Computers in Human Behavior 75 (2017) 811–825

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study

Dimitris Potoglou [a, *], Fay Dunkerley [b], Sunil Patil [b], Neil Robinson [b]

[a] School of Geography and Planning, Cardiff University, CF10 3WA, Cardiff, UK
[b] RAND Europe, Westbrook Centre, Cambridge, CF4 1YG, UK

ARTICLE INFO

Article history:
Received 30 January 2017
Received in revised form
4 June 2017
Accepted 6 June 2017
Available online 20 June 2017

Keywords:
Privacy
Surveillance
Data access
Data sharing
Data storage
Privacy enhancing technologies

ABSTRACT

This paper examines public preferences regarding privacy implications of internet surveillance. The study was based on a pan-European survey and included a stated preference discrete choice experiment (SPDCE) involving the choice of an Internet Service Provider (ISP) offering varying levels of storage, access and sharing of internet activity, continuous surveillance and privacy enhancing technologies. The survey obtained 16,463 individual responses across the European Union's 27 member-states[1]. Respondents expressed highest levels of concern about: Internet facilitated crime, namely using the internet to share and publish child pornography (68.2%); individual data protection and security threats – i.e., personal information not being handled in a legitimate way (62%); computer viruses (61.4%) and finally the theft of financial data or identity (61.4%). Such levels of concern affect trust in the Internet: 27.7% of respondents trusted websites for information exchange and a similar figure, 30.7% reported they trust websites for business transactions. Given this context, following our analysis of preferences, on average, respondents were more likely to choose an ISP that would not store any internet activity, would retain any data for up to 1 month and would not share data with anyone else. Interestingly, respondents did recognise the potential benefit for continuous state-surveillance (by the police), but only under an appropriate accountable legal basis. Also, respondents were in favour of an array of privacy enhancing technologies that would enhance their privacy when using the Internet. Finally, the analysis shows that in some cases, significant differences in preferences across countries and socio-economic characteristics suggest that individual privacy-preferences do vary across cultural/national settings, age, gender and education level.

1. Introduction

The Internet has become an increasingly necessary and important facet of everyday life. In 2015, 83% of households in the European Union's 28 Member States (EU28) had internet access, an increase of 28 percentage points compared to 2007 figures (Eurostat, 2016a). As of June 2016, there were 412 million Internet users in the EU28 who used the Internet every day (Internet World Stats, 2016) and according to e-commerce statistics, two thirds of these users made online purchases of goods or services (Eurostat, 2016b). However, EU figures show that only 22% of Europeans had full trust in e-commerce sites.

Criminals and terrorists have also taken an interest in the Internet for nefarious purposes. Cyber criminals seek to exploit the increasing economic importance of use of the Internet through perpetrating fraud, identity theft and other forms of economic crime against individuals and businesses. According to Symantec's Internet Security Threat Report, the total cost of cybercrime in 2016 was estimated at US$575 billion (ISTR, 2016). Terrorists have also been quick to exploit the potential of the Internet. Groups such as Islamic State/Daesh and others use the Internet to recruit, radicalise and incite terrorism, post videos of atrocities online and employ encrypted communications platforms like Telegram (Inayatullah & Milojević, 2015).

Latterly, nation-states are developing increasingly sophisticated capabilities in cyberspace to enhance traditional espionage, further national security objectives or maintain the resilience of critical infrastructure (e.g Stoddart, 2016). Governments also employ these

* Corresponding author. School of Geography and Planning, Cardiff University, Glamorgan Building, King Edward VII Avenue, Cardiff, CF10 3WA, Wales, UK.
E-mail address: potogloud@cardiff.ac.uk (D. Potoglou).

[1] The study was commissioned prior to Croatia becoming member of the European Union.

http://dx.doi.org/10.1016/j.chb.2017.06.007

surveillance capabilities to identify, disrupt or mitigate the socio-economic impact of the misuse of the Internet by criminals and terrorists. This surveillance has the potential to encroach upon the privacy and convenience of Internet users. For example the UK's 'Draft Investigatory Powers Bill' (Home Office, 2015) involves having the details of users' browsing history stored so they are easily accessible to police and other security forces in the event of a state of emergency being declared. The monitoring and interception of Internet communications is regarded by law enforcement and security authorities as an essential tool in addressing these threats. As a case in point, in investigating the recent attacks in Brussels and Paris, the authorities were reportedly hampered by the lack of surveillance capabilities, a framework for sharing information and investigatory powers (Politico, 2015; The Guardian, 2016). While it is impossible to say whether these capabilities would have necessarily prevented such attacks, their absence is often lamented by security authorities. With these kind of threats and the constantly evolving technological pace of change, law enforcement and intelligence agencies are increasingly concerned about 'going dark' – i.e., losing their ability to lawfully intercept and monitor Internet based communications (Berkman, 2016). Ultimately, the authorities charged with security have to reconcile these two competing interests (Waldron, 2003).

This process is not necessarily visible to the end-user of the security infrastructure (i.e., everyday citizens) since generally the competing drivers of security and privacy that must be reconciled are either implicit or difficult for the layman to fully understand. In democratic societies, citizens are only infrequently able to exercise their choice in how this challenge is solved through voting in different political parties. The complexity of the exercise of choice between different security mechanisms is also due in part to the nature of security as a public good and the debate about whether is possible to meaningfully exercise choice between different providers of national security.

In the face of the security rationale for surveillance offered by governments, there is evidence to suggest that users are becoming interested (albeit over the short term) in implementing privacy controls to redress the balance (Preibusch, 2015). One way users may exercise control over their personal information is through tools that can enhance or improve their online privacy, known as Privacy Enhancing Technologies (PETs). PETs can be defined as technologies that aim to preserve the privacy of individuals or groups of individuals (Heurix, Zimmerman, Neubauer, & Fenz, 2015). Examples of PETs include technology that can anonymise internet usage (e.g. The Onion Router or ToR), protect communications through encryption or anonymise data.

