topic for cybercriminal gangs in the Deep Web or the target of doxing. "Revenge hacking" and doxing have caused serious consequences to victims (Branigan, 2011; Dascalescu, 2018). Participating in social media is a form of individual expression and there is some research-in-progress on the effects of perceived security threats on user's social media behavior (Alqubaiti et al., 2016).

Users spend significant time performing self-protective cybersecurity and privacy-related tasks. This time detracts from the amount of time users have available for other preferred activities. For example, when using open WiFi connectivity in a public space or vehicle, spending time connecting to a secure VPN or updating the security software will leave less time for messaging and for checking social media updates. The excess use of time spent waiting can be merely a perception but may still have negative consequences in terms of user experience or perception of the services for which the waiting is done (Dellaert & Kahn, 1999). Another study has been performed to determine how consumers react when web pages of shopping websites take too much time to load (Anonymous, 2010). It found that 70% of respondents reported that they abandon shopping on a site if the site takes more than 10 seconds to load and 35% said they would not return if the loading delays take "too long." On the other hand, the tolerance of users to the amount of time spent waiting will vary according to the individual and the context (Katz & Martin, 1989). During Internet usage, a loading delay may be experienced with most mouse-clicks or screen taps. However, the need to spend time waiting for a security software update process to complete occurs relatively infrequently, e.g. weekly or monthly.

Excessive non-ideal time consumption, therefore, can be said to detract from more desirable activities and may cause a negative perception of offerings associated with waiting. Frustration with excessive time consumption can result in a negative attitude toward, and possibly abandonment of, desirable online content and activities.

Controversial expression in an online communications context is affected by other factors. Such factors include perceived anonymity and familiarity with other online community participants (Luarn & Hsieh, 2014). Luarn and Hsieh studied the expression behavior of users in a laboratory-controlled virtual community. The virtual community simulated different online group communications environments. They found that users were more willing to express controversial opinions when their identities were anonymous or when they were familiar with other members of the community. When users in the study were not anonymous, they were more reluctant to express such opinions. They also found that there was no effect of anonymity or member familiarity on users' willingness to express non-controversial opinions.

Prior research has shown that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications. They found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome. Negative expressions (e.g., unpleasant or aggressive) can result in unwanted consequences. Internet users may be reluctant to express themselves because of concerns about such consequences. The time they spend on personal cybersecurity issues may further discourage their controversial expressionism.

It is of note that Booth and other researchers utilize the Human Freedom Index (HFI) (Vasquez & Porcnik, 2017). Included in the HFI measures are those that measure freedom of expression. Among those measures are "Laws and Regulations that Influence Media Content," "Political Pressures and Controls on Media Content," and "State Control over Internet Access." The measures of Laws and Regulations that Influence Media Content and Political Pressures and Controls on Media Content could be useful for this study on the condition that they are applied indirectly. That is to say, for example, that an assumption would be that an average user would feel some reluctance to freely express themselves as a result of the laws and controls. This study addresses reluctance more directly in the survey questions, whereas the subset of HFI measures does not measure reluctance to express. The HFI's "expression freedom" measures have not been examined for their relationship to personal cybersecurity spending. In particular, they do not measure concern regarding the consequences of personal free expression and neither have they been analyzed for their relationship to Internet users' attitudes and behaviors toward purchasing personal cybersecurity protections.

There are also studies observing the impact of demographic factors, such as nationality and age, on Internet behaviour that are relevant to this study. Regan, FitzGerald, and Balint (2013) have evaluated attitudes toward information privacy between age groups (specifically generations). Their analysis revealed a trend where younger generations tend to be more concerned than older ones about wiretapping and data privacy. Chen, Hsu, and Lin (2010) determined that consumers with different levels of computer expertise have different preferences for attributes of shopping websites. Research into culture-based differences in perception of risk for online shopping and other tasks has yielded conflicting results (Sims & Xu, 2012). Sims and Xu (2012) found no significant difference between the UK and Chinese shoppers' perceived risk of online shopping despite those shoppers' differing cultural backgrounds. This conclusion was against their expectations and the contradicted results from prior research that showed differences in risk-aversion between the two cultures (Hofstede, 1980).

Sheehan (2002) found that users' education and age correlate with their level of concern about online privacy. Hazari and Brown (2013) studied whether demographic variables can affect Internet users' privacy concerns and, thus, their attitudes toward using social networking sites. In contrast to the results from Sheehan and from Regan, Fitzgerald, and Balint, their research found that age was not correlated with online privacy concerns. Bandyopadhyay (2011) found that factors such as the level of Internet literacy, social awareness, and cultural background affect Internet users' online privacy concerns. He found that among the possible consequences of such concerns is an unwillingness to use the Internet. Liu et al. (2016) applied social exchange theory to examine perceived risks and rewards of individual users' self-disclosure in social media. The authors found that perceived privacy risk can reduce the willingness of social media users to disclose personal information. There does not seem to be existing research on social exchange theory applied to controversial expression by individual users online. Previous work has examined the effect on willingness to disclose information about oneself. Based on previous research, it can be hypothesized that the reluctance to express oneself on the Internet may be connected with concerns about the consequences. Further, reluctance to express oneself may lead to the use of cybersecurity as a means to protect oneself in these cases. However, there seems not to be previous results addressing this hypothesis.

Previous research has attempted to address the monetary and non-monetary costs of consumer-facing cybercrime (Riek & Böhme, 2018). The research focused on cybercrime incidents such as scams and payment fraud. The costs in Riek and Bohme's research are not the costs of the fear of consequences that could result from expressing oneself online. The feared consequences in the RtoEx subfactor of this study are unspecified and general. They may occur in varying forms including, but not limited to, cybercriminal attacks against the user.

The authors believe that it is important to consider the attitudes of users toward free expression on the Internet and possible consequences resulting from users' reluctance to freely express themselves on the Internet.

RESEARCH MODEL

This study proposes six latent factors: three corresponding to a reluctance to self-express online (RtoEx), one corresponding to a belief that handling security and privacy aspects of one's device requires an excessive amount of one's time (TMT, from "too much time"), and one corresponding to the performance of checking and changing device privacy and security settings (TChS, from "think about and change settings").

The factors are:

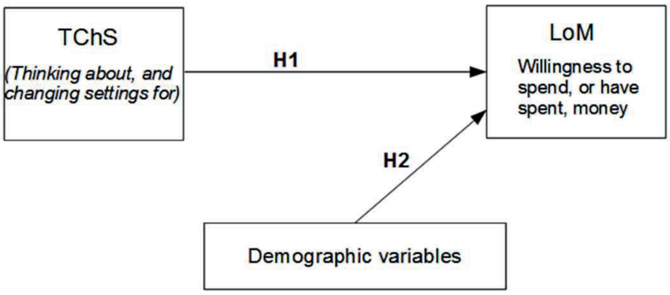
- **Reluctance to Express (RtoEx):** Reluctance to freely self-express online. The reluctance of expressing can be further divided into two factors based on inclusion or exclusion of consequences of the expression, RtoExC and RtoExnonC, respectively.
- **Reluctance to Express When Consequences Mentioned (RtoExC):** Reluctance to Express due to concerns of possible Consequences or safety; The reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.
- **Reluctance to Express When Consequences Not Mentioned (RtoExnonC):** Reluctance to Express when users are not reminded of possible Consequences or safety issues resulting from the expression.
- **Too Much Time (TMT):** The belief that cybersecurity risk amelioration requires excessive usage of one's time
- **Think Change Settings (TChS):** Time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether the time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.
- **Loss of Money (LoM):** Personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

As a demonstration, the authors hypothesize that those users who are conscientious about their online security and privacy will spend both time and money to ensure it. This should be reflected in a significant correlation between TChS and a positive attitude toward purchasing personal cybersecurity products and services (or LoM, for "Loss of Money")(Figure 1).

H1: TChS will be correlated with a positive attitude toward purchasing personal cybersecurity products and services (LoM).

H2: TChS combined with one or more demographic variables will predict LoM.

Figure 1. Latent variables TChS and LoM, and independent demographic variable(s)


TChS
(Thinking about, and changing settings for)
H1
LoM
Willingness to spend, or have spent, money
H2
Demographic variables

Latent Factors and Their Indicators

Each of the latent variables can be derived from sets of indicator questions. Indicator questions for TChS and LoM were included in a survey, and each consisted of responses along a five-point Likert scale from "strongly agree" to "strongly disagree." For data gathering, a survey was administered over the Web to a population composed mainly of Finnish university students and working adults. 191 responses were obtained.

The questions for TMT were as follows: five questions to assess the perception that excessive time has been spent addressing device security and privacy issues and a belief that time spent on device security and privacy aspects has detracted from time intended for other tasks. TChS is established with three questions to assess whether the user has contemplated and checked (and perhaps adjusted) their device's security and privacy settings (available from the authors). Cumulatively, the authors suggest the five "too much time" indicator questions imply that the respondent spends time contemplating and actively addressing security and privacy aspects but tends to feel negative about doing so.

The survey included questions on respondents' behaviors and attitudes regarding personal spending on cybersecurity. Latent variable Loss of Money (LoM) is defined by responses to a set of four indicator questions. The questions for LoM are designed as follows: two questions to ascertain whether the respondent/subject has purchased to enhance his cybersecurity and two questions to ascertain the general attitude of the respondent toward security software purchases (available from the authors). Cumulatively, it is suggested the LoM indicator questions indicate the willingness to buy software products or services that enhance personal cybersecurity.

An Exploratory Factor Analysis with direct oblimin rotation is used to extract latent components from a set of survey questions. The results for TMT, TChS, and LoM confirm three components. Review of the corresponding survey questions indicates that the TMT and TChS responses are differentiated by the mention of security issues detracting time from preferred tasks, or by a belief that addressing security issues takes too much of one's time (Table 1).

A Spearman correlation analysis is performed on the indicator question responses corresponding to TMT (five questions), TChS (three questions), and LoM (four questions). All of the responses within the three respective sets of indicator questions have two-star Spearman correlations with each other (Table 1). Because the indicator questions for the three latent variables have high intercorrelation, the mean scores of the responses were computed and utilized for analysis. SPSS statistical software was used to calculate Pearson correlations between the latent variables as well as the Cronbach's alphas. The Cronbach's alpha values show acceptable reliability between the latent variables' indicators (Table 1).

Table 1. Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alpha

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
TChS	.319**	.485**	.407	.673
TMT	.221**	.772**	.405	.766
LoM	.500**	.863**	.639	.871

Results for TChS and LoM

Analysis of the results (Table 2) for the TChS vs. LoM hypothesis shows a significant correlation, thus H1 is confirmed.

Regression analysis is performed on LoM as the dependent variable against some demographic variables. The analysis shows some correlation with the combination of TChS and age (adjusted R squared = .035, p-value = .013). H2 is therefore valid for age.

When the model is properly applied, hypotheses utilizing the other latent factors may be similarly evaluated.

SOLUTIONS AND RECOMMENDATIONS

From the viewpoint of encouraging open and robust political discourse, governments should ensure the framework and conditions for free expression by their citizens with online regulatory safeguards that correspond to the traditional safeguards in traditional communications media. This could help Internet users feel freer to spend money and time on personal interests instead of diverting spending due to concerns about their online privacy and security. If users would have less reason to be worried about becoming victims of cybercrime, they could spend more time expressing themselves and exploring offerings. In these ways, online merchants could benefit from more confident online consumers, and societies could benefit from the desired online discourse.

The HFI may be enhanced by the inclusion of a measure to assess citizens' reluctance to express legal, but controversial, viewpoints online. Citizens may be reluctant to express such viewpoints despite states' official policies allowing free expression. The concern about consequences resulting from such expression may not necessarily align with states' official policies and the possibility of state-imposed consequences does not necessarily align with states' official policies. The current HFI does not account for citizens' concerns and perceptions of these issues.

In the analysis, some differences between nationalities in the responses were noted. However, further data should be collected. One direction to search for a potential explanation is cultural differences (Hofstede, 1980).

*Table 2. Pearson correlation between LoM and TChS. Two-tailed significance: * to 0.05 level*

	n	Spend time thinking about and changing settings (TChS)
LoM	191	.160*

Better default security and privacy settings could reduce the perceived need for purchasing supplemental personal cybersecurity solutions. This would free up more time and money for users to apply to preferable tasks and transactions. Ideally, users should be confident that their devices have sufficient privacy and security protection “out of the box”. Prior research has shown that users’ trust in the safeguarding of their privacy and security is positively related to their online purchase intentions (Chen & Barnes, 2007).

FUTURE RESEARCH DIRECTIONS

Applied social exchange theory could be expanded to account for Internet users’ reluctance to freely express their thoughts and opinions online. Further research could explore the factors that inhibit users from expressing controversial viewpoints and factors that encourage such expression online.

The indicator questions used in the demonstration study did not examine how, in the case of waiting, the management of time affects the perspective of the person waiting. Examples of such cases could be the users’ management of the time spent waiting for a security software update to install; or the content displayed on screen by the software during the update (Hanyang, et al., 2015).

For the TChS vs LoM hypothesis, future research could examine the impact of attitudes toward, and usage of, free and open source personal cybersecurity solutions. Users who believe they can achieve acceptable levels of personal cybersecurity with free tools would not necessarily be purchasing such tools. This could affect the LoM factor and thus the significance of the correlation between LoM and TChS. Regression analysis showed that age affects the TChS vs LoM correlation. Younger users who take time to contemplate their device settings feel more positive about spending money on personal cybersecurity.

This demonstration study did not consider free and open source personal cybersecurity products and tools that are available. Such tools include Tor browser, ClamAV, and free VPN services. Some respondents may have responded negatively to the survey questions regarding spending because they believe that they can achieve sufficient personal cybersecurity without spending money doing so. Future studies could account for such products.

Using the proposed research model and introduced latent variables, research can be performed to determine the effects of some independent variables (e.g., income and ICT expertise) on the relationships between the latent variables. Research can explore the relationship of certain demographic variables to personal cybersecurity spending and to any reluctance to express oneself online. Users could also be surveyed to directly gauge their concern about being victimized by cybercriminals as a result of their expressions. Subject to available survey data, analysis for geographical region clustering and other clusterings could also be performed.

CONCLUSION

While sales of cybersecurity products and services are suitable for the cybersecurity industry, they also indicate the real cybersecurity concerns of Internet users. Many Internet users go online, but may then be reluctant to freely express themselves, spending their time and money to alleviate perceived cybersecurity risks from political vigilantes, cybercriminals, or other entities. This scenario is not the ideal or optimal use of the Internet by society. Future research can investigate methods to encourage free expression online and reduce the perceived risks of such free expression.

In this chapter, an overview of research pertaining to the chapter topic was presented, and a simple research model was proposed. Six latent factors were proposed; three corresponding to a reluctance to self-express online (RtoEx, RtoExC, and RtoExnonC); one corresponding to a belief that handling the security and privacy aspects of one's device requires an excessive amount of one's time, TMT; one for time considering device cybersecurity and privacy settings aspects, TChS; and one for personal cybersecurity spending, LoM. Based on the factor analysis of the responses to some indicator statements, TChS and LoM were established.

A study using two of the latent variable showed a significant correlation between TChS and LoM, thus hypothesis H1 is confirmed. The association transcended nationality. The correlation was significant only when the entire response set was analyzed. Analysis by nationality did not show a significant correlation for any of the three most prominent nationalities of survey respondents. Regression analysis showed that age and TChS are predictors of LoM. Hypothesis H2 is therefore confirmed for age. Younger users who are conscientious about their device privacy and security settings are more likely to spend money on personal security or feel more positively about doing so.

REFERENCES

Alqubaiti, Z., Li, L., & He, J. (2016). The Paradox of Social Media Security: Users' Perceptions versus Behaviors. In Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16 (pp. 29–34). Boston: ACM Press. doi:10.1145/2978178.2978187

Anonymous. (2010, January). Keeping online customers. Dealerscope, 52(1), 26. Retrieved from https://search-proquest-com.ezproxy.jyu.fi/docview/218956873?accountid=11774

Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. *Journal of Business & Economics Research*, *7*(3). doi:10.19030/jber.v7i3.2269

Baroni, D. (2015, July 3). New Zealand Government To Punish Online Trolls With Prison Time. Retrieved from http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time

Booth, R. E. (2017). The Effect of Freedom of Expression and Access to Information on the Relationship between ICTs and the Well-being of Nations. *Proceedings of the 23nd Americas Conference on Information Systems*.

Branigan, S. (2011, July 31). Revenge Hacking. Retrieved May 17, 2019, from Trends in high tech security website: https://sbranigan.wordpress.com/2011/07/31/revenge-hacking/

Cassidy, P. (2017, November 3). Man petrol bombed homes in revenge for Facebook post. STV News. Retrieved from https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/

Chen, Y., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management & Data Systems*, *107*(1), 21–36. doi:10.1108/02635570710719034

Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research*, *63*(9–10), 1007–1014. doi:10.1016/j.jbusres.2009.01.023

Cooper, A. K. (2000, July 12). China: Government punishes Internet journalists. Committee to Protect Journalists. Retrieved from https://cpj.org/2000/07/china-government-punishes-internet-journalists.php

Curtom, G. (2014, April 24). Students punished for expressing free speech on Twitter. The Cougar. Retrieved from http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/

Dascalescu, A. (2018, January 3). Doxxing Can Ruin Your life. Here's How (You Can Avoid It). Retrieved May 17, 2019, from Heimdal Security website: https://heimdalsecurity.com/blog/doxxing/#doxxingswatting

Dellaert, B. G. C., & Kahn, B. E. (1999). How tolerable is delay?: Consumers' evaluations of internet web sites after waiting. *Journal of Interactive Marketing*, *13*(1), 41–54. doi:10.1002/(SICI)1520-6653(199924)13:1<41:AID-DIR4>3.0.CO;2-S

Emarketer.com. (2014). Worldwide Ecommerce Sales to Increase Nearly 20% in 2014 - eMarketer. Retrieved November 22, 2017, from https://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039

Halder, D., & Jaishankar, K. (2012). *Cyber Crime and the Victimization of Women: Laws*. Rights and Regulations; doi:10.4018/978-1-60960-830-9

Hayes, A. F., Glynn, C. J., & Shanahan, J. (2005). Validating the Willingness to Self-Censor Scale: Individual Differences in the Effect of the Climate of Opinion on Opinion Expression. *International Journal of Public Opinion Research*, *17*(4), 443–455. doi:10.1093/ijpor/edh072

Hazari, S., & Brown, C. (2013). An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. doi:10.1080/15536548.2013.10845689

Ho, S. S., & McLeod, D. M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. *Communication Research*, *35*(2), 190–207. doi:10.1177/0093650207313159

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values* (1st ed.). Beverly Hills, CA: Sage Publications.

Jaschik, S. (2014, September 15). Interview with professor fired by West Bank university who compares himself to Steven Salaita. Inside Higher Ed. Retrieved from https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita

Katz, K. L., & Martin, B. R. (1989). Improving customer satisfaction through the management of perceptions of waiting. Massachusetts Institute of Technology. Retrieved from http://hdl.handle.net/1721.1/37703

Kwon, O., Kim, C., & Kim, G. (2013). Factors affecting the intensity of emotional expressions in mobile communications. *Online Information Review*, *37*(1), 114–131. doi:10.1108/14684521311311667

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management*, *53*(1), 53–63. doi:10.1016/j.im.2015.08.006

Luarn, P., & Hsieh, A.-Y. (2014). Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities. *Online Information Review*, *38*(7), 881–895. doi:10.1108/OIR-03-2014-0076

Lucchi, N. (2011). Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, *19*(3), 645–678.

Luo, H., Wang, J., Han, X., & Zeng, D. (2015). The impact of filler interface on online users' perceived waiting time. In 2015 12th International Conference on Service Systems and Service Management (ICSSSM) (pp. 1–5). Guangzhou, China: IEEE. 10.1109/ICSSSM.2015.7170198

Mony, S. (2017, November 11). Cambodian Netizens Face New Risks as Government Tightens Online Controls. VOA. Retrieved from https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html

Morgan, S. (2017). The Cybersecurity Market Report covers the business of cybersecurity, including market sizing and industry forecasts, spending, notable M&A and IPO activity, and more. Retrieved November 22, 2017, from https://cybersecurityventures.com/cybersecurity-market-report/

Nadi, Y., & Firth, L. (2004). The Internet Implication in Expanding Individual Freedom in Authoritarian States. ACIS 2004 Proceedings.

Ray, A., & Kaushik, A. (2017). *State transgression on electronic expression: is it for real?* Information and Computer Security; doi:10.1108/ICS-03-2016-0024

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation (Abingdon)*, *26*(1–2), 81–99. doi:10.1080/13511610.2013.747650

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates†. *Journal of Cybersecurity*, *4*(1). doi:10.1093/cybsec/tyy004

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), 21–32. doi:10.1080/01972240252818207

Shen, F., & Liang, H. (2015). Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, *27*(1), 111–124. doi:10.1093/ijpor/edu012

Sims, J., & Xu, L. (2012). Perceived Risk of Online Shopping: Differences Between the UK and China. In UK Academy for Information Systems Conference Proceedings (Vol. 25). Academic Press.

Stanton, L. (2014, August 18). Effect of "right to be forgotten" on free expression sparks debate. Cybersecurity Policy Report.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311. doi:10.1177/1077699016630255

UN General Assembly. (1948). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/universal-declaration-human-rights/index.html

UN Human Rights Council. (2016). Resolution on the promotion, protection and enjoyment of human rights on the Internet. Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Vasquez, I., & Porcnik, T. (2017). *The Human Freedom Index 2017: A Global Measurement of Personal, Civil, and Economic Freedom*. Washington, DC: Cato Institute, Fraser Institute, and the Friedrich Naumann Foundation for Freedom.

ADDITIONAL READING

Camulli, E. (2012, November 28). Customer Experience Frustration Points and Their Consequences. CMSWire. Retrieved from https://www.cmswire.com/cms/customer-experience/customer-experience-frustration-points-and-their-consequences-018455.php

Chua, C., Rose, G., Khoo, H. M., & Straub, D. (2005). Technological Impediments to B2C Electronic Commerce: An Update. *Communications of the Association for Information Systems*, 16.

Cushman, T. (2016). The Fate of Freedom of Expression in Liberal Democracies. *Society*, *53*(4), 348–351. doi:10.100712115-016-0047-z

Hayes, A. F. (2005). Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research. *International Journal of Public Opinion Research*, *17*(3), 298–323. doi:10.1093/ijpor/edh073

Hong, S.-B., Zalesky, A., Cocchi, L., Fornito, A., Choi, E.-J., Kim, H.-H., ... Yi, S.-H. (2013). Decreased Functional Brain Connectivity in Adolescents with Internet Addiction. *PLoS One*, *8*(2), e57831. doi:10.1371/journal.pone.0057831

Kraut, R. E., Patterson, M., Lundmark, V., Kiesler, S., Mukhopadhyay, T., & Scherlis, W. (1998). Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being? *The American Psychologist*, *53*(9), 1017–1031. doi:10.1037/0003-066X.53.9.1017

Rose, G. M., Evaristo, R., & Straub, D. (2003). Culture and consumer responses to web download time: A four-continent study of mono and polychronism. *IEEE Transactions on Engineering Management*, *50*(1), 31–44. doi:10.1109/TEM.2002.808262

Ryan, G., & Valverde, M. (2005). Waiting for service on the internet: Defining the phenomenon and identifying the situations. *Internet Research*, *15*(2), 220–240. doi:10.1108/10662240510590379

Strebel, J., O'Donnell, K., & Myers, J. G. (2004). Exploring the connection between frustration and consumer choice behavior in a dynamic decision environment. *Psychology and Marketing*, *21*(12), 1059–1076. doi:10.1002/mar.20037

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. doi:10.1016/j.cose.2016.02.009

KEY TERMS AND DEFINITIONS

HFI: Human freedom index; a numerical measure of the personal and economic freedom available in a country. It is measured annually. The HFI is determined from an evaluation of over 70 different indicators for each measured country.

LoM: Loss of money; personal cybersecurity spending attitude and behavior; the willingness to buy software products or services that enhance personal cybersecurity.

RtoEx: Reluctance to express; the reluctance to freely express oneself online or on the internet.

RtoExC: Reluctance to express due to concerns of possible consequences or safety; the reluctance to freely express oneself online due to concerns of possible consequences or safety issues resulting from the expression.

RtoExnonC: Reluctance to express when users are not reminded of possible consequences or safety issues resulting from the expression.

Social Exchange Theory: A behavioral theory that seeks to explain the interaction between a person and another person or entity. Its fundamental proposition is that the interaction is influenced by the person's evaluation of the interaction's risks versus rewards.

TChS: Thinking about and changing settings; time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether time is consumed specifically for the checking and possibly changing of device settings that relate to security and privacy.

TMT: Too much time; the belief that cybersecurity risk amelioration requires excessive usage of one's time.

P IV

THE EFFECT ON EXPRESSION RELUCTANCE OF SPENDING TIME ON PRIVACY AND SECURITY ISSUES

by

Juhani Rauhala, Nezer Zaidenberg & Pasi Tyrväinen 2021

For submission to the journal Computers and Security

Draft manuscript.

The Effect of Spending Time on Privacy and Security Issues on an Outcome of Expression Reluctance

Juhani Rauhala[1], Nezer Zaidenberg[2], Pasi Tyrväinen[1]
[1]University of Jyväskylä, Jyväskylä, Finland
[2]College of Management Academic Studies, Rishon LeZion, Israel
juhani@acm.org
scipio@scipio.org
pasi.tyrvainen@jyu.fi

Abstract: The Internet is a platform for free expression. However, the Internet's security and privacy risks may cause users to be reluctant to express controversial viewpoints online. Some Internet users spend time on the security settings of their devices and computers. They do this to mitigate the security and privacy risks. Users may feel negatively about doing this. Users may be hesitant to express themselves online because risk mitigation requires too much time. This has been examined in our prior research. We extend the research by applying it to the antecedents-privacy concerns-outcomes (APCO) framework using an expanded data set that includes three latent variables and the moderating effects of income, ICT expertise and gender. We analyze survey data, verify the previous research, apply the APCO model, and verify our moderation hypotheses.

Keywords: Device Security, Privacy, Time Consumption, Online Expression, Device Settings, APCO model

1. Introduction

Many national constitutions including those of most western democratic states and all of the Gulf Cooperation Council states (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates) contain a provision for guaranteeing "freedom of expression" (or a variant statement of similar intent) (Gelber and Stone 2017; Duffy 2014). Indeed, the UN General Assembly (1948) has declared that freedom of expression is a universal human right. The Internet is a global platform for free expression. The UN Human Rights Council (2016) has resolved that unrestricted access to the Internet is also a human right. However, for users who use the Internet to make controversial or provocative expressions, there are potential consequences. Such consequences may originate from other participants and organizations that follow the communication (Baroni 2015; Cassidy 2017; Jaschik 2014).

Users' concerns about such consequences may cause some users to be reluctant to express themselves freely online. Users' reluctance may correlate with their attitudes and behaviors with respect to addressing the security and privacy aspects of their devices. More specifically, their reluctance to express themselves may also correlate with their perception of and attitude toward the time that they spend addressing their devices' security and privacy issues. Previous research has not applied the relationship between online expression aspects and the perception of time consumption used for device privacy and security issues to the APCO model. Neither has it investigated the impact of income, ICT expertise or gender on the relationship. Users may be reluctant to express themselves online because it takes too much time and effort to ensure their online safety. In the context of devices, a device state that is perceived as ensuring sufficient online safety can result from a preferred configuration of device settings for privacy and security. It can also mean a device setting to ensure anonymity. The users may be aware of the various means for anonymity, privacy, and security, but believe that implementation requires too much effort. They could freely express themselves online, but security and safety concerns restrain their behavior. The tools and device settings to improve their cyber safety and security are seen as requiring too much time to use. Thus, the reluctance persists.

Our main goals are to examine users' reluctance to express themselves in relation to their perceptions and attitudes regarding the time they spend on their online security, and then to apply the results to the APCO framework. This is relevant to online expression contexts, which include participation in social media. We establish three latent factors: one for a reluctance to self-express online (RtoEx); one for a perception that addressing privacy and security aspects of one's device requires an excessive amount, i.e., “too much,” of one's time (TMT); and one corresponding to the usage of time to consider device cybersecurity and privacy settings aspects (TChS). We then analyze and find the correlation among these latent factors as well as the correlation between them and the demographic factors. We use the APCO model to assist interpretation. We also perform linear regressions between latent factors, and between latent factors and the demographic factors.

2. Background

The tolerance of users to the amount of time spent waiting will vary according to the individual and the context (Katz and Martin 1989). Chatzitheochari and Arber (2012) studied differences in free time between genders for working people in the UK. In all cases, women had the same or less quantity of pure free time as men. Moreover, womens' free time tended to be of lower quality and more subject to interruptions than mens'. During Internet usage, a loading delay may be experienced with most mouse-clicks or screen taps. However, the need to spend time waiting for a security software update process to complete varies. It may occur, e.g., weekly, monthly, or with each session. The frequency is also dependent on such manual updates that the user performs.

In our prior study we found that users who believe that addressing their device security and privacy issues requires excessive time will be more reluctant to express themselves online (Rauhala et al. 2019a). We have also found that users who tend to be reluctant to express themselves online also tend to have a positive attitude toward spending money for personal cybersecurity protections (Rauhala et al. 2019b).

As a result, excessive non-ideal time consumption can be considered to detract from more desirable activities and may lead to a bad opinion of the offerings for which one is waiting (Dellaert & Kahn, 1999). Excessive time consumption can lead to a negative attitude toward attractive online content and activities, and even the abandonment of them (Business editors, 2002; Anonymous, 2010).

There are also studies observing the impact of demographic factors, such as nationality and age, on Internet behavior that are relevant to this study. Regan et al. (2013) have evaluated attitudes toward information privacy between age groups categorized by generation. Their analysis revealed a trend where older generations tend to be less concerned than younger ones about wiretapping and data privacy. On the other hand, Tsai et al. (2016) found that users' age, income, and education did not affect their "security intentions" (e.g., the intention to download and update antivirus software, adjust browser settings, etc.). Chen et al. (2010) determined that consumers with different levels of computer expertise have different preferences for attributes of shopping websites. Cultural similarity (as measured by cultural distance (Hofstede 2001)) has been found by some studies to affect decision-making in various ways. One such way is in the selection of target countries for market expansion by software firms (Jones and Teegen 2001; Rothaermel et al. 2006). However, other research has found that other variables play a more important role in the selections (Ojala and Tyrväinen 2007). Research into culture-based differences in perception of risk for online shopping and other tasks has yielded conflicting results (Sims and Xu 2012). Sims and Xu (2012) found no significant difference between British and Chinese shoppers' perceived risk of online shopping despite those shoppers' differing cultural backgrounds. This conclusion was against their expectations because of results from prior research that showed differences in uncertainty avoidance between the two cultures (Hofstede 1980).

Researchers have observed differences between genders with respect to privacy concerns. Regan et al. (2013) studied the differences between genders of different generations. They found that for most generations, females are more disapproving of wiretapping than males. The same attitude pattern was seen for a belief that government computer data is a "very serious threat" to privacy. Females generally more concerned about privacy invasion via electronic means than males (Regan et al. 2013). Sheehan (2002), on the other hand, found no significant differences between genders in terms of level of privacy concern.

An overarching research model has been proposed to enhance the development of privacy research. The model is referred to as the Antecedents - Privacy Concerns - Outcomes (APCO) model (Smith et al. 2011). In the model, antecedents can be defined as influential precursors that help to define the levels of privacy concerns for a selected context. The contextualized privacy concerns are then investigated for their predictiveness of the behavioral outcomes (or “changes of state”) under investigation. The ostensible purpose of the model is to help researchers address the many possible antecedents and outcomes that can be identified when conducting privacy research. Interested readers can find more details about the model in the referenced work. Variations of the APCO macro model or models similar to APCO have been applied in other works, e.g., by Benamati et al. (2017), Bandyopadhyay (2009), Sun et al. (2019), Zhang et al. (2013), Dinev et al. (2015), and Ayaburi et al. (2019). Smith et al. (2011) have presented gaps in current information privacy research. Such gaps include the need to address relationships between antecedents and privacy concerns and the privacy calculus stream in their model. Benamati et al. (2017) have partially addressed this by examining privacy awareness, age, and gender as antecedents in an applied model. Benamati, Ozdemir, and Smith used a construct of “privacy protecting behaviors" with reference to Facebook. Their construct included scales of behavior for limitations of friending, of posting, and of adjustments to settings that control the revelation of personal information. A basic diagram of the model presented by Smith et al. is in Fig. 1.

