CATÓLICA LISBON
BUSINESS & ECONOMICS

Does online privacy matter?

-

A comparative study of Portuguese and German millennials

Ian Mallmann Mendes

Dissertation written under the supervision of Mr Nuno Crispim

Dissertation submitted in partial fulfilment of requirements for the MSc in Business, at the Universidade Católica Portuguesa, June 2018.

ABSTRACT

Title: "Does online privacy matter? A comparative study of Portuguese and German millennials"

Author: Ian Mallmann Mendes

The accelerating pace at which the technological landscape is changing has given rise to new challenges and threats that need to be addressed to ensure that technology does not become a tool for nefarious uses that could threaten freedom, happiness, and progress. For companies fighting for market share and reach in any given sector, governments trying to uphold voters' trust in the system and its power to protect them, and consumers looking at new technologies with a mix of awe, curiosity, and unease, addressing these challenges might become a central, potentially existential, concern.

This dissertation focuses one of these concerns, more specifically, consumer privacy concerns. It studies the effect demographic attributes, including culture, have on this concern, as well as how the extent to which this concern is present, affects the adoption of innovative technological products in the form of Internet of Things (IoT) devices.

Findings reveal that privacy concerns were high across all studied groupings, but also that there were differences between cultures. Further, it shows that privacy concerns negatively correlated with technology adoption, and that deemed intrusive, *a posteriori* discoveries about privacy situations negatively impact future technology adoption likelihood.

Keywords: Privacy Concerns, Adoption Intentions, Internet of Things, Culture, Consumer Electronics

SUMÁRIO

Título: “A privacidade online importa? Um estudo comparativo das Gerações do Milénio portuguesa e alemã”

Autor: Ian Mallmann Mendes

O desenvolvimento acelerado de tecnologias na era da informação trouxe novos desafios e ameaças que terão que ser enfrentados para garantir que as novas tecnologias não se tornem ferramentas para fins nefastos que ponham em risco a liberdade, a felicidade e o progresso. Para empresas a lutar por uma parcela de mercado e o alcance de consumidores, a governos a manter a confiança dos seus eleitores e a capacidade do sistema político de os proteger, a consumidores que observam as novas tecnologias com uma mistura de admiração, curiosidade e desconforto, abordar estes desafios pode vir a tornar-se uma preocupação central, até existencial.

Este trabalho foca um desses desafios, nomeadamente, a preocupação pela privacidade na óptica do consumidor. O projecto estuda o efeito de factores demográficos, e principalmente da cultura, na preocupação pela privacidade, tão bem como o nível de preocupação que ocorre nos participantes do estudo, e o efeito dessa preocupação nas intenções de adopção de tecnologias da “Internet das Coisas”.

O estudo revela que a preocupação com a situação de privacidade no mundo *online* é transversalmente alta, mas também que existe uma diferença relevante entre as culturas estudadas. Para além disso, aponta que o nível de preocupação está negativamente correlacionado com a adopção de novas tecnologias, e que descobertas *a posteriori* relativas à situação de privacidade consideradas intrusivas, têm um impacto negativo nas intenções de adopção de tecnologia.

Palavras-chave: Preocupação de privacidade, Intenções de adopção, Internet das Coisas, Cultura, Electrónica de consumo

Acknowledgements

I thank my parents, Tee, and Mr Steve for their continuous and unconditional support.

TABLE OF CONTENTS

Chapter 1: INTRODUCTION

1.1 Information Privacy

In the mid-19th century, pigeon mail, that is correspondence carried over large distances by courier pigeons, was still very much in operation all over the globe, from Europe to New Zealand[1]. Less than 150 years later, in 2007 to be precise, the first iPhone was launched. A year later the HTC Dream, the first Android-powered phone, joined the market. In the past 10 years, these devices have fundamentally changed the way we communicate with each other, interact with our environment, spend our free time and work. In fact, by looking at how we feel when we forget or lose our phone, one can begin to understand the central place this technology has gained in our lives and the abrupt, swift and profound change that it has brought about.

With these devices the underlying technology, architecture and infrastructure equally evolved. Our communication now operates at more than half the speed of light thanks to fibre-optic cables. Running costs have been reduced to electricity cost, given that many services are offered free of charge. Coverage is ubiquitous and increasingly global. In sum, access to the entire world lies in the palm of our hands, convenient, day and night, at negligible cost. Furthermore, a host of functions, tools and hardware are now built into smartphones, which allowed these devices to progressively replace things like compasses, calendars, flashlights, digital cameras, voice recorders, navigation systems, books, alarm clocks, and board games. It is thus no wonder that smartphones have become such a central part of the modern day-to-day life. According to Yahoo! Flurry Analytics, the average US consumer now spends more than 5 hours a day on a mobile device[2]. During this time, whatever is done on, and potentially around, the phone is recorded by its multiple sensors, collected, and compiled into what is known as the digital footprint. Given that the smartphone is at the centre of many of our personal and professional lives, it should come as no surprise that this footprint is highly individualised, detailed, intimate, encompassing and revealing of our habits, preferences and, to some extent, even of our personality.

The uptake of mobile technology has not only affected our personal lives. Its implications and possibilities have also profoundly impacted entire industries. One of these

[1] Great Barrier Island Pigeongram Agency: *Mail Form No. 9* | Collections Online - Museum of New Zealand Te Papa Tongarewa. (n.d.). Retrieved March 10, 2018, from https://collections.tepapa.govt.nz/object/292735

[2] Khalaf, S. (2017). *U.S. Consumers Time-Spent on Mobile Crosses 5 Hours a Day*. Retrieved March 15, 2018, from http://flurrymobile.tumblr.com/post/157921590345/us-consumers-time-spent-on-mobile-crosses-5

industries is without unquestionably the advertising industry. Digital advertising has been a trending topic in the past few years and some of the biggest companies in the world, like Google and Facebook, have built their entire business model on top of this new type of advertising.

Consequently, every consumer's digital footprint, which is the basis on which digital advertising operates on, is collected in diverse way, intensely scrutinized, continuously monitored, and opaquely monetised. Where we go, what we do, what we eat, listen to or watch, even what we want or might want in the future, all these individual characteristics, that once only a handful of people in our innermost circle was privy to, are now shared globally, through social media, third-party smartphone applications (henceforth also referred to simply as "apps"), and soon, with the rise of the Internet of Things (IoT), through mundane objects such as our toothbrush, fridge, wristwatch, clothing, and toilet[3]. However, since it is not always entirely clear what the data collected by these devices will be used for and who will have access to it, the collection and use of personal information has launched a discussion on privacy that has started to gain the attention of civil liberties experts, privacy advocacy groups, and governments alike. Several privacy scandals, most recently and notably the Facebook/Cambridge Analytica scandal, have highlighted the possible, large-scale consequences privacy abuses can have, further fuelling the debate on how governments, companies and consumers should address and protect privacy.

Figure 1 – Graph of Facebook stock price (Please note that the Cambridge Analytica leak occurred on March 16th, 2018. Over the course of the following 10 days the stock price fell by more than 16%)

[3] Murphy, M. (2015*). 18 things that have no business being connected to the internet* — Quartz. Retrieved March 7, 2018, from https://qz.com/563952/18-internet-of-things-devices-that-have-no-business-being-connected-to-the-internet/

In his 2008 biography, Gabriel García Márquez was quoted as having said: "*All human beings have three lives: Public, private, and secret*"[4]. This certainly may have been true in the past century, but today, in the least, the distinction between these three lives is beginning to blur.

The present paper, which will generally focus on European millennials, attempts to frame the importance consumers attribute to the *status quo* proclaimed by García Márquez. Does privacy matter to them? How comfortable are they to opening up their private life to big data companies? And how aware are they of the access to their lives they are granting these companies?

1.2 Problem Statement

This research paper analyses the extent to which privacy concerns impact IoT adoption intentions under consideration of the effect of culture on this relationship by researching and comparing German and Portuguese millennials. More specifically, the paper will study the impact of privacy situation awareness on the adoption intentions of smart speakers, smart home appliances, and fitness trackers.

1.3 Aim

This thesis aims to answer the following research questions:

- Is there a cultural difference in regards to reported privacy concerns?
- Do demographics influence privacy concerns?
- How do privacy concerns impact IoT device adoption intentions?
- How does a privacy awareness situation influence IoT device adoption intentions?

1.4 Scope

Before outlining the body of literature that exists around the concepts in focus the author would like to expose the scope of this project by highlighting what this paper does *not* focus on: First, this project will not focus on the impact any sensor could have on bystanders and other third-party agents, whose voice, movement, or other information might be captured collaterally. While "collateral intrusion"[5], or the possibility of data on people who don't own

[4] Martin, G. (2008). *Gabriel García Márquez: A life* — Bloomsbury Publishing PLC

[5] Scottish Government. (2003). *Covert Surveillance: Code of Practice*. Retrieved May 13, 2018, from http://www.gov.scot/Publications/2003/03/16695/19535

a smartphone by choice, might still end up on a corporate server because it was recorded in the background of someone else's device, certainly is an important consideration in privacy matters, it relates to an involuntary circumstance, while this paper focuses on conscious acts. Second, the present research and literature review will not grapple with the issue of data security in what concerns server security, data theft, and other cases of involuntary loss of data sovereignty for the same reasons as outlined previously. And third, while industrial IoT use cases (e.g. warehouse management, item tracking, inventory monitoring, etc.) make up a great part of the appeal of this technology, this project will focus exclusively on end-consumer applications.

This study exclusively focuses on German and Portuguese millennials, who are enrolled in or have completed at least a Bachelor's degree and use both smartphones and apps daily.

1.5 Research Methodology

This dissertation bases its findings on primary data that was collected in both qualitative and quantitative research. The former consisted of four in-depth interviews, while the latter consisted of an online survey that was built using insights gathered in the literature review process as well as the interviews, pilot-tested, and then electronically distributed to the target population.

1.6 Academic and Managerial Relevance

Information privacy has been called one of the most important ethical issues of the information age (Smith, Milberg, & Burke, 1996). This is especially true since data provided by smartphones, the "pinnacle of mobile communications technology" (Charlesworth, 2009), allows for previously unknown inferences about the user's behaviour, often without their knowledge or consent (Zafeiropoulou, 2014). Coupled with the fact that companies like Facebook and Google have built their entire business model on the "exploitation of personal data" (Cecere, Le Guel, & Soulié, 2015), there is real financial incentive in collecting and harnessing the power of that data.

At the same time research has shown that privacy concerns can negatively impact new technology adoption ((Krasnova, Veltri, & Günther, 2012); (Chang, Liu, & Shen, 2017); (Dinev & Hart, 2004); (H. Li, Sarathy, & Xu, 2010); (Fodor & Brem, 2015); (Xu, Luo, Carroll, & Rosson, 2011), to name but a few), which makes addressing these concerns an important aspect to consider from a managerial perspective.

Chapter 2: **Literature Review**

2.1 The Legal Context

However, in Europe, revealing personal information, in whatever context that may be, is a matter that was addressed as early as 1950, during the first moments of the European Union (EU). In one of its fundamental legal frameworks the EU established that any citizen had a right to privacy[6], and an extensive, regularly updated body of legislation has been put in place to protect it.

It was in 1981, that the EU addressed the more specific issue of data protection as part of the right for privacy for the first time (Alessi, 2017). The Convention 108 aimed to secure every individual's "*rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*"[7]. Further and most recently, the European Parliament and the European Council enacted the General Data Protection Regulation (GDPR), which codifies the "right to be forgotten" that had been recognized by the European Court of Justice in the 2014 case of Google Spain SL vs Agencia Espanola de Proteccion de Datos (AEPD).

The inclusion of a landmark policy framework with globally significant impact (Goddard, 2017), which represents a "seismic shift" in the data management world (Eifrem, 2018)and aims to "significantly transfer control of information usage to individuals" and away from companies (Seo, Kim, Park, Park, & Lee, 2017) is an indicator of the increasing value that privacy has on the international stage.

[6] Council of Europe (1950), *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, Chapter 8, Retrieved on March 14, 2018 from: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c

[7] Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Article 1. Retrieved March 14, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

2.2 Violations of Privacy

Privacy has been the reason for several class-action lawsuits in recent years. While some of these litigations were settled without fines being applied, the cost of some of these litigations rose to multiple billions of dollars.

For example, in 2009, Facebook changed its website in such a way that information that had hitherto been designated as private became public (Federal Trade Commission, 2011). Then, in 2011, Facebook was pressed with charges of "appropriating the names, photographs and identities of users to advertise products without their consent" (Womack, 2013). The law firm that brought the class-action lawsuit against Facebook asked for $15 billion as compensation (Reisinger, 2012). In January 2018, a German regional court ruled that "Facebook's privacy settings and its use of personal data are against German consumer law" (Kennedy, 2018). In March 2018, Facebook was the subject of another breach of its users' privacy. Facebook was accused of granting data mining firm Cambridge Analytica access to millions of Facebook user profiles, which Cambridge Analytica used to build psychographic profiles of some 87 million[8] Facebook users, to then feed those users micro-targeted content that is intended to "change audience behaviour".

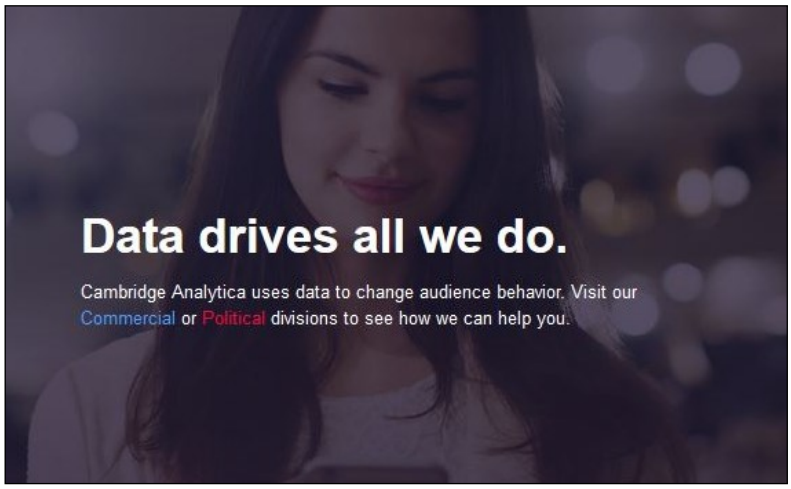


Figure 2 - Cambridge Analytica's landing page

But Facebook is far from being alone at the defendants' table when it comes to privacy litigations in the tech world. In 2010, Google Inc. (henceforth Google) lost a case against Benjamin Joffe, who claimed that Google ruptured the Wiretap Legislation Act when it was collecting the images for Google Maps Street View with Google cars that were taking pictures and simultaneously collecting and listening in on data traffic of private home Wi-Fi networks

[8] Data Protection Working Party WP 223. (2014). *Opinion 8 / 2014 on the on Recent Developments on the Internet of Things*, (September), 1–24. Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm

In 2012, Google was forced to pay $17 million[9] to state attorneys after it was considered guilty of violating its own privacy policy and an additional $22.5 million to the FTC for violating a previous administrative order (FTC, 2012). In 2016, it agreed to pay $5.5 million to settle a legal dispute concerning the tracking of users of the Safari Browser by modifying cookies "in a way that qualified [them] for a loophole in the Safari settings"[10]. Also in 2016, it reached a no-cash settlement when it lost a case against Daniel Matera, who accused Google of building user profiles of non-Gmail users by scanning email traffic sent between these users and Gmail users, and then selling these profiles to advertisers[11].