Nonetheless, the employment of quantitative methodologies to better investigate, understand and measure citizens' preferences for public goods like security should not be discounted. Such approaches have been successfully employed across a number of comparable subject areas including health (Hall, Viney, Haas, & Louviere, 2004) social care (Netten et al., 2012) and value of travel-time savings studies (Hess, Daly, Dekker, Cabral, & Batley, 2017).

Previous studies aimed at investigating individual preferences for privacy, internet surveillance and disclosure of personal information offer findings that are difficult to generalise or compare with other studies. These differences may be due to limitations in study design; most studies, for example, employ convenience-based samples such as university students (Hui, Teo, & Lee, 2007), capture behavioural intentions to disclose personal information via a unidimensional trade-off with a monetary payment (Acquisti, John, & Loewenstein, 2013) or its association with self-reported scales of privacy concern (Pavlou, 2011). Previous reviews of the literature have shown that the majority of studies on privacy of personal information come from the United States (Bélanger & Crossler, 2011 cited in; Pavlou, 2011) thus providing little evidence about individuals' preferences across other countries. Most importantly, the majority of studies refer to individual privacy and personal-information disclosure intentions in the context of e-commerce (Potoglou, Palacios, & Feijóo, 2015) and not state-surveillance practices and individuals' preferences for privacy enhancing technologies.

This paper addresses several of these research gaps. To address the issues of convenience and the US-focused nature of samples in previous studies, this study reports findings using a broadly representative sample of individuals from across the European Union's 27 Member States (EU27) according to age, gender and geographical region. Respondent preferences were captured via a Stated Preference Discrete Choice Experiment (SPDCE) experiment, a survey-based methodology. The SPDCE is the most widely used preference elicitation technique for determining the factors driving individual choices (Hensher, Rose, & Greene, 2005) and has been widely employed in a number of subject areas including health and healthcare (Viney, Lancsar, & Louviere, 2002), environmental valuation (Bateman et al., 2002), transport (Hess et al., 2017), and marketing (Allenby, Shively, Yang, & Garratt, 2004). The SPDCE in this study involved hypothetical scenarios concerning the choice of an Internet Service Provider (ISP). The ISP choice context was also different relative to numerous studies employing e-commerce scenarios, for example, to examine individual privacy and security preferences when using the Internet. Finally, the SPDCE approach allowed the analysis of preferences beyond the traditional model of examining responses to a single dimension of privacy against monetary exchange. In particular, this study offers insights about an array of relevant privacy-related dimensions including the level of storage of internet-users' activity, retention of this information and sharing as well as privacy enhancing technologies.

2. Theoretical background

Information privacy has been studied under different definitions, attributes, contexts and themes including through the prism of law, management, economics, psychology marketing and information systems (Pavlou, 2011). In the context of online communications and e-commerce, online privacy is often seen as being inextricably linked to identity and the policies related to the use of user data (Angriawan & Thakur, 2008). As such, aspects regarding how individuals perceive privacy and control information about themselves are often an important theme in the debate. In contemporary life, there are increasing pressures on this control (Thierer, 2013). These can be imposed externally by governments for security reasons as indicated above or businesses for economic benefit. They may also be internally driven; for example, the desire to construct and express identity (Boyd & Heer, 2006).

Empirical research efforts concerning individual-level online privacy can be consolidated into the Antecedents, Privacy Concerns, Outcomes (APCO) model proposed by Smith, Dinev, and Xu (2011). As shown in Fig. 1, individual privacy-concerns within the APCO model are determined via antecedents such as age, gender, social awareness, personal experience and trust (e.g. Bergström, 2015; Dinev & Hart, 2006; Smith, Milberg, & Burke, 1996). Privacy concerns are routinely captured via psychometric scales including the Concern for Information Privacy (Smith et al., 1996) and Internet Users' Information Privacy Concerns (IUIPC, Malhotra, Kim, & Agarwal, 2004).

Another component in the APCO model links privacy concerns with behavioural intentions such as individuals' willingness to disclose personal information. Behavioural intentions are subject to the assumption that individuals' reactions (or stated intentions) are

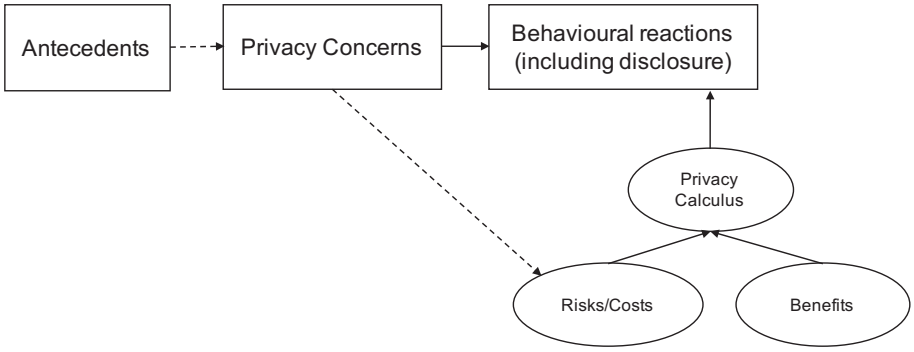


Fig. 1. The APCO Macro model (Smith et al., 2011).

guided by a Privacy Calculus (Dinev & Hart, 2006). The latter reflects a decision-making process – a calculus or trade-off – under which individuals weigh the risks/costs and benefits prior to behavioural reactions or stated intentions. Examples of empirical research include the study of privacy concerns and risk and benefit trade-offs on consumers' intention to engage in e-commerce transactions (Dinev & Hart, 2006), the selection of online retailers (Potoglou, Patil, Gijón, Palacios, & Feijóo, 2013; Tsai, Egelman, Cranor, & Acquisti, 2010) and individuals' willingness to disclose information to retailers under certain privacy conditions or scenarios (Hui et al., 2007). Some empirical studies have attempted to operationalise the APCO model through the analysis of data capturing antecedents, privacy concerns and behavioural reactions (e.g. Chen, Beaudoin, & Hong, 2017; Heirman, Walrave, Ponnet, & Van Gool, 2013; Potoglou et al., 2015).