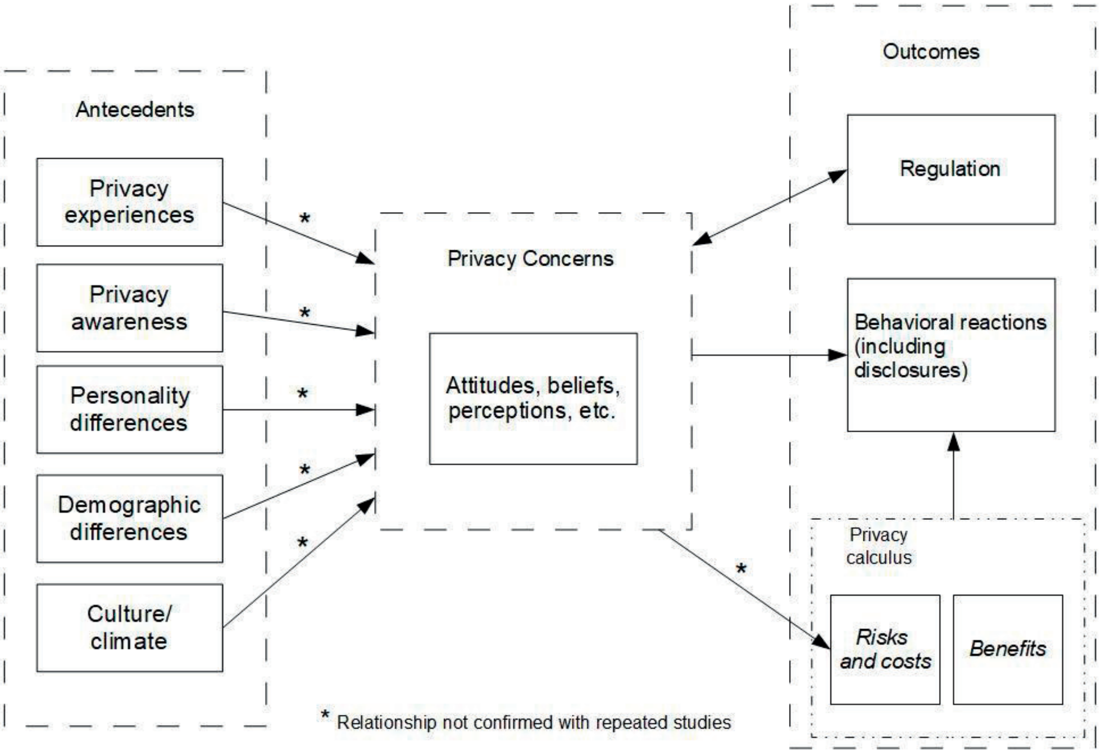


Fig. 1 Diagram of Antecedents->Privacy Concerns->Outcomes model (Smith et al. 2011)

Controversial expressions are those that arouse quarrel or strife or are marked especially by the expression of opposing views (Merriam-Webster n.d.). As such, they may be interpreted as negative, hostile, or provocative. Controversial expression in an online communications context is affected by certain factors. Such factors include perceived anonymity and familiarity with other online community participants (Luarn and Hsieh 2014). Luarn and Hsieh looked at how users expressed themselves in a lab-controlled virtual community. Different online group communications contexts were replicated in the virtual community. Users were more likely to share contentious thoughts when their names were hidden or when they were familiar with other members of the group, according to the researchers. When users in the study were not anonymous, they were more reluctant to express such opinions. This is consistent with Lowry et al.'s (2016) findings insofar as the expressions of cyberbullying can be considered controversial. They also found that there was no effect of anonymity or member familiarity on users' willingness to express non-controversial opinions.

Online expression may take the form of a hostile communication perceived by a reader to be personally directed at him or her. Jane (2015) has commented on problems with existing research regarding hostile personal communications, or "flaming." Jane states that an inordinate amount of research is predicated on preserving the right of the expressor of hostile communication to make such communications. She argues that more attention should be given to the consequences of the communication in those cases where there the recipient perceives that he or she has been flamed. While we acknowledge that in many cases a controversial expression may be strongly worded or hostile, and may be directed at an individual or organization who may perceive the expression as offensive, we assert that free online expression has intrinsic value and significant societal importance, and is thus worth preserving and encouraging. We agree with Jane's recommendation, but do not address the ethical and legal aspects of controversial expressionism in this study.

Prior research shows that negative expressions are received differently than neutral or positive ones. Kwon et al. (2013) studied communications and expressions in a messaging context. They examined the acceptability of negative communications. They found that emotional expressions that accompany negative communications were considered much less acceptable than emotional expressions in positive ones. Negative messages by their nature are less welcome.

We expand prior research by investigating the correlation between perception of time consumption used for addressing device cybersecurity and the willingness to express freely on the Internet. Since unpopular, provocative, or negative expressions can result in unwanted consequences, Internet users may be reluctant to express themselves because of concerns about such consequences. The users may want to express their opinions anonymously. However, the time and effort that they spend on personal cybersecurity issues may further discourage their controversial expressionism. Thus, issues related to device assessment and adjustment may be concerns that relate to a reluctance outcome. Demographics may be antecedents to the concerns. We hypothesize that users are more reluctant to freely express themselves online when they feel that they spend excessive time on their devices' cybersecurity and privacy aspects. We apply the hypotheses and results to the APCO model. This is relevant to the users' participation in online expression contexts that include social media.

3. Research model and theoretical framework

Users' concerns about the possible consequences of their online expressions may reduce those users' intent to express. The potential consequences can lead users to protect themselves by performing certain actions. Among these actions are the consideration and possible adjustment of settings on their device. The purpose of the consideration and adjustment is so that the users will, as a result, be less vulnerable to the consequences mentioned above. Such consideration and adjustment necessarily consume users' time. We examine users' expression reluctance in relation to their perception and attitude about the time that they dedicate to their devices' security and privacy settings.

Time is quantifiable; however, humans' attitudes or perceptions about the utility or quantity of their expended time are more difficult to measure. Ancona et al. (2001) have described a temporal conceptualization category that they call "actors relating to time." This category includes temporal perceptions and temporal personality. Concerning temporal perceptions concept, the responses from our respondents about their perceptions of time usage may be affected by the "novelty of time" effect, as described by Butler (1995) and by "time in retrospect" effect (Hicks et al. 1976). The time in retrospect effect can cause a user to overestimate the length of a period of time if it was one in which the user was occupied by activities. Applying the concept to our study, we say that users who believe that addressing device security settings or notifications takes too much time may have had to perform much activity during such periods. Thus, the time in retrospect effect could cause them to remember a required time(s) as taking longer than it did.

Similarly, if the user experiences the adjustment of device security and privacy settings as unique or different, the experience will be more memorable. Responses influenced by novelty-of-time effect would help the accuracy of survey responses. Responses influenced by time-in-retrospect effect may not be accurate in their assertion of excessive time consumption, but what is most important for our purpose is the belief or perception of the user about the time. We seek the relationship between the attitude of the users and the outcome, not between the objective quantity of time and the outcomes. Our model uses two latent factors for these perceptions of time. One factor measures the perception that addressing device security and privacy aspects requires excessive time (or "too much time"). The factor includes indicators that account for a negative effect on the device usage experience. The other factor measures whether the user has contemplated the security and privacy characteristics of his/her device. It also measures whether he/she has checked and possibly changed the device security and privacy settings. Indicator questions corresponding to these factors (Appendix, Table 11) were implemented in a survey. The survey responses established the factors. The resulting latent factors are denoted as TMT (from "too much time") and TChS (from Thinking about and Changing Settings), respectively.

We verify three factors to be used in the model:

Reluctance to Express (RtoEx): reluctance to freely self-express online
Too Much Time (TMT): the perception that cybersecurity risk amelioration requires excessive usage of one's time

Think Change Settings (TChS): time considering two aspects of one's ICT device – contemplation of the device's cybersecurity aspects and whether time is consumed specifically for the checking and possible adjustment of device settings that relate to security and privacy.

Users may not enjoy dealing with their device's security and privacy settings. The effort to understand and possibly adjust the settings may reasonably be seen as necessary by many users. They have been made aware of online risks such as hacks, viruses, malware, and surveillance by various media. Thus, considering and adjusting their device security settings has become effectively obligatory – like fastening a seat belt. The user may have a negative experience when taking the time to do it. The user may even hyperbolically discount the benefits of changing settings to implement protections as "this is a waste of time" or "this takes too much time," and thus immediately avoid exposing themselves to the risks of making controversial expressions. Such a case may be represented by a "naif" user as described in an economics behavior model proposed by O'Donoghue and Rabin (2000). They compensate by a (perhaps short-term) decision to refrain from freely expressing themselves online as an alternate way to avoid the risks and the cost in time of adjusting the settings. I.e., the benefits of settings adjustment are spread over time, but non-adjustment combined with non-disclosure of controversial expressions has the immediate and continuous benefit of the avoidance of risks and hassle. In the case of a naif user, he may wrongly assume that he will not want to have secure settings in the future either. This "privacy paradox" of the misalignment of privacy intentions and behaviors has been noted and discussed by Acquisti (2004), and time displacement of risk has been researched by Smith et al. (2011) and others. The cases of temporally differentiated user preferences have been studied by O'Donoghue and Rabin but are not addressed in the present work. Together with RtoEx, the TMT and TChS factors are an attempt to measure these attitudes and perceptions in our theoretical framework.

The statistical relationships between the three factors may differ across demographic groupings. Groupings considered in this study are those of income, level of ICT expertise and gender. We investigate potential differences.

Our study uses the APCO research model defined by Smith et al. (2011) as a modeling framework. Variations of the APCO macro model or models similar to APCO have been applied or proposed in other pertinent works in the field, e.g., by Benamati et al. (2017), and by Bandyopadhyay (2009). Smith, et al. (2011) have presented gaps in current information privacy research. Such gaps include the need for addressing relationships between antecedents and privacy concerns, and for the privacy calculus stream in their model. Our work will help to address these. The model may be applied to our research in the following way. As antecedents, we apply ICT Expertise, and Income. The TChS construct is positioned as a "Privacy Concern" influenced by the antecedents. We assert that TChS is a behavioral manifestation of Privacy Concerns. For TMT in the "privacy calculus" construct, we presume that the required time for proper adjustment of privacy and security settings is seen by the user as a precondition to freely expressing themselves online, and that it invokes a risk/benefit analysis from him. Moreover, that such adjustment of the settings is judged by the user to require excessive time.

Finally, RtoEx is the measured outcome construct. By way of comparison to Bandyopadhyay's 2009 theoretical framework, our RtoEx variable may be considered a variation of both 1. Refusal to provide personal information, and 3. Refusal to use the Internet. Bandyopadhyay's framework has implications for online marketers (Bandyopadhyay, 2009), while our application presumes implications for individuals' online expression. In our variation of the framework, there is one outcome - a reluctance to freely express oneself on the Internet.

4. Hypotheses development

We attempt to ascertain causality using the three baseline criteria of Antonakis et al. (2010), those being (to paraphrase) temporality, correlation, and exclusion of other causes. To establish the necessary temporal relationship between the latent variables, we present that the questions in the survey regarding time usage precede the questions regarding a reluctance to express. Hence, there is an acute temporally ordered reminder to the respondent of time consumption used for settings adjustments, before the questions about online expression. The other argument for the proper temporal relation is that the pragmatic user will initially tend to customize or adjust their PC or connected device features and settings before initially using the device. Our prior investigation (Rauhala et al. 2019a) found that most users check and adjust the security and privacy settings of their devices prior to initial use. In addition, many devices and operating systems, such as Android devices, will initially prompt the user to make choices for their settings during first use. The settings include ones for privacy and security. For example, the user is asked whether to enable location services and to choose a PIN for locking their device.

Moreover, users who are aware of “revenge hacking” (Branigan 2011) may be motivated to make adjustments to their privacy and security settings preventively. Such adjustments would help to protect against revenge hacking. The action may be especially necessary prior to making a controversial or provocative expression online. Controversial or provocative online expressions have been the cause of various retaliatory acts. The Internet is often used to commit the retaliation. The second criterion is established upon analysis of the data. The third condition is more difficult, as, by nature, any study is limited in the factors and variables that are elicited by data gathering or by analysis. No study can consider or analyze every possible causal factor of an effect. In this work, we may only assert causality to the extent that the analyzed elicited variables and factors have been included in our analysis. Between Antonakis et al.'s criteria and our discretion, we believe there are reasonable grounds to assert that there is some directional causality between the factors discussed.

TMT and RtoEx

Users' may experience frustration with excessive time consumption that is used to perform tasks or to wait for a desired outcome. Prior research has shown that excessive time consumption can lead to a negative experience or negative perception of the service for which the waiting is done (Dellaert and Kahn 1999). Prior research has shown that users may abandon websites if their loading times are excessive (Anonymous 2010). Self-disclosure online is usually done after consideration, or when parameters, as defined in social exchange theory, are believed to be acceptable by the user. In micro-blogging, for example, such parameters as the potential to build relationships, and trust in the service provider are important considerations for self-disclosure (Liu et al. 2016). Prior research has shown that users may abandon websites if their loading times are excessive (Anonymous 2010). Bandyopadhyay (2011) has theorized that privacy concerns may cause users to be unwilling to use the Internet altogether. Considering TMT as a privacy calculus in the APCO model, it is plausible that the user makes a consequentialist tradeoff of settings-adjustment time cost and online expression benefit (Fig. 2). Such a tradeoff can result in a user refusing or being reluctant to controversially express themselves, rather than making adjustments to privacy and security settings as a precondition for the expression. We believe that the combination of the abovementioned factors (pre-existing reluctance, or requirements for correct conditions before the self-disclosure of sensitive personal information; and the impact on users of temporality-induced frustration with securing their devices) lead to correlation or causality between TMT and RtoEx.

H1: TMT will positively correlate with RtoEx.

TChS and RtoEx

Consumers consider and possibly change their device security privacy settings. It is reasonable to assume that they do so because they are aware of security and privacy risks that come with engagement in online activity. We assert that the same consumers are also more likely to be aware of the risks associated with expressing controversial viewpoints in an online context. Thus, there could be correlation or causation between TChS and RtoEx.

H2: TChS will positively correlate with RtoEx.

TChS and TMT

Users who adjust their device security and privacy settings do so to protect their privacy and security online. Users generally adjust such settings due to an obligation to their safety. Such users judge that performing such a task can reduce potential security and privacy risks. While many users may become accustomed to and accept such necessary precautions as a benign "part of life," some may resent that such extra actions are necessary to use the Internet. Using the Internet has become a significant and even essential part of modern living. It is required in order to perform many transactions, such as those for banking. For many activities, few or no reasonable alternative transaction methods exist. Therefore, users cannot easily opt-out of using the Internet. Thus, users may choose to adjust their security and privacy settings though they would prefer to do something else. They make the choice because they are aware of cyberthreats to their computer or device. Their choice may also be motivated by privacy concerns - that excessive personal information may be exposed and abused. The adjustment of security and privacy settings can be recognized by users as a practical obligation. As the task is done due to obligation rather than preference, users will have a higher tendency to experience the time expenditure for the task negatively. Finally, users should not prejudicially feel TMT if they have not considered and possibly adjusted the settings.

H3: TChS will positively correlate with TMT

ICT expertise, Income and Gender,and TChS

ICT expertise, Income and Gender are hypothesized antecedents to the TChS concern. Tsai et al. (2016) found no correlation between income or education, and "security intentions." A user's loss risk increases with their wealth. Therefore, a wealthier user should have a higher motivation to act to reduce risks to their assets. We hypothesize that income will positively correlate with TChS. ICT expertise can increase risk-awareness in the online environment. Thus, we believe that the ICT expertise antecedent will positively correlate with TChS. Regan et al. (2013) found the females were generally more concerned about privacy threats than males for the scenarios in their study. Other research has found that females are less willing than males to disclose sensitive information when reminded of the Internet's privacy risks (Beaussart and Kaufman 2013). In light of these previous findings, gender should correlate with TChS. Taking a contrarian position, there are well known disparities between the sexes in representation in ICT education and in ICT skills confidence (European Commission 2019; Girl Scout Research Institute 2019). TChS involves making settings adjustments to an ICT device. Therefore, we may not be surprised if males will have the higher tendency to engage in this activity, despite females' greater concern for privacy.

H4a: ICT expertise will positively correlate with TChS
H4b: Income will correlate positively with TChS
H4c: Gender will correlate with TChS

Moderation effects of ICT expertise, income and gender on H3

We investigate the moderating effects of the antecedents on H3. We may expect that users with higher levels of ICT expertise will be more familiar with making adjustments to security software and to device security and privacy settings. As a result, they should be able to make the desired changes to the settings more easily and in less time than users with lower levels of ICT expertise. Hence ICT expertise should negatively moderate H3. Burchardt (2010) has examined the relationship between available free time and income for UK residents. The income earned by working was found to be associated with available free time. Generally, as the subjects' earned income increases, their available free time decreases (Burchardt 2010). Respondents with less free time should be relatively more restrictively conscientious about using their time. We believe Burchardt's work can be extrapolated to our target population, and so income should positively moderate H3. Chatzitheochari and Arber (2012) studied differences in free time between genders for working people in the UK. In all cases, women had the same or less quantity of pure free time as men. Moreover, womens' free time tended to be of lower quality and more subject to interruptions than mens'. Given these gender differences, we assume that women will place a higher premium on their time. Hence, gender should moderate H3.

H5a: ICT expertise moderates H3.
H5b: Income moderates H3.
H5c: Gender moderates H3.

Moderation effects of ICT expertise, income and gender on H2

Female citizens of the EU have been underrepresented in ICT education (European Commission 2019). Girls have been found to have less confidence than boys when it comes to their ICT skills (Girl Scout Research Institute 2019). Therefore, we expect that female respondents may have less confidence in their contemplations of their device security and privacy settings. They should also have less confidence in making adjustments, and in any protective effects that such adjustments may produce. Consequently, gender should moderate H2. Nugent et al. (2016) have reported that individuals (across multiple religions) with higher incomes tend to have more interest in engaging in political activity and a greater belief in the importance of free speech. We expect that income should positively moderate H2. Users with more ICT expertise should be able to adjust their settings more effectively than those with less expertise. They should also be more aware of the actual security and privacy threats on the Internet. Users with more ICT expertise should be able to mitigate such threats appropriately. Hence, they should be less reluctant to express themselves, and ICT expertise should moderate H2.

H6a: ICT expertise moderates H2.
H6b: Income moderates H2.
H6c: Gender moderates H2.

Moderation effects of ICT expertise, income and gender on H1

We investigate the moderating effects of the antecedents on H1. Burchardt (2010) has examined the relationship between available free time and income for UK residents. The income earned by working people was found to be associated with available free time. Generally, as the subjects' earned income increases, their available free time decreases (Burchardt 2010). Users with higher incomes are busier and have a more limited time budget. They should be more restrictively conscientious about using their time. Income should moderate H1. Prior research has shown that women tend to have less free time than men (Chatzitheochari and Arber 2012), thus it may be expected that women may be more discriminating in how they use their time. Regan et al. (2013) found the females were generally more concerned about privacy threats than males for the scenarios in their study. Other research has found that females are less willing than males to disclose sensitive information when reminded of the Internet's privacy risks (Beaussart and Kaufman 2013). Therefore we would expect gender to moderate H1. ICT expertise is not expected to moderate H1. H7a is nonetheless included for exploration.

H7a: ICT expertise moderates H1.
H7b: Income moderates H1.
H7c: Gender moderates H1.

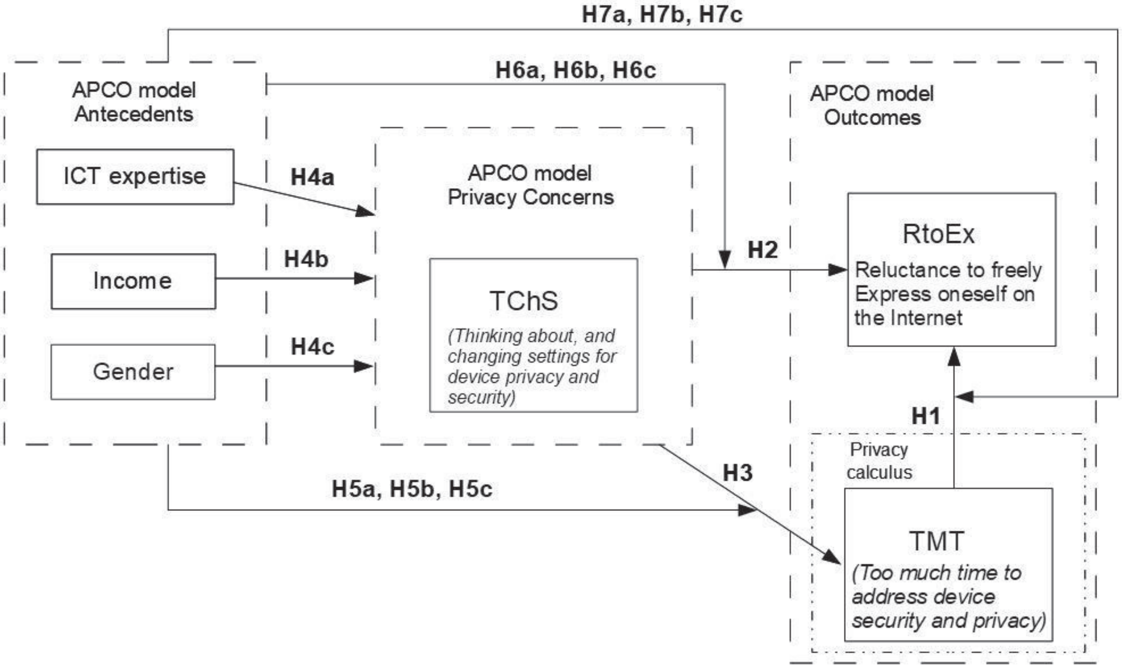

H7a, H7b, H7c
H6a, H6b, H6c
APCO model
Antecedents
ICT expertise
Income
Gender
H4a
H4b
H4c
APCO model
Privacy Concerns
TChS
(Thinking about, and changing settings for device privacy and security)
H2
APCO model
Outcomes
RtoEx
Reluctance to freely Express oneself on the Internet
H1
Privacy
calculus
TMT
(Too much time to address device security and privacy)
H3
H5a, H5b, H5c

Fig. 2 Mapping of the study to the Smith et al. (2011) APCO macro model

5. Study design – Indicators for latent factors

The latent factors' values were measured by sets of indicator questions in a survey. The survey was designed with potential indicator questions and implemented in a prior study (Rauhala et al. 2019a). The survey questions were reviewed and validated during the previous study by the co-authors. Other researchers were also consulted for guidance on survey methods and other survey issues. Such issues included common method bias. The indicator questions were administered to survey participants. Each question permitted a response along a five-point Likert scale ranging from "strongly agree" to "strongly disagree." TMT was established with five questions to assess respondents' perceptions that excessive time is necessary for addressing their devices' security and privacy issues. The questions also assess their perceptions that the time they have used for the issues has detracted from the time that was intended for other tasks. Three questions are used to establish TChS. They assess whether the user has contemplated their devices' privacy and security aspects, and whether they have adjusted privacy and security settings on their device. Cumulatively, we suggest that the five TMT indicator questions can gauge whether a respondent spends time contemplating and actively addressing their devices' security and privacy aspects but that he or she feels negatively about doing so. The respondent feels that the amount of time required is excessive and detracts from preferred activities for which time would otherwise be used.

Previous research has investigated various benefits of and implications on online expression. Shen and Liang (2015) measured the willingness to express opinions online by way of a web forum's view/reply ratio. Other researchers have done similar assessments by asking users how likely they would be to express their opinions in specified online scenarios using a 0-10 or 0-100% scale (Stoycheff 2016; Ho and McLeod 2008). Hayes et al. (2005) established a self-reporting tool consisting of eight five-point Likert questions to measure willingness to self-censor. Hayes et al.'s tool's questions do not specifically measure self-censorship on the Internet, but rather in the general social context. Our research model defines reluctance to freely express oneself on the Internet, or RtoEx, as a latent factor. RtoEx is used for analyzing responses to a set of indicator questions (Appendix, Table 10) asked in a survey. This factor allows for the performance of various analyses against other variables and factors.

Questions for the RtoEx variable ascertain the attitude of respondents toward hypothetical scenarios of their posting controversial content online. Such content can include provocative opinions or artwork. The question set includes one question to ascertain their attitude toward using electronic methods vs. face-to-face communication when discussing a sensitive topic with a friend. We suggest that the responses to this question set can convey the level of the respondents' reluctance to express themselves using electronic methods, including the Internet.

To gather data, a survey was administered over the Internet in the form of a Web questionnaire to a population composed mainly of university students and working adults.

A typical challenge in observational studies is making an account for common method bias. We use a multi-trait single method approach. The cross-sectional study was implemented with an Internet web-based survey. The survey was accessed with a URL that was provided to potential respondents. Some sources of common method bias pertinent to our data gathering method include common scale properties, question ambiguity, and social desirability in wording. We attempt to account for these and other biases as follows.

The questions for individual factors (traits) in our survey were grouped together. The questions on "time spent" were temporally spaced before the questions on "reluctance to express." We believed that grouping of the factor questions together would help the respondent to better ponder the question's topic so that they would be cognitively prepared to answer the subsequent questions about the same factor more accurately. The respondent had the opportunity to ponder the questions without an intermittent clearing of his or her short-term memory by the distraction of new unrelated questions. It was believed that this, in turn, would lead to more accurate, or at least not less accurate, responses to the questions. Research supports the grouping of related survey questions for improved results (Krasnick and Presser 2010), as do companies that specialize in online surveys (Hillmer 2019; SurveyMonkey 2020).

The questions intended to collect responses on latent factors do have a common scale. Each is a five-point Likert scale. This may lead to some bias resulting from the common scale property. The questions' wordings, however, are designed to be maximally clear and unambiguous. The questions on factors are in the form of hypothetical scenarios or opinions with which the respondent agrees or disagrees according to the scale. There are some direct questions to gauge respondents' demographics, and these have little room for ambiguity. For other direct questions, we are interested in the respondents' perceptions. Many prior works have shown that perception is more important than objective measures in influencing the decisions and behavior of people. Studies by Bhattacharya et al. (2014), Clarkson et al. (2010), and Tormala et al. (2006), to name a few, have shown this phenomenon in a variety of contrived and real-world settings.

The social desirability bias should not be a factor in our data. The survey was anonymous, and thus there should not be a reason for respondents to choose their answer with this bias.

We do not anticipate ability factor bias in our data. Our survey was administered in English, and the respondents who are not native English speakers are mainly university students. The ability to understand the questions does not require specialized technical knowledge or complex abstract thinking.

We address the motivational factor with an attempt to improve response accuracy. The survey is voluntary and anonymous, and addresses timely topics that affect most people; those being cybersecurity and self-expression online. The university students in Finland (approximately 130 respondents) were invited to take the survey with a notice that doing so would make them eligible to enter a prize drawing. Because the survey was anonymous, there were no individually attributable social consequences of the responses, and consequently, a respondent should not have a desire to provide a socially acceptable response. Moreover, the nature of the questions is such that there is little or no context for "socially acceptable" responses. In these ways, the bias due to motivation factors is mitigated. We also provided an announcement email containing the survey invitation. The email contained a brief introduction to the survey topic. The first page of the survey was an introductory "welcome page" that contained instructions, a brief description of the questioning style and how the responses would be used, a reminder that the survey was anonymous, and that inexact responses would be acceptable. The page also contained an optional initial free-form text field to allow respondents to write the first thing that came to their mind upon hearing the term "Internet security and privacy." This brief initial "brainstorm" was hoped to have a motivational effect. It was also hoped to have an initial stimulatory but neutral priming effect on the respondents. In psychological terms, the sought effect may be considered positive priming or semantic priming. The respondents would begin filling the survey primed with their initial and unfiltered "gut reaction" to the topic.

To mitigate task factors bias, we tried to avoid presenting long, complex, and abstract questions. We also tried to minimize ambiguity. Every point of the response scale is labeled, and not just the endpoints (Krosnick 1991). We also implemented methodological separation of the questions. The respondents were not allowed to return to previous answers they had already provided. Only four questions at a time were visible to the respondent. The survey did not permit respondents to move back during the survey to check their earlier responses. This restriction partially prevented them from using their previous responses as a basis to provide consistent responses or responses that would be consistent with a perceived implicit theory. This separation also simultaneously mitigated method bias caused by proximity effect. Thus, the potential for task factor bias was at least partially mitigated. Stylistic response bias was mitigated by varying the wording between questions on the latent factors.

During the design and administration of our survey, we attempted to address applicable psychometrics issues as described by DeVellis (2003).

In developing our survey scales to measure TMT, we used a five-step Likert scale ranging from strongly disagree to strongly agree. We believe the range should adequately measure the gradation in the feelings of respondents about the question. Aside from the previously mentioned prior research, the measurement and application of the TMT construct we have described have limited or no existing theoretical basis. Thus, we propose the construct of TMT with a corresponding scale as described herein.

The multi-item scales were designed to be specific to the usage of time for the task, and whether the attitude about such usage may be negative. The negative attitude may result from the required time being excessive, from a resulting interference with preferred activities, or from both. The items were designed with a level of specificity to minimize crossover into related constructs, or into unpredicted constructs that were not intended to be measured.

The question items were brainstormed into a pool from which the most appropriate items were selected for the constructs. Multiple items were selected for each construct. The items have different wordings to qualify as separate questions and are non-trivially redundant. We attempted to avoid making the items too lengthy or difficult. The items were designed to measure the same construct within the scale. Readability analysis was performed on the indicator question sets for each latent variable. The questions for each latent variable were combined into a block for analysis. The RtoEx questions have a 12th (Flesch-Kincaid) or 9th (Dale-Chall) grade readability level.[1] The TMT and TChS questions have a 9th (Flesch-Kincaid) or 12th (Dale-Chall) grade level. Thus, the questions should be readily understood by those respondents with an education equivalent to that of an American high school graduate. The differing results between the Flesch-Kincaid and Dale-Chall analyses between our scale sets may show problems in applying either to a scale questions setting. This issue is left for other researchers to investigate.

The final developed scales are a 10-item scale for RtoEx, a three-item scale for TChS, and a five-item scale for TMT. Our design is validated by the good internal consistency reliability, as indicated by the values of the reliability parameters presented later.

6. Sample

Our sampling frame (Table 1) was a number of Internet users consisting of students at the University of Jyvaskyla in Finland, and of general populations with access to the Internet in Finland, the United States and Israel. 265 responses have been obtained. 131 are from Finnish nationals. The respondents from Finland and Israel are mainly university and college students. The respondents were mainly 15-36 years of age, whose annual income is a maximum of 20,000 euros or US dollars. For Table 1, the scales' means for ICT expertise are shown. ICT expertise was assessed with a combination of four questions. The questions addressed self-assessment of skill in ICT, years of ICT training, hours of daily use of ICT technologies, and years of having used ICT technologies. The responses were transformed and averaged. The ICT expertise of most respondents is high, with an estimated level higher than 3.3 on a 1 (lowest) to 4.5 (highest) scale. Our target population is Internet users of any age (or at least aged 15 and older, the lower age limit in the respective survey question) who reside in western-style democratic societies. We suggest that our survey data enables the inference to this target population. However, the sample size and broad target population mean that our results will have some coverage error.

[1] Grading is based on the U.S. educational system. 9th – 12th grades are U.S. high school level.

Table 1 Sample profile

Variable	Percentage
Gender	
Male	57.4
Female	42.6
Age	
15-25	36.6
26-36	32.5
37-44	14.3
45-54	10.2
55-64	4.9
≥65	1.5
Annual income (euros or US dollars)	
<4,999	27.5
5,000 - 19,999	24.5
20,000 - 39,999	18.9
40,000 - 59,999	11.3
60,000 - 79,999	7.5
80,000 - 99,999	3.4
≥ 100,000	6.8
Nationality	
Finland	49.4
USA	23.8
Israel	19.2
other	7.6
ICT expertise (mean score from scales, 4.5 highest - 1.0 lowest)	
>3.8-4.5	23.0
>3.1-3.8	41.6
>2.4-3.1	30.5
>1.7-2.4	4.8
1.0-1.7	0.8

We extracted the latent components from responses to the survey questions by using an Exploratory Factor Analysis with varimax rotation. The results confirm the two components TMT and TChS. The TMT and TChS responses are differentiated by a perception that addressing security issues takes too much of one's time, or by the mention of security issues detracting time from preferred tasks (Appendix, Table 11). Thus, the three resulting latent factors are RtoEx, TMT, and TChS.