In another instance, several Android flashlight apps were criticised over privacy concerns, with some of these apps requiring the permission to "delete apps, track location, access Bluetooth connectivity, [and] view call details". The identified cause for these permission requests was so that the data collected could be sold to marketers and ad networks[12].

Episodes concerning smart devices have started to create headlines as well. In May 2018 Bloomberg.com, reported on a couple whose conversation was recorded and then sent to an acquaintance by Amazon's smart speaker Echo without the couple's consent[13].

In 2015, Samsung generated unrest amongst consumers[14] when they became aware of a passage of its Smart TV privacy policy that read: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition". Furthermore, at the end of the policy Samsung underlined that these "third parties" were allowed to collect a range of information from the device, and that Samsung "not responsible for these providers' privacy or security practices"[15]. Samsung had to issue several public statements to appease the public and adapted its privacy policy. In 2018, in the aftermath of

[9] Roberts, J. (2016). *Google to Pay $5.5M to Settle Claims It Hacked Apple's Safari Browser*. Fortune. Retrieved March 16, 2018, from http://fortune.com/2016/08/30/google-safari-class-action/

[10] *Id.*

[11] Cabraser, L. (2016). *Class Action Settlement in Google Message Scanning Privacy Lawsuit*. Retrieved March 16, 2018, from https://www.lieffcabraser.com/2016/12/class-action-settlement-announced-in-google-message-scanning-privacy-lawsuit/

[12] Fox-Brewster, T. (2014). *Check the permissions: Android flashlight apps criticised over privacy* | Technology | The Guardian. Retrieved March 28, 2018, from https://www.theguardian.com/technology/2014/oct/03/android-flashlight-apps-permissions-privacy

[13] Soper, S. (2018). *Amazon's Alexa Recorded Couple's Private Convo, Sent to Contacts* - Bloomberg. Retrieved May 25, 2018, from https://www.bloomberg.com/news/articles/2018-05-24/amazon-s-alexa-eavesdropped-and-shared-the-conversation-report

[14] Smith, C. (2014). *Man who owns a smart TV says he's 'afraid' of using it after reading its privacy policy* – BGR. Retrieved May 25, 2018, from http://bgr.com/2014/10/31/smart-tv-privacy-and-security/

[15] Samsung. (2016). *Samsung Global Privacy Policy - Smart TV Supplement*. Retrieved May 25, 2018, from https://www.samsung.com/uk/info/privacy-SmartTV/

the Cambridge Analytica incident, Facebook pursued a similar line of reasoning in regard to third party applications. However, in both cases, that argumentation did not protect the companies against bad press and consumer outrage.

In February 2018, 50 US companies were defending class-action lawsuits pertaining to personal data protection infringements (Knight & Castle, 2018). The authors of the magazine article also noted that there had been a "dramatic uptick in filings (...) in late 2017".

As can be observed, policy breaches have been a recurring issue in today's business world, tech and non-tech alike. With the introduction of the General Data Protection Regulation in the European Union, the number of litigations is prone to rise, which in turn could have a negative impact on the consumers' perception of particular brands, technologies or entire industries.

2.3 Privacy concern in the technological context

The Cambridge English Dictionary defines privacy as "the right to keep personal matters and relationships secret"[16]. Then again, Margulis (2011)admits that privacy is an elusive concept, given that it is neither static nor objective in nature. However, the issue discussed in this paper relates much more to *privacy concern* than to privacy itself.

Malhotra (2004) describes privacy concerns as associated with the collection, unauthorized access, errors, usage, control, and awareness of sensitive or private data. In short, privacy concerns reflect user concerns around personal information disclosure (Y. Li, 2011). Another author describes the risk of information disclosure, in itself a privacy concern, as the use, the sharing, and/or the misuse of information in the processing of social activities (Chang et al., 2017)

A range of studies has been conducted to analyse user behaviour regarding said privacy concern in a technological context. For instance, a study on the use of social network services found that some users have not only become reluctant to reveal personal information in conducting social activities on Facebook but also deactivated their accounts in protest against the way that their personal information has been handled by the social network service (Chang, 2017). The same author also proved that privacy concerns had a significant impact on perceived risk, which in turn negatively affected trust and user continuance intention, which shows that privacy concerns can pose a serious threat to business relationships and revenue streams resulting thereof. However, given the current business practice of take-it-or-leave

[16] Cambridge Dictionary (2016). *Definition of Privacy in the Cambridge English Dictionary*. Cambridge University. Retrieved from https://dictionary.cambridge.org/dictionary/english/privacy

privacy policies (Preibusch, 2013), it can be difficult to determine how extensive the loss of business is, given that privacy-concerned users might not even enter a business relationship, thus not being able to provide the company with insights into their concerns. Nonetheless, a host of authors has found ways to quantify privacy in other ways. For instance, Egelman (2012) demonstrated the value of privacy by presenting research subjects with two similar smartphone apps that only differed in the extent of their privacy policy, and concluded that privacy-conscious participants were willing to pay up to $1.50 over an initial price of $0.49 to use the app with the more protective privacy policy. Note that it is worth interpreting this figure both in absolute terms but also as a ratio of premium over price. And, when surveyed about data protection issues, consumers repeatedly report high concerns about their information privacy (Eurobarometer, 2004). In one instance reflecting these concerns, Hamilton (2013) even concluded that electronic health records were facing adoption challenges because of privacy concerns voiced by consumers. Fodor & Brehm (2015) found that overall privacy concerns negatively impact adoption intentions of location-based services.

At the same time, there is conflicting evidence on how users value and uphold the integrity of their privacy, for example, in the face of short-term incentives. In a field experiment, Beresford (2012) asked subjects to buy a DVD from one of two practically identical stores. However, Store A asked for income and date of birth to complete a purchase, whilst Store B asked for favourite colour and year of birth. Thus, the information requested by the first store was unquestionably more sensitive. Surprisingly, the subjects bought from both stores equally when the price was the same. When the prices in Store A were set to be 1 Euro less, “almost all participants” chose the cheaper store, even though they had to disclose more personal information to benefit from the lower price point. This same mechanics partly explains the reasoning behind loyalty programmes of retail chains (Preibusch, 2013), which oftentimes demand significant disclosure of personal information in the sign-up process in exchange for exclusive discounts and promotions.

This mismatch between self-professed privacy attitudes and awareness on the one hand and privacy-undermining behaviour on the other hand has been called the privacy paradox ((Brown, 2001); (Norberg, 2007); Preibusch, 2013). This mismatch between attitude and behaviour expands beyond personal information disclosed on social network services to other forms of personal data-based services including applications using geographic location (Zafeiropoulou, 2013) and online-shopping apps ((Brown, 2001); (Spiekermann, Grossklags, & Berendt, 2001)). Furthermore, Steinfeld et al. (2016) studied how users read privacy

policies by conducting an eye-tracking experiment. They found that users who had responded that privacy was important to them, that they never provide information online unless they had to, and that they "*always*" or "*sometimes*" read privacy policies, did not spend a significantly greater amount of time on the privacy policy page contained within the experiment than other survey participants. At the same time, the same group of researchers also discovered that, when "*the [time] cost of becoming informed [was] reasonable"*, users did *"tend to actively acquire that information*". They concluded that, "*Nonetheless, with the way privacy policies are being drafted and managed today, it is unreasonable to expect users to actually become informed.*" (p. 998).

Other authors, while agreeing with the existence of the privacy paradox, have also claimed that users are influenced by contextual factors and thus do not make information-sharing decisions as entirely free agents (Zafeiropoulou, 2014). Additionally, several authors have identified a range of biases that influence privacy decisions, namely overconfidence (Brandimarte, Acquisti, & Loewenstein, 2013), optimism bias (Cho, Lee, & Chung, 2010), affect heuristics (Wakefield, 2013). Finally, Sundar et al. (2013) confirmed that privacy-protecting behaviour was, in fact, highly dependent on context: In an experiment, they split the survey participants into two groups and showed one of these groups a video that depicted potential scenarios of personal information misuse, while the other group was shown a video on the benefits of personalised advertisement. In the end, participants who had been primed with the latter disclosed significantly more information than the other group, regardless of previously reported privacy concerns. The study showed that there are ways to circumvent, or potentially shift, privacy concerns.

2.4 The role of Privacy Concerns in Technology Acceptance

A considerable number of theories and models exist that aim at explaining Technology Acceptance. Venkatesh et al. (2003), outlined eight predominant theories that were commonly used to study technology adoption scenario, which his team of researchers then combined into the Unified Theory of Acceptance and Use of Technology (UTAUT) (p. 446). However, it is interesting to note that none of these feature privacy as a dimension of adoption intention (Fodor, 2015), given that they were developed to be applied to work-environment IT tool adoption scenarios, and neither does UTAUT. The extension of UTAUT to UTAUT2 (Venkatesh, Thong, & Xu, 2012) added hedonic motivation, price value and habit to the equation, but still did not mention privacy.

In a 1996 paper, Smith, Milberg, and Burke, stated that there was a ‘‘[...] lack of validated instruments for measuring individuals’ concerns about organizational information privacy practices’’ (Smith, Milberg, & Burke, 1996, p. 168). In an effort of altering the *status quo*, the researchers developed and validated a 15-item instrument to measure four “central dimensions of individuals’ concerns about organisational information privacy” (p. 169): collection of personal information, unauthorized secondary use of personal information (internal and external), errors in personal information, and improper access to personal information.

Since then, many authors (Malhotra (2004), Dinev (2004), and Xu (2012), to name but a few) have updated and adapted Smith’s seminal work to fit various scenarios, including internet and mobile privacy.

Two comprehensive models have been constructed and tested by Fodor & Brehm (2015). Their research compared these two models and evaluated the impact of user’s privacy concerns on their adoption of location-based services. This study represents an instance where technology adoption theories included privacy concerns into the equation.

2.5 Cultural Differences

There is no consensus on the effect of culture or nationality on privacy concerns and the consequences resulting thereof. A cross-cultural comparison of Chinese and American millennials found no difference between the privacy concerns of the two user groups and concluded that concern levels are “universally high” (Pentina, Zhang, Bata, & Chen, 2016).

However, Cecere et. al. (2015), found that regional differences in privacy concern levels did exist across Europe, when they studied more than 22,000 voiced concerns of participants of a 2009 Eurobarometer survey. They concluded that Northern and Eastern European citizens were less concerned about misuse of their personal data than citizens from Central and Southern European countries. They further concluded that both gender and education were significant predictors of privacy concerns, stating that males in general and less educated individuals showed a lower level of privacy concern. Finally, they identified that strong privacy regulation acted as an information campaign, since it increased individuals’ privacy concerns. This could be a relevant factor in this research paper as well, given that the aforementioned European General Data Protection Regulation framework was a recurring element of mainstream news media at the time the study documented in this paper was conducted.

In a separate study, Wu et al. (2012), found that there was cross-cultural effect that moderated the relationship between privacy concerns and the content of privacy policies, presenting partial evidence that privacy policies of different countries were tailored to fit the privacy concerns of the country in case. This could indicate that culture influences privacy concerns.
When comparing US and South Korean students, Park (2008) found significant differences between the students groups in what pertained to the aforementioned privacy paradox. In Korean students the gap between the belief of information privacy rights and daily practices in the digital realm was far wider than in their American counterparts.

Pavlou and Chai (2002) found that cultural differences influence adoption concerns of e-commerce, further highlighting the relevance of culture in the digital realm. In a separate instance, Wu et al. (2012) found that there was a significant difference in willingness to provide personal information between Russian and Taiwanese internet users.

Krasnova et al. (2012) studied how two dimensions of Hofstede's cultural framework impacted German and American Facebook users' self-disclosure willingness on the social network. The researchers found that Individualism and Uncertainty Avoidance significantly impacted the motivation of users to create and share content on social networking sites.
When comparing Portugal and Germany using the Hofstede framework, it quickly becomes apparent that the two cultures differ vastly in most dimensions, as can be seen below:

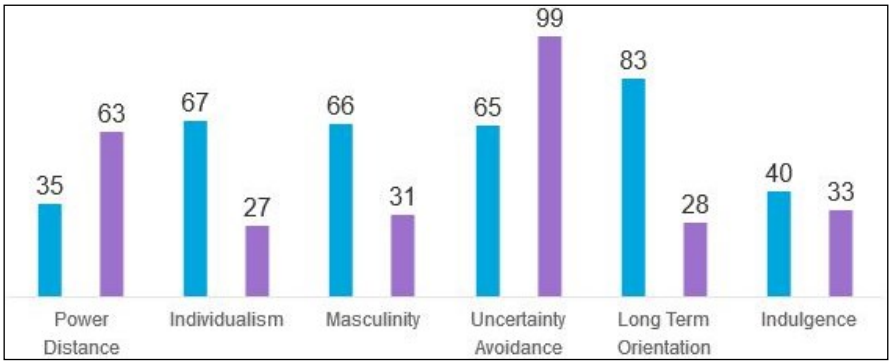


Figure 3 - Hofstede's cultural dimensions for Germany (blue - left) and Portugal (purple - right)

As can be seen, there is at least a 30 point gap separating the two cultures' scores across all dimensions but two (and in a Power Distance the gap is 28). In that sense, the Portuguese and German cultures may be strong candidates for an introductory comparison of privacy concerns in consideration of culture, given their oftentimes opposing scores.
It is interesting to note, that Hofstede relates the Uncertainty Avoidance factor, a dimension that "defines Portugal very clearly"[17], to security, which is an oftentimes referred false

[17] Hofstede. (2017). *Country Comparison Germany/Portugal* - Hofstede Insights. Retrieved May 3, 2018, from https://www.hofstede-insights.com/country-comparison/germany,portugal/

dichotomy to limit or intrude on privacy (Ishii, 2017). At the same time, a higher power distance has been found to correlate with an increased likelihood of tolerance towards the surrendering of privacy to authorities (Wu et al., 2012). However, research has yet to link this increased likelihood to give up privacy to other entities.