The principal aim of this study falls within the Privacy Calculus in the APCO model as it seeks to better understand individual preferences (reactions) relative to variations of features regarding privacy-related risks/costs and benefits across the EU27. The overarching theory that guides this investigation is Social Exchange Theory, which postulates that individuals (rationally) minimise costs and maximise benefits (or rewards) through the comparison of alternatives when considering decisions involving social transactions in both economic and social outcomes (Bergström, 2015; Homans, 1958). Social Exchange Theory incorporates assumptions also found in rational choice theory. The SPDCE designed in this project helps operationalise Social Exchange Theory by employing methods and approaches based on Random Utility Theory (McFadden, 1974) - as explained in Sections 3.4 and 4.2. The employed approach goes beyond opinion polls or traditional psychometric scales and helps to provide a more nuanced insight into the individual preferences by allowing several dimensions of risks and benefits to be controlled for simultaneously.

Given the context dependent nature of privacy (Nissembaum, 2010), this study placed online privacy in the context of individuals choosing an Internet Service Provider (ISP). The concept of subscribing to an ISP is similar to subscribing to a utility (e.g. choosing between two energy providers), which meant respondents had a better likelihood of relating to the scenario. It also rendered the explanation of relevant security and privacy aspects more accessible. The specific research questions this study seeks to address are as follows:

- Would respondents accept ISP storing their routine Internet use such as email, browsing, location and personal contacts?
- To what extent respondents would accept an ISP storing their Internet activity for a period longer than one (1) month?
- Would respondents accept an ISP sharing their Internet activity with authorities at the national, European or Worldwide levels?
- Under which circumstances they would accept an ISP allowing continuous surveillance of their Internet activity by authorities?
- Do respondents place any importance (value) on Privacy Enhancing Technologies and Services that may be offered by ISPs?
- Finally, do preferences vary across respondents and are there any significant variations in preferences across members of the EU27?

3. Methods

3.1. Study participants

The data in this study come from a pan-European survey on the public perception of privacy and security conducted as part of the PACT project (Public perception of Security and privacy: Assessing knowledge, Collecting evidence, Translating research into action), a 3-year research project funded by European Union's 7th Framework Programme, a research and technological development funding programme for 2007–2013 in Europe.

The primary aim of the project was to assess Europeans' preferences between security and privacy. The project focused on three easily recognised real-life situations that collectively: covered different types of security threats, involved different actors and policy sectors and captured a variety of themes relating to privacy and surveillance including dignity, liberty, state security, personal-physical security and security of personal information (Solove, 2010). These situations included: travel by metro/rail (Patil, Patruni, Potoglou, & Robinson, 2016), handling and use of health-related personal data (Patil, Lu, Saunders, Potoglou, & Robinson, 2016) and Internet-user activity and related data. This latter scenario is the focus of this paper.

The target sample in this study was adults aged 18 years or older across the EU27 as the study was conceived and designed prior to Croatia joining the European Union (see, Section 3.5 for details). A summary of the sample characteristics in this study is shown in Table 1.

3.2. Development of the survey questionnaire

The development of the survey questionnaire and the SPDCE were informed by preliminary discussions amongst the consortium members, stakeholder consultations, expert interviews and focus groups conducted in the UK, Lithuania and Greece (Patil, Robinson, & Potoglou, 2012; Potoglou, Robinson, Hellgren, Kobzar, & Patil, 2014a). The questionnaire comprised three sections: (1) demographic questions, (2) attitudes towards privacy concerns when using the Internet, and (3) the SPDCE scenarios involving

Table 1
Sample characteristics (N = 16,463).

	Number of respondents (%)	Country	Survey mode	Language(s)	Number of respondents (%)
Gender		Austria	Online	German	707 (4.3)
Males	8121 (49.3)	Belgium	Online	French, Dutch	769 (4.7)
Females	8342 (50.7)	Bulgaria	Face-to-face	Bulgarian	442 (2.7)
Age (years)		Cyprus	Face-to-face	Greek	455 (2.8)
18 to 24	2190 (13.3)	Czech Republic	Face-to-face	Czech	594 (3.6)
25 to 34	3347 (20.3)	Denmark	Online	Danish	694 (4.2)
35 to 44	3366 (20.5)	Estonia	Online	Estonian	744 (4.5)
45 to 54	2948 (17.9)	Finland	Online	Finnish	707 (4.3)
55–64	2437 (14.8)	France	Online	France	735 (4.5)
65 +	2175 (13.2)	Germany	Mixed	German	647 (3.9)
Household income		Greece	Face-to-face	Greek	435 (2.6)
< €500	1834 (11.1)	Hungary	Face-to-face	Hungarian	530 (3.2)
€500 up to €1500	5079 (30.9)	Ireland	Online	English	692 (4.2)
€1500 up to €3000	4220 (25.6)	Italy	Mixed	Italian	646 (3.9)
€3000 up to €9000	2828 (17.2)	Latvia	Face-to-face	Latvian, Russian	561 (3.4)
More than €9000	168 (1.0)	Lithuania	Face-to-face	Lithuanian	634 (3.9)
Missing/Not stated	2334 (14.2)	Luxembourg	Online	French, German, Luxembourgish	542 (3.3)
Survey Approach		Malta	Face-to-face	Maltese	397 (2.4)
Online	8475 (51)	Netherlands	Online	Dutch	761 (4.6)
Offline	7988 (49)	Poland	Face-to-face	Polish	554 (3.4)
Weekly personal Internet-use		Portugal	Face-to-face	Portuguese	430 (2.6)
20 h or more	4304 (26.1)	Romania	Face-to-face	Romanian	402 (2.4)
Up to 20 h	2375 (72.1)	Slovakia	Face-to-face	Slovak	606 (3.7)
No access	285 (1.7)	Slovenia	Face-to-face	Slovenian	655 (4.0)
Used the internet before		Spain	Online	Spanish	723 (4.4)
'Yes, by myself'	15,935 (96.8)	Sweden	Online	Swedish	688 (4.2)
'Yes, with someone's help'	528 (3.2)	United Kingdom	Online	English	713 (4.3)