To check the adequacy of the data sample, we run a Kaiser-Meyer-Olkin (KMO) test. We also perform a Bartlett's Test of Sphericity to ensure that at least two of the intended factors are correlated. The results (Table 2) show that the data sample is adequate and is suitable for subsequent factor analysis.

Table 2 Results of tests for data sample adequacy

KMO Measure of Sampling Adequacy	.788
Bartlett's Test of Sphericity, sig.	.000

The communalities of the factor loadings are analyzed and checked. Table 3 presentTable 3s the results, and they indicate a sufficient reliability of the analysis.

Table 3 Factor analysis reliability - communalities

Factor	Communality range	Mean
RtoEx	.269 -. 630	.532
TChS	.429 - .715	.595
TMT	.489 - .623	.558

We perform a Spearman correlation analysis on the responses to the indicator questions for the three factors. There is a high correlation between the responses within the three groups. For the responses to the RtoEx questions (Appendix, Table 10), the lowest correlation is .241, and the highest is .697. Both results are three-star significant at the .001 level (two-tailed). For the TMT questions' responses (Appendix, Table 11), the lowest two-tailed correlation is .222 (three-star) and the highest is .695 (three-star).

Similarly, for TChS (Appendix, Table 11), the lowest two-tailed correlation is .314 and the highest is .497, both three-star significant. Based on these correlations, the factor analysis results, and the previous reliability and sample adequacy tests, we used the means of the responses for each set of indicator questions for our primary analysis. The mean values of the responses to the indicator questions were used as representative values of the corresponding latent factors. To evaluate the unidimensionality and reliability of our constructs, we used SPSS statistical software to calculate the Spearman correlations as well as the Cronbach's alphas (Table 4). The results indicate strong unidimensionality. The Cronbach's alpha values show an acceptable to good reliability for the constructs' indicators.

Table 4 Spearman correlations (two-tailed significance at 0.01 level) between indicator question responses for each latent factor; mean correlations; and Cronbach's alpha

Latent Factor	Minimum	Maximum	Mean	Cronbach's Alpha
RtoEx	.241***	.697***	.434	.860
TChS	.314***	.497***	.408	.676
TMT	.222***	.695***	.406	.768

The factor loadings for the indicators are reported in the Appendix (Table 12, Table 13 and Table 14).

7. Results

We perform a Pearson correlation analysis between the three factors RtoEx, TMT, and TChS using SPSS software. The results in Table 5 show a significant positive correlation between a reluctance to express oneself online and a long-perceived time spent on setting device security settings (.238**). On the other hand, there is no significant correlation between the factors RtoEx and TChS, with TChS representing the usage of time for thinking about device security settings. Hypothesis H1 is thus confirmed, and hypothesis H2 is rejected. A positive correlation of .179**, p=.003 was found for TChS and TMT, thus confirming H3. Table 6 shows the results of the factor analysisTable 6.

Table 5 Pearson correlations between RtoEx and TMT and TChS. Two-tailed significances: * to .050 level, ** to .010 level, *** to .001 level

n=265	Device security/privacy takes "too much time" (TMT)	Spend time thinking about and changing settings (TChS)
RtoEx	.238***	.067

Table 6 Correlations between the latent variables, percentage of variance explained and eigenvalues

Latent variable	RtoEx	TMT	% of variance	Eigenvalue
RtoEx	**1**	.238***	**28.121**	4.499
TMT	.238***	**1**	**15.868**	2.539
TChS	.067	.179**	**11.212**	1.794

H4a is also confirmed with a weak positive correlation between ICT expertise and TChS (p=.055) (Table 7). H4c is confirmed with a significant correlation between gender (male respondents) and TChS. No significant correlation was found between income and TChS (0.025, p=.684); thus, H4b is rejected.

Table 7 Correlations between independent antecedents and latent variables

Independent variables	TChS	TMT	RtoEx
ICT expertise	.118	.100	.048
Income	.025	.159**	.101
Gender	.208**	.107	.214***

The moderating effects of the demographic variables for H4 were analyzed in a regression analysis on H1. Gender and income moderate H1 (adjusted R-squared .118, p=.000). Women and those with higher incomes are more likely to be reluctant to express themselves online if their device privacy and security settings require excessive time to address. Regression was also performed on the antecedents against H2 and H3. Income and gender were found to moderate H2 (adjusted R-squared .072, p=.000). For regression of the antecedents against H3 (TChs -> TMT) yieldeded an effect from income. TChS, combined with income, predicted some variance in TMT (adjusted R-squared .049, p=.001). Users with higher income are more likely to decide, upon consideration of their devices' security issues (TChS), that the issues require too much time to address (TMT). Table 7 shows the correlations between the antecedents and the concern factor and outcome factorsTable 7. The results show a confirmation of H4a and H4c, and rejection of H4b, though income moderated H3 and ICT expertise did not.

Figure 3 presents the results in the applied APCO modelFig. 3. Table 8 presents the percentage of respondents tending to agree with TMT, TChS, and RtoEx. Perhaps strikingly, more than half of all respondents are reluctant to make controversial expressions online, with almost two-thirds of female respondents being reluctant.

Table 8 Percentages of respondents who tend to agree or strongly agree with TMT, TChS, and RtoEx

N=265	Overall addressing security and privacy aspects takes too much time (TMT)	Overall spend time thinking about device security and check/change settings (TChS)	Reluctant to express online (RtoEx)
Overall	30.64	59.6	57.7
Male	32.9	67.8	52.0
Female	27.4	48.7	65.5

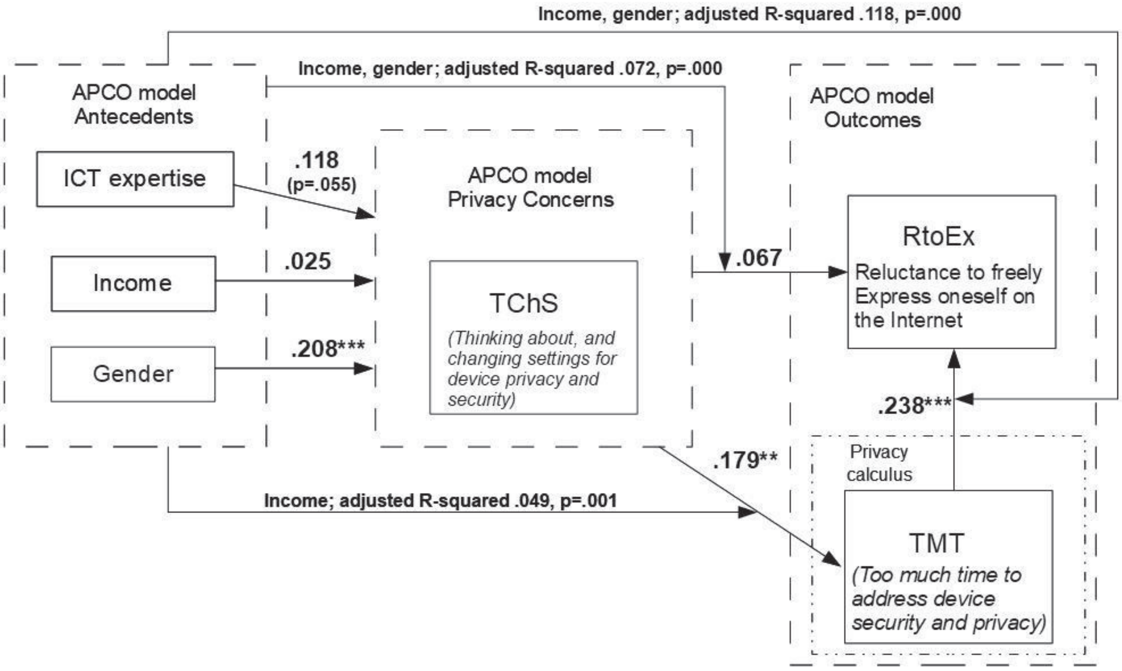

Income, gender; adjusted R-squared .118, p=.000
Income, gender; adjusted R-squared .072, p=.000
APCO model Antecedents
ICT expertise
Income
Gender
.118 (p=.055)
.025
.208***
APCO model Privacy Concerns
TChS
(Thinking about, and changing settings for device privacy and security)
.067
APCO model Outcomes
RtoEx
Reluctance to freely Express oneself on the Internet
.238***
.179**
Privacy calculus
TMT
(Too much time to address device security and privacy)
Income; adjusted R-squared .049, p=.001

Fig. 3 Macro model with results

8. Discussion

Researchers (Smith et al. 2011; Bandyopadhyay 2011) have proposed variations of the APCO model to improve privacy research. Smith et al. (2011) identified gaps in the research based on their review of existing privacy research and its common modeling. Since then, some research has been performed that addresses some of the gaps (Benamati et al. 2017; Zhang et al. 2013; Sun et al. 2019). Our work contributes to the understanding of privacy research by showing relationships between the antecedents of income, ICT expertise and gender; TChS, TMT calculus, and RtoEx outcome. The privacy concern in our application of the model is represented by the latent construct of "thinking about and possibly adjusting security and privacy settings," TChS. We found that income antecedent has a moderating effect on the TChS -TMT correlation. Upon TChS, those users with higher incomes are more likely to experience TMT. Despite our expectations, no such moderating effect was found from ICT expertise. ICT expertise was positively correlated with TChS but did not moderate the relationship between TChS and TMT (H3). We observed that income and gender moderates H1. Women and those with higher incomes are more likely to be reluctant to express themselves online if their device privacy and security settings require excessive time to address. H7b and H7c are confirmed. ICT expertise did not moderate H1, so H7a is rejected.

In this study we used three latent factors; one for RtoEx, *a reluctance to self-express online*; one for TMT which corresponds to *a perception that an excessive amount of one's time is necessary for handling the security and privacy aspects of one's device*; and one for TChS which corresponds to *time being used for considering device cybersecurity and privacy settings aspects*. The factor analysis on the responses to the indicator statements validated our constructs.

Our second goal was to determine the correlations between the factors as well as the correlations between these factors and the two demographic factors. For the 265 responses from our initial survey, the factor correlations between TChS, RtoEx, and TMT were determined as were the correlations between the antecedents and TChS. We found that RtoEx and TMT are positively correlated. A linear regression was also performed on the privacy concern factor TChS and the TMT outcome factor against the RtoEx outcome. The analysis showed that TChS does not moderate TMT against RtoEx. Regression was also performed on the antecedents against H3 (TChs -> TMT). We noted an effect from income. TChS, combined with income, predicted some variance in TMT.

Our findings are in agreement with Tsai et al.'s (2016) findings in that income was not correlated with TChS. TChS is our defined manifestation of “privacy concern.” We did find that ICT expertise was weakly correlated with TChS. Users with more ICT expertise are more likely to TChS. This may be unsurprising in light of the work by Chen et al. (2010), who found that users' preferences for the attributes of shopping websites vary with their levels of computer expertise. Gender was also significantly correlated with TChS thus confirming H4c. Male users are more likely to contemplate and subsequently adjust their device security and privacy settings. This finding has congruency with the statistical data reported by European Commission (2019) and with the research of Girl Scout Research Institute (2019). They found that females are underrepresented in ICT studies (European Commission 2019), and that girls are less confident in their ICT skills than boys (Girl Scout Research Institute 2019). On the other hand, we might have expected that female respondents would be more willing to change settings if they have the necessary skills and the confidence in their skills. This expectation could be inferred based on findings from Regan et al. (2013) and Beaussart and Kaufman (2013).

We found that ICT expertise is weakly correlated with TChS. Sheehan (2002), on the other hand, did not find a significant relationship between intensity of computer usage and privacy concerns. One explanation could be the increase in cyber security awareness in consumers since the time of Sheehan’s study.

Gender, in combination with income, was found to moderate H1, confirming H7b and H7c. The H1 moderation effects of gender and income may be explained by the findings of Chatzitheochari and Arber (2012), Burchardt (2010), and Beaussart and Kaufman (2013). Income and gender also moderated H2, confirming H6b and H6c. This is consistent with findings from Nugent et al. (2016), who reported that individuals (across major religions) with higher incomes tend to have more interest in engaging in political activity and a greater belief in the importance of free speech. The European Commission (2019) and Girl Scout Research Institute (2019) have reported on the ICT education and confidence disparity between genders. Regan et al. (2013) and Beaussart and Kaufman (2013) have reported on the privacy concerns and sensitive disclosure tendencies of females, respectively. Lower ability and confidence to address ICT device settings, and a higher concern about privacy are consistent with our findings.

Zhang et al. (2013) applied the APCO model using CFIP (concern for information privacy) as a proxy for privacy concern. They found that income is not correlated with CFIP in a mobile-commerce context. Our result (income is not found to correlate with TChS) may be consistent with Zhang's finding that income is not correlated with CFIP. We have asserted that TChS corresponds to users' privacy concerns for the purpose of applying the APCO model.

In other previous research applying the APCO model (Sun et al. 2019), mutual online expressions with other social media users over a popular topic (i.e., "hot topic interactivity") has been modeled as an antecedent, agnostic of the controversy of the topic. Sun et al. found that the number of times online shopping per month (this can be construed as “more time spent on the Internet”) had a positive impact on information disclosure behavior (BID). In Sun et al.’s work, BID includes posting personal photos, and personal income information. This subset of BID information is sensitive but not necessarily controversial. Insofar as RtoEx has a negative correspondence with Sun’s BID, and monthly frequency of online shopping can correspond with ICT expertise (our survey’s questions for the ICT expertise construct included a question on the number of years using ICTs and on how many hours a day one uses the Internet), our results differed from Sun et al.’s.

Our earlier work showed a correlation of age to RtoEx (Rauhala et al. 2019b). Sun et al. (2019), on the other hand, found no significant relationship between age and information disclosure. We found no significant correlation of Income and ICT expertise to RtoEx. We have found age to be correlated with TMT, but not with TChS (Rauhala et al. 2019a). This can be considered agreement with Benamati et al. (2017), who found only marginal correlation between age and CFIP (concern about information privacy). Our prior work found that age also moderates the relationship between TMT and RtoEx (Rauhala et al. 2019a). In this study that uses an expanded data set, income was also found to be correlated with TMT, and ICT expertise was found to be weakly correlated with TChS. We have considered the temporal time-in-retrospect and “novelty of time” effects of user perceptions, but such effects are believed to be insignificant to our work. We have shown correlations and effects of the demographic variables income, ICT expertise and gender on an applied APCO model. It should be noted that Benamati et al. (2017) included both limitations of making posts and of making adjustments to Facebook settings into a single construct. In the present paper, we have differentiated and separated out adjustment settings into our TChS construct. The scale for posting limitations has been encompassed by the RtoEx construct.

The excessive time that was spent by one user may be more or less than the excessive time reported by another user. Moreover, with subjective survey questions such as hours, there may even be cases where one respondent's acceptable amount of time may be more than an amount that is considered "too much" by another respondent. However, what is most crucial for TChS is that an amount of time was indeed used for thinking and changing settings; and for TMT that the time spent on security and privacy aspects is judged to be excessive. We assume that a reported excessive (or "too much") time in all cases will be more than an amount of time that the user has deemed as acceptable.

Our results suggest a causal relationship between TMT and RtoEx. Using Antonakis et al.'s (2010) criteria (temporality, correlation, and exclusion of other causes), we assert a temporal relationship by the order of our survey questions and predecession of users' initial device usage by configuration actions (Rauhala et al. 2019a). We should also expect that users should be reluctant to make controversial expressions without cybersecurity protections or privacy protections (e.g., anonymity). Liu et al. (2016) found that users prefer that certain trust conditions should be fulfilled prior to self-disclosure of sensitive personal information. All other possible causes of RtoEx cannot be excluded, but an attitude of TMT implies that the security and privacy settings cannot be accomplished because of insufficient time. Therefore, it is reasonable that RtoEx should follow. TChS was not correlated with RtoEx.

Though there was no correlation between income and TChS, it did moderate the relationship between TChS and TMT (H3). A positive correlation was found between TMT and RtoEx (H1): users who experience TMT are also more likely to experience RtoEx.

9. Limitations

Our study does not examine the effect of time management on the perspective of the person who is waiting. Such time management could include the users' own management of their time while they wait for a security software update. Another example would be the management of the waiting time by a software vendor. The vendor's software could display some content on the user's display during an update (Hanyang et al. 2015). This study also does not account for distortions in the response data caused by time-in-retrospect or "novelty of time" effect. However, the effects of the distortions are believed to be insignificant. This is because users' attitudes and behaviors tend to be guided by their perceptions and not by objective reality.

We have suggested that the survey data from our sample can be inferred to a target population of Internet users of any age who live in western-style democratic societies. However, there is coverage error due to the relatively small sample size.

During statistical analyses of the ordinal Likert response data we have made an assumption of equal intervals. Our results may vary to some degree if there are differences in perceived interval significances by respondents, between individual respondents, or by respondent groups.

There may be some common method bias in the responses. Despite attempting to mitigate implicit theory bias by forbidding the review of earlier than the displayed questions and answers, questions of predicted constructs were often grouped together on the visible page of the survey. The user may have read all of the visible questions before answering them, thus raising a possibility of implicit theory bias.

The survey was administered in English. This could be a limitation because English is not the native language of most of the respondents. However, such respondents were mainly students of college or university level or had already completed their higher education. A readability analysis of the scale questions showed a readability level that ranged from 9th to 12th grade. Many respondents were not native English speakers, so some task factors bias and ability factor bias may be present. The bias may apply for respondents who, for example, are not native English speakers and who study a field in which English is not prevalent in the literature.

We have assumed that the "intratemporal preferences" of our survey respondents are time-consistent. Our study does not differentiate the respondents according to their time-preference dependent behavior choices (e.g., as in O'Donaghue and Rabin, 2000). Future research could categorize survey respondents according to the

O'Donaghue and Rabin behavior framework to gain insight into the online expression reluctance and the privacy and security settings behaviors of Internet users.

With regard to the income variable moderation on the TMT construct, we have assumed that the variable is mainly representative of annual income earned through labor. We have not accounted for other sources of income such as those from investments or gambling. Income from investments or other passive sources do not necessarily require reciprocal time expenditures from users. Gambling income may vary widely with a user's time involvement, as may passive income. Moreover, unlike the time used for the labor income and passive income scenarios, the time spent on gambling may easily result in a very small income, loss of income that was procured from other sources, or debt.

10. Summary and Conclusions

In this study we used three latent factors; one for RtoEx, *a reluctance to self-express online*; one for TMT which corresponds to *a perception that an excessive amount of one's time is necessary for handling the security and privacy aspects of one's device*; and one for TChS which corresponds to *time being used for considering or changing device cybersecurity and privacy settings aspects*. The factor analysis on the responses to the indicator statements validated our constructs. The main results of the present study are presented in Table 9.

Table 9 Summary of results

Hypotheses /observations	Confirmed /rejected	Description	Corroborates, or consistent with	Contradicts, or inconsistent with
H1	***	TMT will positively correlate with RtoEx.	N.A.	N.A.
H2	rejected	TChS will positively correlate with RtoEx.	N.A.	N.A.
H3	**	TChS will positively correlate with TMT	N.A.	N.A.
H4a	(p=.055)	ICT expertise will positively correlate with TChS	Chen, et al. (2010)	Sheehan (2002)
H4b	rejected	Income will positively correlate with TChS	Tsai, et al. (2016) Zhang, et al. (2013)	-
H4c	*** (males)	Gender will correlate with TChS	European Commission (2019) Girl Scout Research Institute (2019)	Sheehan (2002)
H5a	rejected	ICT expertise moderates H3.	N.A.	N.A.
H5b	*	Income moderates H3.	N.A.	N.A.
H5c	rejected	Gender moderates H3	N.A.	N.A.
Observation 1	*	TChS moderates H2	N.A.	N.A.
H6a	rejected	ICT expertise moderates H2	N.A.	N.A.
H6b	**	Income moderates H2	N.A.	N.A.
H6c	***	Gender moderates H2	N.A.	N.A.
Observation 2	rejected	TChS moderates H1	N.A.	N.A.
H7a	rejected	ICT expertise moderates H1	N.A.	N.A.
H7b	*	Income moderates H1	N.A.	N.A.
H7c	***	Gender moderates H1	N.A.	N.A.
Observation 3	rejected	ICT expertise is correlated with RtoEx	-	Sun, et al. (2019)
Observation 4	***	Gender is correlated with RtoEx	Beaussart and Kaufman (2013)	-
Observation 5	**	Income is correlated with TMT	Burchardt (2010)	-

*** = confirmed to three-star significance p ≤ .001, ** = confirmed to two-star significance p ≤ .010, * = confirmed to one-star significance p ≤ .050.

Smith et al.'s (2011) APCO model has aspects that the model's authors believe have been insufficiently addressed in existing privacy research. With our work, we have helped to address this need and contributed to the subset of the antecedents and outcomes of the overarching APCO model. We established the latent factors RtoEx, TMT, and TChS. We have measured and used antecedents (income, ICT expertise and gender) to privacy concerns (TChS) and found a significant result. To increase understanding of the privacy calculus stream within the outcomes construct, we have found the construct TMT and a relationship between it and the RtoEx construct. As an outcome within the model, RtoEx is a measure of online expression reluctance and thus has societal importance as a factor influenced by privacy concerns.

Our analysis revealed some potential differences between responses based on respondents' nationalities. Such differences may be explained by cultural parameters. Relevant cultural parameters for examination in this study's context may include "uncertainty avoidance" or "individualism," as defined by Hofstede (2001). Similar parameters have been defined by House et al. (2004). However, more data in the form of responses from non-Finnish respondents are required for examining this alternative. Variations in the Internet policies of intra-national enterprises and public institutions, as well as in national social media cultures, may also play a role. The cases of online expressions of non-controversial opinions may also be examined further. This research can also be extended by investigating whether users' reluctance to express themselves online is variable with specific topics.

There are some steps that industry and governments could take to improve Internet users' perceptions of online safety. One step that nation-states can take is to modify their cybersecurity strategies. States that have traditionally supported free online expression as a fundamental right for their citizens may choose to create and implement regulations and strategies that improve perceptions of the level of online safety. As a result, their citizens may perceive a reduced need to spend time addressing their device settings or their cybersecurity software. Users would have an increased opportunity to express themselves online or to perform other preferred tasks. The personal cybersecurity products and services industry could design device privacy and security settings to be easier to understand and adjust. The functions to adjust such settings could also be automated more to the background of device or software UIs. One such solution has been studied by Raber and Krueger (2017). Raber and Kreuger propose an algorithm that could predict appropriate privacy and security settings for apps. The predictions are based on an assessment of the user's personality. The settings would then be automatically implemented when the user uses the app. (However, the use of such personality profiling for automated settings adjustments may raise new privacy concerns). In these ways, device security and privacy aspects would require less time for consumers to address. However, the economic motivations for the cybersecurity industry of such enhancements to consumer products and services are not salient.

The differences in attitudes and behaviors between males and females in our study certainly warrant more research. Females are more reluctant to controversially express themselves online. They are also less likely to take steps to improve the cybersecurity of their devices and thus protect their privacy by such steps. This further increases their reluctance to express themselves online. Encouraging and assisting women and girls to receive training in ICT can be one step to address the discrepancies. Respondents who identified as female are also more reluctant to express themselves than males if they perceive that security and privacy settings adjustments take excessive time. The majority of both men and women are reluctant to controversially express themselves online.

Future research can assess the measurable amounts of time that various security software updates or security updates take to complete. This information can be applicable when performing research about users who prefer to update their software manually. Users who manually update can be distinct from users who choose to configure their security software to update automatically, i.e., as background processes.

In the future, research may be applied to an enhanced APCO model, as described by Dinev et al. (2015). Their enhanced model takes more accounting of established behavioral driver concepts from the fields of psychology and economics.

Acknowledgments

[tbd]

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce - EC '04* (p. 21). Presented at the 5th ACM conference, New York, NY, USA: ACM Press. https://doi.org/10.1145/988772.988777

Alqubaiti, Z., Li, L., & He, J. (2016). The Paradox of Social Media Security: Users' Perceptions versus Behaviors. In *Proceedings of the 5th Annual Conference on Research in Information Technology - RIIT '16* (pp. 29–34). Presented at the 5th Annual Conference, Boston, Massachusetts, USA: ACM Press. https://doi.org/10.1145/2978178.2978187

Ancona, D. G., Okhuysen, G. A., & Perlow, L. A. (2001). Taking Time to Integrate Temporal Research. *Academy of Management Review*, *26*(4), 512–529. https://doi.org/10.5465/amr.2001.5393887

Anonymous. (2010, January). KEEPING ONLINE CUSTOMERS. *Dealerscope*, *52*(1), 26.

Antonakis, J., Bendahan, S., Jacquart, P., & Lalive, R. (2010). On making causal claims: A review and recommendations. *The Leadership Quarterly*, *21*(6), 1086–1120. https://doi.org/10.1016/j.leaqua.2010.10.010

Ayaburi, E. W., Wairimu, J., & Andoh-Baidoo, F. K. (2019). Antecedents and Outcome of Deficient Self-Regulation in Unknown Wireless Networks Use Context: An Exploratory Study. *Information Systems Frontiers*, *21*(6), 1213–1229. https://doi.org/10.1007/s10796-019-09942-w

Bandyopadhyay, S. (2011). Antecedents And Consequences Of Consumers Online Privacy Concerns. *Journal of Business & Economics Research (JBER)*, *7*(3). https://doi.org/10.19030/jber.v7i3.2269

Baroni, D. (2015, July 3). New Zealand Government To Punish Online Trolls With Prison Time. *Reaxxion.com*. http://www.reaxxion.com/10115/new-zealand-government-to-punish-online-trolls-with-prison-time. Accessed 10 February 2018

Beaussart, M. L., & Kaufman, J. C. (2013). Gender differences and the effects of perceived internet privacy on self-reports of sexual behavior and sociosexuality. *Computers in Human Behavior*, *29*(6), 2524–2529. https://doi.org/10.1016/j.chb.2013.06.014

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents – Privacy Concerns – Outcomes model. *Journal of Information Science*, *43*(5), 583–600. https://doi.org/10.1177/0165551516653590

Bhattacharya, T., Brown, J., Jaroszynski, M., & Batuhan, T. (2014). The Effects of Perception vs. "Reality" on Travel Behavior after a Major Transit Service Change: The Case of Tallahassee, Florida. *Journal of Public Transportation*, *17*(2), 1–26. https://doi.org/10.5038/2375-0901.17.2.1

Branigan, S. (2011, July 31). Revenge Hacking. *Trends in high tech security*. https://sbranigan.wordpress.com/2011/07/31/revenge-hacking/. Accessed 17 May 2019

Burchardt, T. (2010). Time, income and substantive freedom: A capability approach. *Time & Society*, *19*(3), 318–344. https://doi.org/10.1177/0961463X10369754

Business editors. (2002, July 31). New Study Says Poor Web Site Performance Can Cost Millions in Wasted Marketing Money; Study Cites High Level of Frustration & Abandonment for Popular Sites. *Business Wire*, p. 1. New York.

Butler, R. (1995). Time in organizations: Its Experience, Explanations and Effects. *Organization Studies*, *16*(6), 925–950. https://doi.org/10.1177/017084069501600601

Cassidy, P. (2017, November 3). Man petrol bombed homes in revenge for Facebook post. *STV News*. https://stv.tv/news/east-central/1401461-man-petrol-bombed-houses-in-revenge-for-facebook-post/

Chatzitheochari, S., & Arber, S. (2012). Class, gender and time poverty: a time-use analysis of British workers' free time resources: Class, gender and time poverty. *The British Journal of Sociology*, *63*(3), 451–471. https://doi.org/10.1111/j.1468-4446.2012.01419.x

Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. *Journal of Business Research*, *63*(9–10), 1007–1014. https://doi.org/10.1016/j.jbusres.2009.01.023

Clarkson, J. J., Hirt, E. R., Jia, L., & Alexander, M. B. (2010). When perception is more than reality: The effects of perceived versus actual resource depletion on self-regulatory behavior. *Journal of Personality and Social Psychology*, *98*(1), 29–46. https://doi.org/10.1037/a0017539

Cooper, A. K. (2000, July 12). China: Government punishes Internet journalists. *Committee to Protect Journalists*. https://cpj.org/2000/07/china-government-punishes-internet-journalists.php. Accessed 10 February 2018

Curtom, G. (2014, April 24). Students punished for expressing free speech on Twitter. *The Cougar*. Houston. http://thedailycougar.com/2014/04/24/students-punished-expressing-free-speech-twitter/. Accessed 10 February 2018

Dascalescu, A. (2018, January 3). Doxxing Can Ruin Your Life. Here's How (You Can Avoid It). *Heimdal Security*. https://heimdalsecurity.com/blog/doxxing/#doxxingswatting. Accessed 17 May 2019

Dellaert, B. G. C., & Kahn, B. E. (1999). How tolerable is delay?: Consumers' evaluations of internet web sites after waiting. *Journal of Interactive Marketing*, *13*(1), 41–54. https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<41::AID-DIR4>3.0.CO;2-S

DeVellis, R. F. (2003). *Scale development: theory and applications* (2nd ed.). Thousand Oaks, Calif: Sage Publications, Inc.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Duffy, M. J. (2014, April 30). Freedom of Expression in the Gulf Region. *Global Freedom of Expression, Columbia University*. https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/02/Matt-Duffy_Freedom-of-Expression-in-the-Gulf-Region_0.pdf

European Commission. (2019, April 25). Female students under-represented in ICT. *Eurostat*. https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/EDN-20190425-1. Accessed 12 June 2020

Gandel, S. (2020, January 29). Facebook struggles to stem spread of coronavirus misinformation. *CBS News*. https://www.cbsnews.com/news/facebook-coronavirus-posts-spread-misinformation-on-deadly-outbreak/. Accessed 17 April 2020

Gelber, K., & Stone, A. (2017). Constitutions, gender and freedom of expression: the legal regulation of pornography. In *Constitutions and Gender* (pp. 463–481). Edward Elgar Publishing. https://doi.org/10.4337/9781784716967

Gibson, K. (2020, February 3). Twitter bans Zero Hedge after it posts coronavirus conspiracy theory. *CBS News*. https://www.cbsnews.com/news/twitter-bans-zero-hedge-coronavirus-conspiracy-theory/. Accessed 17 April 2020

Girl Scout Research Institute. (2019). *Decoding the Digital Girl - Defining and Supporting Girls' Digital Leadership* (p. 3). Girl Scouts of the USA. https://www.girlscouts.org/content/dam/girlscouts-gsusa/forms-and-documents/about-girl-scouts/research/GSUSA_GSRI_Decoding-the-Digital-Girl_Full-Report.pdf. Accessed 12 June 2020

Hanyang Luo, Jingjing Wang, Xinwei Han, & Dandan Zeng. (2015). The impact of filler interface on online users' perceived waiting time. In *2015 12th International Conference on Service Systems and Service Management (ICSSSM)* (pp. 1–5). Presented at the 2015 12th International Conference on Service Systems and Service Management (ICSSSM), Guangzhou, China: IEEE. https://doi.org/10.1109/ICSSSM.2015.7170198

Hayes, A. F. (2005). Willingness to Self-Censor: A Construct and Measurement Tool for Public Opinion Research. *International Journal of Public Opinion Research*, *17*(3), 298–323. https://doi.org/10.1093/ijpor/edh073

Hegarty, S. (2020, February 6). The Chinese doctor who tried to warn others about coronavirus. *BBC News*. https://www.bbc.com/news/world-asia-china-51364382. Accessed 17 April 2020

Hicks, R. E., Miller, G. W., & Kinsbourne, M. (1976). Prospective and Retrospective Judgments of Time as a Function of Amount of Information Processed. *The American Journal of Psychology*, *89*(4), 719. https://doi.org/10.2307/1421469

Hillmer, B. (2019, June 6). Leading Practices: Understanding and Reducing Bias in Your Surveys. https://help.surveygizmo.com/help/survey-bias. Accessed 8 April 2020

Ho, S. S., & McLeod, D. M. (2008). Social-Psychological Influences on Opinion Expression in Face-to-Face and Computer-Mediated Communication. *Communication Research*, *35*(2), 190–207. https://doi.org/10.1177/0093650207313159

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values* (1st ed.). Beverly Hills: Sage Publications.

Hofstede, G. H. (2001). *Culture's consequences: comparing values, behaviors, institutions, and organizations across nations* (2nd ed.). Thousand Oaks, Calif: Sage Publications.

House, R. J., & Global Leadership and Organizational Behavior Effectiveness Research Program (Eds.). (2004). *Culture, leadership, and organizations: the GLOBE study of 62 societies*. Thousand Oaks, Calif: Sage Publications.