2.6 IoT Industry

To understand how the Internet of Things (IoT) relates to the topic of smartphone privacy it is important to understand the relationship between smartphones and IoT devices. To that end, it is useful to look at one definition of what the IoT actually is. To cite Deshmukh and Sonavane (2017):

The Internet of Things (IoT) is the network of physical objects or devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity which enable these objects to collect and exchange data. (p. 71)

Given that smartphones gather all these characteristics, it is possible to deduce that, in their own way, smartphones *are* IoT devices. Having reached that conclusion, the next conclusion would be that smartphones are the first wide-spread IoT device (given that computers and laptops, the immediate predecessors, don't have any sensors like gyroscopes, accelerometers, GPS navigation systems, etc.). Finally, given that smartphones are themselves IoT devices, it seems logical to use them to inspect the next generation of specialised IoT devices

The range of potential use cases expands continuously as more and more products enter the market, promising to make life easier, safer, more efficient, and, to use the new millennia's buzzword, *smarter*. Peppet (2014) identified five categories of such consumer IoT use cases: Health and Fitness devices, Automobile sensors, Home and Electricity applications, Employee sensors (which this paper will not focus on, given that their adoption is mostly involuntary as it is part of the company policy), and Smartphone sensors. Within each of these categories further categorisation is possible, and each subcategory gathers a multitude of devices under its umbrella. Thus, application scenarios are extremely diverse, ranging from highly intimate and even physically invasive to overarching, infrastructural settings. *Implants*

or *intimate contact sensors*, like the Looncup, the *world's first smart menstrual cup*[18], which provides the user with menstrual cycle analysis and real-time fluid volume tracking[19], to non-invasive *wearables*, such as the BodyGuardian, a topical patch which monitors the heart behaviour of cardiac arrhythmia patients as they go about their normal lives and can provide doctors with remote access to data in a critical situation[20], promise new ways to quantify our performance and pose numerous opportunities for the healthcare industry. Home applications such as the Google Home or Amazon Echo smart speaker ranges, which offer a wide range of voice-command enabled services, will give its users new ways of interacting with their home by enabling them to control a variety of other connected home appliances like ovens[21] [22], lighting systems[23], security systems[24] [25], amongst many others. And infrastructural, large-scale applications such as Echelon's Smart Lighting System have proven to be very effective at deploying city council resources in a highly efficient manner (Echelon's products reduced the street light grid energy consumption of Bellington, USA by 70%), thus adding an additional layer to the IoT environment future consumers might live in. As a result, WoodsideCap (2015) predicted as many as 50 billion devices will be connected to the IoT by 2020.

In a world where connected devices vastly outnumber the user population the term "sensor fusion" coined by computer scientists might play an important role. Sensor fusion dictates that the information collected by two disparate sensing devices is, when combined, greater than the sum of each device's isolated data streams (Peppet, 2014). A simple example of this can be found in any fitness tracker, where accelerometer records the speed at which the user is moving, while a heartbeat monitor tracks cardiovascular activity, thus allowing for

[18] LoonCup – *The world's first SMART menstrual cup.* by LOON Lab, Inc. (2015). Retrieved May 6, 2018, from https://www.kickstarter.com/projects/700989404/looncup-the-worlds-first-smart-menstrual-cup/description

[19] Brown, T. J. (2017). Is The Looncup Menstrual Tracker A Scam? – The Establishment. Retrieved March 9, 2018, from https://theestablishment.co/the-strange-dark-fate-of-the-looncup-menstrual-tracker-95a4a334626c

[20] *BodyGuardian Heart*. Retrieved April 20, 2018, from http://www.preventicesolutions.com/services/body-guardian-heart.html

[21] *GE WiFi Connect - Ranges & Ovens*. (n.d.). Retrieved May 4, 2018, from http://www.geappliances.com/ge/connected-appliances/ranges-ovens-cooking.htm

[22] *Bosch Wall Ovens with Home Connect*. (n.d.). Retrieved May 1, 2018, from https://www.bosch-home.com/us/experience-bosch/home-connect/home-connect-wallovens

[23] Phelan, D. (2018). 10 best smart lighting | The Independent. Retrieved May 4, 2018, from https://www.independent.co.uk/extras/indybest/house-garden/lighting/best-smart-light-bulbs-lighting-alexa-google-home-philips-app-a8177256.html

[24] iSmartAlarm. (n.d.). iSmartAlarm - The Leader in DIY Smart Home Security. Retrieved May 4, 2018, from https://www.ismartalarm.com/

[25] Verisure - Smart Alarms. (n.d.). Retrieved May 4, 2018, from https://www.verisure.pt/alarmes/g/alarmes-para-casa_nova.html?ds_rl=1257732&pkw=alarme&

insights into the user's state of health that neither of these sensors could provide individually. However, in more complex scenarios, this means that two IoT sensors could allow for unexpected inferences and the deduction of potentially sensitive information[26]. As outlined by the European Commission's Working Party for Data Protection, while the user may be "comfortable with sharing the original information for one specific purpose, he/she may not want to share this secondary information that could be used for totally different purposes"[27].

In conclusion, to Peppet (2014), sensor fusion in the Internet of Things context may mean that "every thing may reveal everything."[28] Thus, the IoT, with its potential to take data-driven knowledge to a new level, also increases the potential for exploitation and ever-more-powerless customers (De Cremer, 2017).

Chapter 3: **Methodology and Data Collection**

The following chapter outlines the methodology applied in the conduction of this study. It details the research method, the procedures for data collection, and the deployed variables set.

3.1 Research Focus

Public opinion polls show rising levels of concern about privacy (Smith, 1996). At the same time, people are concerned about their privacy to different extents (Malhotra, 2004). With the IoT prone to open up a new frontiers on data collection and use, where unprecedented amounts of personal information will be shared among a "myriad of often invisible players who use it for a host of purposes" (Office of the Privacy Commissioner of Canada, 2016), these concerns could be aggravated further (Xu, 2012). To that end, this paper will shine a light into the current state of affairs of privacy concerns of a segment of millennials and their purchase intentions of IoT devices, by focussing on the following questions:

RQ1: Is there a cultural difference in regards to reported privacy concerns?

RQ2: Do demographics influence privacy concerns?

[26] Data Protection Working Party WP 223. (2014*). Opinion 8 / 2014 on the on Recent Developments on the Internet of Things*, (September), 1–24. Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm

[27] *Id.*

[28] Peppet, S. (2014). *Regulating the Internet of things: First steps toward managing discrimination, privacy, security, and consent*. Texas Law Review, 93(1), p. 93. Retrieved March 8, 2018, from http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=3&sid=8de633d7-0f68-4fea-913b-53194578b5cf%40sessionmgr4006

RQ3: How do privacy concerns impact IoT device adoption intentions?

RQ4: How does a privacy awareness situation influence IoT device adoption intentions?

3.2 Hypotheses

To answer these research questions the following hypotheses were developed:

H1 – German millennials report higher privacy concern levels than Portuguese millennials.

Research conducted by Zhang et al. (2007), analysed the online privacy policies of leading international companies in the USA, China, Japan, UK, and Australia. They found significant differences in the focus of these policies across the countries under study, which may indicate that the cultural background is an aspect to consider in the privacy concern debate.

Further, Sheehan (2000) found that women are generally more concerns with the collection of personal information, while Culnan (1995) found that age and income both had a positive impact on privacy concerns. This paper further investigates these findings:

H2 – Demographics affect privacy concerns.

H2a – Older participants show higher privacy concerns than younger ones.

H2b – Income positively impacts privacy concerns.

H2c – Female participants report higher privacy than males.

A host of authors have found that privacy concerns negatively impact adoption, engagement, or personal information disclosure willingness for social media (Krasnova, 2012; Chang, 2017), e-commerce (Dinev, 2004; Li, 2010), location-based services (Fodor & Brehm, 2015), e-banking services (Jahangir & Begum, 2008) and electronic health records (Hamilton, 2013).

Furthermore, Xu (2011), found that users are unlikely to adopt and use mobile apps if they suspect opportunistic behaviour by their mobile service providers. However, the adoption intentions of IoT technology under consideration of privacy concerns do not yet seem to be a well-studied subject.

Given that the IoT will create new data streams that will collect large amounts of personal data (Peppet, 2014), this paper aims to explore how the previously analysed privacy concerns translate into IoT adoption intentions:

H3 – Level of privacy concerns has a negative impact on IoT adoption intentions.

H3a – Privacy concerns and IoT device ownership are negatively correlated.

Much like before, the role of culture will be studied by analysing its moderating impact on the relationship between privacy concerns and IoT adoption intentions:

H3b – German millennials report lower IoT adoption intentions than Portuguese millennials.

Taking up research conducted by Malhotra et al. (2004) and Hallam et al. (2017), who identified and confirmed, respectively, awareness of privacy practices to be one of the dimensions of internet user information privacy concerns this paper will test the following hypothesis:

H4 – Checking smartphone app permissions, more severely hampers IoT purchase intentions of German respondents than of Portuguese respondents.

H5 – Perceptions about the appropriateness of app permissions affect IoT device adoption intentions.

Finally, this survey will adapt the experiment previously conducted by Egelman et al. (2012) to test the hypothesis that German survey participants are more willing to pay a premium for smartphone applications that promise the user the non-disclosure of personal information. This hypothesis directly targets the quantitative nature of the value of privacy.

H6 – German millennials are willing to pay a higher premium for privacy protecting applications than Portuguese respondents.

3.3 Research Method

In an effort to ensure scientific rigour while respecting the time constraints placed on this project, the research was conducted using a four step approach to find answers for the research questions outlined in Chapter 1.

First, the existing literature was collected, compiled and grouped into logical blocks to shed light into the different aspects to consider when studying privacy concerns as well as providing insights into procedures and tools deployed in previous research.

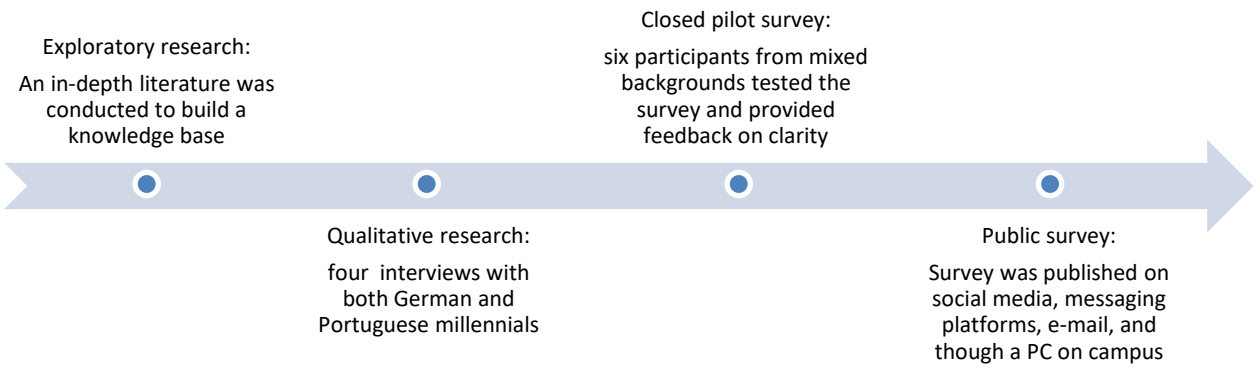
In a second step four in-depth interviews were conducted with individuals from the target population. The interviews served as insights into consumption behaviours, privacy concerns, adopted privacy protection measures, and further revealed information about the perception of the privacy situation in the technology world amongst participants.

In a third step, taking in and building on the insights provided by the interviews, and factoring in findings of previous research as uncovered through the literature review, an online survey was built using the Qualtrics survey tool. Subsequently, this survey was pilot tested by six peers, who were specifically selected by the researcher. The sample equally represented both genders and featured two Portuguese and two German participants. The remaining two participants were a New Zealand and a United States citizen, which were approached for their English native speaking competences. The six participants delivered valuable insights into a layout error that hid the path to the app permission settings on iOS devices, some English spelling mistakes, and feedback regarding the general clarity and understandability of the questions. Most importantly, they confirmed the accuracy of the instructions provided to find the app permission settings.

Their concerns and suggestions were addressed before the survey was launched to the general public. The replies of the six participants were discarded, given that they did not reply to the final version of the survey that was published after their feedback.

Finally, the survey was distributed online via e-mail, social media and messaging platforms, as well as filled out on the researcher's own computer, which was made available to students on the university campus. Students who filled out the survey on said computer, in no way received aid or clarifications from the researcher, in order to keep maintain the equality of survey answering conditions.

Given that the survey mainly reached individuals in the researcher's immediate circle of acquaintances, the sample classifies as a non-probability, convenience sample, according to the sampling technique framework as described by Saunders et al. (2009). An overview of the research method can be found below:



3.4 Research instruments

3.4.1 Qualitative research instrument

The qualitative research of this study consisted of four in-depth and unstructured interviews. They were conducted individually, either in person or over Skype with Católica students. The selection was not random, as the individuals were specifically chosen to abide by certain criteria of heterogeneity: It was made sure that both nationalities and genders were equally represented. Furthermore, three participants were pursuing degrees in different fields (more specifically social sciences, natural sciences and business studies), while the fourth was studying law and interning at a law firm.

The main goal of the interviews was to gain a more diverse spectrum of insights into the topic of privacy, the importance it has to users, their thoughts and knowledge of IoT, how they use their smartphones, as well as their awareness of the Cambridge Analytica situation. Further, it tested whether the path to the app permissions settings applied to a range of different smartphones and operating systems, given that the same paths would be part of the survey that would be sent out to students for the quantitative part of the research. At the same time, the degree of ease to locate the app permission settings using this path was assessed.
The detailed interview guide can be found under Annex 1.