hypothetical choices of ISP. Testing the internal validity of the questionnaire was carried out through cognitive interviews in the UK, Hungary and Portugal (Patil, Robinson, Potoglou, Burge, & Hellgren, 2013b). The primary aim of the cognitive interviews was to ensure that respondents understood the SPDCE scenarios. Pilot surveys were additionally conducted in Denmark, Italy and Romania (Patil, Hui, Patruni, Potoglou, & Robinson, 2012). The survey questionnaire was translated into 24 languages to include all the official language(s) in each of the EU27 member states.

3.3. Attitudes towards data protection and individual security concerns

As part of the survey, respondents' concerns regarding data protection, national and individual security, internet surveillance and trust in websites were captured through 5 sets of psychometric scales. The statements shown in Table 2 corresponded to previously validated scales (Buchanan, Paine, Joinson, & Reips, 2007; Dinev & Hart, 2006) with the exception of the scales in 'Concern for Internet Surveillance and Trust in Websites', which were developed as part of this study (Patil et al., 2013b). Survey participants also provided information about their age, gender and household income.

3.4. Stated-preference scenarios of internet service provider

The design of the SPDCE scenarios was informed by the Privacy Calculus concept (Dinev & Hart, 2006; Smith et al., 2011), a theoretical framework that embodies the assumption that consumers' behavioural reactions or stated intentions – including their willingness to disclose information – occur following a calculus between risks/costs and benefits as a consequence of that reaction. Thus, the SPDCE approach helped to examine a range of hypotheses covering individuals' preferences relating to security, surveillance and privacy. The hypotheses also covered broader societal and socio-economic issues that can affect these preferences (Patil, Fuchs, Potoglou, & Robinson, 2013a).

Each respondent was presented with five different choice cards (choice scenarios) in the format shown in Fig. 2. To introduce the choice experiment, respondents were asked to imagine that they were about to purchase (or renew) an Internet connection with an Internet Service Provider. Each card included two ISP options with different privacy-related configurations and respondents were asked to choose the one they would prefer the most. The opt-out option allowed respondents not to choose any of the ISP on offer thus allowing them to decline choosing an undesired alternative.

In line with Privacy Calculus concept, potential risks to privacy include collection and type of information, handling errors, unauthorised secondary use (e.g. third party access and sharing) and improper access to personal information. To capture the above elements in the context of Internet use in the SPDCE, we introduced relevant attributes referring to: the type of and retention-time of users' Internet-activity that would be stored, the breadth of access to that information – e.g. whether information remained with the ISP, was shared with authorities in the country of residence or across Europe and finally, whether potentially continuous surveillance was authorised or unauthorised (see, Fig. 2 and Table 3). The data-storage attributes described above relate to individuals' willingness to render information, which are commonly seen in the context of social networking sites and e-commerce, where incentives for disclosure may also be implied or offered (Potoglou et al., 2015).

An additional attribute, 'how long information is stored', captured preferences for Internet-activity data retention by the ISP. While data retention is a well-developed topic in the area of law enforcement (Crump, 2003), citizens' reactions and preferences are less well-known, especially in the context of Internet surveillance. This experiment presents an opportunity to test respondents' preferences regarding data retention. As shown in Table 3, the possibilities for data retention by an Internet Service Provider in the experiment ranged from 1 month up to 5 years.

Authorised or unauthorised surveillance and storage of users' Internet-use information by an ISP pertains directly to information privacy. Users may seemingly balance the convenience of some data being stored against the possibility of misuse or

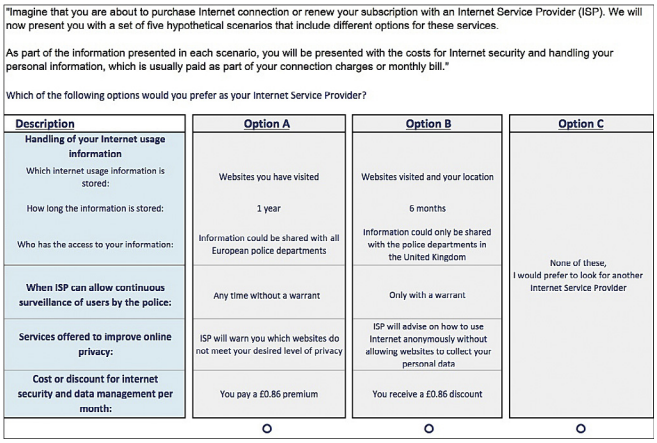
Table 2
Concerns on data protection, security, surveillance and trust.