Jane, E. A. (2015). Flaming? What flaming? The pitfalls and potentials of researching online hostility. *Ethics and Information Technology*, *17*(1), 65–87. https://doi.org/10.1007/s10676-015-9362-0

Jaschik, S. (2014, September 15). Interview with professor fired by West Bank university who compares himself to Steven Salaita. *Inside Higher Ed*. Washington, D.C. https://www.insidehighered.com/news/2014/09/15/interview-professor-fired-west-bank-university-who-compares-himself-steven-salaita

Jones, G. K., & Teegen, H. J. (2001). Global R&D activity of U.S. MNCs: Does national culture affect investment decisions. *Multinational Business Review*, *9*(2), 1–7.

Katz, K. L., & Martin, B. R. (1989). *Improving customer satisfaction through the management of perceptions of waiting*. Massachusetts Institute of Technology. Retrieved from http://hdl.handle.net/1721.1/37703

Krasnick, J. A., & Presser, S. (2010). Question and Questionnaire Design. In *Handbook of Survey Research* (2nd ed., pp. 263–314). Bingley, UK: Emerald Group Publishing Limited. https://web.stanford.edu/dept/communication/faculty/krosnick/docs/2009/2009_handbook_krosnick.pdf

Kwon, O., Kim, C., & Kim, G. (2013). Factors affecting the intensity of emotional expressions in mobile communications. *Online Information Review*, *37*(1), 114–131. https://doi.org/10.1108/14684521311311667

Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese micro-blogging: A social exchange theory perspective. *Information & Management*, *53*(1), 53–63. https://doi.org/10.1016/j.im.2015.08.006

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. *Information Systems Research*, *27*(4), 962–986. https://doi.org/10.1287/isre.2016.0671

Luarn, P., & Hsieh, A.-Y. (2014). Speech or silence: The effect of user anonymity and member familiarity on the willingness to express opinions in virtual communities. *Online Information Review*, *38*(7), 881–895. https://doi.org/10.1108/OIR-03-2014-0076

Lucchi, N. (2011). Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression. *ARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW*, *19*(3), 645–678.

McGrath, J. E. (Ed.). (1988). *The Social psychology of time: new perspectives*. Newbury Park, Calif: Sage Publications.

McGrath, J. E., & Kelly, J. R. (1986). *Time and human interaction: toward a social psychology of time*. New York: Guilford Press.

Merriam-Webster. (n.d.). Controversy. *Merriam-Webster.com*. https://www.merriam-webster.com/dictionary/controversy. Accessed 24 April 2020

Mony, S. (2017, November 11). Cambodian Netizens Face New Risks as Government Tightens Online Controls. *VOA*. Washington, D.C. https://www.voanews.com/a/cambodian-netizens-new-risks-governmentonline-controls/4111483.html. Accessed 10 February 2018

Nadi, Y., & Firth, L. (2004). The Internet Implication in Expanding Individual Freedom in Authoritarian States. In *ACIS 2004 Proceedings*. Presented at the ACIS 2004.

Nugent, J. B., Switek, M., & Wu, F. (2016). Socio-political attitudes across the world: to what extent are they affected by one’s religion, its importance, majority status and relative income? †. *Middle East Development Journal*, *8*(2), 291–328. https://doi.org/10.1080/17938120.2016.1225456

O’Donoghue, T., & Rabin, M. (2001). Choice and Procrastination. *The Quarterly Journal of Economics*, *116*(1), 121–160. https://doi.org/10.1162/003355301556365

O’Donoghue, Ted, & Rabin, M. (2000). The economics of immediate gratification. *Journal of Behavioral Decision Making*, *13*(2), 233–250. https://doi.org/10.1002/(SICI)1099-0771(200004/06)13:2<233::AID-BDM325>3.0.CO;2-U

Ojala, A., & Tyrväinen, P. (2007). Market Entry and Priority of Small and Medium-Sized Enterprises in the Software Industry: An Empirical Analysis of Cultural Distance, Geographic Distance, and Market Size. *Journal of International Marketing*, *15*(3), 123–149. https://doi.org/10.1509/jimk.15.3.123

Phelan, J. (2014, March 24). This is how these 12 countries will punish you for insulting their heads of state. *GlobalPost / PRI*. https://www.pri.org/stories/2014-03-12/how-these-12-countries-will-punish-you-insulting-their-heads-state. Accessed 9 September 2019

Raber, F., & Krueger, A. (2017). Towards Understanding the Influence of Personality on Mobile App Permission Settings. In R. Bernhaupt, G. Dalvi, A. Joshi, D. K. Balkrishan, J. O’Neill, & M. Winckler (Eds.), *Human-Computer Interaction – INTERACT 2017* (Vol. 10516, pp. 62–82). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-68059-0_4

Rauhala, J., Tyrväinen, P., & Zaidenberg, N. (2019a). Does Time Spent on Device Security and Privacy Inhibit Online Expression? In *Proceedings of the 18th European Conference on Cyber Warfare and Security* (pp. 394–402). Presented at the 18th European Conference on Cyber Warfare and Security, S.l.: ACPIL.

Rauhala, J., Tyrväinen, P., & Zaidenberg, N. (2019b). Online Expression and Spending on Personal Cybersecurity. In *Proceedings of the 18th European Conference on Cyber Warfare and Security* (pp. 387–393). Presented at the 18th European Conference on Cyber Warfare and Security, S.l.: ACPIL.

Ray, A., & Kaushik, A. (2017). State transgression on electronic expression: is it for real? *Information and Computer Security*, 00–00. https://doi.org/10.1108/ICS-03-2016-0024

Regan, P. M., FitzGerald, G., & Balint, P. (2013). Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, *26*(1–2), 81–99. https://doi.org/10.1080/13511610.2013.747650

Rothaermel, F. T., Kotha, S., & Steensma, H. K. (2006). International Market Entry by U.S. Internet Firms: An Empirical Analysis of Country Risk, National Culture, and Market Size. *Journal of Management*, *32*(1), 56–82. https://doi.org/10.1177/0149206305277793

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), 21–32. https://doi.org/10.1080/01972240252818207

Shen, F., & Liang, H. (2015). Cultural Difference, Social Values, or Political Systems? Predicting Willingness to Engage in Online Political Discussion in 75 Societies. *International Journal of Public Opinion Research*, *27*(1), 111–124. https://doi.org/10.1093/ijpor/edu012

Sims, J., & Xu, L. (2012). Perceived Risk of Online Shopping: Differences Between the UK and China. In *UK Academy for Information Systems Conference Proceedings* (Vol. 25).

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487. https://doi.org/10.2307/25750688

Smith, Dinev, & Xu. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Stanton, L. (2014, August 18). EFFECT OF “RIGHT TO BE FORGOTTEN” ON FREE EXPRESSION SPARKS DEBATE. *Cybersecurity Policy Report*. New York.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*, *93*(2), 296–311. https://doi.org/10.1177/1077699016630255

Sun, Y., Fang, S., & Hwang, Y. (2019). Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce. *Sustainability*, *11*(12), 3311. https://doi.org/10.3390/su11123311

SurveyMonkey. (2020). How to create a survey that delivers valuable responses in 10 easy steps. https://www.surveymonkey.com/mp/how-to-create-surveys/. Accessed 8 April 2020

Tak-ho, F., Siu-fung, L., Qiao, Q., & Mudie, L. (2020, March 13). Property Tycoon “Cannon” Ren Incommunicado After Critical Article Appears. *Radio Free Asia*. https://www.rfa.org/english/news/china/tycoon-incommunicado-03132020155224.html. Accessed 17 April 2020

Tormala, Z. L., Clarkson, J. J., & Petty, R. E. (2006). Resisting persuasion by the skin of one’s teeth: The hidden success of resisted persuasive messages. *Journal of Personality and Social Psychology*, *91*(3), 423–435. https://doi.org/10.1037/0022-3514.91.3.423

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

UN General Assembly. (1948). *Universal Declaration of Human Rights*. Paris. https://www.un.org/en/universal-declaration-human-rights/index.html

UN Human Rights Council. (2016). *Resolution on the promotion, protection and enjoyment of human rights on the Internet*. Geneva. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Walonick, D. S. (2013). *Survival statistics*. StatPac Incorporated. https://www.statpac.com/surveys/question-order.htm. Accessed 8 April 2020

Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile Commerce and Consumer Privacy Concerns. *Journal of Computer Information Systems*, *53*(4), 31–38. https://doi.org/10.1080/08874417.2013.11645648

Appendix

Table 10 Survey questions to indicate level of reluctance to express (RtoEx)

1. I would never post a controversial message in an online forum.
2. If I have a controversial opinion about something, I'm hesitant to publish it on the Internet.
3. I am, or would be, reluctant to display any of my controversial artwork (writing, music, drawings, etc.) online.
4. It's usually not a good idea to post controversial comments or opinions online.
5 I would never post a controversial message in an online forum, because someone or some organization could get revenge against me.
6. I have decided against posting my political opinion on a discussion forum/message board, because I was concerned about consequences to myself or to someone I care about.
7. When discussing something with a good friend, I feel more safe to express controversial opinions face to face, than by electronic communication.
8. I have decided against posting my controversial opinion on a discussion forum, because of concern that someone, or some organization (including government), might use it against me in the future.

Table 11 Survey questions to indicate that the user contemplates device security aspects (TChS), and perception that dealing with them requires too much of one's time (TMT)

1. When using my computer or smartphone, I spend time making sure that its security software is up to date. (TChS)
2. When I begin using a new computer or smartphone, I first check its privacy settings, and adjust them to my preference. (TChS)
3. I have had less time to finish a task I wanted to do, due to a device security or software security issue. (TMT)
4. It has taken me longer to finish a task I wanted to do, due to a device security or software security issue. (TMT)
5. The security alerts and pop-up notifications of security software take too much time to deal with. (TMT)
6. I have spent a lot of time thinking about my device and software security. (TChS)
7. I would spend more time performing online tasks I want to do, but my device and software security often needs to be considered. (TMT)
8. Device and software security issues take up much of my time. (TMT)

Table 12 Factor loadings of RtoEx scales from order of Table 10

Scale	R1	R2	R3	R4	R5	R6	R7	R8
Loading	.772	.766	.759	.731	.715	.710	.697	.492

Table 13 Factor loadings of TMT scales, in order of scale labelling in Table 11

Scale	TM1	TM2	TM3	TM4	TM5
Loading	.780	.735	.724	.690	.613

Table 14 Factor loadings of TChS scales, in order of scale labelling in Table 11

Scale	TC1	TC2	TC3
Loading	.839	.799	.595

P V

PHYSICAL WEAPONIZATION OF A SMARTPHONE BY A THIRD PARTY

by

Juhani Rauhala 2021

Accepted manuscript; to be published December 2021 in Cyber Security

Physical Weaponization of a Smartphone by a Third Party

Juhani Rauhala

University of Jyväskylä, jussi@ieee.org

Abstract In the literature and media, the treatment of the dangers and exposures posed by smartphones has generally focused on information security or privacy concerns. There have also been reports of fires, explosions, electric shocks, or loss of phone functionality due to faulty design or manufacture. This article provides an overview of acute physical and physiological dangers of smartphones that can be induced or triggered by a third party. It proposes a categorical discussion framework to describe and define the dangers in terms of attack vectors, effects on the smartphone, harms, and potential culprits/instigators. Counterfeit smartphones are themselves a significant potential threat in this context. Finally, some possible solutions and mitigation are suggested as preventive measures. Some templates for threat assessment forms are also proposed.

Keywords: technology acceptance, smartphone dangers, technology abuse, unorthodox weaponization

1 Introduction

It may soon be possible to remotely “self-destruct” a smartphone (Hsu, 2017). Previous reports have shown that ISPs and mobile operators may soon be able to disable smartphones remotely (FoxNews, 2012). Smartphone self-destruction differs from remote disablement in that consumers are not only able to disable their device (similar to PIN locking) but also destroy device data and even components at the hardware level (Hughes, 2017). Self-destruction would make the device unusable for a thief, even if a sophisticated thief could override a disabled state to reactivate the device. User data cannot be physically restored.

A common signal-initiated (or software-based) disablement that can be activated by a user or operator is different from self-destruction. With software-based disabling, a smartphone’s memory cards and chips remain intact, so data may be recoverable. In the self-destruction method described in Hughes (2017), the system data or hardware of the device would be destroyed, making reactivation, data recovery, and use of the device impossible.

The problems and threats related to malicious software and hardware hacking are well known in the cybersecurity community. Connected devices such as computers and even automobiles have been hacked remotely. Such hacking has been done for eavesdropping, remote control of functions, or other purposes. Smartphone cameras and microphones have been activated remotely, and recent WikiLeaks revelations show that remote hacking is possible, at least on Android and iPhone devices (WikiLeaks, 2017a). It was revealed that it is possible for an intelligence agency to override smartphone firmware in the supply chain (Durden, 2017). Android and Apple smartphones have also been subject to malware attacks by actors such as individual hackers who are not affiliated with any government (Brewster, 2015; Eadicicco, 2017). In addition, there are software methods that allow complete remote control of some iPhone and Android phones by a third party (Pagliery, 2015; Wikileaks, 2017a).

This chapter deals with hypothetical actions that are intended to impact the owner of a given smartphone, or more precisely, the primary user (either as an actual or misidentified target, either by design or coincidence). The use of the smartphone by the primary user is assumed to be typical, i.e., users use their devices in ordinary ways. The literature seems to lack an overview of potential third-party induced acute direct manipulations of smartphone hardware that result in physical or psychological threats and dangers. Our intention is to draw attention to the issue, *hoping* that such attention will catalyze preventive and mitigating measures by stakeholders. We attempt to present a discussion framework outlined by a profile of potential threats. Profiling is done by characterizing potential threat vectors, potential third-party actors or culprits, and estimated consequences for the user.

In this work, we do not address certain non-physical dangers posed by weaponized smartphones, such as fraud, privacy threats, security threats, financial loss, or identity theft. Nor do we deal with the weaponization of information, such as an attack on a user by software, messages, or signaling designed to manipulate the user. The misuse of smartphones to trigger the detonation of externally connected explosives (e.g., a roadside bomb to which the phone is connected) is also excluded. We do not treat the abuse of smartphones as blunt force instruments or projectiles. We do not deal with technical details.

The terms “smartphone”, “phone” and “device” are used interchangeably.

2 Remote Destruction of the Smartphone

Researchers have developed a method to remotely trigger the destruction of a smartphone by directing power from the smartphone battery to heat and expand the phone material. The material expands to physically destroy some critical hardware, rendering device data physically unrecoverable and the phone useless (Hughes, 2017). While the remote destruction capability of a smartphone is legal and useful under the intended use scenario, it may lead to more severe and damaging results that can extend far beyond the small integrated circuits and components of the target device. Every smartphone has a battery, a lithium cell, designed to store enough energy to run the device for as long as possible. With the development of battery technology, it has been possible to design and manufacture more efficient batteries. Lithium-ion batteries commonly used in smartphones have a very high energy density (CEI, 2021) and are around 90% efficient (Xiong, 2019). A typical smartphone battery contains about 5 Wh of energy, which is equivalent to 18,000–20,000 J. Utilizing information from Herskowitch (1963) and Wikipedia (2020), this can be calculated to be roughly equivalent to the energy of five grams of TNT or about two M-80 firecrackers (Fig. 1).

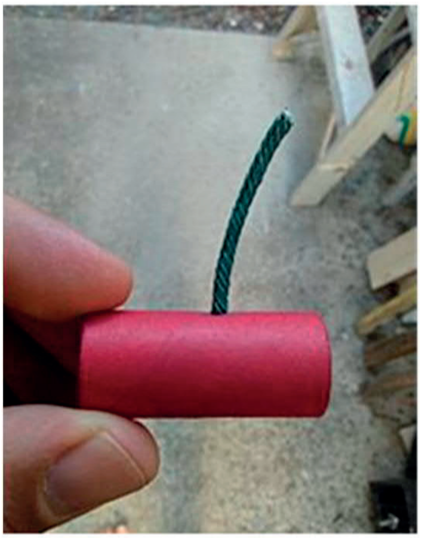


Fig. 1. M-80 firecracker (Wikipedia, 2020)

These small and efficient batteries are not always harmless. Problems with the design or manufacture of the battery can cause malfunctions that result in fires or explosions. Some battery issues can be caused by smartphone design, user operations, or software errors. Explosions in a smartphone battery have been sufficient to cause a short-term shock, injury, or fire (Brown, 2013; Kerr, 2013). In cases where the user does not suffer physical harm, many users consider the loss of a smartphone alone to cause almost as much stress as the threat of terrorism (PhySoc, 2017).

A smartphone is typically owned and used by a single individual. Most people carry their smartphones with them or keep them close all day. Once a person and their smartphone are identified, it is reasonably sure that most of the day the person will carry the smartphone with them, the person will handle it, or it will be close to them. It is conceivable that techniques similar to those described by Hughes (2017) (which trigger a rapid rise in the internal temperature of the device with battery electrodes) could be applied to rapidly cause an uncontrolled thermal reaction of the battery. This in turn can result in a fire or explosion. Thus, it may be possible for a remote hacker to attack a device, causing physical harm to the user. For example, unauthorized tampering with the device firmware or operating system can cause a fire in the device or an explosion of the battery. Hacking could also cause the device to malfunction, which drains the battery very quickly. Indeed, there are smartphone apps freely available that are designed to cause rapid but safe battery discharge (Kushwaha, 2020).

High ambient temperature is one factor known to cause battery fires (Chen & Goode, 2016). Overcharging, abnormally rapid discharge, or short circuiting can cause the smartphone components to overheat, heating the battery, which in turn can cause an explosion or fire. Alternatively, firmware hacking can result in activity that could cause the battery to explode or catch fire. Explosive destruction of the phone battery can even result in the death of the user, see Fig. 2 (Beschizza, 2007; India, 2019; DailyMail, 2009; Prabhu, 2018; Stewart, 2019; Zamfir, 2018). At least one death has been reported due to electric shock when the phone was connected to a charger (Azman, 2019). It should be noted that some of the reported deaths or injuries due to smartphone explosions appear to be hoaxes (Ram, 2014; Yarow, 2010).

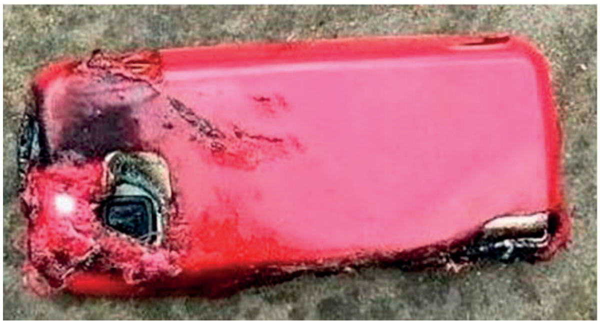


Fig. 2. This explosion caused a user's death (CEN, 2018)

Battery-powered devices that are frequently used with smartphones may also pose threats. Smartphone accessories, such as headphones, are known to overheat or explode, causing burns to the user's face, see Fig. 3 (FoxNews, 2016; Olding, 2017). Even if smartphone batteries are designed to withstand hacking (e.g., with robust short-circuit protection), hacking into any of the user's battery-powered accessories can still pose a danger. Such accessories can be wireless headphones (Olding, 2017) or a Bluetooth earpiece that is used very close to the ear. Bluetooth speakers are also known to burst into flames (Strahan & Novini, 2017).

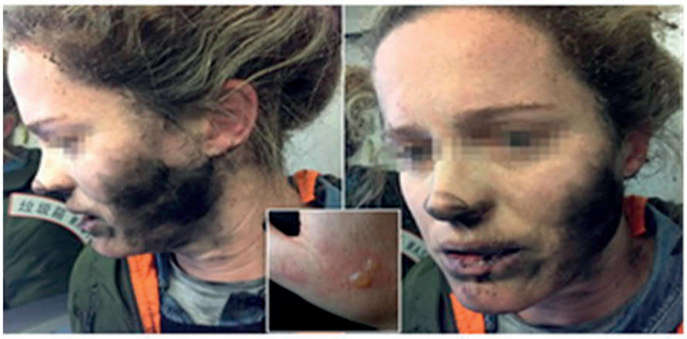


Fig. 3. Battery-operated headphones exploded while the passenger was listening to music (ATSB, 2017)

Hackers or culprits who produce and distribute malware or commit cyberattacks can be individuals or organizations. Recent WikiLeaks documents have revealed the extensive hacking capabilities of a national intelligence agency (WikiLeaks, 2017a). Hacking against smart TVs was developed in cooperation with intelligence agencies in different nations (Wikileaks, 2017b). Some governments around the world are certainly able to develop and implement such hacking or install backdoor capabilities on after-market devices. This ability could give powerful bad actors a personal level "kill switch" to an affected smartphone or accessory. The device could be disabled or destroyed by causing a fire or explosion in the battery. Bad actors could also develop a program or hack that causes the device to emit radiofrequency (RF) radiation at high levels. If the user becomes aware of such an attack, they may feel psychological distress. The distress would depend on their concern about possible radiation exposure and where they usually keep the device relative to their body.

3 Categorical Framework for Smartphone Dangers

Various threat modeling techniques and frameworks exist, but many of them are intended to model threats to large organizations or other high-stakes targets. Examples of such models are listed by Shevchenko (2018). Some of these techniques can be applied, perhaps in awkward ways, to model the threats to individual smartphone users. Based on the author's literature review, there are currently no threat modeling techniques designed to model the specific threats that this chapter focuses on.

3.1 Characteristics of Attack Effect

To assess the potential harm caused by a third-party, we propose the following parameters to facilitate categorization, discussion, and thus understanding:

- Acute vs. chronic,
- Sudden vs. long-term,
- Obvious/salient vs. hidden/obscured,
- Catastrophic vs. undetectable:,
- Maintained functionality vs. compromised functionality vs. eliminated functionality.

Is the effect sudden or long-term? This applies to the first two parameters. For example, a battery explosion will have sudden consequences while increased radio frequency emissions will have a long-term effect. The effect is obvious to the user, for example, when the phone overheats or ignites. An example of a non-obvious effect would be intensified radio frequency emissions. The catastrophic effect significantly impairs the functionality of the smartphone and threatens the user's well-being. Otherwise, the user will not detect any inconvenience or danger during normal use.

An example of the effect of maintaining functionality (excluding battery life) is the increase in radio frequency emissions. Compromised functionality is a scenario in which some functions, such as an Internet connection or a camera/gallery or other function, are forced off, but other important functions, such as the ability to make a call, remain. Eliminated functionality means a case where the smartphone is completely disabled or “bricked.”

3.2 Attack Vectors

Different attack vectors can be used to carry out a smartphone attack:

- Implanted software,
- Voluntarily downloaded software,
- Hijacked default or hijacked downloaded software,
- Implanted firmware,
- Update with malicious firmware,
- Rogue or fake cell towers,
- Using a counterfeit smartphone.

Implanted software is malware or other software that is designed to cause a particular effect through an embedded payload. Voluntarily downloaded software is malware that a user has intentionally downloaded from the Internet. Hijacked default or hijacked downloaded software is firmware or apparently legitimate software that has been infected with a payload of malware. Implanted firmware is firmware that has malware embedded on it when it comes from the factory. Update with malicious firmware occurs when a user updates his/her device with malware-embedded firmware. The user has obtained it from a malicious website or elsewhere.

Rogue or fake cell towers spoof an authentic operator tower. This vector enables communication monitoring of connected devices and the sending of spoofed text messages to these devices (Leiva-Gomez, 2014). Thus, it is possible to organize SMS-based hacking from a fake tower to the victim, such as receiving an image as a text message as described by Pagliery (2015). When using a counterfeit smartphone, the user is using an unauthorized copy of the branded smartphone product. The device manufacturer has not been authorized to manufacture this device and may not be known.

3.3 Attack Perpetrators

The culprit/perpetrator/source of the attack may be

- Single hacker,
- Hacker group,
- Nation state actor,
- Private company,
- Criminal gang/organization.

The perpetrator of an attack may be an individual using one of the attack vectors. In the case of a group of hackers, the attack is carried out in cooperation by several hackers. A national state actor is any entity with the resources and operational support of a national government. A private company refers to a criminal company or part of a private company that makes an attack. A criminal gang/organization is an organized criminal group that carries out an attack, perhaps as part of a turf war or through proxies.

3.4 Weaponizable Components

A weaponizable component can be one of the following:

- RF transmitter,
- Battery,
- User interface (UI) function.

An RF transmitter is a (radio frequency) hardware module that could transmit electromagnetic signals abnormally. The battery inside the smartphone may be damaged. The interactive UI components of the device may start to malfunction.

3.5 Attack Effects

Effects of an attack on a smartphone can be

- Device heating/overheating,
- Battery swelling,
- Battery fire,
- Battery explosion,
- Excessive abnormal radiation from the device,
- Disabling the device,
- Destruction of the device.

As a result of the attack, the device may become hot or overheated. The battery generates enough heat to cause injury to the user and damage the smartphone. Swelling of the battery will damage the operation of the smartphone due to physical damage to the device. When a battery catches fire, it causes (typically) a hot and rapid fire in the smartphone. Explosive energy from the battery can cause injury to the user but may not necessarily destroy data on the device or its functions.

An attack may cause excessive abnormal radiation from the device. In this case, the device's RF modules and antennas emit abnormally high levels of electromagnetic radiation. This can cause the battery to discharge quickly as well as distress to the user. A direct or indirect (timed or user-triggered) disablement of the device by a remote/third party will cause some or all of the device's functions to stop. The functions that are disabled may be critical for a particular user. The remote/third party may cause the device to be destroyed so that no operations can be performed and all data is destroyed. This could be accomplished by a battery explosion or by less visible means, e.g., expansion of a polymer layer that destroys essential components, as described by Hughes (2017).

The harm caused to the user by an attack can be physical. For example, the user suffers from a burn or physiological shock. Psychological consequences can include distress, anxiety, or emotional shock.

In addition to the acute effects, the realization of an attack may have significant secondary effects. Consider a passenger flight. Nearly every passenger carries a battery-powered device. If the battery of the passenger’s device burns or explodes during a flight, the flight may be disrupted. Secondary social impacts may include decreased user confidence in smartphone technology and willingness to use smartphones. Some people who have learned of the incident, and especially its victims and witnesses, may become reluctant to fly.

A hypothetical assessment of weaponizable smartphone components can be found in Table 1 in the Appendix. Using Tables 2, 3, and 4 in the Appendix, a researcher or threat analyst can cross-reference the above parameters against each other to analyze threats. The cells in the tables can be filled with a suitable scale parameter, such as a number ranging from zero to ten. For example, 0 means no threat is detected, and 10 means that the combination has a certain or current manifestation. The tables can also be applied to the analysis of other types of threat scenarios.

4 Nation State as a Bad Actor

Advances in technology have made it possible for various entities to abuse technology. Such entities include nation-states with significant sovereign authority and access to substantial resources. Because of the scale of the influence of nation states, the potential abuse of technology by them is a threat to human rights. Determination and awareness of the threats of abuse often follow mass adaption to new technology.

WikiLeaks' Vault 7 revelations have revealed state-sponsored hacking and malware used on smartphones. NightSkies 1.2, designed to enable complete remote control and management of iPhones, has apparently been implanted in devices during the product supply chain (Durden, 2017). With RoidRage software, a third party can monitor the device's RF functions and SMS messages (Paganini, 2017). The Vault 7 revelations were released in 2008 and comprised only 1% of the leaks (Wikileaks, 2017c). Thus, there is no doubt that more sophisticated hijacking and surveillance tools exist today.

Apps such as TikTok and at least one private technology company that manufactures smartphones have been accused of being channels for international espionage (Kaska et al., 2019; Ryan et al., 2020). The benefits and risks of remotely activated self-destruction of a smartphone should be thoroughly considered for possible abuse. The damaging effects of unethical or illegal hacking on a smartphone battery could be prevented by physical protection measures during design and manufacture. However, manufacturers of counterfeit smartphones, batteries, and accessories may not implement all of the safety features of copied products.

5 Counterfeit Smartphones

Arguably, one of the most significant risk factors for the threats described in this chapter is the widespread availability of counterfeit smartphones. The counterfeit electronics industry as a whole is in the order of US$100 billion and it is estimated that 10% of the world's electronics are counterfeit (Spiegel, 2009). Counterfeit smartphones are relatively cheap to buy, widely available online, and compose a US$48 billion market (Gilchrist, 2017). Authorities have fought against such trafficking (HK-CED, 2018; US-CBP, 2019). A carefully manufactured counterfeit smartphone may appear nearly identical to authentic ones (Evans, 2019). Thus, some consumers may not be able to distinguish counterfeit smartphones. Consumers may also knowingly use a counterfeit without much concern for the risks involved. A study by Liao and Hsieh (2013) found that consumers agreed with the perceived risks of buying counterfeit (or "grey-market") smartphones. However, they only slightly disagreed with the idea or intention of purchasing them: the mean user response was 2.78 on the Likert scale (from 1 = strongly disagree to 5 = strongly agree).

It can be extremely difficult for a consumer to discover or begin to suspect hidden functionalities or backdoors that can be designed for any smartphone. Counterfeit smartphones pose additional risks (Evans, 2019). Detecting malicious or exploitable features that can be embedded in tiny integrated circuits used in smartphones can require considerable technical expertise and expensive sophisticated equipment. At the technology level, counteracting the use of counterfeit smartphones, batteries, and accessories can be difficult. It requires a great deal of involvement from the original manufacturers. One measure to prevent the use of counterfeit batteries has required advanced cryptographic security-based technology (Bush, 2014). Counterfeit devices are often designed and manufactured in areas where government quality control, regulations, and policies are questionable.

In addition to counterfeit smartphones, counterfeit batteries and chargers are widely available. The varying quality of these devices poses its own danger (Best, 2017). With modern technology, it is possible to embed concealed electronics or functionality in a counterfeit product housing, including smartphone accessories. As the Vault 7 revelations suggest, very sophisticated concealed functionality can be embedded in legal and authentic devices. Hidden functionalities could also be embedded in authentic batteries or accessories. One possible scenario is a counterfeit battery installed in an authentic smartphone (or an authentic battery in a counterfeit smartphone) that, together with a malware app, can cause unexpected or dangerous damage. In other words, a malware app or firmware could perform as Hsu (2017) suggests but in a malicious way, weaponizing the smartphone by causing an explosive reaction in the battery. Alternatively, the malware app or firmware may act as a malicious variation of the battery drainage app (Kushwaha, 2020), causing a rapid drainage and (assuming the battery has sufficient charge) a significant temperature rise inside the device. This could also pose a danger to the device and the user.

The use of smartphones is very widespread. Globally, about 6.4 billion people use smartphones (O'Dea, 2021). Entities that can control remote connections to such devices generally have, figuratively speaking, the vicinity of each smartphone user in a wireless tether. The vicinity is either the user's pocket, hand, handbag, nightstand and so on.

6 Discussion

When considering a potential threat posed by a remote-weaponized smartphone, the cybersecurity officer should take security measures as appropriate. For example, for high-profile or VIP personnel gatherings or meetings, a protocol can be implemented that requires attendees to hand over their smartphones to a separate and secure location. Alternatively, guests may be asked to remove the batteries from their phones (which is unfortunately impossible on most modern smartphones). Another possible security measure would be to prevent potential wireless signal triggers by creating an RF interference field around the secured area. RF jamming can also block connections from fake cell towers. During the jamming, smartphones are also rendered incapable of normal wireless communication.

Prevention of the described hypothetical threats can be promoted by advising smartphone users to avoid downloading unknown or unauthorized apps and opening suspicious messages from unknown senders. However, compliance with the advice is not effective against modified firmware embedded in a supply chain or against text message hacking that is activated merely upon delivery. If a bad actor has significant technology resources and expertise at its disposal, threat prevention can be difficult or impossible. Such actors may include a manufacturer of counterfeit phones under the control of a criminal organization or an arm of an authoritarian regime.

Designers could choose materials and configuration models for the smartphone chassis so that the smartphone body would withstand a catastrophic battery fire or explosion. This would provide the user with some protection from injury. This mitigation is problematic in the case of counterfeit phones – not to mention phones specifically designed to be weaponized.

Further research could focus on analyzing suspected counterfeit smartphones and batteries for malicious or dangerous functions. The analyses should include studies of whether such functions are designed or coincidental, whether they are in the smartphone ICs or battery, and whether they are pre-programmed into software or firmware. If a physically harmful function is found, the analyzes should try to determine its triggering mechanisms.