The interviews revealed that opinions regarding privacy concerns were widely different across participants. For instance, one participant reported that privacy was not a concern to him. This surprisingly blunt statement resulted in the addition of a new question, which directly asked participants to evaluate the statement “Online privacy is important to me”. On the other end of the spectrum, a participant reported that she valued privacy a lot, and that she used privacy enhancing features like a VPN and the NoScript add-on on her Firefox browser, which disables JavaScripts on webpages unless these are expressly whitelisted by the user.

It was also interesting to see that all four participants had at least a rough understanding of the Cambridge Analytica incident, although some were more concerned about the implications of the incident than others.

Some of the interviewees already knew about the app permissions feature, which made it clear that this could be a good item within the privacy concern scale rather than being only a part of the experiment at the end of the survey. Thus, the question “I often look at app permissions before downloading a new app” was added to the Privacy concern construct.

All in all, the conversation about privacy was a stimulating one, even with the participant that was not concerned about it. When asked why privacy was not something he was concerned about he merely replied: “It’s too late. They already know everything anyway.”

3.4.2 Quantitative research instrument

For the main part of the data collection process an online survey was deemed the most effective way, both logistically and time-wise, to gather a critical mass of responses to allow for statistical hypothesis testing.

The survey was available on social media and was also sent out to target individuals, in an effort to maintain a balance between German and Portuguese survey respondents. The collection period lasted for one week in mid-May 2018 and during that time 168 answers were collected.

The survey was built using the Qualtrics online platform. It was written in English and featured 30 questions, which were divided into five content blocks: The first block concerned demographics data, the second targeted the respondents’ smartphone usage profile, the third pertained to privacy, the fourth their IoT device purchase intentions, while the last requested feedback on the settings check respondents were asked to conduct.

The demographics block was placed first because nationality is a central dimension in several research questions of this project. Research conducted by Teclaw et al. (2011) concluded that placing demographics at the beginning of a survey unsurprisingly resulted in higher response rates to this relevant set of question, but also did not influence the results of what was tested thereafter[29]. Furthermore, it seemed sensible to introduce participants to the survey mechanics by offering them easy to answer questions that required little to no reflection. The section requested information about the participants’ gender, age, educational background, nationality, as well as household net income.

The second section focused on smartphone ownership, application use, and IoT device ownership. Participants were asked to select any IoT devices they owned from a predetermined list that featured the most popular IoT devices. Moreover, this section was used as a platform to ask the survey participants directly about how important online privacy was to them.

[29] An exception to this are tests that could produce race-based stereotype threat, or, “the tendency for minority group performance on cognitive measures to decrease as a result of anxiety associated with confirming negative stereotypes about intelligence. In this particular research, this threat was assumed to be not applicable, thus demographics were placed at the beginning of the survey.

The following section addressed the privacy concerns of survey participants, as an independent variable. A total of 11 questions aimed at different dimensions of privacy, of which nine were selected from scales developed in previous scientific studies. Attention was placed on targeting a broad range of dimensions studied by the authors of these papers. Annex 2 lists the sources, as well as the dimensions, the questions were derived from. The last question in this section mimicked the study conducted by Egelman et al. (2012), which tested the research participants' willingness to pay for a privacy protecting smartphone app.

The fourth section concerned IoT device adoption intentions. In this section four IoT devices were listed and participants were asked to rate their agreeableness with the statement "I intend to buy [device] in the next three years". The devices were chosen to cover a broad range of application scenarios, underlying privacy implications, and sensor features. The selected devices were a fitness tracker, a smart speaker, smart home appliances, and a car telematics system. Each question featured a short product description to ensure that participants understood the utility of the device. At this point, and taking into consideration that in the next section participants would be asked to navigate away from the survey to go to their smartphone's setting menu, an attention check question was inserted, that would allow to validate all previous responses should the survey participant forget to return to the survey at this point, and thus not reply to the remaining questions, yielding a partial survey response.
The final section, evaluated the participants' response to the settings check that users were asked to perform. Three questions targeted different aspects of that experience in an attempt to capture the participants' emotional reaction. The final question then asked participants if they thought their IoT adoption intentions had shifted due to the experience.

The full survey may be found in the Annex section (Annex 17).

3.5 Data Review

To ensure that the tests that would be run to test the hypotheses would remain within the denounced scope of the project the data collected through the online survey was subjected to several checks of relevance: First, all responses from participants who were not Portuguese or German were removed. Second, individuals that did not classify as "Millennials", i.e. which did not report an age between 16 and 35 years old, were excluded. The definition of Howe & Strauss (2000), who have been credited with naming that generation, was used to establish these cut-offs. Then, the attention check question was examined. Even though it was not at the end of the survey, it was also used as a definition of a "complete" response, given

that important insights had already been gathered up to this point in the survey, and the following section of the questionnaire asked participants to check their app permissions, which was assumed distract some participants away from the survey.

Abiding by these criteria, these checks identified that out of the one hundred and sixty-eight (168) collected responses one hundred and forty-five (145) responses matched the outlined target population.

Finally, in an effort of safeguarding the integrity of the results, and given the centrality of privacy concerns in the context of this study, an outlier analysis on the 11 items pertaining to this construct was conducted before any of the other test and descriptive statistics was run. The selected method to identify said outliers was a multivariate outlier analysis, which aimed to detect unlikely combinations of responses within the dimension of privacy concerns for each participant. To this end, the Mahalanobis distance was calculated and participant responses that failed to meet the $p > .001$ criterion were excluded from the analysis. The analysis revealed five responses that were eliminated from the study, reducing the final number of responses to be used for the hypotheses testing to one hundred and forty (140).
Please also note, that all tests were conducted at a 95% confidence interval, unless stated otherwise.

Chapter 4: **Findings**

4.1 Sample Characterisation

In the scope of this study, one hundred and forty (140) valid responses were collected through the online survey.

The majority of survey respondents were female (53%) and the nationalities being studied were almost perfectly equally represented (48% Portuguese). More than half (54.3%) of the sample was between 21 and 25 years old, while another 35% were between 26 and 30 years old, meaning that close to 90% of the sample fell within these two brackets. Around 11% of the participants had a high school diploma as their highest academic degree, 33% had either completed or were enrolled in a Bachelor's degree, and about 53% had completed or were enrolled in a Master's degree, while there was one MBA candidate as well as four PhD candidates amongst the respondents. There was a large discrepancy amongst survey participants and their disposable household income. Broadly speaking, 25% of respondents reported earning less than 10,000€, another 20% of respondents fell within the next 10,000€ bracket, while close to 75% reported earnings of 50,000€ or less.

4.2 Scale Reliability & Distribution

Given that the scale that measured Privacy Concerns (PC) was adapted from the existing body of literature, an analysis of the scale's reliability was deemed necessary, especially when taking into account that the scale had been complemented by the author. The Coefficient (or Cronbach's) Alpha was selected to assess the multi-item consistency of the scales, as it is the most widely used measure of scale reliability and the "measure of choice for estimating reliability" (Peterson, 1994).

As shown below, the score of the 11 items was 0.889. That being the case, no items were deleted from the scale.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.889	.895	11

It could be argued that the willingness to buy IoT devices, as expressed through the four proxies (Fitness tracker, Smart Speaker, Smart Home Appliance, and Car Telematics), could equally be subjected to a reliability test. However, since these devices were chosen specifically for their different attributes and selling points, they are assumed to be independent, as buying any of the tested devices does not necessarily correlate with buying another, much less all four.

4.3 Hypotheses testing

H1 – German millennials report higher privacy concern levels than Portuguese millennials.

To identify the tests that would be suitable to test this hypothesis, the distribution of the responses to all PC variables was analysed between the two nationality groups to determine normality. As can be seen in Annex 3 all variables of the PC construct were non-normally distributed. Even though in some cases the z-values for some skewness and kurtosis measures were between -1.96 and 1.96, as would be expected in normally distributed cases (Field, 2009), none of the cases reported a Shapiro-Wilk test significance of $p > .05$, which would indicate normal distribution (Shapiro & Wilk, 1965).

To test the null hypothesis (H_0: There is no statistically significant difference across reported privacy concerns between the two nationalities (H_0: $\mu_1 = \mu_2$)) several independent samples Mann-Whitney U tests (Mann & Whitney, 1947) were conducted. This test is

appropriate to study non-normally distributed data sets, as it had fewer underlying assumptions, to the extent that they are also referred to as "assumption-free tests" (Field, 2009, p. 540).

First, the direct question asking how important online privacy was to each respondent was tested. The test revealed that, on average, the perceived importance of PC in German participants (Mean Rank = 77.01, n = 73) exceeded that of Portuguese participants (Mean Rank = 63.40, n = 67), (U = 2921, z = 2.14, p = .032, two tailed) (Annex 4). The effect size was small, at r = 18%.

The same test was then run on the 11 variables targeting PC. The dimension pertaining to the frequency with which participants looked at app permissions before downloading a new app showed statistically significant differences between the habits of German participants (Mean Rank = 77.50, n = 73) and Portuguese participants (Mean Rank = 62.87, n = 67), (U = 2956.5, z = 2.20, p = .028, two tailed) (Annex 5). Again, the effect size was small, at r = 19%. In the other 10 items, there was no statistically significant difference to be found.

However, as outlined by Sullivan (2015), tests for normality can be subject to low power, which can lead to Type I errors (i. e. rejecting a true null hypothesis, or in this case, rejecting normal distribution). That being said, a parametric independent sample t-test was conducted in the same configuration as the Mann-Whitney U tests before.

After confirming the homogeneity of variances using the Levene's test, the independent samples t-test revealed that German respondents more frequently looked at the app permissions before downloading a new app (M = 4.95, SD = 1.972) than Portuguese respondents (M = 4.24, SD = 1.972) ($t(134) = -2.131$, $p < .05$) (Annex 6).

In the other 10 items, there was no statistically significant difference to be found.

In sum, for the items relating to the between-groups differences in the reported importance of online privacy, as well as the frequency with which they check app permissions before downloading a new app, the null hypotheses were rejected, meaning that German participants both rated the importance of online privacy higher, as well as more frequently checked app permissions requirements before downloading a new app than Portuguese respondents.

H2 – Demographics affect privacy concerns.

H2a – Older participants show higher privacy concerns than younger ones.

To test this hypothesis an ANOVA between the independent variable (IV) Age (as measured in four age groups: Group 1 – 16-20 years old, Group 2 – 21-25 y.o., Group 3 – 26-

30 y.o., Group 4 – 31-35 y.o.) and the 11 PC items as dependent variables (DV). Within the direct dimension that asked about the importance of online privacy (Q11) significant differences were found ($F(3,136) = 5.041$, $p < .01$). However, as Fisher's LSD post-hoc test revealed, the trend proposed by the hypothesis could not be confirmed in all cases using this approach. For instance, while Group 1 ranked the importance of online privacy significantly lower than Group 3 (Mean Difference = -.91, $p < .05$) and a similar relationship was found between Groups 2 and 3 (Mean Difference = -.34, $p < .05$), Group 4 also reported lower importance of online privacy when compared to Group 3 (Mean Difference = -.95, $p < 0.001$). In fact, the reported importance of online privacy was statistically significantly higher in Group 3 compared to all three other groups (Annex 7), both younger and older.

However, there were large asymmetries between age groups in terms of number of respondents in each group (the youngest bracket counted four individuals, while the oldest counted 11, the remaining 125 respondents were distributed across the two brackets in-between). To adjust for these asymmetries and to subject the data to more testing, the four age brackets were condensed into two. This created a younger age bracket (aged 16 to 25 years) with 80 participants, and an older bracket (aged 26 years and above) with 60 participants.

Still, neither the Mann-Whitney U test nor an independent samples t-test revealed any significant differences across the two groups in regards to the 11-item PC scale.

In sum, there were some indications that there might be a relationship between age and privacy concerns, although the evidence found in this paper is insufficient to provide a clear and statistically sound assessment of that relationship.

H2b – Income positively impacts privacy concerns.

The scarcity of responses in some categories of income was even more pronounced than in the age variable described above. While an ANOVA with post-hoc contrast test was attempted, the results were insignificant for Q11 (Importance of online privacy) as well as 10 out of the 11 items of PC. And in the one item with significant results (Q13 regarding the uncertainty regarding how app permissions will be used) ($F(9,130) = 2.92$, $p < .01$), the post-hoc results were contradictory[30].

In a second attempt to uncover a relationship, an ANOVA was run to test differences between the several income groups in regards to the average score of PC across the 11

[30] Apart from being void of sensical information, the test report to this ANOVA with LSD post-hoc testing was 29 pages long, and was thus not included in this document.

dimensions. No statistically significant effect of income on PC was identified ($F(1,138) = 1.08$, $p > .05$) (Annex 8).

In a third step, this matter was addressed as for H2a, that is, by creating two condensed income brackets of relatively equal size: 68 individuals in the groups that reports earnings up to 19,999€ per year and 77 respondents that classified in the 20,000€+ bracket.

A Mann-Whitney U did not find a significant difference between the two groups in regards to any of the PC dimensions.

Finally, the null hypothesis was retained, concluding that income had no effect on PC.

H2c – Female participants report higher privacy than males.

The same method performed for H1 was also applied to test the impact of gender on PC. A preliminary Mann-Whitney U test showed that female participants indeed showed a higher concern in the questions concerning being aware and knowledgeable about how their personal information will be used (Q22) ($\text{Mean Rank}_{\text{Females}} = 78.91$, $n = 74$, vs. $\text{Mean Rank}_{\text{Males}} = 61.07$, $n = 66$) ($U = 1819.5$, $z = -2.835$, $p = .005$, two tailed, $r = -24\%$) as well as being able to control that information (Q23) ($\text{Mean Rank}_{\text{Females}} = 78.97$, $n = 74$, vs. $\text{Mean Rank}_{\text{Males}} = 61.01$, $n = 66$), ($U = 1815.5$, $z = -2.814$, $p = .005$, two tailed, $r = -24\%$) (Annex 9).

The independent sample t-test partially confirmed that finding. There was statistical significance in the difference of importance of awareness and knowledge about information use in female participants ($M = 6.38$, $SD = 1.043$) and male participants ($M = 5.85$, $SD = 1.384$) ($t(138) = 2.575$, $p < .05$). In the control over personal information dimension females' concern was higher ($M = 6.35$, $SD = 0.957$) than males' ($M = 5.88$, $SD = 1.157$) ($t(138) = 2.643$, $p < .01$) (Annex 9).