	Observations (Total)	% Concerned or very concerned
(Internet) Data protection concern (source: Dinev & Hart, 2006)		
Your information such as age, gender, location shared with websites or companies which you don't use	16287	52.5
Your internet usage information (including details of items you searched or purchased) shared with websites or companies which you don't use (third-party)	16267	54.8
Your personal information is not handled in a legitimate way (for example, the personal information you provided when opening an account with a website is not deleted when you closed the account).	16208	62.0
Concern for internet surveillance (source: Patil et al., 2013b)		
Your private conversations on the internet being monitored	16238	55.0
Your internet usage monitored by a police department in a different country	16150	48.3
Public security concern (source: Buchanan et al., 2007)		
Use of internet by terrorists for training and planning attacks	16230	46.2
Use of internet for creating panic and/or spreading hatred	16294	47.3
Use of internet to share and publish child pornography	16295	68.2
Use of internet to perpetrate organised crime	16285	59.5
Individual security concern (source: Dinev & Hart, 2006)		
A computer virus which harms your computer	16315	61.6
Harassment or threatening comments on internet	16290	34.1
Theft of financial data (such as credit card information) or identity theft and theft of personal information to be used for impersonating [you]	16328	61.4
Trust in websites (source: Patil et al., 2013b)		**% Agree or strongly agree**
Most internet websites are safe environments in which to exchange information with others	16057	27.7
Most internet websites are reliable environments in which to conduct business transactions	15883	30.7

misappropriation. Monitoring of personal data by the ISP in this way can be considered to infringe personal security as it could lead to identity theft, for example. This is distinct from national security concerns, however, which involve surveillance of and access to personal information by security authorities. For the purposes of this study, we defined 'police' as including all security authorities likely to need to or perform this kind of surveillance as this was better understood by all participants. Indeed, this kind of access may well be outside the control of an ISP, although for consistency we frame the question in terms of a service offered by them.

ISP options also varied according to the level of access that security authorities (e.g. at the national or pan-European level) could have on Internet-user data and whether continuous monitoring of Internet use could occur. The latter was captured by the attribute 'when ISP can allow continuous surveillance of its Internet users by the police' (see Table 3). In the most restrictive, privacy-protective case, as also shown in Table 3, an ISP would store no information related to Internet use and never allow continuous surveillance of its customers by the police (i.e., security authorities).

Potential benefits for Internet users involved monetary


"Imagine that you are about to purchase Internet connection or renew your subscription with an Internet Service Provider (ISP). We will now present you with a set of five hypothetical scenarios that include different options for these services.

As part of the information presented in each scenario, you will be presented with the costs for Internet security and handling your personal information, which is usually paid as part of your connection charges or monthly bill."

Which of the following options would you prefer as your Internet Service Provider?

Description	Option A	Option B	Option C
Handling of your Internet usage information Which internet usage information is stored: How long the information is stored: Who has the access to your information:	Websites you have visited 1 year Information could be shared with all European police departments	Websites visited and your location 6 months Information could only be shared with the police departments in the United Kingdom	None of these, I would prefer to look for another Internet Service Provider
When ISP can allow continuous surveillance of users by the police:	Any time without a warrant	Only with a warrant	
Services offered to improve online privacy:	ISP will warn you which websites do not meet your desired level of privacy	ISP will advise on how to use Internet anonymously without allowing websites to collect your personal data	
Cost or discount for internet security and data management per month:	You pay a £0.86 premium	You receive a £0.86 discount	

Fig. 2. An example of the Internet Service Provider choice card (Patil et al., 2013b).

discounts or ISP services that help improve control of their personal information and their Internet activity. Internet service providers may offer services to improve their customers' experience and help them address issues around online privacy. Such services may involve advice, warning or actively encrypting user information. These types of services are also offered commercially. As experience with websites may vary across the EU27, framing the survey questions at the level of the ISP provides a context for examining all these issues whilst also as comprehensible as possible for survey respondents. As shown in Table 3, the corresponding levels of this attribute included: no additional services, advice on how to use Internet anonymously, warning the user which websites do not meet their desired level of privacy or the ISP actively hiding information about their internet use from others.

By presenting a set of services offered by an ISP, it was also possible to attach a cost element with each choice. The premium/discount values ranged between a discount of 3 Euros per month up to a payment of 1 Euro per month and included a 'no charge' level. As with all attributes, the range and values (levels) presented as part of the 'premium or discount for Internet security and data management' attribute were specified following consultation with an expert panel and focus-group sessions conducted in London (UK), Athens (Greece) and Vilnius (Latvia). Smaller price denominations were avoided as the potential information gain may have been disproportionate to the cost of the survey (e.g. larger number of scenarios). The chosen levels and subsequent model specification provided sufficient range to estimate the marginal utility of premiums, discounts and the 'no charge' level within the range of discount and premium values introduced in the experiment.

Given the large number of possible alternatives that could be generated from combinations of the levels of the six attributes describing ISP options, we used a D-efficient experimental design based on the multinomial logit model (MNL) to search for a candidate subset of alternative configurations to create a design matrix. Efficient designs require prior information ('priors') on the model parameters to be estimated and these priors are usually obtained from previous studies. Given that this was the first time that such experiment was developed efficient-design matrices were generated assuming that priors were equal to zero (Bliemer & Rose, 2009; Huber & Zwerina, 1996). The design matrix was generated using the software Ngene (ChoiceMetrics, 2010) and incorporated a blocking algorithm to reduce the choice scenarios to a feasible number for each participant. Thus, each respondent in the Internet context was presented with five choice cards.

Table 3
Attributes and levels for configurations used in the Internet Service Provider choice context (Patil et al., 2013b).