7 Conclusion

The pervasive use of smartphones creates a potentially highly vulnerable target for those malicious parties with sufficient technical means. The technology developed to enable remote-triggered self-destruction of a smartphone could be maliciously abused by a third party to cause catastrophic battery fires and explosions. For the victim, severe heating or explosion of the device can cause distress (about the destruction of the device and the data contained in it and possible thermal damage to property), injury or, at worst, death. The widespread availability of counterfeit devices makes it more difficult to combat such threats. Simply disabling the smartphone can cause significant stress to the victim. A third party guilty of physical weaponization of a smartphone can be any actor, including a nation state-sponsored actor, organization, mafia, company, criminal gang, hacker group, or individual hacker. Regardless of possible culprits, authorities should consider the interests of citizens and fundamental human rights, the role of regulators, and the interests of operators and the high-tech industry when proactively assessing the potential threats and preventive measures.

By no means does the author imply or suggest that any individual or organization was or will be involved as a perpetrator or culprit for any of the hypothetical malicious attack scenarios described. The author is also not aware of any realizations of the attack scenarios that are the focus of this chapter.

References

ATSB (2017). Battery explosion mid-flight prompts passenger warning. Australian Transport Safety Bureau, https://www.atsb.gov.au/media/news-items/2017/battery-explosion-mid-flight/

Azman, K. K. (2019). Man dies of electrocution after his counterfeit phone charger caused an explosion. Says, https://says.com/my/news/man-dies-of-electrocution-after-his-counterfeit-charger-caused-an-explosion

Beschizza, R. (2007). Man killed by exploding cell phone. Wired, https://www.wired.com/2007/07/man-killed-by-e/

Best, S. (2017). Use an iPhone? Check your charger NOW: Study finds 98% of fake Apple power leads risk causing fatal `electric shocks or house fires'. MailOnline, https://www.dailymail.co.uk/sciencetech/article-5155765/98-fake-iPhone-chargers-users-risk-DEATH.html

Brewster, T. (2015). Stagefright: It only takes one text to hack 950 million Android phones. Forbes, https://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/

Brown, H. (2013). Student's cell phone battery explodes, starts a fire. CBS Minnesota, http://minnesota.cbslocal.com/2013/02/21/students-cell-phone-battery-explodes-starts-a-fire/

Chen, A., & Goode, L. (2016). The science behind exploding phone batteries. The Verge, http://www.theverge.com/2016/9/8/12841342/why-do-phone-batteries-explode-samsung-galaxy-note-7

CEI (2021). Lithium-ion battery. Clean Energy Institute, University of Washington. https://www.cei.washington.edu/education/science-of-solar/battery-technology/

DailyMail (2009). Man killed after his mobile phone explodes, severing an artery in his neck. Daily Mail, http://www.dailymail.co.uk/news/article-1134838/Man-killed-mobile-phone-explodes-severing-artery-neck.html

Durden, T. (2017). Wikileaks releases "NightSkies 1.2": Proof CIA bugs "factory fresh" iPhones. The Liberty Beacon, https://www.thelibertybeacon.com/wikileaks-releases-nightskies-1-2-proof-cia-bugs-factory-fresh-iphones/

Eadicicco, L. (2017). Watch out for this iPhone-crashing text message. Time, https://time.com/4637574/iphone-crash-text-2017/

Evans, C. (2019). From the depths of counterfeit smartphones. Trail of Bits, https://blog.trailofbits.com/2019/08/07/from-the-depths-of-counterfeit-smartphones/

FoxNews (2012). Wireless providers to disable stolen phones. Fox News, http://www.foxnews.com/politics/2012/04/10/wireless-providers-to-disable-stolen-phones.html

FoxNews (2016). Cell phone battery catches fire aboard Delta Air Lines flight to Atlanta. Fox News, http://www.foxnews.com/travel/2016/09/16/cell-phone-battery-catches-fire-aboard-delta-air-lines-flight-to-atlanta.html

Gilchrist, K. (2017). Fake smartphone sales cost global industry $48 billion. CNBC, https://www.cnbc.com/2017/02/28/fake-smartphone-sales-cost-global-industry-48-billion.html

Herskowitch, J. (1963). The combustion of a granular mixture of potassium perchlorate and aluminum considered as either a deflagration or a detonation. Technical report, 3063. Picatinny Arsenal, Dover, NJ, https://apps.dtic.mil/sti/pdfs/AD0296417.pdf

HK-CED (2018). Hong Kong Customs combats sale of suspected counterfeit smartphones and accessories. Press release, Customs and Excise Department, Government of the Hong Kong

Special Administrative Region of the People's Republic of China, https://www.customs.gov.hk/en/publication_press/press/index_id_2372.html

Hsu, J. (2017). Self-destructing gadgets made not so mission impossible. IEEE Spectrum, https://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/selfdestructing-gadgets-made-not-so-mission-impossible

Hughes, O. (2017). Mission possible: Self-destructing phones are now a reality. International Business Times, http://www.ibtimes.co.uk/mission-possible-self-destructing-phones-are-now-reality-1605897

India (2019). 22-year-old man dies as mobile phone explodes while charging. India News, https://www.india.com/technology/22-year-old-man-dies-as-mobile-phone-explodes-while-charging-3840866/amp/

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Kerr, D. (2013). Samsung cell phone battery explodes in man's pocket. CNET, https://www.cnet.com/news/samsung-cell-phone-battery-explodes-in-mans-pocket/

Kushwaha, N. (2020). 6 best free battery drain apps for Android. List Of Freeware. https://listoffreeware.com/free-battery-drain-apps-for-android/

Leiva-Gomez, M. (2014). Everything you need to know about fake cell towers. Make Tech Easier, https://www.maketecheasier.com/fake-cell-towers/

Liao, C.-H., & Hsieh, I.-Y. (2013). Determinants of consumer's willingness to purchase gray-market smartphones. *Journal of Business Ethics*, 114(3), 409–424. Doi: 10.1007/s10551-012-1358-7.

O'Dea, S. (2021). Number of smartphone users worldwide from 2016 to 2026 (in billions). Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Olding, R. (2017). Safety warning after passenger's headphones explode on Beijing to Melbourne flight. The Sydney Morning Herald, https://www.smh.com.au/technology/safety-warning-after-passengers-headphones-explode-on-beijing-to-melbourne-flight-20170315-guy6va.html

Paganini, P. (2017). WikiLeaks Vault 7 data leak: Another earthquake in the intelligence community. Infosec Resources, https://resources.infosecinstitute.com/topic/wikileaks-vault-7-data-leak-another-earthquake-intelligence-community/

Pagliery, J. (2015). Android phones can be hacked with a simple text. CNN Business. https://money.cnn.com/2015/07/27/technology/android-text-hack/index.html

PhySoc (2017). Stress in modern Britain. The Physiological Society, https://static.physoc.org/app/uploads/2020/02/20131612/Stress-in-modern-Britain.pdf

Prabhu, A. (2018). Cradle Fund CEO killed by smartphone explosion. Gizbot, https://www.gizbot.com/mobile/news/smartphone-explosion-kills-ceo-cradle-fund-051647.html

Ram, S. (2014). This FB post about a boy getting killed due to an exploding phone is a hoax. Says, https://says.com/my/tech/explosion-of-exploding-phone-that-killed-10-year-old-boy-is-a-hoax

Ryan, F., Fritz, A., & Impiombato, D. (2020). TikTok and WeChat: Curating and controlling global information flows. Australian Strategic Policy Institute, https://www.aspi.org.au/report/tiktok-wechat

Shevchenko, N. (2018). Threat modeling: 12 available methods. Carnegie Mellon University, https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

Spiegel, R. (2009). Counterfeit components remains a huge electronics supply chain problem. Engineering Design News, https://www.edn.com/counterfeit-components-remains-a-huge-electronics-supply-chain-problem/

Stewart, W. (2019). Girl, 14, killed in her sleep 'by exploding phone' after going to bed listening to music while device was charging. The Sun. https://www.thesun.co.uk/news/10032279/schoolgirl-14-killed-sleep-exploding-smartphone-listening-music-device-charging/?utm_campaign=sunmainfacebook300919&utm_medium=Social&utm_source=Facebook#comments

Strahan, T. & Novini, R. (2017). Bluetooth speaker starts smoking on bed, bursts into flames. NBC New York, http://www.nbcnewyork.com/news/local/Bluetooth-Speaker-Bursts-into-Flames-Seen-Smoking-on-Bed-Sources-417596643.html

US-CBP (2019). Philadelphia CBP seizes nearly $1 million in counterfeit smartphones from China. United States Customs and Border Protection, https://www.cbp.gov/newsroom/local-media-release/philadelphia-cbp-seizes-nearly-1-million-counterfeit-smartphones-china

WikiLeaks (2017a). Vault 7: CIA hacking tools revealed. WikiLeaks, https://wikileaks.com/ciav7p1/

Wikileaks. (2017b). Weeping angel (extending) engineering notes. In Vault 7: CIA Hacking Tools Revealed. WikiLeaks, https://wikileaks.org/ciav7p1/cms/page_12353643.html

WikiLeaks (2017c). WikiLeaks has released less than 1% of its #Vault7 series in its part one publication yesterday `Year Zero'. Twitter, https://twitter.com/wikileaks/status/839475557721116672

Wikipedia (2020). M-80 (explosive). Wikipedia, Retrieved September 2, 2020, from https://en.wikipedia.org/wiki/M-80_(explosive)

Xiong, S. (2019). A study of the factors that affect lithium ion battery degradation. M.Sc. thesis, University of Missouri-Columbia. https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/73777/Xiong-Shihui-Research.pdf?sequence=1&isAllowed=y

Yarow, J. (2010). The Droid phone that exploded and blew up a guy's ear? It was just dropped, says Motorola source. Business Insider. https://www.businessinsider.com/droid-phone-explosion-motorola-2010-12?international=true&r=US&IR=T

Zamfir, G. (2018). Girl, 18, killed when mobile phone explodes while she is chatting to relative. Mirror, https://www.mirror.co.uk/news/world-news/girl-18-killed-mobile-phone-12215521

Appendix: Threat analysis

Table 1. Threat analysis of third-party induced weaponization of a smartphone, a hypothetical example

Component/module	Potential result	Attack vector / trigger
RF transmitter	Unnecessary exposure to higher than normal levels of RF radiation	Firmware programming (call to certain number, opening of certain website [malicious code in the site, firmware sniffing for opening of the site,…]
	Heating	Firmware trigger for permanent abnormally excessive transmission strength with every activity that requires a transmission.
		Firmware trigger for maximum transmission power during mundane background transmission activity and/or disabling of OLPC (open-loop power control).
Battery	Swelling	Remote activation
	Fire	Firmware programming (Timer, push-button sequence, phone call, download, malicious app [malware, …]
	Explosion	
UI functionality	Stress and distress to users via disabling of partial or all functionality.	Firmware (implanted during manufacture, or malicious update)
		Malware/virus
		Fake cell tower (via malicious or rogue (hacked) base station)
		Physical damage (via “self-destruct” or battery damage hack)
		Rogue operator employee

Table 2. Threat assessment table: Threat vs. potential culprit

		Culprit				
		Hacker	**Nation-state actor(s)**	**Private corporation**	**Criminal gang/organization**	**Hacker group**
Threat	Device emits excessive heat / overheats					
	Battery swelling					
	Battery fire					
	Battery explosion					
	Abnormal RF emissions					
	Remotely induced disablement of device					
	Remotely induced destruction of device					

Table 3. Threat assessment table: Threat vs. potential trigger/attack vector

		Potential trigger/attack vector						
		Implanted software	Voluntarily downloaded software	Hijacked default or hijacked downloaded software	Implanted firmware	Updated with malicious firmware	Rogue or fake cell towers	Using a counterfeit smartphone
Threat	Device emits excessive heat / overheats							
	Battery swelling							
	Battery fire							
	Battery explosion							
	Abnormal RF emissions							
	Remotely induced disablement of device							
	Remotely induced destruction of device							

Table 4. Threat assessment table: Potential trigger/attack vector vs. potential culprit

		Potential culprit				
		Hacker	Nation-state actor(s)	Private corporation	Criminal gang/organization	Hacker group
Potential trigger/attack vector	Implanted software					
	Voluntarily downloaded software					
	Hijacked default or hijacked downloaded software					
	Implanted firmware					
	Updated with malicious firmware					
	Rogue or fake cell towers					
	User is using a counterfeit smartphone					
	User is using a counterfeit battery/accessory					

P VI

STORAGE PROFILES

by

Juhani Rauhala 2013

Patent No.: US 8,583,689,
Date of Patent: Nov. 12, 2013

US008583689B2

(12) **United States Patent**
Rauhala

(10) **Patent No.: US 8,583,689 B2**
(45) **Date of Patent: *Nov. 12, 2013**

(54) **STORAGE MANAGEMENT OF PROFILES IN MOBILE DEVICES**

(75) Inventor: **Martti Juhani Rauhala**, Lievestuore (FI)

(73) Assignee: **Core Wirless Licensing S.A.R.L.**, Luxembourg (LU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 36 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/239,595**

(22) Filed: **Sep. 22, 2011**

(65) **Prior Publication Data**

US 2012/0011160 A1 Jan. 12, 2012

Related U.S. Application Data

(63) Continuation of application No. 12/041,798, filed on Mar. 4, 2008, now Pat. No. 8,135,745.

(51) **Int. Cl.**
G06F 7/00 (2006.01)
G06F 17/30 (2006.01)

(52) **U.S. Cl.**
USPC **707/784**; 707/813; 707/822

(58) **Field of Classification Search**
USPC 707/705, 781, 783, 784, 785, 813, 821, 707/822, 827
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,754,953	A	5/1998	Briancon
5,867,781	A	2/1999	Hoffmann
5,887,254	A	3/1999	Halonen
5,913,037	A	6/1999	Spofford
5,974,509	A	10/1999	Berliner
6,006,034	A	12/1999	Heath
6,023,620	A	2/2000	Hansson
6,026,366	A	2/2000	Grube
6,052,600	A	4/2000	Fette
6,108,534	A	8/2000	Bourgeois
6,122,523	A	9/2000	Zicker
6,178,443	B1	1/2001	Lin
6,226,739	B1	5/2001	Eagle
6,256,711	B1	7/2001	Berliner
6,381,741	B1	4/2002	Shaw

(Continued)

FOREIGN PATENT DOCUMENTS

CA	2267549	9/2000
EP	0459344	12/1991

(Continued)

OTHER PUBLICATIONS

Khungar, et al., "A Context Based Storage System for Mobile Computing Applications," ACM SIGMOBILE Mobile Computing and Communications Review, Jan. 2005, vol. 9, No. 1, pp. 64-68.

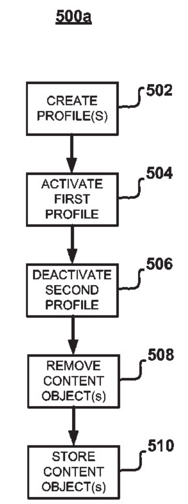
(Continued)

Primary Examiner — Marc Somers
(74) *Attorney, Agent, or Firm* — Winstead PC

(57) **ABSTRACT**

A user may select a profile to serve as an active profile on a device, and content objects associated with the active profile may be stored on the device responsive to the selection. Content objects that are not associated with the active profile may be transferred to one or more additional devices based on a prioritization scheme. Content object download operations may take advantage of the prioritization scheme to determine a storage device for a downloaded content object.

19 Claims, 7 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,393,496	B1	5/2002	Schwaderer
6,411,804	B1	6/2002	Isomichi
6,956,562	B1	10/2005	O'Hara
2002/0022973	A1	2/2002	Sun
2002/0132610	A1	9/2002	Chaplin
2004/0158829	A1	8/2004	Beresin
2004/0255289	A1	12/2004	George
2006/0046696	A1	3/2006	Knowles
2006/0183462	A1	8/2006	Kolehmainen
2006/0200570	A1	9/2006	Stirbu
2006/0242273	A1	10/2006	Fiducci
2007/0081787	A1	4/2007	Hong
2007/0185899	A1	8/2007	Ziv
2007/0240126	A1	10/2007	Allen
2007/0254697	A1	11/2007	Sugio
2008/0034008	A1	2/2008	Burke

FOREIGN PATENT DOCUMENTS

EP	0991290	4/2000
EP	1035741	9/2000
JP	11331911	11/1999
WO	9838820	9/1998
WO	0058838	10/2000
WO	0239231	5/2002

OTHER PUBLICATIONS

Hess, et al., "An Application of a Context-Aware File System," Personal and Ubiquitous Computing, Nov. 14, 2003, vol. 7, No. 6, pp. 339-352.

International Search Report and Written Opinion for PCT/FI2009/050150, dated Jun. 12, 2009.

Jamadagni, et al., "A PUSH Download Architecture for Software Defined Radios", International Conference on Personal Wireless Communications 2000 IEEE, Dec. 17-20, 2000, pp. 404-407, XP002902145.

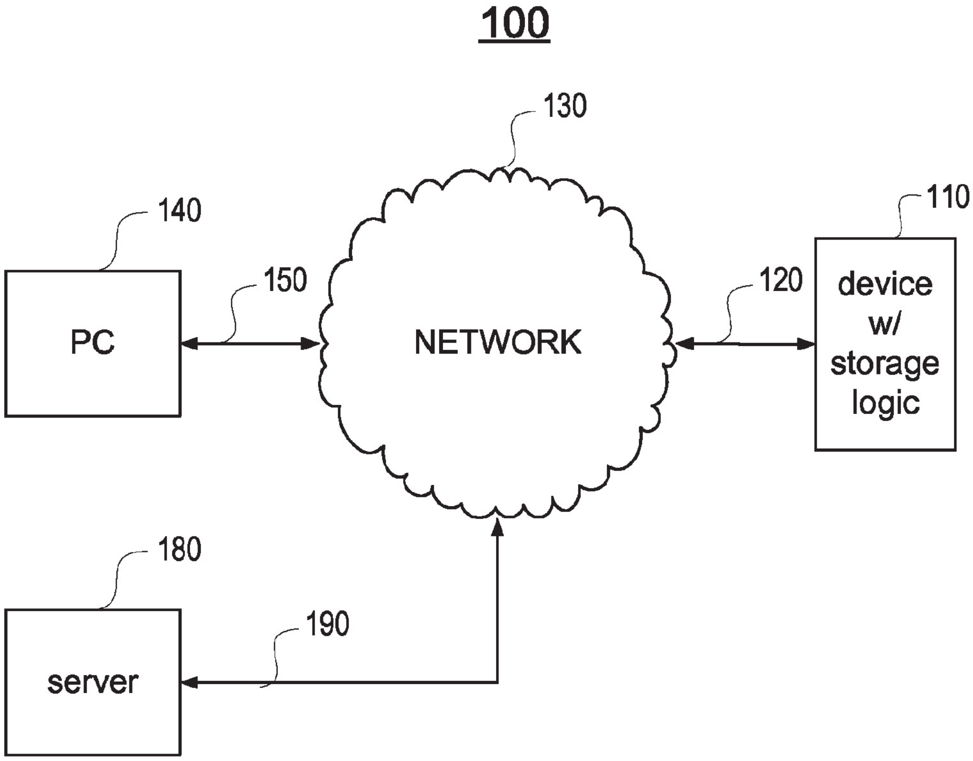

100
130
NETWORK
140
PC
150
110
device
w/
storage
logic
120
180
server
190

FIG. 1

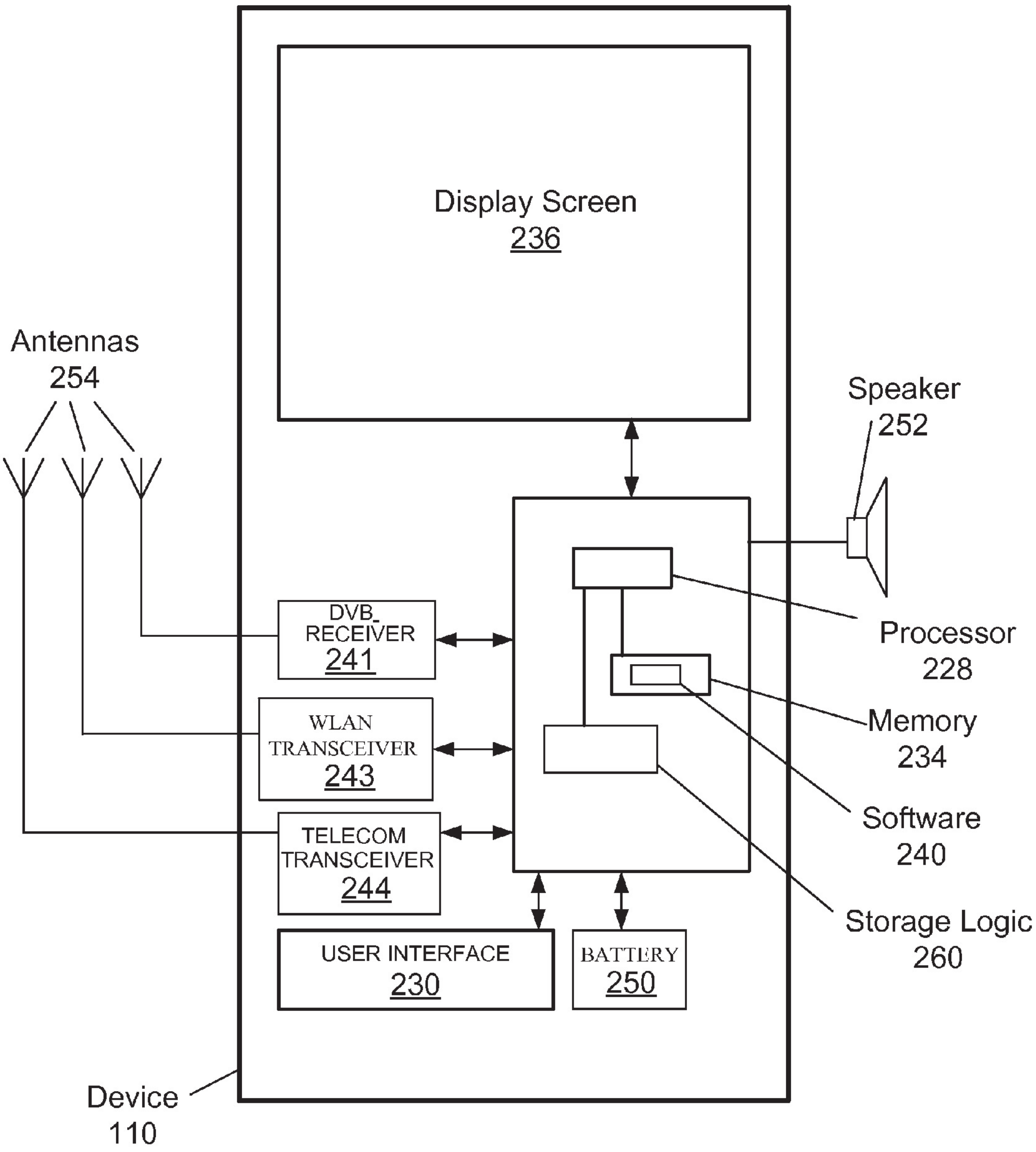
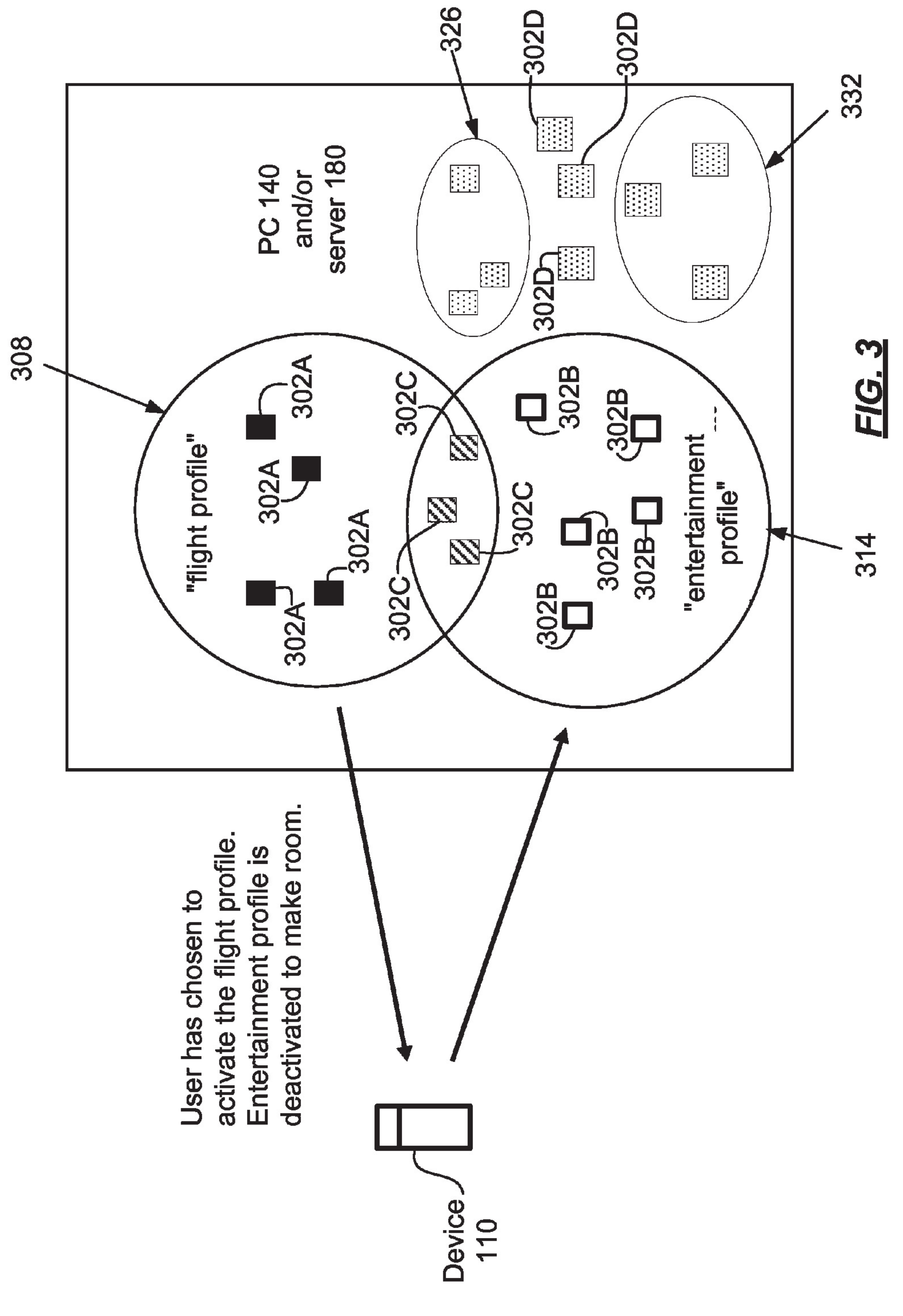

Display Screen
236
Antennas
254
Speaker
252
DVB
RECEIVER
241
WLAN
TRANSCEIVER
243
TELECOM
TRANSCEIVER
244
USER INTERFACE
230
BATTERY
250
Processor
228
Memory
234
Software
240
Storage Logic
260
Device
110

FIG. 2



User has chosen to activate the flight profile. Entertainment profile is deactivated to make room.

FIG. 3

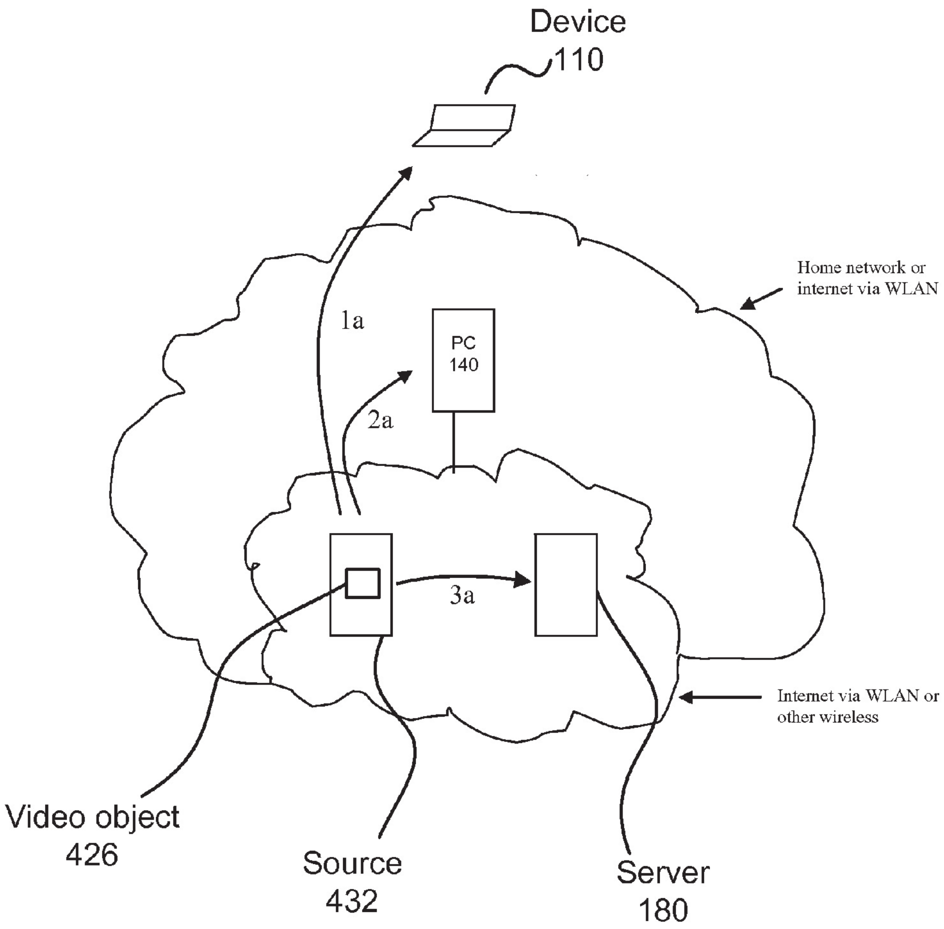

Device
110
Home network or
internet via WLAN
1a
PC
140
2a
3a
Internet via WLAN or
other wireless
Video object
426
Source
432
Server
180

FIG. 4A

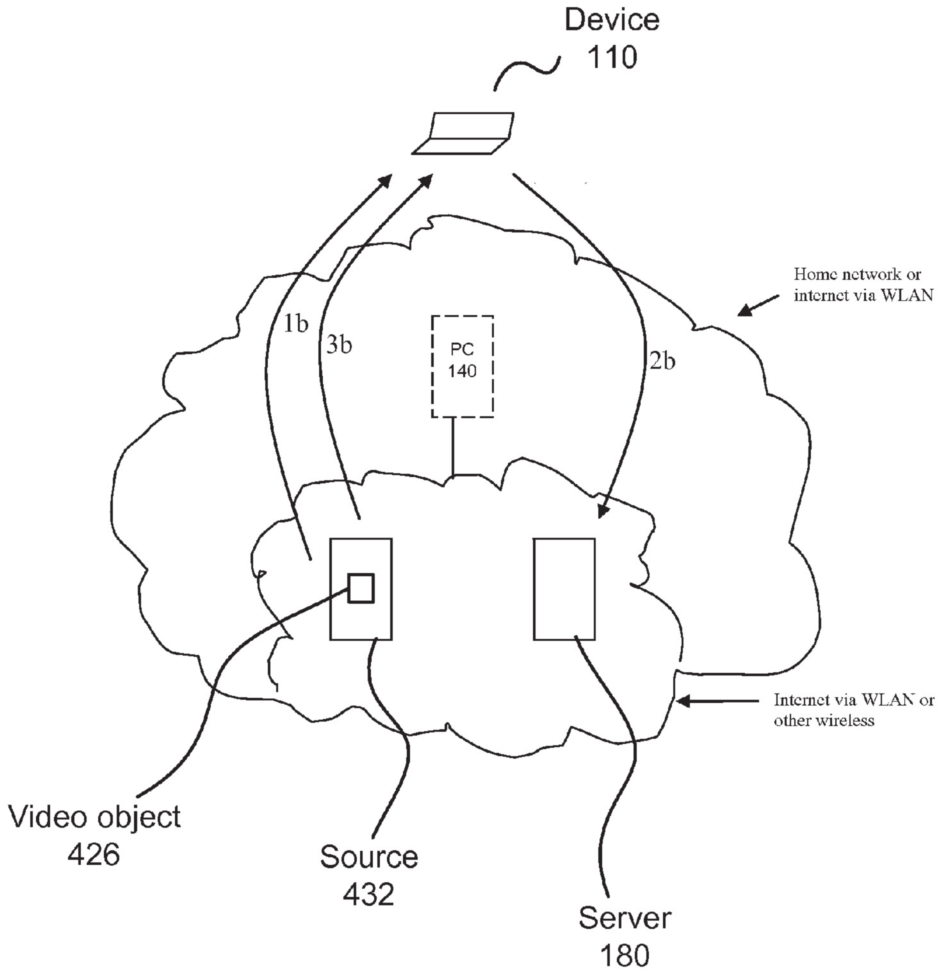

Device
110
Home network or
internet via WLAN
1b
3b
PC
140
2b
Internet via WLAN or
other wireless
Video object
426
Source
432
Server
180