Thus, the null hypothesis was partially rejected, based on the fact that female respondent did value some dimensions of privacy statistically significantly more than male respondents.

H3 – Level of privacy concerns has a negative impact on IoT adoption intentions.

To study the relationship between PC and IoT adoption intentions an unorthodox method was employed. In a first step, the responses on the 11-item PC scale were averaged into a new variable. The same was done for the four proxies of IoT adoption intention (Fitness tracker, smart speaker, smart home appliances, and car telematics). The problem with this approach is that the Likert scales used are not interval scales, meaning that the differences

between Strongly disagree and Disagree, and Disagree and Slightly disagree, for instance, are not necessarily equal. However, this dissertation is concerned about identifying trends, relationships and correlations, rather than accurately quantifying and predicting outcomes and effect sizes.

That being said, that the researcher was aware that this method is controversial and the results found in this section should be considered with care and bearing in mind the procedure with which they were derived.

After removing participants who reported that they already owned one of the devices that would be tested in the IoT adoption section, a linear regression was run to examine a potential relationship between these two newly created variables. The results are highly statistically significant and show that, indeed, higher PC negatively affect IoT adoption intentions as measured by the four proxies ($F(1,117) = 13.41$, $p < .001$). The model explained around 10% of the variance in the dependent variable ($R^2=.095$) (Annex 10).

In the case of H3, the null hypothesis was rejected, as strong statistical evidence was found that privacy concerns were in fact a significant predictor of IoT adoption intentions.

H3a – Privacy concerns and IoT device ownership are negatively correlated.

A linear regression between average PC (IV) and IoT device ownership (DV), calculated as the sum of owned connected devices, was run to test this hypothesis. The results showed that there was no statistically significant relationship between these two constructs ($F(1,138) = .015$, $p > .05$) (Annex 11).

Running multiple regressions of the 11 PC items as IVs and the number of connected devices each respondent owned as DV showed no significant correlations, and neither did a simple linear regression with Reported importance of online privacy (Q11) as IV and owned IoT devices as DV.

Consequently, the null hypothesis was rejected, as no correlation between PC and connected device ownership was found.

H3b - German millennials report lower IoT adoption intentions than Portuguese millennials.

The same two-step procedure as outlined under *H1* was repeated to test this hypothesis. First, the nonparametric Mann-Whitney U test identified that there was indeed a difference in the responses of German participants regarding their IoT adoption intentions

(Mean Rank = 63.44, n = 74) and the intentions manifested by Portuguese participants (Mean Rank = 82.96, n = 71) (U = 1919.5, z = -2.804, p = .005, two tailed, *r* = -.23) (Annex 12)

In the second layer of analysis, an independent sample t-test confirmed that this difference was indeed statistically significant (t(143) = 2.841, p < .01) (Annex 12).

This led to a rejection of the null hypothesis, as significant evidence was found that German respondents reported lower IoT adoption intentions.

H4 – Checking smartphone app permissions, more severely hampers IoT purchase intentions of German respondents than of Portuguese respondents.

A Mann-Whitney U test showed that, indeed, there were differences across the two studied nationality groups in terms of reported IoT purchase likelihoods after the app permission check, as measured by the question "After checking my app permissions, I am [Much less likely ←→ Much more likely] to purchase connected devices". German participants (Mean Rank = 59.78, n = 72) reported an overall lower score than Portuguese respondents (Mean Rank = 80.1, n = 66) (U = 1676.5, z = -3.176, p < .001, two tailed, r = -.27) (Annex 13).

Since the "Mean Rank" categorisation from a Mann-Whitney U test is not easily translatable into meaningful figures, an independent sample t-test was conducted to further investigate the preliminary finding. It reported that the difference in the responses of German (M = 3.11, SD = 1.273) and Portuguese (M = 3.77, SD = 1.20) participants was significant (t(138) = 3.134, p < .01) (Annex 13). It is noteworthy to point out that the score of 4 was labelled "About the same" in the questionnaire, thus representing the neutral centre of the Likert scale for this item. Bearing this in mind and looking at the mean scores of the two groups under scrutiny, reveals that German respondents tended more strongly towards a reduction in the likelihood of buying IoT devices than Portuguese respondents.

Thus, the null hypothesis was rejected, since checking the app permissions more severely hampered IoT purchase likelihood of German participants than of Portuguese respondents.

H5 – Perceptions about the appropriateness of app permissions affect IoT device adoption intentions.

The goal of determining the impact of the three variables (Q33, Q34, Q35) deployed to measure the reaction to the app permission check experiment on a potential change in connected devices purchasing intention (Q36) was explored by performing a multiple linear

regression. To avoid over-fitting the model, the selected method was "stepwise", which allowed SPSS to only add additional predictors to the model, if they explained a significant amount of additional variance. The results show that all three predictors significantly and positively correlated with a change in IoT devices purchase likelihood (Adj. R^2 = .20, $F(1,134) = 15.2$, $p < .05$). The correlation table revealed however that the "Surprised" variable (Q33) did not significantly correlate with the outcome variable ($\beta = .007$, $p > .05$) (Annex 14). Thus, the null hypothesis was rejected, demonstrating that the adequacy of app permissions predicted with future technology engagement, even though the effect was weak, at 20%.

H6 – German millennials are willing to pay a higher premium for privacy protecting applications than Portuguese respondents.

After plotting the amounts survey participants were willing to pay for an app version that protected privacy, some values were considered suspicious or, at least, unrealistic. To correct for these data points, an outlier analysis was conducted to ensure more meaningful results. To conduct this test, a box plot of the Willingness to Pay variable (*WTP*) was created using SPSS, and values with an interquartile range multiplier of 3 were considered outliers and excluded from the analysis. The identified cut-off value was 31€ (Annex 15).

In a next step, the normality of the distribution was tested using the method applied outlined under *H1*. Again, the data was not found to be normally distributed, and thus a Mann Whitney U test was conducted. The test revealed that there was no statistically significant difference between the WTP of German participants (Mean Rank = 73.10, n = 66) and Portuguese participants (Mean Rank = 64.16) ($U = 2613.5$, $z = 1.34$, $p = .182$, two tailed) (Annex 16).

An independent samples t-test reported similar findings ($t(134) = -1.652$, $p > .05$) (Annex 16) and so the null hypothesis was retained, meaning that no statistically significant difference was found between the WTP of German and Portuguese participants.

Chapter 5: **Conclusion**

5.1 Main findings

The following chapter will use the statistical findings to answer the research questions posed at the beginning of this dissertation.

RQ1: Is there a cultural difference in regards to reported privacy concerns?

Fundamentally, this dissertation seems to affirm that there is indeed a cultural difference regarding privacy concerns (H1). As found already by Krasnova et al. (2012), the cultural background of consumers plays a role in their concerns about privacy.

The present piece of research underlines this finding, after discovering that German participants did in fact report higher concerns in regards to privacy than Portuguese participants across some of the studied dimensions. First, German participants generally ranked their concern higher than Portuguese ones. Furthermore, it is interesting to note that in German respondents this concern seemed to translate into palpable action, given that significant differences between nationalities were found in a privacy concern dimension that specifically inquired about a privacy protecting measure. Especially in the context of the privacy paradox, this is a relevant finding that counts as evidence toward the position that privacy concerns may very well translate into concrete action and premeditated checks of potential privacy intrusions that may be trying to slip past a user's attention. At the same time it should be noted, that it is unclear how this check and this examination of app permissions then affects the user's final decision of actually downloading an app, or checking up and disabling the app permissions that rose suspicion during the app acquisition phase.

Being aware of these behaviours and the levels of privacy awareness in different markets can help companies mitigate the negative effects of perceived privacy breaches (as discussed under RQ4) by being transparent and sensible about app permission requirements, especially now that popular application markets allow easy access to the app permission requirements before a download is initiated. For many smaller apps that face a significant amount of competition this could be a strong selling point to those aware users.

At the same time, although this study could not find any statistically significant difference between German and Portuguese respondents in regards to their willingness to pay for a privacy-protecting app (H6), it did show that this willingness to pay for additional privacy protecting reassurances. This shows that privacy has a monetary value to users and could be leveraged by companies as an additional source of revenue, by allowing privacy concerned users to opt for a paid app that ensures that their data will not be sold to third parties. It is also interesting to note, that study participants were willing to pay a premium without knowing how that money would be put to use and what those extra privacy measures consisted of. At the same time it could be inferred, that there is a general sense of distrust in the current privacy policy model and how it protects users.

RQ2: Do demographics influence privacy concerns?

In the aspect of demographic influences on privacy concerns this study was unable to detect a large body of evidence to support the idea that increasing age (H2a) or income (H2b) could exacerbate privacy concerns. This is in line with findings from studies like Hoofnagle's (2010) and Taddicken (2014), who found that both young and old Americans were concerned about their privacy in statistically equal proportions.

At the same time however, this paper confirms that there are some differences in privacy concerns across genders (H2c). More specifically, female study participants were found to place increased value on the awareness and knowledge about how their personal data would be used, as well as on the ability to control the information that they have provided to companies. The former dimension was appropriated from the scale proposed by Malhotra et al. (2004), who coincidentally found no differences across genders (p. 348), when they deployed the exact same question.

This may result from the finding that women are more likely to disclose information about themselves (Fogel & Nehmad, 2009) and thus may also require additional knowledge about how information is going to be used, as well as the certainty that they can edit or delete the shared information. Other researchers too, have found that females are more concerned about privacy than males (Acquisti & Gross, 2006), while Cecere (2015) that women are more concerned about the potential misuse of personal information, which would further explain why the need for control over data is coherent.

As mentioned under RQ1, from a managerial stand point, this knowledge can be of value especially in the ultra-customisable technological realm. Knowing what different users value could allow companies to build a competitive advantage around offering adaptive privacy settings, or to tailor default privacy settings around user expectations and requirements. This is especially true, when the effect of privacy situation awareness or even suspicion of privacy breaches (as discussed under RQ4) is taken into account.

RQ3: How do privacy concerns impact IoT device adoption intentions?

In particular in regards to this question this dissertation offers some interesting findings. First and foremost, it showed that there is a clear negative correlation between privacy concerns and IoT adoption intentions, albeit a small one (H3). In a world where one technological innovation chases the next, it is important to assess how the technology of today and the relationship users have with it, can influence the adoption intentions of tomorrows'

inventions. If companies fail to address consumer concerns today they could be harming the sales of their future products.

At the same time, it should be mentioned that this study could find no correlation between expressed privacy concerns and the number of connected devices the respondent already owned (H3a), which could be regarded as an instance of the much-debated privacy paradox. On the other hand, German respondents reported lower IoT device purchase intentions than Portuguese respondents (H3b), and their higher privacy concerns offer a possible explanation for this.

RQ4: How does a privacy awareness situation influence IoT device adoption intentions?

Finally, the study conducted an experiment that required respondent to browse their app permission. Dependent on whether respondents considered the permissions that they saw as adequate for the function and scope of the app, as well as authorised by them, correlated with a favourable change in terms of connected device purchase likelihood (H5). In this aspect, culture seemed to be an influencing factor as well, as German respondents reported to be more strongly negatively affected in their IoT adoption intentions than Portuguese respondents (H4). It was also shown that negatively perceived privacy realisations, in this case about apps that had permissions to certain smartphone functionalities that seemed inadequate, had a reported negative impact on adoption of future technology that was assumed to expose privacy even further. That respondents were aware of the personal data implications of additional connected devices, was evidenced by the overwhelmingly agreeing responses to the question "The more connected devices I own, the more personal data about me will be available to companies."

On the one hand, this shows once again that the perception of the current privacy situation has an impact on how much users are willing to further engage and expose themselves to other technology. As such, a "best practices" code of conduct regarding privacy policies, as proposed by the US Federal Trade Commission (2015), would not only protect the consumer from data misuse, but also be in the interest of companies, by levelling the playing field with transversal rules and increasing transparency and accountability.

In conclusion, and to pick up the fundamental relationship that was outlined in the Problem statement, this research project found significant evidence that privacy concerns did indeed negatively impact technology adoption. Moreover, it found that privacy concerns were at high levels across different levels of income, different ages, and both genders. Participants

seem weary to interact more with these new devices and privacy concerns seem to have some part in that reluctance. As one interviewee put it: “I don’t want Google to listen to me, while I sing in the shower”.

5.2 Limitations

The results outlined in the previous section were derived using carefully planned statistical analysis. However, the researcher is aware that averaging Likert scales can distort results and as such the statistical reports are to be considered more as a trend analysis rather than concrete prediction models. This is also the case for the linear regression models, as it is important to remember that this technique does not, in and of itself, prove causality, but merely correlation. Without doubt, there are a wide range of dimensions in technology adoption models, and this paper aimed at shedding light at the involvement of privacy concerns in that equation; something that has been disregarded in previous research, as outlined under section 2.4.

As a side note, the researcher recognizes that the question concerning income was too unspecific in regards to its scope, by asking about household rather than personal income, which would have allowed for a more accurate study of the relationship between income and privacy concerns.

The survey completion rate was surprisingly high (over 90%), which may indicate that survey participants did not check their settings as requested. A possible, yet cumbersome, way to address this issue in future research would be to place participants under observation to ensure that the instruction would be executed as intended.

Finally, the relatively small and non-probabilistic sample makes limits the applicability of these findings to the larger population.

5.3 Future research

Furthermore, it would be interesting to study the relationship of trust in technology adoption (e.g. Amazon Echo, Google Home, Apple Home Pod). For instance, Bergström (, (2015) found that trust in other people was the most important factor explaining privacy concerns when using online media. Bhattacherjee (2014) has developed a scale that allows researchers to gauge consumer trust in online firms.

Equally interesting, could be to explore the differences between Android and iOS users, in regards to whether Android users have higher privacy concerns than Apple user, or vice-versa.

5.4 Discussion

The next months will show how the GDPR will affect the privacy perception of European citizens. As of May 2018, users of online services have been receiving a substantial amount of emails from companies that are updating their privacy policies to be compliant with the new regulation. Time will tell how the framework will affect tech behemoths like Google, Facebook, and Amazon. And several other questions are still open: How will the connected home, the place that for so long was the individual's refuge and private area, be changed by the introduction of smart home functionalities? What is free will, when companies like Cambridge Analytica can leverage seemingly mundane data to profile user groups and gradually shift their opinion? What is going to happen to all the data that has already been collected? As one interview participants bluntly put it: "I don't think Google is really using all the data it has on us yet. When it does, it will change the game."