Attribute	[Level] Description
Which internet usage information is stored	[1] No information will be stored (Reference Level) [2] Websites you have visited [3] Websites visited and your location [4] Websites visited, your location, and list of persons you contact on the Internet [5] All internet activities including what you write in emails or type on websites
How long information is stored	[1] 1 month (Reference Level) [2] 6 months [3] 1 year [4] 5 years
Who has access to your information (if seen needed by judge/court)	[1] Information will not be shared with anyone else (Reference Level) [2] Information could only be shared with the police departments in [Home Country] [3] Information could be shared with all European police departments [4] Information could be shared with police departments worldwide
When an ISP can allow continuous surveillance of its Internet users by the police	[1] Any time without a warrant [2] Only with a warrant [3] Without a warrant but only under government declared state of emergency [4] Never (Reference Level)
Services offered to improve online privacy	[1] ISP will not offer any service to improve your online privacy (Reference Level) [2] ISP will advise on how to use the Internet anonymously without allowing websites to collect your personal data [3] ISP will warn you which websites do not meet your desired level of privacy [4] ISP will actively hide information on your internet use from others
Monthly cost or discount for internet security and data management	[1] You receive a 3 Euros discount [2] You receive a 1 Euro discount [3] There is no impact on price [4] You pay a 1 Euro premium

3.5. Survey implementation

The survey instrument was deployed across the EU27 with the aim of recruiting 1000 participants aged 18 years and older in each country, In Cyprus, Luxembourg and Malta due to their smaller population sizes, the target for each country was set at 750 participants (Johnson & Lucica, 2013b). Internet surveys were conducted across 12 countries with the highest levels of Internet access according to official statistical data (Eurostat, 2013). Face-to-face interviews were carried out in the remaining 13 countries with the lowest Internet-access rates. In Italy and Germany, the survey was conducted by employing a mixed-mode approach – i.e., 500 responses were collected online and 500 interviews were conducted face-to-face. This approach enabled validity testing against the survey mode.

The main-survey data collection was carried out between August and November 2013. In countries where the survey was carried out online, respondents were recruited from online panels in each country. The sampling design was structured by nationally representative quotas, resembling the profile of the general population in each country according to age, gender and region of residence. In countries where the survey was conducted using face-to-face interviews, the sampling approach followed a three-step approach: (a) stratification and selection of local area sampling points, (b) selection of addresses within each of the sampling points and (c) selection of individuals within each household. Following this process, households were then selected through a predefined random walk procedure. This is a standard approach followed in previous pan-European surveys such as the Eurobarometer[2]. Within an identified household, respondents were selected according to quotas, reflecting the profile of the general population in each country according to age and gender (either crossed quotas or simple quotas, depending upon local procedures in each country). Only one respondent was interviewed in each household (Johnson & Lucica, 2013a).

Eligible respondents in the Internet-user activity scenarios reported in this paper were those who had previously used the Internet either by themselves or with someone's help, but did not necessarily have access to the Internet at the time of the survey. This respondent-screening approach excluded respondents who had never used the Internet before but did collect preferences from a small proportion of participants who at the time had no access to the Internet (285 respondents or 1.7% of the sample, see Table 1).

4. Analysis

4.1. Privacy concern index

Using the first two sets of questions in Table 2, an abstract 'Internet Privacy Index' was developed to capture respondents' level of concern for data protection and privacy when using the Internet. The Index classified respondents into four groups depending on the number of 'concerned' responses reflecting:

- 'high concern' when respondents gave 4 or 5 'concerned' answers;
- 'medium concern' when respondents gave 3 'concerned' answers;
- 'low concern' where respondents gave 1 or 2 'concerned' answers, and
- 'no concern' when no concern answers were reported.

This procedure was in the line with the development of similar indices that have been validated using large panels across different countries such as the Westin-Harris Distrust Index (Kumaraguru & Cranor, 2005).

4.2. Analysis of stated preferences for surveillance, data retention and privacy enhancing services

The analysis of the SPDEC data corresponding to respondents' choices in the Internet Service Provider scenarios was conducted using the multinomial logit model (MNL), a discrete choice analysis method based on Random Utility Theory (RUT) (McFadden, 1974). Under RUT, a consumer n by choosing alternative-option i (i.e., an Internet Service Provider) maximises their utility U_{in}, which represents the level of 'satisfaction'/benefit from choosing that option. The Utility is the sum of a deterministic (observed) part V_{in} and a random (unobserved) part ε_{in} (McFadden, 1974):

$$U_{in} = V_{in} + \varepsilon_{in} = \beta' * x_{in} + \delta' * z_n + \varepsilon_{in} \quad (1)$$

V_{in} is a linear-in parameters function of the attributes of the alternatives x and individuals z;

[2] http://www.gesis.org/eurobarometer-data-service/survey-series/standard-special-eb/sampling-and-fieldwork/.

β' and δ' are vectors of coefficients to be estimated and each representing the influence of attributes of the alternatives and individuals, respectively;
ε_{in} is a random parameter that incorporates unobserved or unobservable attributes, unobserved taste variations and measurement or specification errors (Ben-Akiva & Lerman, 1985).