FIG. 4B

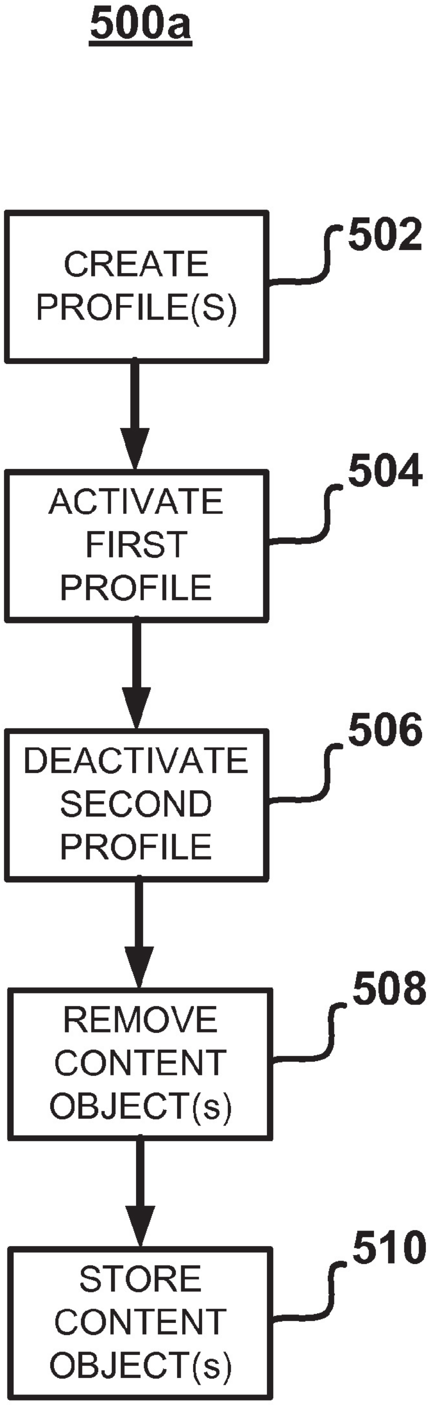

500a
CREATE PROFILE(S)
502
ACTIVATE FIRST PROFILE
504
DEACTIVATE SECOND PROFILE
506
REMOVE CONTENT OBJECT(s)
508
STORE CONTENT OBJECT(s)
510

FIG. 5A

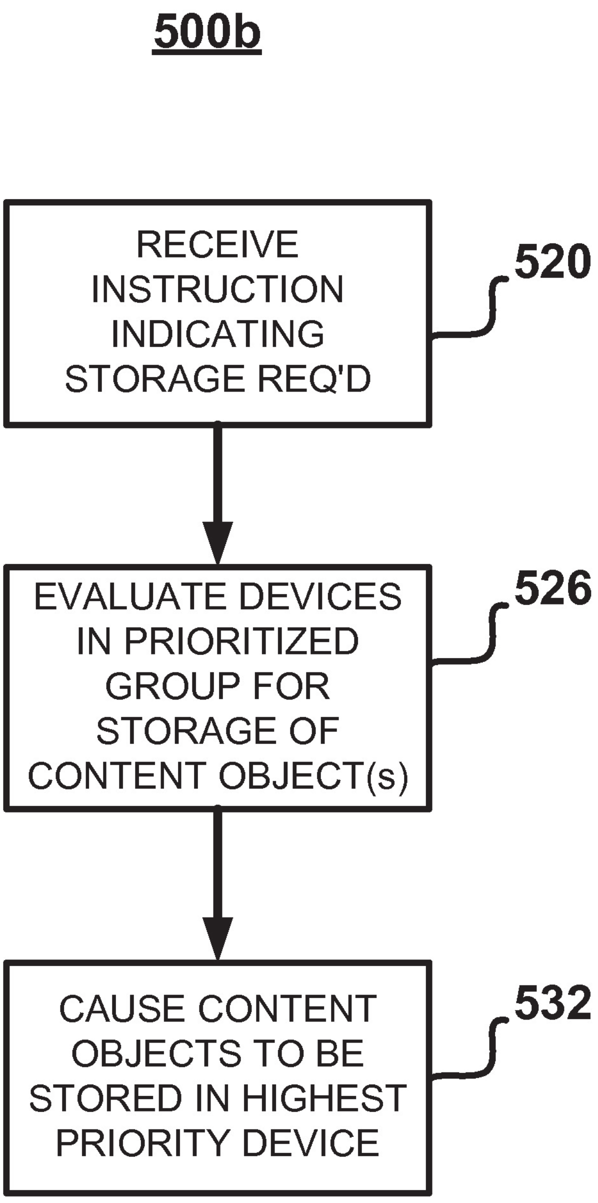

500b
RECEIVE INSTRUCTION INDICATING STORAGE REQ'D
520
EVALUATE DEVICES IN PRIORITIZED GROUP FOR STORAGE OF CONTENT OBJECT(s)
526
CAUSE CONTENT OBJECTS TO BE STORED IN HIGHEST PRIORITY DEVICE
532

FIG. 5B

STORAGE MANAGEMENT OF PROFILES IN MOBILE DEVICES

CROSS-REFERENCES TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 12/041,798, filed Mar. 4, 2008. The contents of the foregoing application are incorporated by reference.

FIELD

This description generally relates to storage of data on electronic devices and management of resources utilized for such storage.

BACKGROUND

Improvements in technology have changed the way people interact with their surrounding environment. These improvements provide opportunities and abilities for users of wireless technology to obtain numerous types of application programs, data files, etc., in almost any location. Today, there is a large amount of content available for downloading from the Internet, and a large number of applications supporting various file types. For example, a user may download a music video clip to her mobile handheld device while at a neighborhood park on Saturday, and may proceed to play it on her device for purposes of entertaining herself and those around her. The same user may be at an airport on Monday morning to take a business trip and wish access to business reports for purposes of giving a presentation. Accordingly, the user receives an email on the same mobile handheld device from a co-worker that includes the desired business reports as an attachment.

Improvements in memory density (e.g., the amount of memory capacity provided per unit area) have enabled users to store an increasing amount of data on devices so as to accommodate these and innumerable other scenarios. Memory capacity is still finite, however, and there are practical limits as to how much data may be stored on a given device at any particular moment. These limits are particularly pronounced in the context of mobile devices, as recent trends suggest that smaller devices are desirable.

By way of illustration, and returning to the previous example, the emailed business reports may require more storage space than is currently free in the mobile device's memory(ies). Although the user may be able to delete one or more currently-stored items to make room for the business reports, this is often undesirable. For example, the user may have recently taken a number of high resolution pictures of the birth of her friend's baby and not wish to lose those images.

BRIEF SUMMARY

The following presents a simplified summary of aspects of certain embodiments. This summary is not an extensive overview, and is not intended to identify key or critical elements or to delineate the scope of the claims.

In some embodiments sets of content objects are associated with content management profiles for a device. When a user activates a content management profile, the content objects in the set of content objects associated with that profile are (to the extent not already present on the device) stored in the device memory. In certain embodiments, storage space in the device for content objects of the activated profile is made available by deactivating a second profile. Content objects in the deactivated profile that are not also in the set of objects associated with the activated profile are removed from the device by deletion or by transferral for storage in another device.

Additional embodiments permit a first device to determine where one or more content objects should be stored. Upon receiving an instruction that corresponds to a requirement for storage capacity, one or more devices in a prioritized group are evaluated for an ability to store the one or more content objects. The content object(s) are then stored on the highest priority device able to store those objects. The prioritized group may or may not include the first device. In some cases, for example, the one or more content objects are being retrieved from a remote source and there is a desire to store those objects on the first device. In such a circumstance, the first device is part of the prioritized group of devices and has the highest priority. In other cases, the one or more content objects are already stored on the first device and there is a desire to remove those content objects from the first device in order to store new content objects. In these circumstances, the first device is not part of the prioritized group.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing summary and the following detailed description are better understood when read in conjunction with the accompanying drawings, which are included by way of example, and not by way of limitation. In the drawings, like reference numbers indicate like features.

FIG. **1** illustrates a network communication environment in which one or more devices are operated and/or one or more methods performed according to some embodiments.

FIG. **2** is a block diagram of a mobile handheld device according to some embodiments.

FIG. **3** is a diagram illustrating the use of content management profiles according to some embodiments.

FIG. **4**A is a diagram illustrating storage of content objects according to some embodiments.

FIG. **4**B is another diagram illustrating storage of content objects according to some embodiments.

FIG. **5**A is a flow chart showing an algorithm according to at least some embodiments.

FIG. **5**B is another flow chart showing an algorithm according to at least some embodiments.

DETAILED DESCRIPTION

In the following description of the various embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown by way of illustration various embodiments in which one or more aspects of the invention may be practiced. It is to be understood that other embodiments may be utilized and structural and functional modifications may be made.

As used herein, "content object" generically refers to any of various types of data. A content object may be, without limitation, one or more of a data object or file (e.g., an image file, a video file, a text file, a spreadsheet, an audio file, a file having one or more slides or other types of presentation(s), etc.) an application program or component thereof, an operating system program or component thereof, a driver, etc.

FIG. **1** is a diagram of a network communication environment **100** in which one or more devices according to some embodiments are operated, and in which one or more methods according to some embodiments are performed. A first device **110** includes logic for managing profiles and for determining an appropriate storage location for content objects and is connected to a network **130** via a connection **120**. Network **130** may include the Internet, an intranet, wired or wireless networks, or any other network suitable for facilitating communication between devices in general. Network **130** may also be a group of interconnected networks. For example, device **110** may communicate with a wireless mobile network, which in turn communicates via the Internet with one or more devices on a remotely-located LAN (local area network) or wireless LAN (WLAN) in a home or office. Also shown in FIG. **1** is a second device **140** connected to network **130** via a connection **150**. In the embodiment of FIG. **1**, device **140** is a personal computer. Further shown in FIG. **1** is a third device **180**. In the embodiment of FIG. **1**, device **180** is a file server (or collection of file servers). Device **180** is in a different location from device **140**, although this need not be the case. Device **180** communicates with network **130** via a connection **190**. By virtue of the connectivity shown, devices **110**, **140**, and **180** communicate with one another. Such communications enable the exchange of various types of information as described herein.

The actual connections represented by connections **120**, **150**, and **190** may be embodied in various forms. For example, one or more of connections **120**, **150**, and **190** may be hardwired/wireline connections. Alternatively, one or more of connections **120**, **150**, and **190** may be wireless connections. Connections **120**, **150**, and **190** are shown in FIG. **1** as supporting bi-directional communications (via the dual arrow heads on each of connections **120**, **150**, and **190**). Alternatively, or additionally, network communication environment **100** may be structured to support dissimilar forward and reverse channel connections between various network entities (e.g., use of one media for communication in one direction and use of a different media for communication in a different direction).

Communication environment **100** may be part of a larger network consisting of additional devices. For example, devices **140** and/or **180** may exchange communications with a plurality of other devices (not shown) in addition to device **110**, and/or device **110** may exchange communications with devices in addition to PC **140** and/or server **180**. Communications in environment **100** may be conducted using one or more of numerous communication protocols. Furthermore, communication environment **100** may include one or more intermediary nodes (not shown) that may forward, buffer, store, route, or otherwise process communications between the various devices.

FIG. **2** is a block diagram of device **110** according to some embodiments. Device **110** could be any of various types of portable electronic devices (e.g., a laptop computer, a notebook computer, some other type of portable computing device, a personal digital assistant, a smart phone, a mobile telephone, some other type of wireless communication device, etc.). All of the components shown in FIG. **2** need not be present in all embodiments. Although various components of device **110** are represented as a single block, device **110** may include more than one of a particular component represented by a given block in FIG. **2**. As shown in FIG. **2**, device **110** includes a processor **228** connected to a user interface **230**, a memory **234** and/or other storage, and a display screen **236**. User interface **230** may further include a keypad, touch screen, voice interface, four arrow keys, joy-stick, stylus, data glove, mouse, roller ball, touch screen, or the like. Device **110** also includes a battery **250**, a speaker **252**, and one or more antennas **254**.

Also included within device **110**, as part of one or more programs executed by processor **228**, is storage logic **260**. Although shown as a separate component in FIG. **2**, storage logic **260** may be included in memory **234** with one or more other programs accessed by processor **228**. In some embodiments, storage logic **260** configures processor **228** to create, execute and otherwise process data in accordance with one or more content management profiles. The operation of content management profiles according to some embodiments is described below. Storage logic **260** further configures processor **228** to determine locations for storage of content objects in memory of device **110**, in device **140**, in device **180**, or elsewhere. The determination of storage locations is also discussed below. In alternate embodiments, storage logic **260** may configure processor **228** to perform less than all of these operations. In still other embodiments, all or part of storage logic **260** may be located in device **140**, device **180**, or in some other location.

As indicated above, executable instructions and data used by processor **228** and other components within device **110** are (in some embodiments) stored in a machine-readable memory **234**. Memory **234** may be implemented with any combination of read only memory modules or random access memory modules, optionally including both volatile and nonvolatile memory. Software **240** (which may include some or all of the elements of storage logic **260**) may be stored within memory **234** (and/or other storage within device **110**) to provide instructions to processor **228** for enabling device **110** to perform various functions described herein. Alternatively, some or all of the instructions executed by processor **228** may be embodied in hardware or firmware (not shown). For example, the executable instructions may be embodied in one or more integrated circuits such as application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), or the like. One of skill in the art will appreciate that integrated circuits may include logic circuits, and that the logic circuits may be configured using one or more programmable files, fuse maps, or the like.

Device **110** may also include additional hardware, software and/or firmware. For example, device **110** may be configured to receive, decode and process digital broadband broadcast transmissions that are based, for example, on the Digital Video Broadcast (DVB) standard, such as DVB-H, DVB-T or DVB-MHP, through a specific DVB receiver **241**. Device **110** may also be provided with other types of receivers for digital broadband broadcast transmissions or for other types of broadcasts (e.g., AM/FM radio). Additionally, device **110** is configured to transmit, receive, encode, decode and process transmissions through one or more of WLAN transceiver **243**, telecommunications transceiver **244**, or other type of wireless communication interface. Device **110**, in at least some embodiments, may also include one or more short-range wired interfaces (e.g., USB) or wireless interfaces (e.g., BLUETOOTH). Additional formats and protocols may be used to convey information, data, messages and the like.

Some embodiments include a machine-readable media holding instructions that, when executed (e.g., by one or more processors within device **110**), cause device **110** and/or other elements in environment **100** to perform various operations as described herein. For example, product implementations may include a series of machine-readable instructions fixed on a tangible storage medium (e.g., a diskette, CD-ROM, ROM, DVD, fixed disk, thumb drive, etc.) or transmittable to device **110** (e.g., via a modem or other interface). The machine-readable instructions may embody all or part of the functionality with respect to a system (e.g., network communication environment **100** of FIG. **1**) or device (e.g., device **110**, device **140** and/or device **180**), and can be written in any of various programming languages for use with many different computer architectures and/or operating systems, as would be readily appreciated by one of ordinary skill. Various embodiments of the invention may also be implemented as hardware, firmware or a combination of software, hardware and/or firmware.

FIG. **3** is a diagram that illustrates the use of content management profiles according to some embodiments. More specifically, FIG. **3** illustrates the use of content management profiles to manage one or more sets of user-defined content objects according to some embodiments. In the example of FIG. **3**, and building on a previous example, a user of device **110** is preparing to board an aircraft for purposes of taking a business trip. During the trip the user will want to access a collection of content objects, shown in FIG. **3** as solid squares **302**A, as well as a collection of objects shown in FIG. **3** as cross-hatched squares **302**C. Those objects may be, e.g., text files, spreadsheets, images, slides, etc. needed to prepare for a meeting. Accordingly, the user inputs commands into device **110** that causes processor **228** to execute instructions to activate a first profile. That first profile ("flight profile" **308**) is associated with the set of content objects the user wishes to access in order to prepare for her meeting. In order to create storage space on device **110** for the content objects in flight profile **308**, a second profile ("entertainment profile" **314**) is deactivated. This deactivation may result from a separate user instruction or may occur automatically in response to activation of flight profile **308**. When entertainment profile **314** is deactivated, content objects associated with profile **314** and which are not associated with profile **308** (shown as white boxes **302**B in FIG. **3**) are deleted and/or transferred.

As used herein, "deleting" a content object from device **110** refers to re-allocation of memory used to store the deleted object for storage of other data. The re-allocated memory may be immediately reused to store other content objects or other data, may be securely erased (e.g., by overwriting with random ones (1s) and zeros (0s)), or simply flagged as available to store other data. "Transferring" a content object refers to re-allocation of the memory used to store the transferred object in conjunction with causing the transferred object to be stored elsewhere (e.g., PC **140**, server **180**, etc.). "Removing" a content object refers to either deleting or transferring that object.

A user may create a profile in any of various ways. In some cases, a user associates content objects with a profile using device **110**. In response to received user instructions defining content objects as part of a set of objects to be associated with a profile, device **110** tags those content objects as associated with that profile. In other cases, a user may create a profile (and define content objects associated with that profile) using a PC (e.g., PC **140**) or other device, and then make that profile (and its associated content objects) available to device **110**. In the example of FIG. **3**, some content objects (shown as cross-hatched boxes) are included within both profile **308** and profile **314**, though this need not be the case. Although only two profiles are shown in FIG. **3**, any number of profiles can be created.

When a user first creates a content object, the user is in some embodiments requested to define which profile(s) (if any) the content object should be associated with. In some embodiments, a newly-created content object is provided with a default tag that automatically serves to associate the newly-created object with one or more default profiles.

Associating content objects with profiles allows the user to load all content objects associated with a given profile by simply specifying the profile. In this manner, a user is not required to remember or search for individual content objects at times when it may be inconvenient to do so. Instead, a user simply instructs device **110** (via an appropriate command) that a particular profile should be made active. In response, processor **228** loads the content objects associated with that activated profile (to the extent any such objects are not already stored on device **110**). Those objects may be loaded from PC **140**, from server **180**, or from some other location. If necessary, processor **228** can also make room for content objects associated with the activated profile by deleting objects in a profile being deactivated and/or by transferring one or more of those objects to PC **140**, sever **180** or to some other location.

In some embodiments, one or more data files storing the association (e.g., a mapping) between content objects and profiles may be stored at device **110** (e.g., in memory **234** of FIG. **2**). In other embodiments, the association data files may also (or alternatively) be stored at another device (e.g., PC **140**, server **180**, etc.).

To the extent a content object in an activated profile is also part of a profile being deactivated, no action is needed. Thus, if the user of device **110** in the example of FIG. **3** is deactivating entertainment profile **314** and activating flight profile **308**, the content objects common to both of those profiles (i.e., the cross-hatched boxes **302**C in FIG. **3**) are already in place and need not be loaded. Although the present example assumes only one profile is active, this need not be the case, and a user may activate more than one profile.

Alternatively, or additionally, one or more of the content objects associated with an active profile might not be physically stored on device **110** as a result of profile activation. Instead, some content objects may be referenced by a link located on device **110**. Linking may be used in some embodiments to preserve memory capacity on device **110**, particularly when a content object requires a large amount of memory capacity relative to a storage capacity required by a link and/or where interruption of network connectivity is not expected.

In some embodiments, and as shown in FIG. **3**, the profiles (e.g., flight profile **308**, entertainment profile **314**, and other profiles **326** and **332**) and content objects **302** are stored on PC **140**, server **180**, and/or other devices. Such devices will often (though not necessarily) have a higher storage capacity than device **110**. Some content objects (e.g., content object **302**D) might not be associated with any profile.

When the user deactivates a profile in some embodiments (e.g., deactivating profile **314** in favor of flight profile **308**), and as discussed above, content objects (e.g., content objects **302**B) not belonging to an active profile are removed from device **110** (e.g., deleted or transferred to another device). In other embodiments, it is desirable to limit the number of content object transactions that occur when activating one profile and deactivating another profile. For example, in order to conserve (battery) power on device **110** or to conserve communication network bandwidth, it may be desirable to limit the number of content objects added to or removed from device **110**. Additional considerations may dictate minimizing the number of content object transactions in order to conserve processing resources on device **110**. For example, device **110** may be running a resource intensive application that requires a majority of the processing resources available on device **110**. In the example of FIG. **3**, content objects in flight profile **308** require a total of 3.5 GB of storage memory and device **110** has 0.5 GB of available storage capacity not being used by entertainment profile **314** or by other data. If the additional content objects added to device **110** as a result of activating profile **308** (e.g., the blackened objects in FIG. **3**) do not exceed 0.5 GB, then removal of content objects will not take place in some embodiments. Conversely, if the content objects being added to device **110** require more than 0.5 GB, at least one content object not in an active profile may require removal.

In some embodiments, device **110** is configured to remove a minimum number of content objects necessary to create sufficient storage capacity to facilitate adding the content objects associated with activated profile **308**. The selection of which content objects to delete from device **110** may be based on various criteria. The selection may be based on a storage capacity required by inactive profile content objects. For example, device **110** may be configured to delete the largest content objects (in terms of memory capacity required to support their storage) first in order to minimize the number of content objects that need to be deleted. The selection of which content objects to delete could also (or alternatively) be based on frequency of use. For example, those content objects that have not been accessed for a relatively long amount of time may be deleted in order to allocate storage capacity on device **110** for content objects associated with a profile being activated. Other criteria may be used to determine which content object(s) to remove from device **110** in order to allocate sufficient storage capacity for flight profile **308**.

In some embodiments, the user receives a warning or indication message on device **110** requesting the user to confirm that it is acceptable for a content object (or group of content objects) to be deleted. The user may thereafter press a key or button on device **110**, provide a verbal command (e.g., in conjunction with speech recognition techniques or the like) or allow a timer on device **110** to expire to confirm the deletion. In some embodiments, device **110** provides the user with a listing of content objects that it recommends as the best candidates for deletion, and the user may be able to select from the recommended candidates.

In some embodiments, processor **228** of device **110** executes one or more algorithms to decide where content objects should be transferred when attempting to create storage space in device **110**. These algorithms can be performed in connection with activating/deactivating one or more profiles, and/or in connection with content that is not associated with a profile. For example, server **180** may be subject to excessive loading at times due to a relatively large number of users attempting to simultaneously access server **180**. Accordingly, device **110** in some embodiments attempts to first transfer content objects to PC **140**. If an attempt to transfer objects to PC **140** is unsuccessful (e.g., if PC **140** is not available because it is offline) device **110** next attempts to transfer content objects to server **180**.

In some embodiments, the capacity available at each of multiple storage locations is analyzed to determine the most appropriate location for content object storage. FIG. **4**A is a diagram showing storage of content objects according to at least one such embodiment. In the example of FIG. **4**A, a user of device **110** initiates a content object download operation to retrieve a music video content object **426** from a source **432**. In the example of FIGS. **4**A and **4**B, device **110** is part of a wireless communication network; that wireless network is in communication with source **432** and server **180** via the Internet, and in communication with PC **140** via the Internet and a home network in which PC **140** is located. Embodiments of the invention include implementations in one or more other types of networks. For example, device **110** may be part of a wireless local area network (WLAN), with that WLAN connected to the Internet. PC **140** could be on that same WLAN.

As shown in FIG. **4**A by arrow **1***a*, device **110** first receives data from source **432** indicating storage space needed for video object **426**. Device **110** compares the size of video object **426** with the available storage capacity at device **110** to determine if device **110** has sufficient storage capacity to support video object **426**. In the example of FIG. **4**A, the memory of device **110** is full (or nearly full). Accordingly, device **110** determines if PC **140** has sufficient memory capacity to store video object **426**. If PC **140** does have sufficient storage capacity, and as shown with arrow **2***a*, video object **426** is saved in storage of PC **140**. If PC **140** does not have sufficient storage capacity (or is offline), device **110** then determines if server **180** is capable of storing video object **426**. If so, device **110** causes video object **426** to be stored at server **180** (arrow **3***a*). If server **180** cannot store video object **426** or is offline, other storage locations (not shown) could be checked, the download of video object **426** aborted (or suspended), or storage capacity made available in device **110** by deleting or transferring other content objects.

As can be appreciated from FIG. **4**A and the foregoing, several storage locations are prioritized. A highest priority is given to device **110**, a lower priority is given to PC **140**, and a still lower priority is assigned to server **180**. The prioritization scheme of FIG. **4**A is only one example, however, and other priority schemes can be used. Priority schemes can be based on bandwidth considerations, security concerns, and/or various other factors.

In some embodiments, a user is able to dictate the priorities associated with devices via one or more directives. The one or more directives may include commands, instructions, or the like. For example, a user downloading a personal banking statement may have previously directed that all downloads from a particular source (e.g., the user's bank) go either to device **110** or to PC **140**, with a higher priority assigned to device **110** in comparison to the priority assigned to PC **140**. Thereafter, the user may, via one or more directives, assign a higher priority to PC **140** (in comparison to device **110**) so as to cause one or more content objects to be stored in PC **140** in preference to device **110**.

In some embodiments, a prioritization scheme is operative with respect to all content objects. For example, a prioritization scheme may serve to prioritize storage in one device (e.g., device **110**) in comparison to another (e.g., PC **140**), and as a result, a downloaded content object may be preferentially routed to the highest priority device (e.g., device **110**) for storage irrespective of the nature of the content object. Alternatively, in some embodiments the prioritization scheme may be related to the nature of the content object. For example, a user may be able to specify via a prioritization scheme that content objects related to entertainment should preferably be routed to device **110** (instead of PC **140**), whereas content objects related to business reports should preferably be routed to PC **140** (instead of device **110**).

In some embodiments, a user may also be able to change devices in a prioritized group by directing that one or more devices be added to or removed from the group. For example, and building on the preceding example, a user may initially include device **110** and PC **140** in a prioritized group for purposes of storing a downloaded personal banking statement. The user may subsequently decide that she wants to use the storage capacity available on device **110** (only) for content objects related to entertainment. Accordingly, the user may remove device **110** from the prioritized group. The user may also add one or more devices (e.g., server **180**) to the prioritized group.

FIG. **4**B is a diagram illustrating another example of storage of content objects according to some embodiments. In the example of FIG. **4**B, video object **426** from a source **432** is again to be downloaded via the Internet and other networks. As shown in FIG. **4**B by arrow **1***b*, device **110** first receives data from source **432** indicating storage space needed for video object **426**. Device **110** compares the size of video object **426** with the available storage capacity at device **110** to determine if device **110** has sufficient storage capacity to store video object **426**. In the example of FIG. **4**B, the memory of device **110** is full (or nearly full). Accordingly, device **110** determines if PC **140** is online and has sufficient storage capacity to accommodate one or more content objects presently stored in memory of device **110**. If PC **140** does have sufficient storage capacity (and is online), device **110** may transfer those content objects to PC **140** by transmitting them to PC **140**. After transmitting the one or more content objects to PC **140**, device **110** may thereafter store video object **426** in its memory. If PC **140** does not have sufficient storage capacity to store one or more content objects (or is unavailable), device **110** determines if server **180** has sufficient storage capacity to store one or more content objects currently stored in memory of device **110**. If server **180** does have sufficient storage capacity, device **110** transmits the one or more content objects stored in memory of device **110** to server **180**. After transmitting the one or more content objects to server **180**, device **110** may thereafter store video object **426** in its memory. In some embodiments, one or more of the content objects being removed from device **110** (in order to accommodate new content object(s)) may be local copies of content objects also stored on PC **140** or server **180**. In such a circumstance, it would not be necessary to transmit that content object to PC **140**, or server **180**, and the locally stored copy could simply be deleted.

As can be appreciated from FIG. **4**B and the foregoing, several storage locations are again prioritized. A first priority is given to PC **140** and a lower priority is assigned to server **180**. A content object (e.g., video object **426**) is "forced" into being stored in device **110**. If device **110** is full, one or more content objects already stored on device **110** are removed by deletion or transfer to another device (e.g., PC **140**, server **180**, etc.) based on relative priorities. As with operations shown in FIG. **4**A, the user of device **110** may (in connection with operations shown in FIG. **4**B) change devices in a prioritized group and/or modify priorities assigned to devices.

One of skill in the art will appreciate that additional levels of storage may be employed in either the scenario of FIG. **4**A or in the scenario of FIG. **4**B (e.g., a user may have access to PCs on multiple LANs). Moreover, one of skill in the art will appreciate that at least some of the embodiments described herein enable one to access and save a content object that is only available for a limited duration. For example, a content object may be a coupon offer that is going to be removed from a commercial server within an hour of viewing it. If a user is two hours away from her home, she might not be able to take advantage of the offer using more traditional methods. Embodiments described herein allow the user to save the coupon offer on her device **110**, PC **140** or server **180** for later access.

In some embodiments, device **110** is configured to display information (e.g., on display screen **236** of FIG. **2**) related to a download progress associated with a download of a content object (e.g., a content object **302** of FIG. **3**, video object **426** of FIGS. **4**A-B, etc.). The display information may be depicted as a bar graph, a pie chart or the like. Alternatively, or additionally, in some embodiments device **110** provides an indication as to what step (e.g., what arrow number in accordance with the arrows/arrow numbers shown in FIGS. **4**A-B) of the download process is being executed at a given point in time. Device **110** may provide an option for canceling the download. Alternatively, or additionally, device **110** may implement a timer such that when the timer expires or reaches a threshold value the download operation is canceled.

FIG. **5**A illustrates an algorithm **500***a* according to at least some embodiments. In the first step of algorithm **500***a* (block **502**), a user creates one or more profiles for device **110**. As explained above, the user may create such profiles using device **110** or using some other device (e.g., PC **140**). In the next step of algorithm **500***a* (block **504**), the user activates one of the previously-created profiles. In some embodiments, a user activates a profile using an explicit command input to device **110**. In other embodiments, a profile may be automatically activated based on some other event. For example, mobile device **110** may detect that it has joined a WLAN corresponding to the user's home and automatically activate a profile the user has selected for use of device **110** when at home. In the next step (block **506**), a second profile is deactivated in conjunction with activation of the first profile. In block **508**, one or more content objects associated with the second profile are removed from device **110** in order to make room for content objects associated with the first profile. In block **510**, content objects associated with the first profile are (to the extent not already present) stored on device **110**.

FIG. **5**B illustrates an algorithm **500***b* according to at least some embodiments. In the first step (block **520**), an instruction is received at device **110** that indicates storage capacity will be required. In at least some embodiments, this instruction corresponds to a request by the user to download content to device **110** from a remotely-located source (e.g., source **432** shown in FIGS. **4**A and **4**B), and the required storage capacity will be at least the amount of storage needed for the content to be downloaded. In the next step (block **526**), one or more devices in a prioritized group of devices are evaluated to determine if one of the evaluated devices has storage capacity that equals or exceeds that storage needed for the content to be downloaded. In some cases, and as explained in connection with FIG. **4**A, storage on some device other than device **110** will be permitted if there is insufficient storage available capacity on device **110**. In such a scenario, device **110** is part of the group of prioritized devices that are evaluated. In other cases, and as explained in connection with FIG. **4**B, the downloaded content will be stored on device **110** even if device **110** does not currently have sufficient available storage capacity. In this scenario, one or more content objects may be transferred from device **110** in order to create storage capacity for the content to be downloaded. Accordingly, the group of prioritized devices includes the devices (other than device **110**) to which the one or more content objects may be transferred. In the next step (block **532**), device **110** causes one or more content objects to be stored on the highest-priority device that was determined (in the evaluation of block **526**) to be able to store those objects. In the scenario of FIG. **4**A, the one or more objects being stored in block **532** are the content that is being downloaded from remote source **432**. In the scenario of FIG. **4**B, the one or more objects being stored in block **532** are the objects being transferred from device **110** to make room for the content being downloaded from remote source **432**.

In some embodiments, device **110** is configured to perform both the algorithm **500***a* of FIG. **5**A and the algorithm **500***b* of FIG. **5**B. In other embodiments, a device such as device **110** is only configured to perform one of algorithms **500***a* or **500***b*. In still other embodiments, algorithms **500***a* and **500***b* are combined into a single algorithm. In yet other embodiments, various steps in algorithms **500***a* and/or **500***b* are omitted and/or rearranged.