5.5 Final words

The numbing and cynicism with which some people face online privacy in the information age has recently gotten a name: "Privacy fatigue" (Choi, 2018). Choi said that "*repeated consumer data breaches have given people a sense of futility*" and that "*increasing difficulty in managing one's online personal data leads to individuals feeling a loss of control*". It is perhaps a somewhat pessimistic outlook on what privacy could become in the future.

On the other hand, technology has made improved our living conditions in a multitude of ways, and today, many aspects of our lives would be unimaginable without the devices we use on a daily basis. However, at no point in time, does that progress have to come at the cost of privacy. As Ayn Rand, the famous Russian-American novelist once put it:

"Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men."

- in The Fountainhead (1943)

Bibliography

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook BT - Privacy Enhancing Technologies. In G. Danezis & P. Golle (Eds.), Privacy Enhancing Technologies (pp. 36–58). Berlin, Heidelberg: Springer Berlin Heidelberg.

Alessi, S. (2017). Eternal Sunshine: The Right to be Forgotten in the European Union after the 2016 General Data Protection Regulation. Emory International Law Review, 32(1), 145–171. Retrieved from http://widgets.ebscohost.com/prod/customerspecific/ns000290/authentication/index.php?url=http%3A%2F%2Fsearch.ebscohost.com%2Flogin.aspx%3Fdirect%3Dtrue%26AuthType%3Dip%2Ccookie%2Cshib%2Cuid%26db%3Da9h%26AN%3D127057193%26lang%3Dpt-br%26site%3Deds-live%26sc

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. Economics Letters, 117(1), 25–27. https://doi.org/10.1016/J.ECONLET.2012.04.077

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. Computers in Human Behavior, 53, 419–426. https://doi.org/10.1016/j.chb.2015.07.025

Bhattacherjee, A. (2014). Individual Trust in Online Firms: Scale Development and Initial Test. Journal of Management Information Systems, 19(1), 211–241. https://doi.org/10.1080/07421222.2002.11045715

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. Social Psychological and Personality Science, 4(3), 340–347. https://doi.org/10.1177/1948550612455931

Brown, B. (2001). Studying the Internet Experience. Retrieved from https://www.sciencedirect.com/science/refhub/S0167-4048(15)00101-7/sr0075

Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. Technological Forecasting and Social Change, 96, 277–287. https://doi.org/10.1016/j.techfore.2015.01.021

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of Facebook and LinkedIn. Computers in Human Behavior, 69, 207–217. https://doi.org/10.1016/j.chb.2016.12.013

Charlesworth, A. (2009). The ascent of smartphone. Engineering & Technology, 4(3), 32–

33(1). Retrieved from http://digital-library.theiet.org/content/journals/10.1049/et.2009.0306

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. Computers in Human Behavior, 26(5), 987–995. https://doi.org/10.1016/J.CHB.2010.02.012

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51. https://doi.org/10.1016/J.CHB.2017.12.001

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. Journal of Direct Marketing, 9(2), 10–19. https://doi.org/10.1002/dir.4000090204

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. Journal of Marketing Management. https://doi.org/10.1080/0267257X.2016.1247517

Deshmukh, S., & Sonavane, S. S. (2017). Security protocols for Internet of Things: A survey. In 2017 International Conference On Nextgen Electronic Technologies: Silicon to Software, ICNETS2 2017 (pp. 71–74). IEEE. https://doi.org/10.1109/ICNETS2.2017.8067900

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents -measurement validity and a regression model. Behaviour and Information Technology, 23(6), 413–422. https://doi.org/10.1080/01449290410001715723

Egelman, S., & Felt, A. P. (2012). Choice Architecture and Smartphone Privacy : There ' s A Price for That.

Eifrem, E. (2018). GDPR Compliance -- Leveraging the Power of Graph Technology. Credit Control. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=heh&AN=128028326&site=eds-live

Eurobarometer, F. (2004). Data Protection in the European Union. Flash Barometer, (225), 22. Retrieved from http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf

Federal Trade Commission. (2011). Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises | Federal Trade Commission. Retrieved March 16, 2018, from https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

Field, A. (2009). Discovering Statistics using SPSS (3rd ed.). https://doi.org/10.1234/12345678

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. Computers in Human Behavior, 53, 344–353. https://doi.org/10.1016/j.chb.2015.06.048

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior, 25(1), 153–160. https://doi.org/10.1016/J.CHB.2008.08.006

FTC. (2012). United States of America, Plaintiff, v. Google Inc., Defendant, (Cv), 1–9.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703. https://doi.org/10.2501/IJMR-2017-050

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Computers in Human Behavior, 68, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hamilton, B. (2013). Electronic Health Records. Parliamentary Office of Science and Technology.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1589864

Howe, N., Strauss, W., & Matson, R. J. (Robert J. (2000). Millennials rising : the next great generation. Vintage Books. Retrieved from https://books.google.pt/books?id=To_Eu9HCNqIC&redir_esc=y&hl=pt-PT

Ishii, K. (2017). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. AI and Society, pp. 1–25. https://doi.org/10.1007/s00146-017-0758-8

Jahangir, N., & Begum, N. (2008). The role of perceived usefulness , perceived ease of use , security and privacy , and customer attitude to engender customer adaptation in the context of electronic banking. African Journal of Business Management, 2(1), 32–40.

Jin Park, Y. (2008). Privacy regime, culture and user practices in the cyber-marketplace. Info, 10(2), 57–74. https://doi.org/10.1108/14636690810862811

Kennedy, J. (2018). Facebook privacy settings broke German laws, rules Berlin court. Retrieved March 16, 2018, from https://www.siliconrepublic.com/enterprise/privacy-settings-facebook-german-law-vzbv

Knight, A., & Castle, P. (2018). Employers Face a Rise in Biometric Privacy Lawsuits – Workforce Magazine. Retrieved March 16, 2018, from

http://www.workforce.com/2018/02/07/employers-face-rise-biometric-privacy-lawsuits/

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture intercultural dynamics of privacy calculus. Business and Information Systems Engineering, 4(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. Journal of Computer Information Systems, 51(1), 62–71. Retrieved from https://www.scopus.com/record/display.uri?eid=2-s2.0-78649949513&origin=inward&txGid=972cfe78b0ad0185f23346363c8c8fe4

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. Communications of the Association for Information Systems, 28(1), 453–496. Retrieved from https://www.scopus.com/record/display.uri?eid=2-s2.0-81055132875&origin=inward&txGid=191215cb16ea9686f7848bb958474299

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mann, H. B., & Whitney, D. R. (1947). On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. The Annals of Mathematical Statistics, 18(1), 50–60. https://doi.org/10.1214/aoms/1177730491

Margulis, S. T. (2011). Three Theories of Privacy: An Overview. In S. Trepte & L. Reinecke (Eds.), Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web (pp. 9–17). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21521-6_2

Norberg, P., Horne, D., & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Office of the Privacy Commissioner of Canada. (2016). Consent and privacy: A discussion paper exploring enhancements to consent under the Personal Information Protection and Electronic Documents Act. Retrieved from https://www.priv.gc.ca/media/1806/consent_201605_e.pdf

Pavlou, P., & Chai, L. (2002). What Drives Electronic Commerce across Cultures? A Cross-Cultural Empirical Investigation of the Theory of Planned Behavior. Jounal of Electronic Commerce Research, 3(4), 240–253. https://doi.org/10.1.1.144.1549

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. Computers in Human Behavior, 65, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Peppet, S. (2014). Regulating the Internet of things: First steps toward managing discrimination, privacy, security, and consent. Texas Law Review, 93(1), 85–176. Retrieved from http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=3&sid=8de633d7-0f68-4fea-913b-53194578b5cf%40sessionmgr4006

Peterson, R. (1994). A Meta-Analysis of Cronbach's Coefficient Alpha. Journal of Consumer Research, 21, 381–391.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. International Journal of Human Computer Studies, 71(12), 1133–1143. https://doi.org/10.1016/j.ijhcs.2013.09.002

Rand, A. (1943). The Fountainhead.

Reisinger, D. (2012). Facebook sued for $15 billion over alleged privacy infractions - CNET. Retrieved March 16, 2018, from https://www.cnet.com/news/facebook-sued-for-15-billion-over-alleged-privacy-infractions/

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2017). An analysis of economic impact on IoT under GDPR. In 2017 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 879–881). IEEE. https://doi.org/10.1109/ICTC.2017.8190804

Shapiro, S. S., & Wilk, M. B. (1965). An Analysis of Variance Test for Normality (Complete Samples). Biometrika, 52(3/4), 591–611. https://doi.org/10.2307/2333709

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern among Online Consumers. Journal of Public Policy & Marketing, 19(1), 62–73. Retrieved from http://www.jstor.org/stable/30000488

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly, 20(2), 167. https://doi.org/10.2307/249477

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2Nd Generation E-commerce: Privacy Preferences Versus Actual Behavior. In Proceedings of the 3rd ACM Conference on Electronic Commerce (pp. 38–47). New York, NY, USA: ACM. https://doi.org/10.1145/501158.501163

Steinfeld, N. (2016). "i agree to the terms and conditions": (How) do users read privacy

policies online? An eye-tracking experiment. Computers in Human Behavior, 55, 992–1000. https://doi.org/10.1016/j.chb.2015.09.038

Sullivan, L. (2015). When to Use a Nonparametric Test. Boston University School of Public Health, 20–22. Retrieved from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/BS/BS704_Nonparametric/BS704_Nonparametric2.html

Sundar, S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox: do cognitive heuristics hold the key? CHI'13 Extended Abstracts …, 811–816. https://doi.org/10.1145/2468356.2468501

Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. Journal of Computer-Mediated Communication, 19(2), 248–273. https://doi.org/10.1111/jcc4.12052

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425–478. Retrieved from http://www.jstor.org/stable/30036540

Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer acceptance and user of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157–178. https://doi.org/10.1111/j.1365-2729.2006.00163.x

Wakefield, R. (2013). The influence of user affect in online information disclosure. The Journal of Strategic Information Systems, 22(2), 157–174. https://doi.org/10.1016/J.JSIS.2013.01.003

Womack, B. (2013). Facebook Seeks to Clarify How It Uses Member Data for Ads - Bloomberg. Retrieved March 16, 2018, from https://www.bloomberg.com/news/articles/2013-08-29/facebook-seeks-to-clarify-how-it-uses-member-data-for-ads

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior, 28(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42–52. https://doi.org/10.1016/j.dss.2010.11.017

Zafeiropoulou, A. M. (2014). A Paradox of Privacy: Unravelling the Reasoning behind Online Location Sharing, (198).

Annexes

Annex 1 – Qualitative Survey Guide

Personal experience
How much time to you think you spend using Apps in a typical day?
Do you know what app permissions are?
How would you describe the personal data privacy situation today?
What smartphone feature do you feel most protective about? (E.g. Location, Contacts, Images, Camera access, Purchase history, etc.)

Cambridge Analytica
Have you heard of the Cambridge Analytica scandal?
(CA built psychographic profiles, i. e. profiles that reflect a user's opinions, beliefs, values, which in turn were inferred through the user's activity on Facebook such as likes, pages viewed, ads clicked. It used these profiles to then change user behaviours by targeting tailored content to them.) It is currently being discussed if the practices of CA, as well as the involvement of Facebook, were legal. What do you think about this?

IoT
Explanation: "The Internet of Things is the network of devices and sensors that transmit and exchange data, and that will enable new connections between people and people, people and things, and things and things."
What do you think of the following IoT devices?
Smart speakers, Car tracker for insurance purposes, Fitness trackers, Smart Home appliances

How would you evaluate your privacy protection? (e.g. incognito mode browsing, usage of privacy-protecting browser extensions, checking app permissions before downloading new apps)

Experiment
Have the survey participant open her/his phone and check the app permissions overview.
Browse the settings with the participant and develop on the insights.

Android: Settings -> Apps -> Advanced -> App permissions	iOS: Settings -> Privacy

How do you feel after looking at your app permissions?
How do you think privacy protection could be improved?
Have your thoughts on the previously mentioned IoT devices changed?

Annex 2 – Sources of the 11-item privacy concern construct

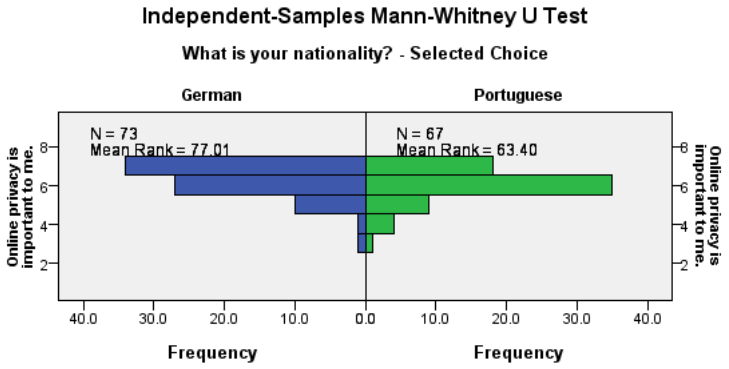
Q11 Online privacy is important to me.	Self-developed
Q12 I often take a look at the required app permissions (access to camera, microphone, storage, location, etc.) before downloading an app.	Self-developed
Q13 I am often unsure about how certain app permissions will be used.	Self-developed
Q14 Companies should never share personal information with other entities unless authorized by me.	Smith 1996: Unauthorized secondary use,
Q15 Companies should never sell the personal information in their computer databases to other companies.	Smith 1996: Unauthorized secondary use,
Q16 I believe that the location of my mobile device is monitored at least part of the time, even when I am not using a navigation app.	Adapted from Xu 2012: Perceived surveillance
Q17 I am concerned that mobile apps may monitor my activities on my mobile device, even when I am not using them.	Adapted from Xu 2012: Perceived surveillance
Q18 I am concerned that mobile apps are collecting too much personal information about me.	Adapted from Smith 1996: Collection
Q19 I feel that as a result of my using mobile apps, companies know more about me than I am comfortable with.	Adapted from Xu 2008: Perceived intrusion
Q20 I believe that because of me using mobile apps, information about me that I consider private is now more readily available to companies than I would want.	Adapted from Xu 2008: Perceived intrusion
Q22 It is very important to me that I am aware and knowledgeable about how my personal information will be used.	Malhotra 2004: Awareness
Q23 Being able to control the personal information I provide to a company is important to me.	Dinev 2004: Control