Given that the formulation of the Utility in Eq. (1) includes a stochastic component, it is only possible to describe the probability of choosing alternative i over another alternative k as:

$$P_{in} = Prob(V_{in} + \varepsilon_{in} > V_{kn} + \varepsilon_{kn}; \forall k \in C) = Prob(V_{in} - V_{kn} > \varepsilon_{kn} - \varepsilon_{in}) \quad (2)$$

where C is the choice set and corresponds to the set of the alternative options that are available to an individual n. Assuming that the random part, ε_{in}, is Type I Extreme Value independently and identically distributed across alternatives, the probability of choosing alternative i takes the form of the multinomial logit model (McFadden, 1974)[3]:

$$P_{in} = \frac{exp(\beta' * x_{in} + \delta' * z_n)}{\sum_j exp(\beta' * x_{jn} + \delta' * z_n)} \quad (3)$$

The choices made by survey respondents across the different sets of alternative scenarios allowed the estimation of the parameters β' and δ' and subsequently, the estimation of the probability that an ISP i is chosen among the set of two ISPs. In order to capture variation in preferences due to differences across countries and groups of respondents we used segmentation analysis so that country-specific and socio-demographic variables were introduced with a separate coefficient into the model (Train, 2003).

The estimated MNL model in this study has been developed using data from respondents across all EU27 countries. Hence, a single weight is estimated for each attribute level, which corresponds to the EU average. When pooling data from different country samples, however, it was necessary to consider potential variations in unobserved factors or error-variation in the models between countries. These variations can include measurement errors across samples and other unobserved cultural and contextual factors. Furthermore, surveys in some countries were carried out online, while others were undertaken 'face to face'. These two types of survey modes may also give rise to variations in unobserved factors or error-variation in the models, which need to be controlled for. Accordingly, the variation in quality of responses across the following two dimensions was taken into account via:

- Country scales to control for country-specific unobserved factors such as difference in quality of data and survey implementation across the EU27.
- Scales by survey mode to control for variation in response quality between the online and face-to-face surveys.

Finally, to account for correlations between multiple SPDCE responses by a single respondent, a panel specification can be applied. A panel specification, however, increases the model estimation time considerably given the large sample size in this project. Hence in order to correct for model mis-specification and take into account the repeated nature of the SP data a bootstrap resampling procedure was employed on the final model (Efron & Tibshirani, 1994).

[3] Different assumptions about the distribution of the error terms give rise to different modelling structures (e.g. probit, mixed logit).

5. Results

The total number of participants in the PACT survey across the EU27 were 26,443 comprising 12,861 online observations and 13,582 observations collected via face-to-face interviews (Patruni et al., 2014; see Appendix B). The response rates in the face-to-face interviews varied between 20% (Romania) and 68% (Bulgaria) (Patruni et al., 2014; see Appendix A). It was not possible to accurately compute the response rate in the online survey as respondents were recruited via an Internet panel. The sample size satisfied set targets and the sample was broadly representative for each country against age, gender and region of residence, the three key dimensions that were defined for sample representativeness (Patruni et al., 2014). In Austria, Estonia and Spain respondents aged 65 years or older were significantly under-represented. Respondents aged 65 years or older were over-represented in Cyprus and Malta. Additionally, in Malta respondents aged between 55 and 64 years were under-represented. The majority of the respondents were able to engage with the choice tasks. On average, only 5% of respondents in the Internet experiment reported being unable to understand the choice tasks. The available sample size for the experiment concerning an ISP was 16,463 (62%) respondents, of which 56% were surveyed online and 44% face-to-face (see also, Table 1).

5.1. Attitudes and internet privacy concerns across the EU27

Overall, as shown in Table 2, respondents expressed low levels of trust in the Internet. Approximately, one third of respondents agreed that websites were safe and reliable and safe environments to exchange information (27.7%) and conduct business transactions (30.7%). Some of the highest levels of concern were expressed regarding: use of the Internet to share and publish child pornography (68.2% were concerned or highly concerned), handling of personal information (62%), computer viruses that may harm computers (61.2%), theft of financial data (61.4%) and the amount of personal data collected and stored by internet websites and internet service providers (60.8%).

Fig. 3 shows the variation in the proportion of respondents falling into the category of 'High Concern' for privacy when using the Internet across the EU27 according to the 'Internet Privacy Index' computed in Section 4.1 (see, Appendix A for country codes). The highest proportions of respondents with 'No Concern' for Internet privacy were observed in Slovakia and Slovenia, three Nordic countries (Denmark, Sweden and Finland) and Netherlands. On the other hand, the highest proportion of respondents with 'High Concern' regarding Internet privacy were observed in Lithuania, Latvia Spain, Greece and Portugal.

5.2. Preferences for privacy, surveillance and privacy enhancing tools

Estimated coefficients in the MNL model are presented in the following two tables. Table 4 presents baseline (average) preferences for ISPs and for different data-privacy configurations across the EU27 and Table 5 shows statistically significant country-, age- and education-level-specific effects. The model also accounts for measurement errors, survey mode and country-specific differences, which are captured by the coefficients reported in Appendix B.

In Table 4, each coefficient corresponds to the strength of preference (or weight) that respondents placed upon an attribute level relative to the reference level of the corresponding attribute. In