Numerous characteristics, advantages and embodiments have been described above with reference to the accompanying drawings. However, the above description and drawings are illustrative only. The invention is not limited to the illustrated embodiments, and all embodiments of the invention need not necessarily achieve all of the advantages or purposes, or possess all characteristics, identified herein. Various changes and modifications may be effected by one skilled in the art without departing from the scope or spirit of the invention. Although example devices and components have been described, the invention is not limited to such devices or components unless specifically required by the language of a claim. The elements and uses of the above-described embodiments can be rearranged and combined in manners other than specifically described above, with any and all permutations within the scope of the invention.

What is claimed is:

1. A method comprising:

deactivating a first profile selected from a plurality of profiles in response to a received instruction, said deactivating including selecting a content object of a first set of content objects associated with the first profile and removing the content object of the first set from a mobile device based at least in part on a size and a frequency of use of the content object of the first set.

2. The method of claim **1**, wherein associations between a second profile and content objects in a second set and associations between the first profile and content objects in the first set are stored at the mobile device.

3. The method of claim **1**, wherein associations between the first profile and content objects in the first set and associations between a second of the plurality of profiles and content objects in a second set are stored on a second device.

4. The method of claim **1**, wherein the content objects include at least one object chosen from the group that includes an image file, a video file, a text file, a spreadsheet, an audio file, and a file having one or more slides or other types of presentations.

5. The method of claim **1**, wherein the first set of content objects includes at least one content object that is in a second set of content objects associated with a second of the plurality of profiles, and wherein the first set of content objects includes at least one content object that is not in the second set of content objects.

6. The method of claim **1**, further comprising: receiving an instruction to download one or more content objects included in a second set of content objects to the mobile device from a remotely located device.

7. The method of claim **1**, further comprising:

receiving an instruction corresponding to a requirement for a storage capacity in one or more memories of the mobile device;

responsive to the received instruction corresponding to the requirement for a storage capacity, evaluating one or more devices in a prioritized group of devices for an ability to store one or more content objects; and

causing the one or more content objects to be stored on the highest priority device of the group able to store the one or more content objects.

8. The method of claim **1**, further comprising:

presenting, on the mobile device, the content object of the first set as a candidate for removal from the mobile device; and

receiving an indication at the mobile device that the content object of the first set is to be removed from the mobile device,

wherein the removing of the content object of the first set from the mobile device is responsive to receiving the indication.

9. The method of claim **8**, wherein the indication comprises at least one of: depression of a key or button on the mobile device, a verbal command, and expiration of a timer on the mobile device.

10. The method of claim **1**, further comprising:

referencing via at least one link, at the mobile device, a second set of content objects that are associated with a second profile responsive to activating the second profile.

11. An apparatus comprising:

at least one processor; and

memory storing instructions that, when executed by the at least one processor, cause the apparatus to:

deactivate a first of a plurality of profiles in response to a received instruction, said deactivating including selecting a content object of a first set of content objects associated with the first profile and removing the content object of the first set from the apparatus based at least in part on a size and a frequency of use of the content object of the first set.

12. The apparatus of claim **11**, wherein associations between the first profile and content objects in the first set and associations between a second of the plurality of profiles and content objects in a second set are stored at the apparatus.

13. The apparatus of claim **11**, wherein associations between the first profile and content objects in the first set and associations between a second of the plurality of profiles and content objects in a second set are stored on a second apparatus.

14. The apparatus of claim **11**, wherein the content objects include at least one object chosen from the group that includes an image file, a video file, a text file, a spreadsheet, an audio file, and a file having one or more slides or other types of presentations.

15. The apparatus of claim **11**, wherein the first set of content objects includes at least one content object that is in a second set of content objects associated with a second of the plurality of profiles, and wherein the first set of content objects includes at least one content object that is not in the second set of content objects.

16. The apparatus of claim **11**, wherein the instructions, when executed by the at least one processor, cause the apparatus to:

receive an instruction to download one or more content objects included in a second set of content objects to the apparatus from a remotely located device.

17. The apparatus of claim **11**, wherein the instructions, when executed by the at least one processor, cause the apparatus to:

receive an instruction corresponding to a requirement for a storage capacity in one or more memories of the apparatus;

responsive to the received instruction corresponding to the requirement for a storage capacity, evaluate one or more devices in a prioritized group of devices for an ability to store one or more content objects; and

cause the one or more content objects to be stored on the highest priority device of the group able to store the one or more content objects.

18. The apparatus of claim **11**, wherein the instructions, when executed by the at least one processor, cause the apparatus to:

present the content object of the first set as a candidate for removal from the apparatus; and

receive an indication at the apparatus that the content object of the first set is to be removed from the apparatus, wherein the removal of the content object of the first set from the apparatus is responsive to receiving the indication.

19. The apparatus of claim **11**, wherein the instructions, when executed by the at least one processor, cause the apparatus to:

reference via at least one link, at the apparatus, a second set of content objects that are associated with a second profile responsive to activating the second profile.

* * * * *

P VII

STORAGE MANAGEMENT

by

Juhani Rauhala 2012

Patent No.: US 8,135,745,
Date of Patent: March 13, 2012.

US008135745B2

(12) United States Patent
Rauhala

(10) **Patent No.: US 8,135,745 B2**
(45) **Date of Patent: Mar. 13, 2012**

(54) **STORAGE MANAGEMENT**

(75) Inventor: **Martti Juhani Rauhala**, Lievestuore (FI)

(73) Assignee: **Core Wireless Licensing S.A.R.L.**, Luxembourg (LU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 314 days.

(21) Appl. No.: **12/041,798**

(22) Filed: **Mar. 4, 2008**

(65) **Prior Publication Data**

US 2009/0228536 A1 Sep. 10, 2009

(51) **Int. Cl.**
G06F 7/00 (2006.01)
G06F 17/30 (2006.01)

(52) **U.S. Cl.** **707/784**; 707/813; 707/822

(58) **Field of Classification Search** 707/705, 707/781, 783, 784, 785, 813, 821, 822, 827
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,754,953	A	5/1998	Briancon et al.	
5,867,781	A	2/1999	Hofmann	
5,887,254	A	3/1999	Halonen	
5,913,037	A	6/1999	Spofford et al.	
5,974,509	A	10/1999	Berliner	
6,006,034	A	12/1999	Heath et al.	
6,023,620	A	2/2000	Hansson	
6,026,366	A	2/2000	Grube	
6,052,600	A	4/2000	Fette et al.	
6,108,534	A	8/2000	Bourgeois et al.	
6,122,523	A	9/2000	Zicker et al.	
6,178,443	B1	1/2001	Lin	
6,226,739	B1	5/2001	Eagle	
6,256,711	B1	7/2001	Berliner	
6,381,741	B1	4/2002	Shaw	
6,393,496	B1	5/2002	Schwaderer et al.	
6,411,804	B1	6/2002	Isomichi et al.	
6,956,562	B1	10/2005	O'Hara et al.	
2002/0022973	A1 *	2/2002	Sun et al.	705/3
2002/0132610	A1	9/2002	Chaplin et al.	
2004/0158829	A1	8/2004	Beresin et al.	
2004/0255289	A1 *	12/2004	George et al.	717/174
2006/0046696	A1 *	3/2006	Knowles et al.	455/412.1
2006/0183462	A1 *	8/2006	Kolehmainen	455/411
2006/0200570	A1	9/2006	Stirbu et al.	
2006/0242273	A1 *	10/2006	Fiducci	709/220

(Continued)

FOREIGN PATENT DOCUMENTS

CA	2267549	9/2000

(Continued)

OTHER PUBLICATIONS

Khungar, et al., "A Context Based Storage System for Mobile Computing Applications", ACM SIGMOBILE Mobile Computing and Communications Review, Jan. 2005, vol. 9, No. 1, pp. 64-68.

(Continued)

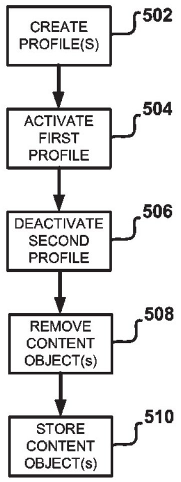
Primary Examiner — Marc Somers
(74) *Attorney, Agent, or Firm* — AlbertDhand LLP

(57) **ABSTRACT**

A user may select a profile to serve as an active profile on a device, and content objects associated with the active profile may be stored on the device responsive to the selection. Content objects that are not associated with the active profile may be transferred to one or more additional devices based on a prioritization scheme. Content object download operations may take advantage of the prioritization scheme to determine a storage device for a downloaded content object.

20 Claims, 7 Drawing Sheets

500a



U.S. PATENT DOCUMENTS

2007/0081787	A1*	4/2007	Hong et al.	386/83
2007/0185899	A1*	8/2007	Ziv et al.	707/102
2007/0240126	A1	10/2007	Allen	
2007/0254697	A1*	11/2007	Sugio et al.	455/556.2
2008/0034008	A1*	2/2008	Burke et al.	707/201

FOREIGN PATENT DOCUMENTS

EP	0459344	12/1991
EP	0991290	4/2000
EP	1035741	9/2000
JP	11331911	11/1999
WO	9838820	9/1998
WO	0058838	10/2000
WO	0239231	5/2002

OTHER PUBLICATIONS

Hess, et al., "An Application of a Context-Aware File System", Personal and Ubiquitous Computing, Nov. 14, 2003, vol. 7, No. 6, pp. 339-352.

International Search Report and Written Opinion for PCT/FI2009/050150 dated Jun. 12, 2009.

Jamadagni, et al., "A PUSH Download Architecture for Software Defined Radios", International Conference on Personal Wireless Communications 2000 IEEE, Dec. 17-20, 2000, pp. 404-407, XP002902145.

* cited by examiner

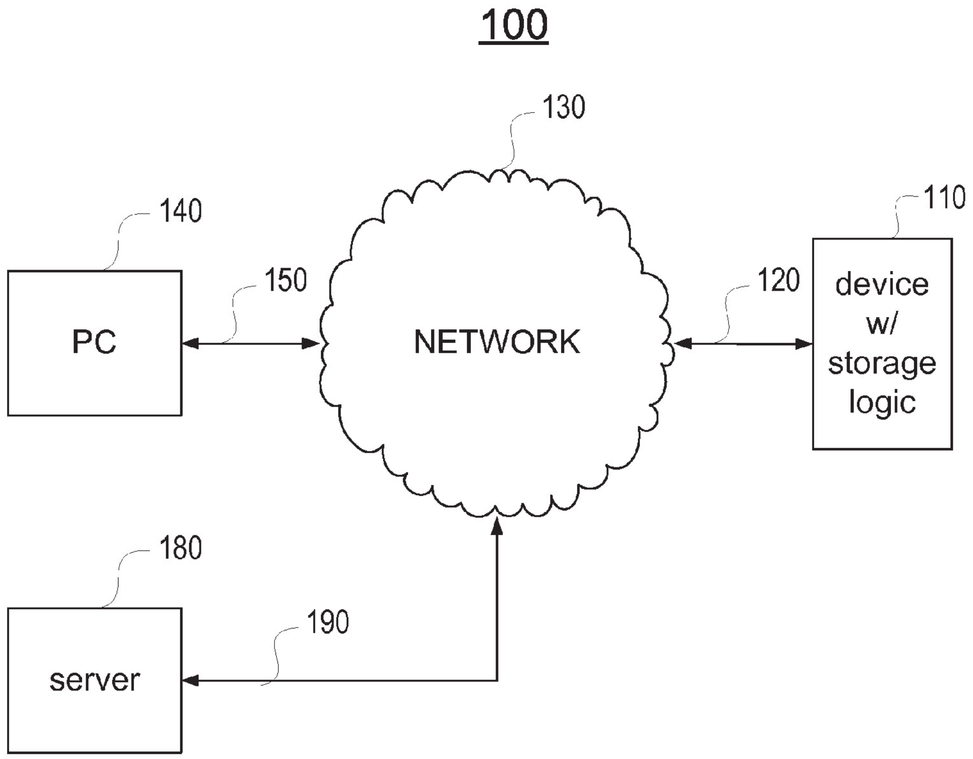

100
130
140
110
150
120
PC
NETWORK
device
w/
storage
logic
180
190
server

FIG. 1

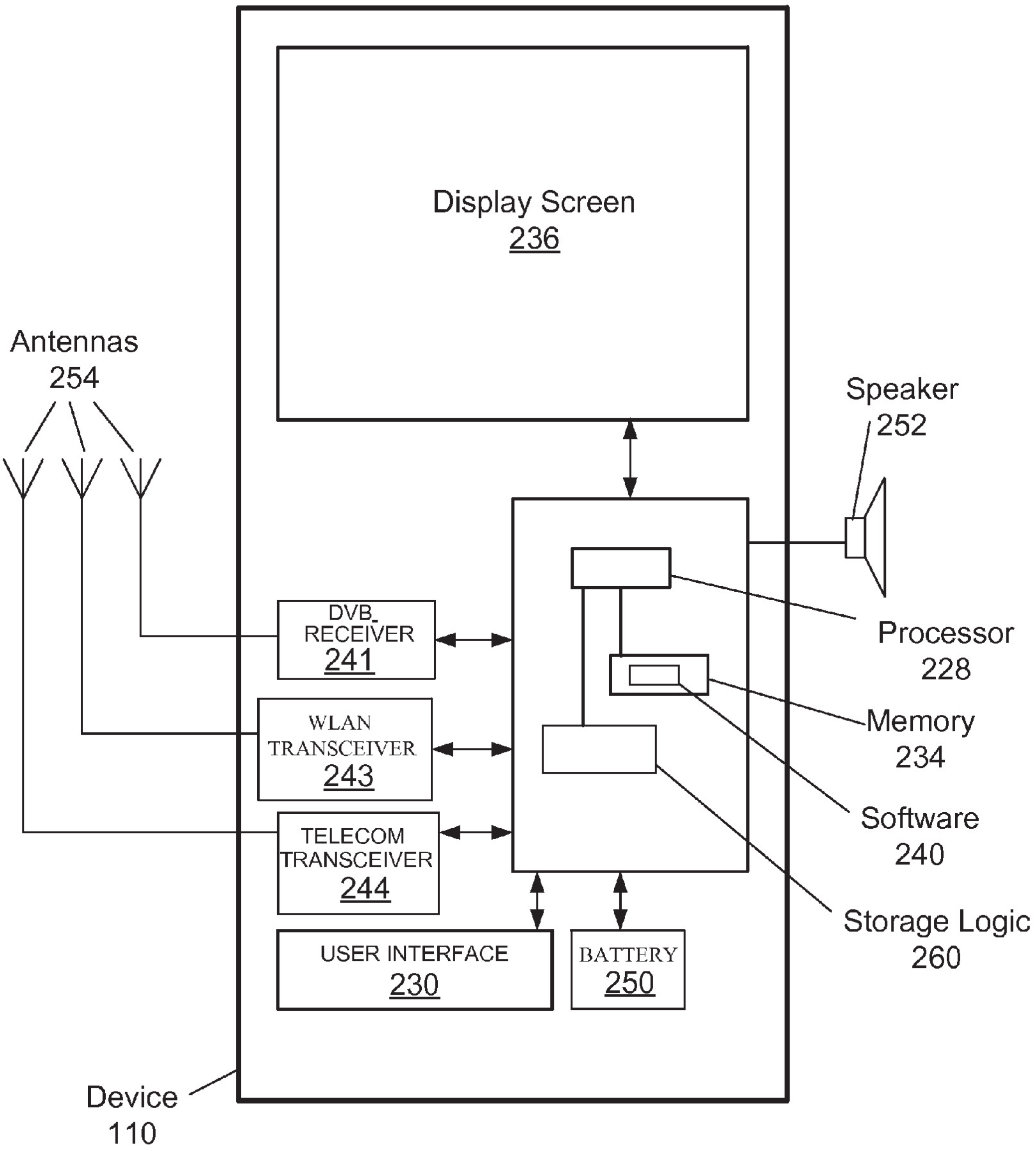
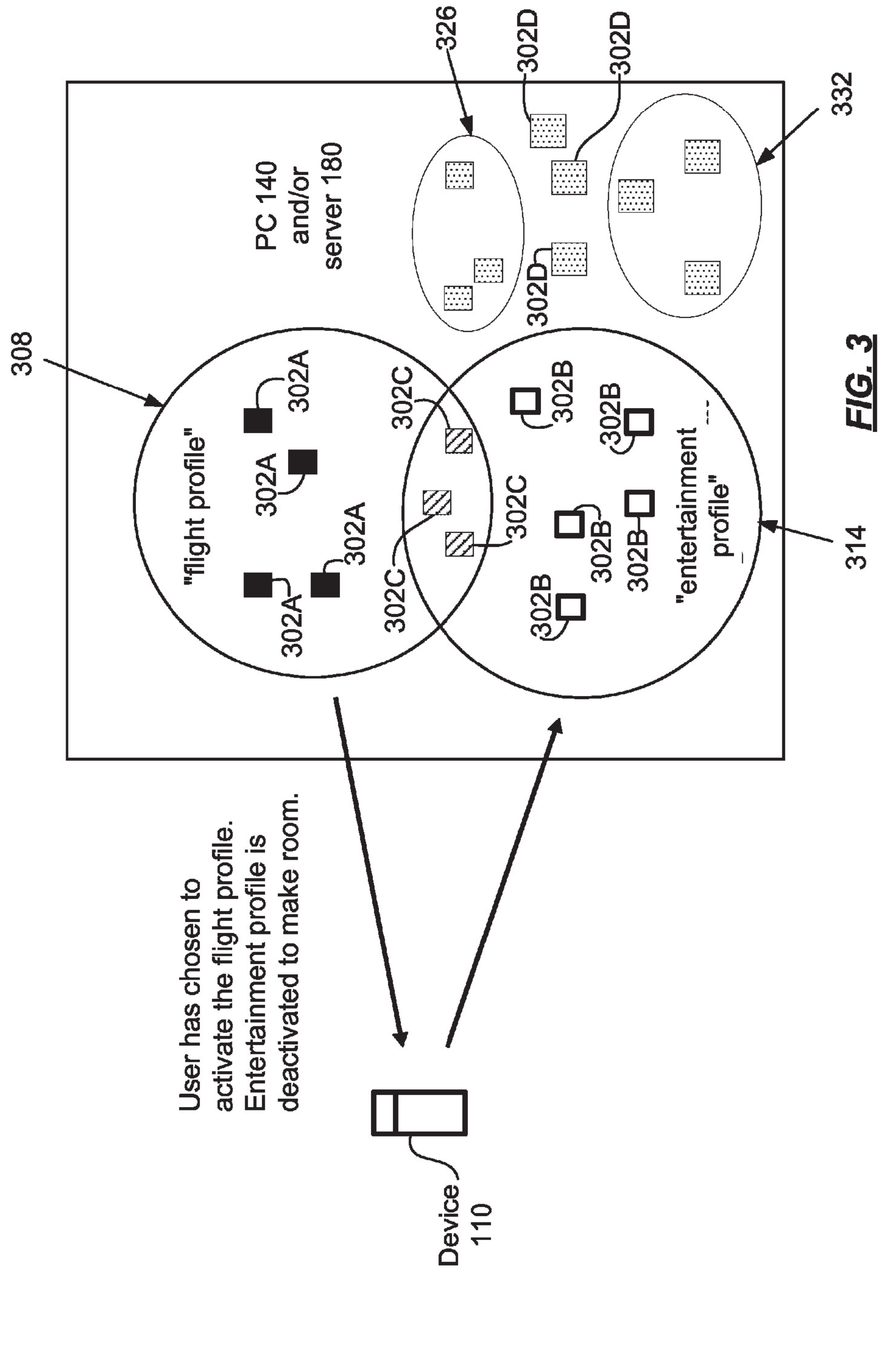

Display Screen
236
Antennas
254
Speaker
252
DVB
RECEIVER
241
WLAN
TRANSCEIVER
243
TELECOM
TRANSCEIVER
244
USER INTERFACE
230
BATTERY
250
Processor
228
Memory
234
Software
240
Storage Logic
260
Device
110

FIG. 2



User has chosen to activate the flight profile. Entertainment profile is deactivated to make room.

FIG. 3

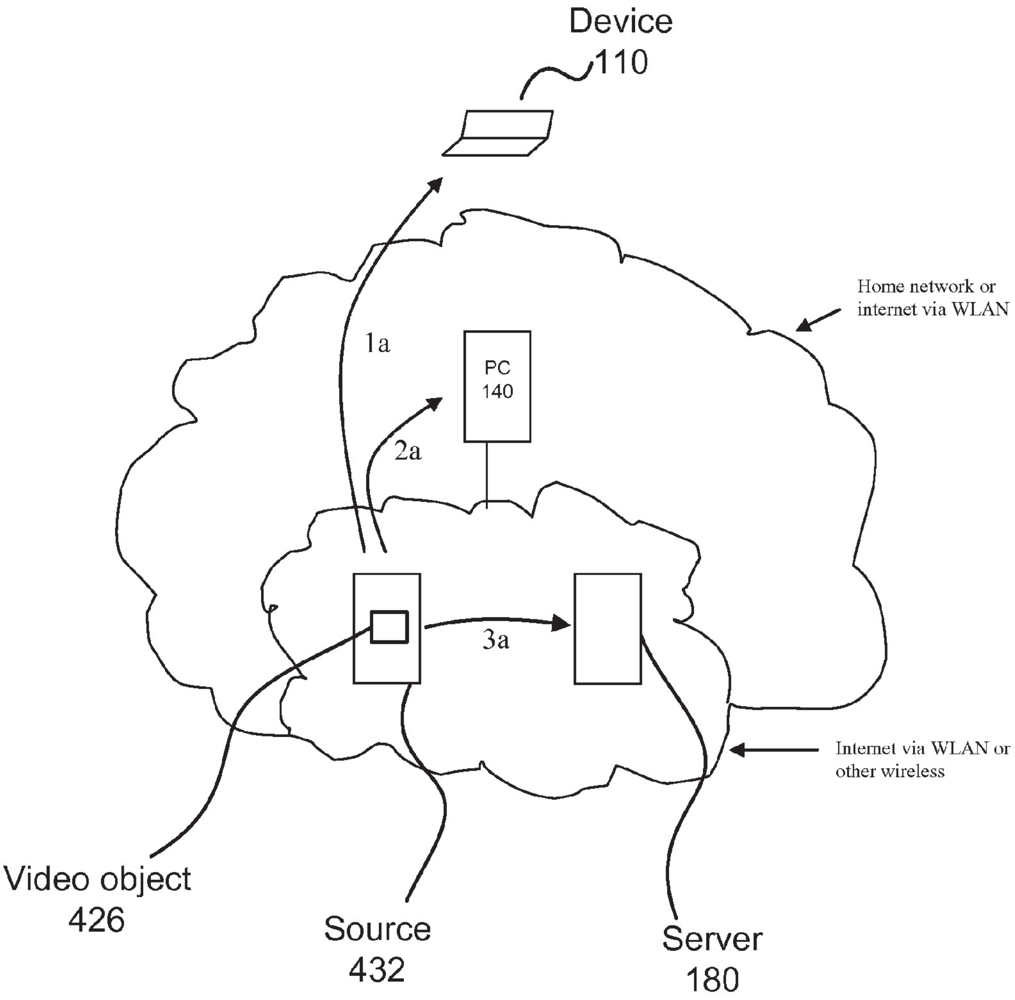

Device
110
Home network or
internet via WLAN
1a
PC
140
2a
3a
Internet via WLAN or
other wireless
Video object
426
Source
432
Server
180

FIG. 4A

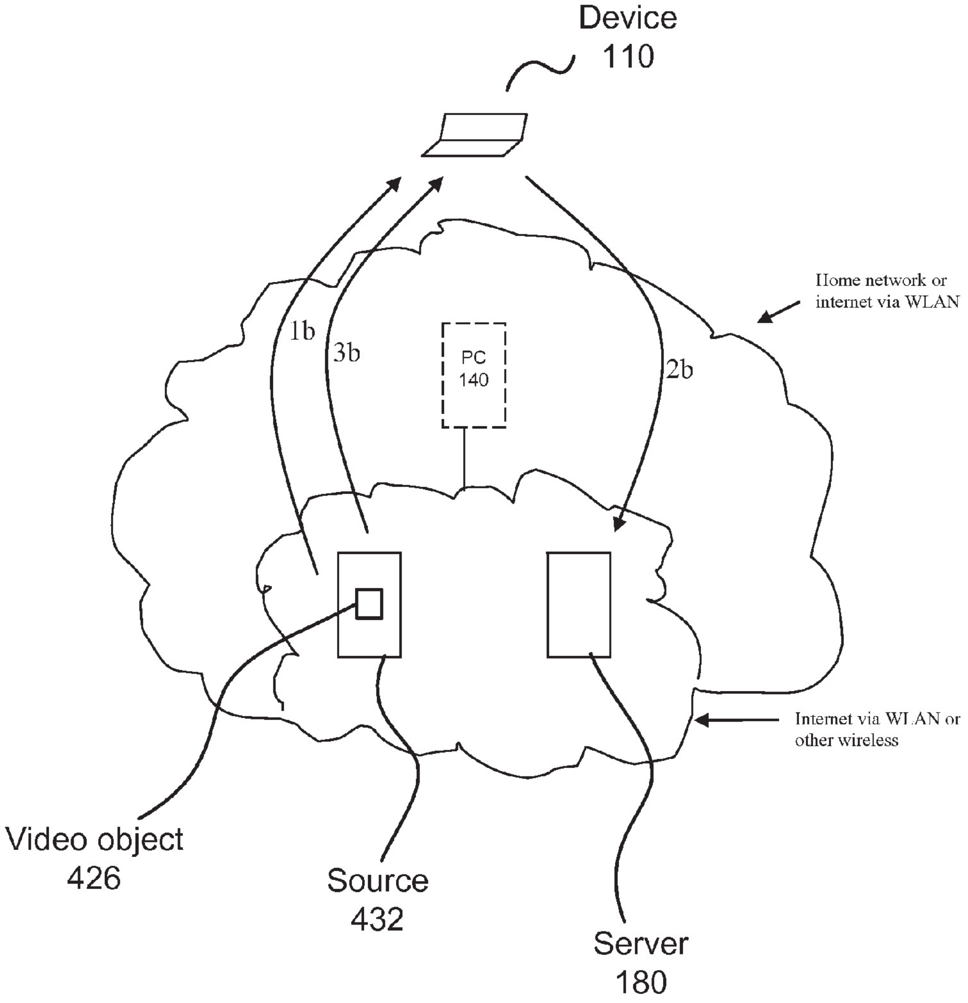

Device
110
Home network or internet via WLAN
1b
3b
PC
140
2b
Internet via WLAN or other wireless
Video object
426
Source
432
Server
180

FIG. 4B

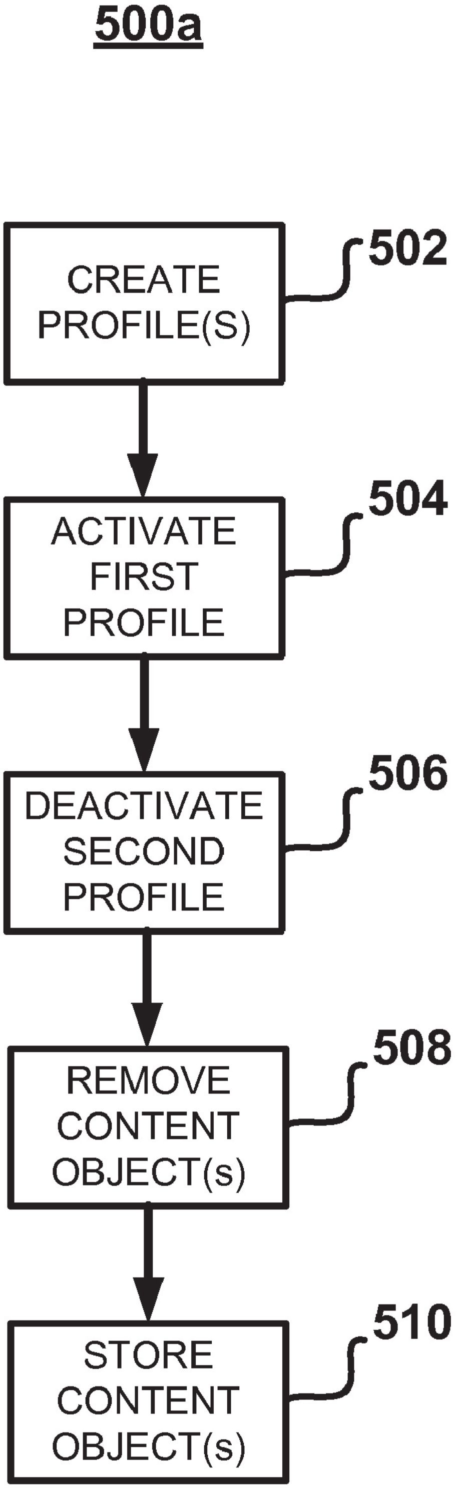

500a
CREATE PROFILE(S)
502
ACTIVATE FIRST PROFILE
504
DEACTIVATE SECOND PROFILE
506
REMOVE CONTENT OBJECT(s)
508
STORE CONTENT OBJECT(s)
510

FIG. 5A

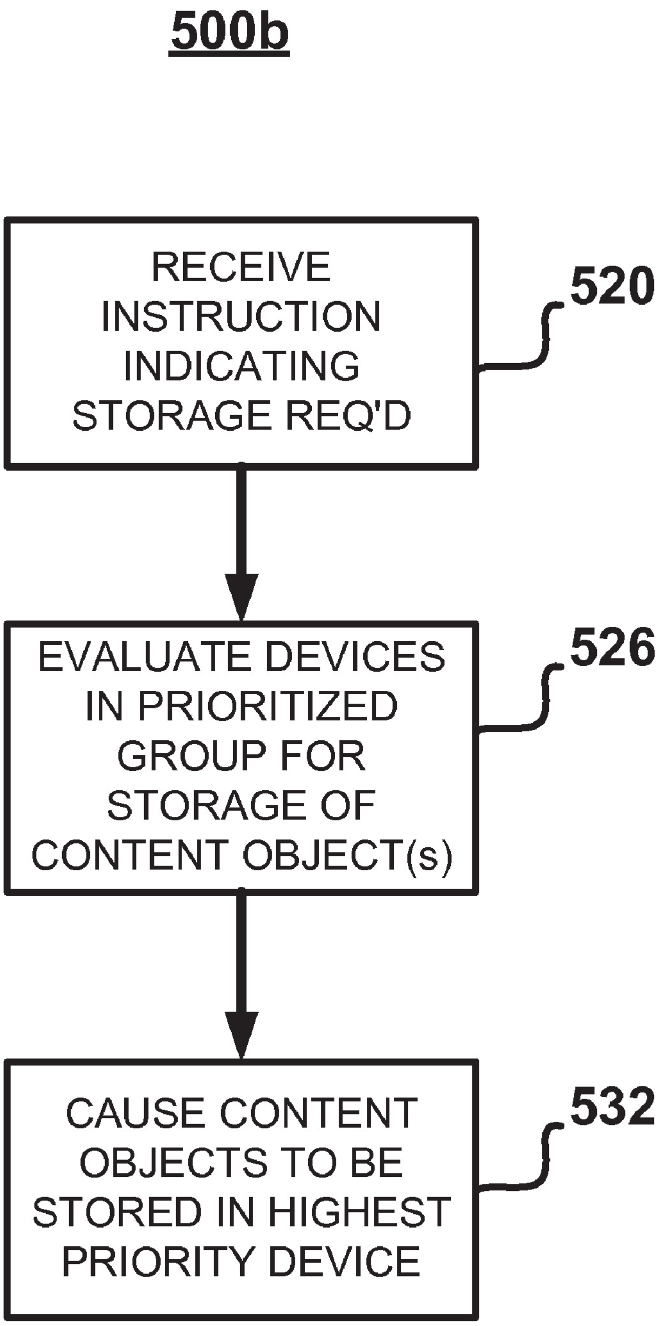

500b
RECEIVE INSTRUCTION INDICATING STORAGE REQ'D
520
EVALUATE DEVICES IN PRIORITIZED GROUP FOR STORAGE OF CONTENT OBJECT(s)
526
CAUSE CONTENT OBJECTS TO BE STORED IN HIGHEST PRIORITY DEVICE
532

FIG. 5B

STORAGE MANAGEMENT

FIELD

This description generally relates to storage of data on electronic devices and management of resources utilized for such storage.