Annex 3 – Tests of Normality for PC

			Statistic	Std. Error	z-Values	Shapiro-Wilk
Online privacy is important to me.	Portuguese	Mean	5.972	.104		.000
		Skewness	-.987	.285	-3.467	
		Kurtosis	1.286	.563	2.287	
	German	Mean	6.243	.100		.000
		Skewness	-1.167	.279	-4.181	
		Kurtosis	1.655	.552	2.999	
I often take a look at the required app permissions (access to camera, microphone, storage, location, etc.) before downloading an app.	Portuguese	Mean	4.282	.230		.000
		Skewness	-.157	.285	-.550	
		Kurtosis	-1.536	.563	-2.730	
	German	Mean	5.014	.222		.000
		Skewness	-.950	.279	-3.402	
		Kurtosis	-.494	.552	-.896	
I am often unsure about how certain app permissions will be used.	Portuguese	Mean	5.620	.135		.000
		Skewness	-.932	.285	-3.273	
		Kurtosis	.743	.563	1.322	
	German	Mean	5.365	.164		.000
		Skewness	-1.343	.279	-4.811	
		Kurtosis	1.824	.552	3.306	
Companies should never share personal information with other entities unless authorized by me.	Portuguese	Mean	6.549	.122		.000
		Skewness	-2.756	.285	-9.676	
		Kurtosis	7.900	.563	14.045	
	German	Mean	6.595	.081		.000
		Skewness	-1.698	.279	-6.081	
		Kurtosis	2.265	.552	4.106	
Companies should never sell the personal information in their computer databases to other entities.	Portuguese	Mean	6.268	.145		.000
		Skewness	-1.754	.285	-6.158	
		Kurtosis	2.425	.563	4.311	
	German	Mean	6.257	.143		.000
		Skewness	-1.695	.279	-6.071	
		Kurtosis	2.129	.552	3.859	
I believe that the location of my mobile device is monitored at least part of the time, even when I am not using a navigation app.	Portuguese	Mean	5.859	.157		.000
		Skewness	-1.218	.285	-4.276	
		Kurtosis	.710	.563	1.262	
	German	Mean	6.027	.112		.000
		Skewness	-1.090	.279	-3.904	
		Kurtosis	1.254	.552	2.273	
I am concerned that mobile apps may monitor my activities on my mobile device, even when I am not using them.	Portuguese	Mean	5.268	.198		.000
		Skewness	-.689	.285	-2.418	
		Kurtosis	-.702	.563	-1.248	
	German	Mean	5.743	.155		.000
		Skewness	-1.251	.279	-4.482	
		Kurtosis	1.132	.552	2.052	

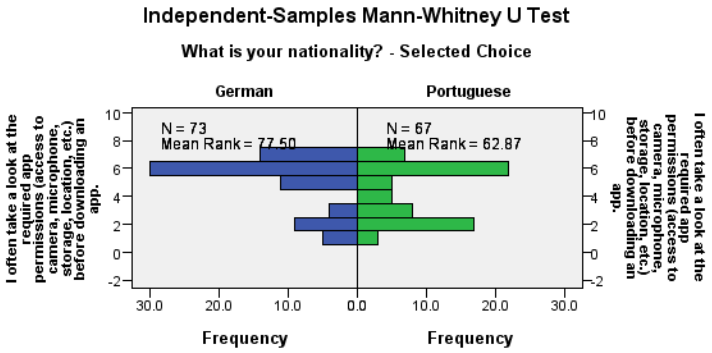
I am concerned that mobile apps are collecting too much personal information about me.	Portuguese	Mean	5.704	.169		.000
		Skewness	-.911	.285	-3.197	
		Kurtosis	-.066	.563	-.117	
	German	Mean	5.649	.181		.000
		Skewness	-1.159	.279	-4.150	
		Kurtosis	.252	.552	.456	
I feel that as a result of my using mobile apps, companies know more about me than I am comfortable with.	Portuguese	Mean	5.352	.190		.000
		Skewness	-.749	.285	-2.630	
		Kurtosis	-.366	.563	-.650	
	German	Mean	5.649	.168		.000
		Skewness	-1.030	.279	-3.689	
		Kurtosis	.292	.552	.529	
I believe that because of me using mobile apps, information about me that I consider private is now more readily available to companies than I would want.	Portuguese	Mean	5.493	.178		.000
		Skewness	-.899	.285	-3.155	
		Kurtosis	-.299	.563	-.532	
	German	Mean	5.797	.157		.000
		Skewness	-1.217	.279	-4.360	
		Kurtosis	.749	.552	1.357	
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	Portuguese	Mean	6.085	.160		.000
		Skewness	-1.844	.285	-6.475	
		Kurtosis	3.280	.563	5.831	
	German	Mean	6.095	.142		.000
		Skewness	-1.727	.279	-6.187	
		Kurtosis	2.917	.552	5.287	
Being able to control the personal information I provide to a company is important to me.	Portuguese	Mean	6.211	.124		.000
		Skewness	-1.691	.285	-5.939	
		Kurtosis	2.917	.563	5.186	
	German	Mean	6.027	.133		.000
		Skewness	-1.287	.279	-4.611	
		Kurtosis	1.130	.552	2.048	

Annex 4 – Mann-Whitney U test for "Online Privacy is important" and Nationality



Total N	140
Mann-Whitney U	2,921.000
Wilcoxon W	5,622.000
Test Statistic	2,921.000
Standard Error	222.236
Standardized Test Statistic	2.140
Asymptotic Sig. (2-sided test)	.032

Annex 5 – Mann-Whitney U test for "Frequency of checking app permissions" and Nationality



Total N	140
Mann-Whitney U	2,956.500
Wilcoxon W	5,657.500
Test Statistic	2,956.500
Standard Error	232.012
Standardized Test Statistic	2.202
Asymptotic Sig. (2-sided test)	.028

Annex 6 – Independent samples t-test of "Frequency of checking app permissions" between Nationalities

Group Statistics

What is your nationality? - Selected Choice		N	Mean	Std. Deviation	Std. Error Mean
Online privacy is important to me.	Portuguese	67	5.97	0.887	0.108
	German	73	6.26	0.850	0.100
I often take a look at the required app permissions (access to camera, microphone, storage, location, etc.) before downloading an app.	Portuguese	67	4.28	1.960	0.239
	German	73	5.04	1.911	0.224

Independent Samples Test

		Levene's Test for Equality of Var		t-test for Equality of Means				
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Online privacy is important to me.	Equal variances assumed	1.134	0.289	-1.975	138	0.050	-0.290	0.147
I often take a look at the required app permissions (access to camera, microphone, storage, location, etc.) before downloading an app.	Equal variances assumed	2.632	0.107	-2.314	138	0.022	-0.758	0.327

Annex 7 – ANOVA & LSD post-hoc on PC between age groups

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Online privacy is important to me.	Between Groups	10.701	3	3.567	5.041	0.002
	Within Groups	96.235	136	0.708		
	Total	106.936	139			

Multiple Comparisons - LSD

Dependent Variable	(I)	(J)	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Online privacy is important to me.	16 - 20	21 - 25	-0.565	0.432	0.192	-1.42	0.29
		26 - 30	-.908*	0.437	**0.040**	-1.77	-0.04
		31 - 35	0.045	0.491	0.926	-0.93	1.02
	21 - 25	16 - 20	0.565	0.432	0.192	-0.29	1.42
		26 - 30	-.342*	0.154	**0.028**	-0.65	-0.04

		31 - 35	.611*	0.271	**0.026**	0.07	1.15
	26 - 30	16 - 20	.908*	0.437	**0.040**	0.04	1.77
		21 - 25	.342*	0.154	**0.028**	0.04	0.65
		31 - 35	.954***	0.281	**0.001**	0.40	1.51
	31 - 35	16 - 20	-0.045	0.491	0.926	-1.02	0.93
		21 - 25	-.611*	0.271	**0.026**	-1.15	-0.07
		26 - 30	-.954***	0.281	**0.001**	-1.51	-0.40

* significant at p < .05, **significant at p < .01, *** significant at p < .001

Annex 8 – ANOVA on AveragePC between age groups

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.987	1	.987	1.075	.302[b]
	Residual	126.667	138	.918		
	Total	127.654	139			

a. Dependent Variable: PCAvg

b. Predictors: (Constant), What is your household's total annual after-tax income? (in Euros)

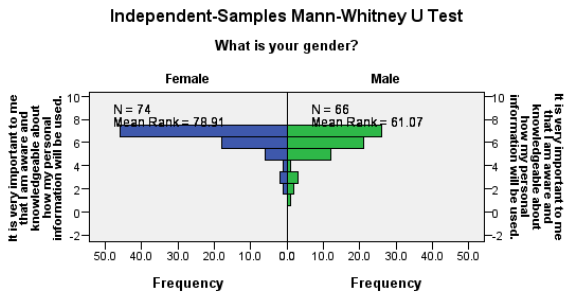
Annex 9 – Independent samples t-test & Mann-Whitney U test on PC between genders

Group Statistics

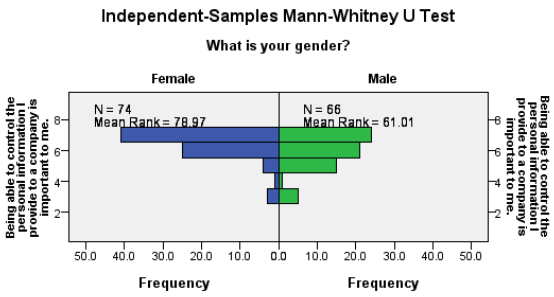
What is your gender?		N	Mean	Std. Deviation	Std. Error Mean
It is very important to me that I am aware and knowledge-able about how my personal information will be used.	Female	74	6.38	1.043	0.121
	Male	66	5.85	1.384	0.170
Being able to control the personal information I provide to a company is important to me.	Female	74	6.35	0.957	0.111
	Male	66	5.88	1.157	0.142

Independent Samples Test

	Levene's Test for Equality of Variances		t-test for Equality of Means				
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
It is very important to me that I am aware and knowledgeable about how my personal information will be used. (Equal variances assumed)	2.752	0.099	2.575	138	0.011	0.530	0.206
Being able to control the personal information I provide to a company is important to me. (Equal variances assumed)	2.305	0.131	2.643	138	0.009	0.473	0.179



Total N	140
Mann-Whitney U	1,819.500
Wilcoxon W	4,030.500
Test Statistic	1,819.500
Standard Error	219.585
Standardized Test Statistic	-2.835
Asymptotic Sig. (2-sided test)	.005



Total N	140
Mann-Whitney U	1,815.500
Wilcoxon W	4,026.500
Test Statistic	1,815.500
Standard Error	222.387
Standardized Test Statistic	-2.817
Asymptotic Sig. (2-sided test)	.005

Annex 10 – Simple Linear Regression between AveragePC (IV) and IoT

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.321[a]	.103	.095	1.418176

a. Predictors: (Constant), PCAvg

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	26.964	1	26.964	13.407	.000[b]
	Residual	235.313	117	2.011		
	Total	262.277	118			

a. Dependent Variable: WTBAvg

b. Predictors: (Constant), PCAvg

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	5.991	.777		7.712	.000
	PCAvg	-.488	.133	-.321	-3.662	.000

a. Dependent Variable: WTBAvg

Annex 11 – Linear Regression Model Summary of AveragePC (IV) and IoT device ownership (DV)

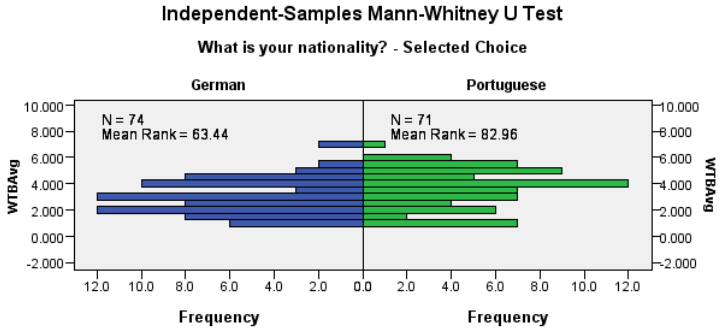
Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.011[a]	0.000	-0.007	0.854	0.000	0.015	1	138	0.902

a. Predictors: (Constant), PCAvg

b. Dependent Variable: Sum IoT

Annex 12 – Mann-Whitney U test & independent sample t-test on IoT adoption intentions between Nationalities



Total N	145
Mann-Whitney U	1,919.500
Wilcoxon W	4,694.500
Test Statistic	1,919.500
Standard Error	252.295
Standardized Test Statistic	-2.804
Asymptotic Sig. (2-sided test)	.005

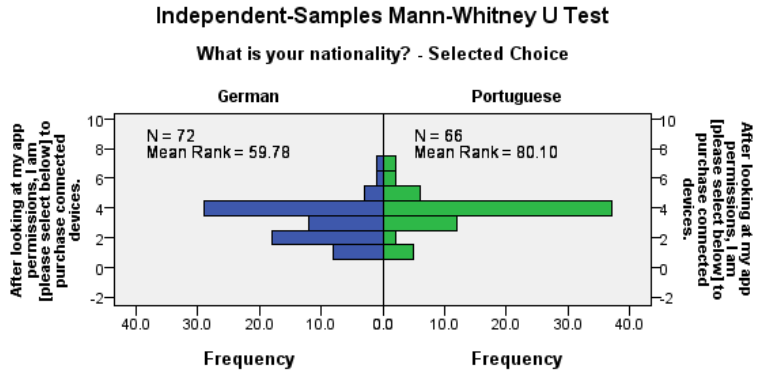
Group Statistics

	What is your nationality? - Selected Choice	N	Mean	Std. Deviation	Std. Error Mean
WTBAvg	Portuguese	71	3.60915	1.518771	.180245
	German	74	2.92568	1.376621	.160029

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means				
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
WTB Avg	Equal variances assumed	0.865	0.354	2.841	143	0.005	0.683479	0.240543

Annex 13 – Mann-Whitney U test & independent samples t-test on IoT adoption intention change between Nationalities



Total N	138
Mann-Whitney U	1,676.500
Wilcoxon W	4,304.500
Test Statistic	1,676.500
Standard Error	220.240
Standardized Test Statistic	-3.176
Asymptotic Sig. (2-sided test)	.001

Group Statistics

	What is your nationality? - Selected Choice	N	Mean	Std. Deviation	Std. Error Mean
After looking at my app permissions, I am [please select below] to purchase connected devices.	Portuguese	66	3.77	1.200	.148
	German	72	3.11	1.273	.150

Independent Samples Test

	Levene's Test for Equality of Variances		t-test for Equality of Means				
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
After looking at my app permissions, I am [please select below] to purchase connected devices. (Equal variances assumed)	3.557	0.061	3.134	136	0.002	0.662	0.211

Annex 14 – Pearson Correlations & Multiple Regression Analysis of the three app permission check reaction variables to the DV "Change in IoT adoption likelihood" (Q36)

Correlations

		After looking at my app permissions, I am [please select below] to purchase connected devices.	I was surprised by some of the permissions.	I gave all the permissions willingly and consciously.	All permissions seemed adequate for the purpose of the respective apps.
Pearson Correlation	After looking at my app permissions, I am [please select below] to purchase connected devices.	1.000	0.007	0.348	0.373
	I was surprised by some of the permissions.	0.007	1.000	-0.364	-0.350
	I gave all the permissions willingly and consciously.	0.348	-0.364	1.000	0.500
	All permissions seemed adequate for the purpose of the respective apps.	0.373	-0.350	0.500	1.000
Sig. (1-tailed)	After looking at my app permissions, I am [please select below] to purchase connected devices.		0.466	0.000	0.000
	I was surprised by some of the permissions.	0.466		0.000	0.000
	I gave all the permissions willingly and consciously.	0.000	0.000		0.000
	All permissions seemed adequate for the purpose of the respective apps.	0.000	0.000	0.000	

Model Summary[d]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.373[a]	0.139	0.133	1.190	0.139	22.002	1	136	0.000
2	.417[b]	0.174	0.162	1.170	0.035	5.665	1	135	0.019
3	.461[c]	0.212	0.195	1.147	0.038	6.534	1	134	0.012

a. Predictors: (Constant), Q35

b. Predictors: (Constant), Q35, Q34

c. Predictors: (Constant), Q35, Q34, Q33

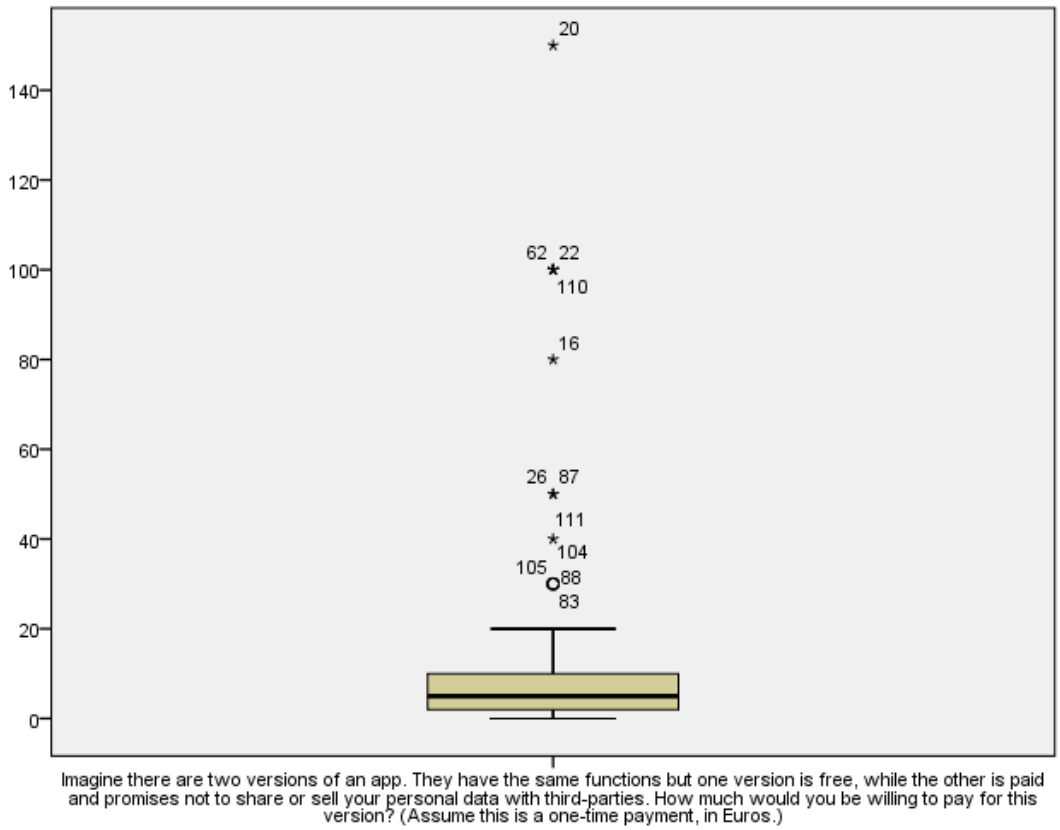
d. Dependent Variable: Q36

Coefficients[a]

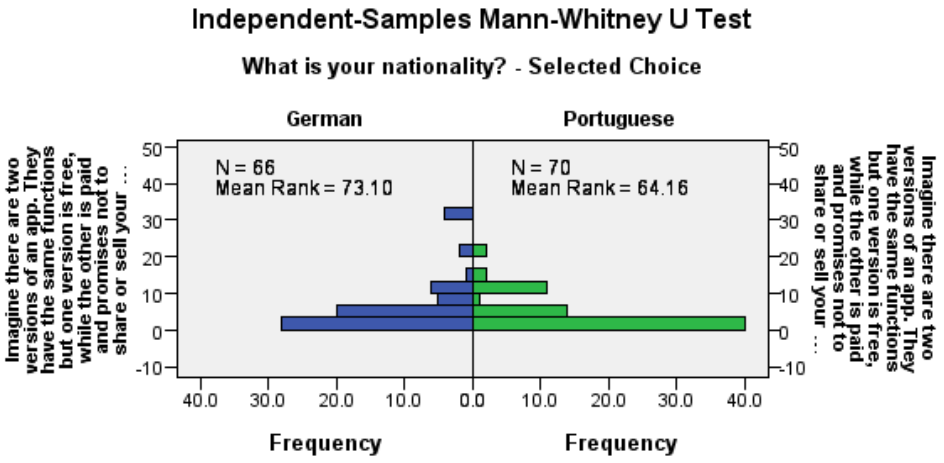
Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	2.379	0.245		9.692	0.000
	All permissions seemed adequate for the purpose of the respective apps.	0.272	0.058	0.373	4.691	0.000
2	(Constant)	2.030	0.282		7.192	0.000
	All permissions seemed adequate for the purpose of the respective apps.	0.194	0.066	0.266	2.943	0.004
	I gave all the permissions willingly and consciously.	0.160	0.067	0.215	2.380	0.019
3	(Constant)	1.129	0.448		2.518	0.013
	All permissions seemed adequate for the purpose of the respective apps.	0.229	0.066	0.314	3.469	0.001
	I gave all the permissions willingly and consciously.	0.200	0.068	0.269	2.958	0.004
	I was surprised by some of the permissions.	0.142	0.055	0.215	2.556	0.012

a. Dependent Variable: After looking at my app permissions, I am [please select below] to purchase connected devices.

Annex 15 – Boxplot of Willingness to Pay with Outlier identification (Cut-off = 31€)



Annex 16 – Mann-Whitney U test & independent samples t-test on IoT adoption



Total N	136
Mann-Whitney U	2,613.500
Wilcoxon W	4,824.500
Test Statistic	2,613.500
Standard Error	227.257
Standardized Test Statistic	1.335
Asymptotic Sig. (2-sided test)	.182

Group Statistics

What is your nationality? - Selected Choice		N	Mean	Std. Deviation	Std. Error Mean
Imagine there are two versions of an app. They have the same functions but one version is free, while the other is paid and promises not to share or sell your personal data with third-parties. How much would you be willing to pay for this version? (Assume this is a one-time payment, in Euros.)	PT	70	4.44	4.672	0.558
	DE	66	6.18	7.418	0.913

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means				
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
(See previous table)	Equal variances assumed	3.332	0.070	-1.652	134	0.101	-1.746	1.057

Annex 17 – Online Survey

Start of Block: Block 1

Q1
A small step for mankind, a giant leap for me.

In order to complete my Master's degree at Católica Lisbon School of Business and Economics I am studying privacy concerns in connection with the Internet of Things, and the following survey will help me with that.

It will take about 7 minutes to complete, there are no right or wrong answers, and your answers are strictly anonymous and confidential. It includes a little experiment towards the end, so please don't forget to come back to the survey after that.

Thank you for your time!

Q2 What is your gender?

Female (1) Male (2)

Q3 Which group below includes your age?

16 - 20 (1) 21 - 25 (2) 26 - 30 (3) 31 - 35 (4) 36 - 40 (5) 41 - 45 (6) 46 - 50 (7) 51+ (8)

Q4 What is the highest degree you have completed or are currently enrolled in?

High school (1) Bachelor degree (2) Master degree (3) MBA (4) PhD (5)

Q5 What is your nationality?

Portuguese (1) German (2) Other (please specify): (3)

Q6 What is your household's total annual after-tax income? (in Euros)

Less than €10,000 (11) €10,000 - €19,999 (12) €20,000 - €29,999 (13) €30,000 - €39,999 (14) €40,000 - €49,999 (15) €50,000 - €59,999 (16) €60,000 - €69,999 (17) €70,000 - €79,999 (18) €80,000 - €89,999 (19) €90,000 - €99,999 (20) More than €100,000 (22)

End of Block: Block 1

Start of Block: Block 2

Q7 For how long have you owned a smartphone?

I don't own a smartphone (6) 1 year (1) 2 years (2) 3 years (3) 4 years (4) 5 or more years (5)

Q8 Approximately how many apps on your smartphone do you use on a daily basis?

None (1) 1-2 (2) 3-4 (3) 5-6 (4) 7-8 (5) 8+ (6)

Q9 Do you own any of the following connected devices? (Multiple Choice)

Fitness tracker (1) Smart watch (2) Smart speaker (3) Smart TV (4) Smart fridge (5) Smart home security system (6) Smart lighting system (7) Other (please specify): (8)

End of Block: Block 2

Start of Block: Block 2

TEXT: This section concerns your attitude towards online privacy. Online privacy involves the ability to control what information you reveal about yourself online, and who could access that information.
[Note: The following questions all featured the following responses:

Strongly disagree (1), Disagree (2), Somewhat disagree (3), Neither agree nor disagree (4), Somewhat agree (5), Agree (6), Strongly agree (7)]

Q11 Online privacy is important to me.

Q12 I often take a look at the required app permissions (access to camera, microphone, storage, location, etc.) before downloading an app.

Q13 I am often unsure about how certain app permissions will be used.

Q14 Companies should never share personal information with other entities unless authorized by me.

Q15 Companies should never sell the personal information in their computer databases to other entities.

Q16 I believe that the location of my mobile device is monitored at least part of the time, even when I am not using a navigation app.

Q17 I am concerned that mobile apps may monitor my activities on my mobile device, even when I am not using them.

Q18 I am concerned that mobile apps are collecting too much personal information about me.

Q19 I feel that as a result of my using mobile apps, companies know more about me than I am comfortable with.

Q20 I believe that because of me using mobile apps, information about me that I consider private is now more readily available to companies than I would want.

Q21 I should get paid for the information I am sharing.

Q22 It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Q23 Being able to control the personal information I provide to a company is important to me.

Q24 The more Internet-connected devices I own, the more personal data about me will be available to companies.

Q25 Imagine there are two versions of an app. They have the same functions but one version is free, while the other is paid and promises not to share or sell your personal data with third-parties. How much would you be willing to pay for this version? (Assume this is a one-time payment, in Euros.)

_____

End of Block: Block 2

Start of Block: Block 5

TEXT: In the following sections I would like to know more about your purchase intentions for certain connected devices.
[Note: The following questions all featured the following responses:

Strongly disagree (1), Disagree (2), Somewhat disagree (3), Neither agree nor disagree (4), Somewhat agree (5), Agree (6), Strongly agree (7)]

Q27 I intend to buy a smart speaker within the next three years. [Smart speakers, like the Amazon Echo or Google Home, are voice controlled devices with an integrated virtual assistant that can perform a range of tasks, like playing music, checking the weather, or controlling other smart home devices.]

Q28 I intend to buy a fitness tracker within the next three years. [Fitness trackers record data like distance run, calories expended, heartbeat, and sleep quality, among others.]

Q29 I intend to buy a smart home appliance within the next three years. [Smart home appliances, like smart temperature regulators, smart fridges, or smart ovens, are appliances that can be controlled remotely via smartphone.]

Q30 I intend to equip my car with a telematics sensor within the next three years. [Telematics sensors register car speed, direction, and location, and are used by insurance companies to offer adaptive prices to their customers, based on driving style.] (If you don't own a car, please assume that you do.)

Q31 This is an attention check question. Please select Somewhat disagree from the options below.

End of Block: Block 5

Start of Block: Block 3

TEXT: Now, a short experiment! I would like you check the app permissions on your phone. Please, take a minute to scroll through the microphone, location, camera, and photos/storage categories. You can find them here:
Android (6.0 and later): Settings > Apps > Advanced > App permissions
iOS (iPhone 5S and later): Settings > Privacy
Most important of all, please come back to the survey afterwards. You only have 4 questions to go. Thank you!

End of Block: Block 3

Start of Block: Block 4

Q33 I was surprised by some of the permissions.

I couldn't find the app permissions page. (8) Strongly disagree (1) Disagree (2) Somewhat disagree (3) Neither agree nor disagree (4) Somewhat agree (5) Agree (6) Strongly agree (7)

Q34 I gave all the permissions willingly and consciously.

Strongly disagree (1), Disagree (2), Somewhat disagree (3), Neither agree nor disagree (4), Somewhat agree (5), Agree (6), Strongly agree (7)]

Q35 All permissions seemed adequate for the purpose of the respective apps.

[see Q34]

Q36 After looking at my app permissions, and assuming that other connected devices will collect personal data as well, I am [please select below] to purchase connected devices.

Much less likely (1) Moderately less likely (2) Slightly less likely (3) About the same 4) Slightly more likely (5) Moderately more likely (6) Much more likely (7)

End of Block: Block 4