BACKGROUND

Improvements in technology have changed the way people interact with their surrounding environment. These improvements provide opportunities and abilities for users of wireless technology to obtain numerous types of application programs, data files, etc., in almost any location. Today, there is a large amount of content available for downloading from the Internet, and a large number of applications supporting various file types. For example, a user may download a music video clip to her mobile handheld device while at a neighborhood park on Saturday, and may proceed to play it on her device for purposes of entertaining herself and those around her. The same user may be at an airport on Monday morning to take a business trip and wish access to business reports for purposes of giving a presentation. Accordingly, the user receives an email on the same mobile handheld device from a co-worker that includes the desired business reports as an attachment.

Improvements in memory density (e.g., the amount of memory capacity provided per unit area) have enabled users to store an increasing amount of data on devices so as to accommodate these and innumerable other scenarios. Memory capacity is still finite, however, and there are practical limits as to how much data may be stored on a given device at any particular moment. These limits are particularly pronounced in the context of mobile devices, as recent trends suggest that smaller devices are desirable.

By way of illustration, and returning to the previous example, the emailed business reports may require more storage space than is currently free in the mobile device's memory(ies). Although the user may be able to delete one or more currently-stored items to make room for the business reports, this is often undesirable. For example, the user may have recently taken a number of high resolution pictures of the birth of her friend's baby and not wish to lose those images.

BRIEF SUMMARY

The following presents a simplified summary of aspects of certain embodiments. This summary is not an extensive overview, and is not intended to identify key or critical elements or to delineate the scope of the claims.

In some embodiments sets of content objects are associated with content management profiles for a device. When a user activates a content management profile, the content objects in the set of content objects associated with that profile are (to the extent not already present on the device) stored in the device memory. In certain embodiments, storage space in the device for content objects of the activated profile is made available by deactivating a second profile. Content objects in the deactivated profile that are not also in the set of objects associated with the activated profile are removed from the device by deletion or by transferral for storage in another device.

Additional embodiments permit a first device to determine where one or more content objects should be stored. Upon receiving an instruction that corresponds to a requirement for storage capacity, one or more devices in a prioritized group

are evaluated for an ability to store the one or more content objects. The content object(s) are then stored on the highest priority device able to store those objects. The prioritized group may or may not include the first device. In some cases, for example, the one or more content objects are being retrieved from a remote source and there is a desire to store those objects on the first device. In such a circumstance, the first device is part of the prioritized group of devices and has the highest priority. In other cases, the one or more content objects are already stored on the first device and there is a desire to remove those content objects from the first device in order to store new content objects. In these circumstances, the first device is not part of the prioritized group.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing summary and the following detailed description are better understood when read in conjunction with the accompanying drawings, which are included by way of example, and not by way of limitation. In the drawings, like reference numbers indicate like features.

FIG. **1** illustrates a network communication environment in which one or more devices are operated and/or one or more methods performed according to some embodiments.

FIG. **2** is a block diagram of a mobile handheld device according to some embodiments.

FIG. **3** is a diagram illustrating the use of content management profiles according to some embodiments.

FIG. **4**A is a diagram illustrating storage of content objects according to some embodiments.

FIG. **4**B is another diagram illustrating storage of content objects according to some embodiments.

FIG. **5**A is a flow chart showing an algorithm according to at least some embodiments.

FIG. **5**B is another flow chart showing an algorithm according to at least some embodiments.

DETAILED DESCRIPTION

In the following description of the various embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown by way of illustration various embodiments in which one or more aspects of the invention may be practiced. It is to be understood that other embodiments may be utilized and structural and functional modifications may be made.

As used herein, "content object" generically refers to any of various types of data. A content object may be, without limitation, one or more of a data object or file (e.g., an image file, a video file, a text file, a spreadsheet, an audio file, a file having one or more slides or other types of presentation(s), etc.) an application program or component thereof, an operating system program or component thereof, a driver, etc.

FIG. **1** is a diagram of a network communication environment **100** in which one or more devices according to some embodiments are operated, and in which one or more methods according to some embodiments are performed. A first device **110** includes logic for managing profiles and for determining an appropriate storage location for content objects and is connected to a network **130** via a connection **120**. Network **130** may include the Internet, an intranet, wired or wireless networks, or any other network suitable for facilitating communication between devices in general. Network **130** may also be a group of interconnected networks. For example, device **110** may communicate with a wireless mobile network, which in turn communicates via the Internet with one or more devices on a remotely-located LAN (local area network) or wireless LAN (WLAN) in a home or office. Also shown in FIG. **1** is a second device **140** connected to network **130** via a connection **150**. In the embodiment of FIG. **1**, device **140** is a personal computer. Further shown in FIG. **1** is a third device **180**. In the embodiment of FIG. **1**, device **180** is a file server (or collection of file servers). Device **180** is in a different location from device **140**, although this need not be the case. Device **180** communicates with network **130** via a connection **190**. By virtue of the connectivity shown, devices **110**, **140**, and **180** communicate with one another. Such communications enable the exchange of various types of information as described herein.

The actual connections represented by connections **120**, **150**, and **190** may be embodied in various forms. For example, one or more of connections **120**, **150**, and **190** may be hardwired/wireline connections. Alternatively, one or more of connections **120**, **150**, and **190** may be wireless connections. Connections **120**, **150**, and **190** are shown in FIG. **1** as supporting bi-directional communications (via the dual arrow heads on each of connections **120**, **150**, and **190**). Alternatively, or additionally, network communication environment **100** may be structured to support dissimilar forward and reverse channel connections between various network entities (e.g., use of one media for communication in one direction and use of a different media for communication in a different direction).

Communication environment **100** may be part of a larger network consisting of additional devices. For example, devices **140** and/or **180** may exchange communications with a plurality of other devices (not shown) in addition to device **110**, and/or device **110** may exchange communications with devices in addition to PC **140** and/or server **180**. Communications in environment **100** may be conducted using one or more of numerous communication protocols. Furthermore, communication environment **100** may include one or more intermediary nodes (not shown) that may forward, buffer, store, route, or otherwise process communications between the various devices.

FIG. **2** is a block diagram of device **110** according to some embodiments. Device **110** could be any of various types of portable electronic devices (e.g., a laptop computer, a notebook computer, some other type of portable computing device, a personal digital assistant, a smart phone, a mobile telephone, some other type of wireless communication device, etc.). All of the components shown in FIG. **2** need not be present in all embodiments. Although various components of device **110** are represented as a single block, device **110** may include more than one of a particular component represented by a given block in FIG. **2**. As shown in FIG. **2**, device **110** includes a processor **228** connected to a user interface **230**, a memory **234** and/or other storage, and a display screen **236**. User interface **230** may further include a keypad, touch screen, voice interface, four arrow keys, joy-stick, stylus, data glove, mouse, roller ball, touch screen, or the like. Device **110** also includes a battery **250**, a speaker **252**, and one or more antennas **254**.

Also included within device **110**, as part of one or more programs executed by processor **228**, is storage logic **260**. Although shown as a separate component in FIG. **2**, storage logic **260** may be included in memory **234** with one or more other programs accessed by processor **228**. In some embodiments, storage logic **260** configures processor **228** to create, execute and otherwise process data in accordance with one or more content management profiles. The operation of content management profiles according to some embodiments is described below. Storage logic **260** further configures processor **228** to determine locations for storage of content objects in memory of device **110**, in device **140**, in device **180**, or elsewhere. The determination of storage locations is also discussed below. In alternate embodiments, storage logic **260** may configure processor **228** to perform less than all of these operations. In still other embodiments, all or part of storage logic **260** may be located in device **140**, device **180**, or in some other location.

As indicated above, executable instructions and data used by processor **228** and other components within device **110** are (in some embodiments) stored in a machine-readable memory **234**. Memory **234** may be implemented with any combination of read only memory modules or random access memory modules, optionally including both volatile and non-volatile memory. Software **240** (which may include some or all of the elements of storage logic **260**) may be stored within memory **234** (and/or other storage within device **110**) to provide instructions to processor **228** for enabling device **110** to perform various functions described herein. Alternatively, some or all of the instructions executed by processor **228** may be embodied in hardware or firmware (not shown). For example, the executable instructions may be embodied in one or more integrated circuits such as application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), or the like. One of skill in the art will appreciate that integrated circuits may include logic circuits, and that the logic circuits may be configured using one or more programmable files, fuse maps, or the like.

Device **110** may also include additional hardware, software and/or firmware. For example, device **110** may be configured to receive, decode and process digital broadband broadcast transmissions that are based, for example, on the Digital Video Broadcast (DVB) standard, such as DVB-H, DVB-T or DVB-MHP, through a specific DVB receiver **241**. Device **110** may also be provided with other types of receivers for digital broadband broadcast transmissions or for other types of broadcasts (e.g., AM/FM radio). Additionally, device **110** is configured to transmit, receive, encode, decode and process transmissions through one or more of WLAN transceiver **243**, telecommunications transceiver **244**, or other type of wireless communication interface. Device **110**, in at least some embodiments, may also include one or more short-range wired interfaces (e.g., USB) or wireless interfaces (e.g., BLUETOOTH). Additional formats and protocols may be used to convey information, data, messages and the like.

Some embodiments include a machine-readable media holding instructions that, when executed (e.g., by one or more processors within device **110**), cause device **110** and/or other elements in environment **100** to perform various operations as described herein. For example, product implementations may include a series of machine-readable instructions fixed on a tangible storage medium (e.g. a diskette, CD-ROM, ROM, DVD, fixed disk, thumb drive, etc.) or transmittable to device **110** (e.g., via a modem or other interface). The machine-readable instructions may embody all or part of the functionality with respect to a system (e.g., network communication environment **100** of FIG. **1**) or device (e.g., device **110**, device **140** and/or device **180**), and can be written in any of various programming languages for use with many different computer architectures and/or operating systems, as would be readily appreciated by one of ordinary skill. Various embodiments of the invention may also be implemented as hardware, firmware or a combination of software, hardware and/or firmware.

FIG. **3** is a diagram that illustrates the use of content management profiles according to some embodiments. More specifically, FIG. **3** illustrates the use of content management profiles to manage one or more sets of user-defined content objects according to some embodiments. In the example of FIG. **3**, and building on a previous example, a user of device **110** is preparing to board an aircraft for purposes of taking a business trip. During the trip the user will want to access a collection of content objects, shown in FIG. **3** as solid squares **302**A, as well as a collection of objects shown in FIG. **3** as cross-hatched squares **302**C. Those objects may be, e.g., text files, spreadsheets, images, slides, etc. needed to prepare for a meeting. Accordingly, the user inputs commands into device **110** that causes processor **228** to execute instructions to activate a first profile. That first profile ("flight profile" **308**) is associated with the set of content objects the user wishes to access in order to prepare for her meeting. In order to create storage space on device **110** for the content objects in flight profile **308**, a second profile ("entertainment profile" **314**) is deactivated. This deactivation may result from a separate user instruction or may occur automatically in response to activation of flight profile **308**. When entertainment profile **314** is deactivated, content objects associated with profile **314** and which are not associated with profile **308** (shown as white boxes **302**B in FIG. **3**) are deleted and/or transferred.

As used herein, "deleting" a content object from device **110** refers to re-allocation of memory used to store the deleted object for storage of other data. The re-allocated memory may be immediately reused to store other content objects or other data, may be securely erased (e.g., by overwriting with random ones (1s) and zeros (0s)), or simply flagged as available to store other data. "Transferring" a content object refers to re-allocation of the memory used to store the transferred object in conjunction with causing the transferred object to be stored elsewhere (e.g., PC **140**, server **180**, etc.). "Removing" a content object refers to either deleting or transferring that object.

A user may create a profile in any of various ways. In some cases, a user associates content objects with a profile using device **110**. In response to received user instructions defining content objects as part of a set of objects to be associated with a profile, device **110** tags those content objects as associated with that profile. In other cases, a user may create a profile (and define content objects associated with that profile) using a PC (e.g., PC **140**) or other device, and then make that profile (and its associated content objects) available to device **110**. In the example of FIG. **3**, some content objects (shown as cross-hatched boxes) are included within both profile **308** and profile **314**, though this need not be the case. Although only two profiles are shown in FIG. **3**, any number of profiles can be created.

When a user first creates a content object, the user is in some embodiments requested to define which profile(s) (if any) the content object should be associated with. In some embodiments, a newly-created content object is provided with a default tag that automatically serves to associate the newly-created object with one or more default profiles.

Associating content objects with profiles allows the user to load all content objects associated with a given profile by simply specifying the profile. In this manner, a user is not required to remember or search for individual content objects at times when it may be inconvenient to do so. Instead, a user simply instructs device **110** (via an appropriate command) that a particular profile should be made active. In response, processor **228** loads the content objects associated with that activated profile (to the extent any such objects are not already stored on device **110**). Those objects may be loaded from PC **140**, from server **180**, or from some other location. If necessary, processor **228** can also make room for content objects associated with the activated profile by deleting objects in a profile being deactivated and/or by transferring one or more of those objects to PC **140**, sever **180** or to some other location.

In some embodiments, one or more data files storing the association (e.g., a mapping) between content objects and profiles may be stored at device **110** (e.g., in memory **234** of FIG. **2**). In other embodiments, the association data files may also (or alternatively) be stored at another device (e.g., PC **140**, server **180**, etc.).

To the extent a content object in an activated profile is also part of a profile being deactivated, no action is needed. Thus, if the user of device **110** in the example of FIG. **3** is deactivating entertainment profile **314** and activating flight profile **308**, the content objects common to both of those profiles (i.e., the cross-hatched boxes **302**C in FIG. **3**) are already in place and need not be loaded. Although the present example assumes only one profile is active, this need not be the case, and a user may activate more than one profile.

Alternatively, or additionally, one or more of the content objects associated with an active profile might not be physically stored on device **110** as a result of profile activation. Instead, some content objects may be referenced by a link located on device **110**. Linking may be used in some embodiments to preserve memory capacity on device **110**, particularly when a content object requires a large amount of memory capacity relative to a storage capacity required by a link and/or where interruption of network connectivity is not expected.

In some embodiments, and as shown in FIG. **3**, the profiles (e.g., flight profile **308**, entertainment profile **314**, and other profiles **326** and **332**) and content objects **302** are stored on PC **140**, server **180**, and/or other devices. Such devices will often (though not necessarily) have a higher storage capacity than device **110**. Some content objects (e.g., content object **302**D) might not be associated with any profile.

When the user deactivates a profile in some embodiments (e.g., deactivating profile **314** in favor of flight profile **308**), and as discussed above, content objects (e.g., content objects **302**B) not belonging to an active profile are removed from device **110** (e.g., deleted or transferred to another device). In other embodiments, it is desirable to limit the number of content object transactions that occur when activating one profile and deactivating another profile. For example, in order to conserve (battery) power on device **110** or to conserve communication network bandwidth, it may be desirable to limit the number of content objects added to or removed from device **110**. Additional considerations may dictate minimizing the number of content object transactions in order to conserve processing resources on device **110**. For example, device **110** may be running a resource intensive application that requires a majority of the processing resources available on device **110**. In the example of FIG. **3**, content objects in flight profile **308** require a total of 3.5 GB of storage memory and device **110** has 0.5 GB of available storage capacity not being used by entertainment profile **314** or by other data. If the additional content objects added to device **110** as a result of activating profile **308** (e.g., the blackened objects in FIG. **3**) do not exceed 0.5 GB, then removal of content objects will not take place in some embodiments. Conversely, if the content objects being added to device **110** require more than 0.5 GB, at least one content object not in an active profile may require removal.

In some embodiments, device **110** is configured to remove a minimum number of content objects necessary to create sufficient storage capacity to facilitate adding the content objects associated with activated profile **308**. The selection of which content objects to delete from device **110** may be based on various criteria. The selection may be based on a storage capacity required by inactive profile content objects. For example, device **110** may be configured to delete the largest content objects (in terms of memory capacity required to support their storage) first in order to minimize the number of content objects that need to be deleted. The selection of which content objects to delete could also (or alternatively) be based on frequency of use. For example, those content objects that have not been accessed for a relatively long amount of time may be deleted in order to allocate storage capacity on device **110** for content objects associated with a profile being activated. Other criteria may be used to determine which content object(s) to remove from device **110** in order to allocate sufficient storage capacity for flight profile **308**.

In some embodiments, the user receives a warning or indication message on device **110** requesting the user to confirm that it is acceptable for a content object (or group of content objects) to be deleted. The user may thereafter press a key or button on device **110**, provide a verbal command (e.g., in conjunction with speech recognition techniques or the like) or allow a timer on device **110** to expire to confirm the deletion. In some embodiments, device **110** provides the user with a listing of content objects that it recommends as the best candidates for deletion, and the user may be able to select from the recommended candidates.

In some embodiments, processor **228** of device **110** executes one or more algorithms to decide where content objects should be transferred when attempting to create storage space in device **110**. These algorithms can be performed in connection with activating/deactivating one or more profiles, and/or in connection with content that is not associated with a profile. For example, server **180** may be subject to excessive loading at times due to a relatively large number of users attempting to simultaneously access server **180**. Accordingly, device **110** in some embodiments attempts to first transfer content objects to PC **140**. If an attempt to transfer objects to PC **140** is unsuccessful (e.g., if PC **140** is not available because it is offline) device **110** next attempts to transfer content objects to server **180**.

In some embodiments, the capacity available at each of multiple storage locations is analyzed to determine the most appropriate location for content object storage. FIG. **4**A is a diagram showing storage of content objects according to at least one such embodiment. In the example of FIG. **4**A, a user of device **110** initiates a content object download operation to retrieve a music video content object **426** from a source **432**. In the example of FIGS. **4**A and **4**B, device **110** is part of a wireless communication network; that wireless network is in communication with source **432** and server **180** via the Internet, and in communication with PC **140** via the Internet and a home network in which PC **140** is located. Embodiments of the invention include implementations in one or more other types of networks. For example, device **110** may be part of a wireless local area network (WLAN), with that WLAN connected to the Internet. PC **140** could be on that same WLAN.

As shown in FIG. **4**A by arrow **1***a*, device **110** first receives data from source **432** indicating storage space needed for video object **426**. Device **110** compares the size of video object **426** with the available storage capacity at device **110** to determine if device **110** has sufficient storage capacity to support video object **426**. In the example of FIG. **4**A, the memory of device **110** is full (or nearly full). Accordingly, device **110** determines if PC **140** has sufficient memory capacity to store video object **426**. If PC **140** does have sufficient storage capacity, and as shown with arrow **2***a*, video object **426** is saved in storage of PC **140**. If PC **140** does not have sufficient storage capacity (or is offline), device **110** then determines if server **180** is capable of storing video object **426**. If so, device **110** causes video object **426** to be stored at server **180** (arrow **3***a*). If server **180** cannot store video object **426** or is offline, other storage locations (not shown) could be checked, the download of video object **426** aborted (or suspended), or storage capacity made available in device **110** by deleting or transferring other content objects.

As can be appreciated from FIG. **4**A and the foregoing, several storage locations are prioritized. A highest priority is given to device **110**, a lower priority is given to PC **140**, and a still lower priority is assigned to server **180**. The prioritization scheme of FIG. **4**A is only one example, however, and other priority schemes can be used. Priority schemes can be based on bandwidth considerations, security concerns, and/or various other factors.

In some embodiments, a user is able to dictate the priorities associated with devices via one or more directives. The one or more directives may include commands, instructions, or the like. For example, a user downloading a personal banking statement may have previously directed that all downloads from a particular source (e.g., the user's bank) go either to device **110** or to PC **140**, with a higher priority assigned to device **110** in comparison to the priority assigned to PC **140**. Thereafter, the user may, via one or more directives, assign a higher priority to PC **140** (in comparison to device **110**) so as to cause one or more content objects to be stored in PC **140** in preference to device **110**.

In some embodiments, a prioritization scheme is operative with respect to all content objects. For example, a prioritization scheme may serve to prioritize storage in one device (e.g., device **110**) in comparison to another (e.g., PC **140**), and as a result, a downloaded content object may be preferentially routed to the highest priority device (e.g., device **110**) for storage irrespective of the nature of the content object. Alternatively, in some embodiments the prioritization scheme may be related to the nature of the content object. For example, a user may be able to specify via a prioritization scheme that content objects related to entertainment should preferably be routed to device **110** (instead of PC **140**), whereas content objects related to business reports should preferably be routed to PC **140** (instead of device **110**).

In some embodiments, a user may also be able to change devices in a prioritized group by directing that one or more devices be added to or removed from the group. For example, and building on the preceding example, a user may initially include device **110** and PC **140** in a prioritized group for purposes of storing a downloaded personal banking statement. The user may subsequently decide that she wants to use the storage capacity available on device **110** (only) for content objects related to entertainment. Accordingly, the user may remove device **110** from the prioritized group. The user may also add one or more devices (e.g., server **180**) to the prioritized group.

FIG. **4**B is a diagram illustrating another example of storage of content objects according to some embodiments. In the example of FIG. **4**B, video object **426** from a source **432** is again to be downloaded via the Internet and other networks. As shown in FIG. **4**B by arrow **1***b*, device **110** first receives data from source **432** indicating storage space needed for video object **426**. Device **110** compares the size of video object **426** with the available storage capacity at device **110** to determine if device **110** has sufficient storage capacity to store video object **426**. In the example of FIG. **4**B, the memory of device **110** is full (or nearly full). Accordingly, device **110** determines if PC **140** is online and has sufficient storage capacity to accommodate one or more content objects presently stored in memory of device **110**. If PC **140** does have sufficient storage capacity (and is online), device **110** may transfer those content objects to PC **140** by transmitting them to PC **140**. After transmitting the one or more content objects to PC **140**, device **110** may thereafter store video object **426** in its memory. If PC **140** does not have sufficient storage capacity to store one or more content objects (or is unavailable), device **110** determines if server **180** has sufficient storage capacity to store one or more content objects currently stored in memory of device **110**. If server **180** does have sufficient storage capacity, device **110** transmits the one or more content objects stored in memory of device **110** to server **180**. After transmitting the one or more content objects to server **180**, device **110** may thereafter store video object **426** in its memory. In some embodiments, one or more of the content objects being removed from device **110** (in order to accommodate new content object(s)) may be local copies of content objects also stored on PC **140** or server **180**. In such a circumstance, it would not be necessary to transmit that content object to PC **140**, or server **180**, and the locally stored copy could simply be deleted.

As can be appreciated from FIG. **4**B and the foregoing, several storage locations are again prioritized. A first priority is given to PC **140** and a lower priority is assigned to server **180**. A content object (e.g., video object **426**) is "forced" into being stored in device **110**. If device **110** is full, one or more content objects already stored on device **110** are removed by deletion or transfer to another device (e.g., PC **140**, server **180**, etc.) based on relative priorities. As with operations shown in FIG. **4**A, the user of device **110** may (in connection with operations shown in FIG. **4**B) change devices in a prioritized group and/or modify priorities assigned to devices.

One of skill in the art will appreciate that additional levels of storage may be employed in either the scenario of FIG. **4**A or in the scenario of FIG. **4**B (e.g., a user may have access to PCs on multiple LANs). Moreover, one of skill in the art will appreciate that at least some of the embodiments described herein enable one to access and save a content object that is only available for a limited duration. For example, a content object may be a coupon offer that is going to be removed from a commercial server within an hour of viewing it. If a user is two hours away from her home, she might not be able to take advantage of the offer using more traditional methods. Embodiments described herein allow the user to save the coupon offer on her device **110**, PC **140** or server **180** for later access.

In some embodiments, device **110** is configured to display information (e.g., on display screen **236** of FIG. **2**) related to a download progress associated with a download of a content object (e.g., a content object **302** of FIG. **3**, video object **426** of FIGS. **4**A-B, etc.). The display information may be depicted as a bar graph, a pie chart or the like. Alternatively, or additionally, in some embodiments device **110** provides an indication as to what step (e.g., what arrow number in accordance with the arrows/arrow numbers shown in FIGS. **4**A-B) of the download process is being executed at a given point in time. Device **110** may provide an option for canceling the download. Alternatively, or additionally, device **110** may implement a timer such that when the timer expires or reaches a threshold value the download operation is canceled.

FIG. **5**A illustrates an algorithm **500**a according to at least some embodiments. In the first step of algorithm **500***a* (block **502**), a user creates one or more profiles for device **110**. As explained above, the user may create such profiles using device **110** or using some other device (e.g., PC **140**). In the next step of algorithm **500***a* (block **504**), the user activates one of the previously-created profiles. In some embodiments, a user activates a profile using an explicit command input to device **110**. In other embodiments, a profile may be automatically activated based on some other event. For example, mobile device **110** may detect that it has joined a WLAN corresponding to the user's home and automatically activate a profile the user has selected for use of device **110** when at home. In the next step (block **506**), a second profile is deactivated in conjunction with activation of the first profile. In block **508**, one or more content objects associated with the second profile are removed from device **110** in order to make room for content objects associated with the first profile. In block **510**, content objects associated with the first profile are (to the extent not already present) stored on device **110**.

FIG. **5**B illustrates an algorithm **500***b* according to at least some embodiments. In the first step (block **520**), an instruction is received at device **110** that indicates storage capacity will be required. In at least some embodiments, this instruction corresponds to a request by the user to download content to device **110** from a remotely-located source (e.g., source **432** shown in FIGS. **4**A and **4**B), and the required storage capacity will be at least the amount of storage needed for the content to be downloaded. In the next step (block **526**), one or more devices in a prioritized group of devices are evaluated to determine if one of the evaluated devices has storage capacity that equals or exceeds that storage needed for the content to be downloaded. In some cases, and as explained in connection with FIG. **4**A, storage on some device other than device **110** will be permitted if there is insufficient storage available capacity on device **110**. In such a scenario, device **110** is part of the group of prioritized devices that are evaluated. In other cases, and as explained in connection with FIG. **4**B, the downloaded content will be stored on device **110** even if device **110** does not currently have sufficient available storage capacity. In this scenario, one or more content objects may be transferred from device **110** in order to create storage capacity for the content to be downloaded. Accordingly, the group of prioritized devices includes the devices (other than device **110**) to which the one or more content objects may be transferred. In the next step (block **532**), device **110** causes one or more content objects to be stored on the highest-priority device that was determined (in the evaluation of block **526**) to be able to store those objects. In the scenario of FIG. **4**A, the one or more objects being stored in block **532** are the content that is being downloaded from remote source **432**. In the scenario of FIG. **4**B, the one or more objects being stored in block **532** are the objects being transferred from device **110** to make room for the content being downloaded from remote source **432**.

In some embodiments, device **110** is configured to perform both the algorithm **500***a* of FIG. **5**A and the algorithm **500***b* of FIG. **5**B. In other embodiments, a device such as device **110** is only configured to perform one of algorithms **500***a* or **500***b*. In still other embodiments, algorithms **500***a* and **500***b* are combined into a single algorithm. In yet other embodiments, various steps in algorithms **500***a* and/or **500***b* are omitted and/or rearranged.

Numerous characteristics, advantages and embodiments have been described above with reference to the accompanying drawings. However, the above description and drawings are illustrative only. The invention is not limited to the illustrated embodiments, and all embodiments of the invention need not necessarily achieve all of the advantages or purposes, or possess all characteristics, identified herein. Various changes and modifications may be effected by one skilled in the art without departing from the scope or spirit of the invention. Although example devices and components have been described, the invention is not limited to such devices or components unless specifically required by the language of a claim. The elements and uses of the above-described embodiments can be rearranged and combined in manners other than specifically described above, with any and all permutations within the scope of the invention.

What is claimed is:

1. A method comprising:

receiving an instruction to activate a first of a plurality of profiles for a mobile device, wherein each profile of the plurality is associated with a distinct set of user-defined content objects;

activating the first profile in response to the received instruction, wherein said activation includes storing on the mobile device a first set of content objects associated with the first profile; and

deactivating a second of the plurality of profiles in response to the received instruction, said deactivating including selecting a content object of a second set of content objects associated with the second profile and removing the content object of the second set from the mobile device based at least in part on a size and a frequency of use of the content object of the second set.

2. The method of claim **1**, wherein associations between the first profile and content objects in the first set and associations between the second of the plurality of profiles and content objects in the second set are stored at the mobile device.

3. The method of claim **1**, wherein associations between the first profile and content objects in the first set and associations between the second of the plurality of profiles and content objects in the second set are stored on a second device.

4. The method of claim **1**, wherein the content objects include at least one object chosen from the group that includes an image file, a video file, a text file, a spreadsheet, an audio file, and a file having one or more slides or other types of presentations.

5. The method of claim **1**, wherein the first set of content objects includes at least one content object that is in the second set of content objects associated with the second of the plurality of profiles, and wherein the first set of content objects includes at least one content object that is not in the second set of content objects.

6. The method of claim **1**, wherein the receiving an instruction further includes receiving an instruction to download one or more content objects included in the first set of content objects to the mobile device from a remotely located device.

7. The method of claim **1**, further comprising:

receiving an instruction corresponding to a requirement for a storage capacity in one or more memories of the mobile device;

responsive to the received instruction corresponding to the requirement for a storage capacity, evaluating one or more devices in a prioritized group of devices for an ability to store one or more content objects; and

causing the one or more content objects to be stored on the highest priority device of the group able to store the one or more content objects.

8. The method of claim **1**, further comprising:

presenting, on the mobile device, the content object of the second set as a candidate for removal from the mobile device; and

receiving an indication at the mobile device that the content object of the second set is to be removed from the mobile device,

wherein the removing of the content object of the second set from the mobile device is responsive to receiving the indication.

9. The method of claim **8**, wherein the indication comprises at least one of:

depression of a key or button on the mobile device, a verbal command, and expiration of a timer on the mobile device.

10. The method of claim **1**, further comprising:

referencing via at least one link, at the mobile device, a third set of content objects that are associated with the first profile responsive to activating the first profile.

11. An apparatus comprising:

a processor; and

memory storing instructions that, when executed by the processor, cause the apparatus to:

receive an instruction to activate a first of a plurality of profiles for the apparatus, wherein each profile of the plurality is associated with a distinct set of user-defined content objects;

activate the first profile in response to the received instruction, wherein said activation includes storing on the apparatus a first set of content objects associated with the first profile; and

deactivate a second of the plurality of profiles in response to the received instruction, said deactivating including selecting a content object of a second set of content objects associated with the second profile and removing the content object of the second set from the apparatus based at least in part on a size and a frequency of use of the content object of the second set.

12. The apparatus of claim **11**, wherein associations between the first profile and content objects in the first set and associations between the second of the plurality of profiles and content objects in the second set are stored at the apparatus.

13. The apparatus of claim **11**, wherein associations between the first profile and content objects in the first set and associations between the second of the plurality of profiles and content objects in the second set are stored on a second apparatus.

14. The apparatus of claim **11**, wherein the content objects include at least one object chosen from the group that includes an image file, a video file, a text file, a spreadsheet, an audio file, and a file having one or more slides or other types of presentations.

15. The apparatus of claim **11**, wherein the first set of content objects includes at least one content object that is in the second set of content objects associated with the second of the plurality of profiles, and wherein the first set of content objects includes at least one content object that is not in the second set of content objects.

16. The apparatus of claim **11**, wherein the receiving an instruction further includes receiving an instruction to download one or more content objects included in the first set of content objects to the apparatus from a remotely located device.

17. The apparatus of claim **11**, wherein the processor is further configured to perform operations that include:

receiving an instruction corresponding to a requirement for a storage capacity in one or more memories of the apparatus;

responsive to the received instruction corresponding to the requirement for a storage capacity, evaluating one or more devices in a prioritized group of devices for an ability to store one or more content objects; and

causing the one or more content objects to be stored on the highest priority device of the group able to store the one or more content objects.

18. The apparatus of claim **11**, wherein the instructions, when executed by the processor, cause the apparatus to:

present the content object of the second set as a candidate for removal from the apparatus; and

receive an indication at the apparatus that the content object of the second set is to be removed from the apparatus,

wherein the removal of the content object of the second set from the apparatus is responsive to receiving the indication.

19. The apparatus of claim **11**, wherein the instructions, when executed by the processor, cause the apparatus to:

reference via at least one link, at the apparatus, a third set of content objects that are associated with the first profile responsive to activating the first profile.

20. An apparatus comprising:

means for receiving an instruction to activate a first of a plurality of profiles for the apparatus, wherein each profile of the plurality is associated with a distinct set of user-defined content objects;

means for activating the first profile in response to the received instruction, wherein said activation includes storing on the apparatus a first set of content objects associated with the first profile; and

means for deactivating a second of the plurality of profiles in response to the received instruction, said deactivating including selecting a content object of a second set of content objects associated with the second profile and removing the content object of the second set from the apparatus based at least in part on a size and a frequency of use of the content object of the second set.

* * * * *