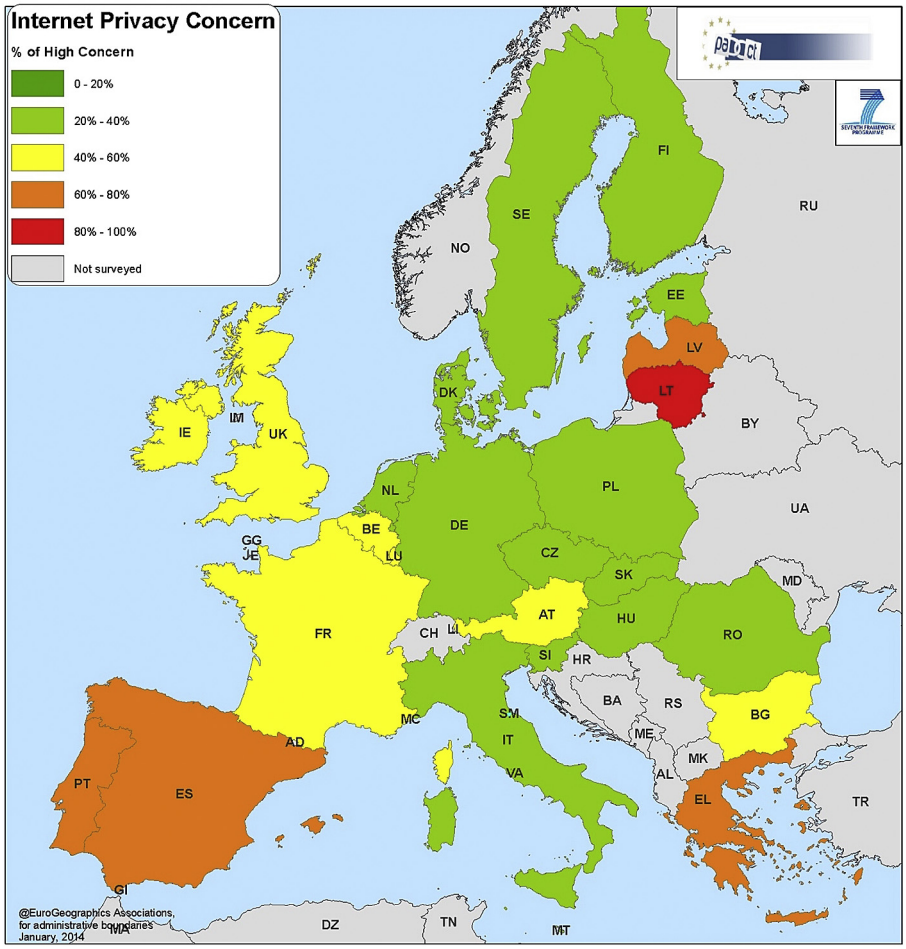


Fig. 3. Proportion of respondents with high Internet Privacy Concern Index across the EU27.

most cases, the reference level was selected to represent the smallest degree of intrusion in terms of information privacy and surveillance. A positive coefficient means that – all else being equal – a respondent was more likely to choose a scenario that included the attribute level attached to the coefficient than its reference level for which the coefficient was set equal to zero. On the other hand, a negative coefficient means that – all else being equal – respondents were more likely to choose a scenario involving the reference level than the attribute level with a negative coefficient. The interpretation is similar for the coefficients corresponding to country-specific and socio-economic and demographic effects. For example, the coefficients in Table 5 show that respondents aged between 18 and 34 years and those who only attended primary education were less likely to choose the 'none' option. Regarding the ISPs options, within a given attribute (e.g. how long information is stored), attribute-level coefficients can be compared with each other and provide the relative magnitude of respondents' strength of preference (e.g. data retention of 6 months vs. 1 year). The results for each attribute are summarised in the remainder of this section.

5.2.1. Which internet usage information is stored

Across the EU27, and relative to the reference level "no information will be stored", the negative coefficients of the remaining levels of this attribute indicate that respondents were less likely to choose an ISP that stored any type of Internet-activity (see, Table 4). Specifically, respondents were averse to ISPs storing "websites visited" (coef: −0.333; $p < 0.001$), "websites visited and location" (coef: −0.464; $p < 0.001$), "websites visited, location and personal contacts" (coef: −0.721; $p < 0.001$), and "all internet activities including email content and types of websites" (coef: −0.847; $p < 0.001$).

The analysis further helps to uncover differences in respondents' choices across countries and socio-demographic characteristics. As shown in Table 5, in the case of storage of Internet-use information, we found that respondents in Bulgaria, Finland, Ireland, Lithuania and Latvia exhibited either different preferences or different strength of preference relative to the rest of the EU27. In particular, respondents in Finland expressed significantly stronger preferences for the "no information will be stored" level (coef: 0.282; $p < 0.01$) and stronger aversion for "all internet activities" level (coef: −0.353; $p < 0.001$) when compared to the EU27 average. On the other hand, preferences for the "no information will be stored" level were weaker across Bulgaria (coef: −0.609; $p < 0.001$), Latvia (coef: −0.682; $p < 0.001$) and Lithuania (coef: −0.887; $p < 0.001$).

Fig. 4 summarises these choice patterns showing that respondents in Bulgaria (BG) and Latvia (LV) were in favour of accepting internet-use storage but up to the point where only websites and location were stored. Contrary to the rest of the EU27, respondents in Lithuania (LT) were more likely to choose scenarios that stored any type of information with the highest preference being for the "websites visited" level. Finally, respondents in Ireland (IE) were strongly averse to the storage of "all internet activities" (coef: −0.406; $p < 0.001$).

With regard to socio-demographic characteristics, women and

Table 4
Model estimates on preferences regarding internet surveillance, data retention and privacy enhancing services across Europe (baseline group).

Model parameter	Estimate	t-ratio
Which internet usage information is stored		
No information will be stored	Reference level	
Websites you have visited	−0.333***	−7.7
Websites visited and your location	−0.464***	−11.4
Websites visited, your location, and list of persons you contact on the Internet	−0.721***	−16.3
All Internet activities including what you write in emails or type on websites	−0.847***	−19.4
How long information is stored		
1 month	Reference level	
6 months	−0.122***	−4.6
1 year	−0.222***	−7.7
5 years	−0.466***	−15.9
Who has access to Internet information		
Information will not be shared with anyone else	Reference level	
Information could only be shared with police departments in [home country]	−0.144***	−5.4
Information could be shared with all European police departments	−0.510***	−16.5
Information could be shared with police departments worldwide	−0.644***	−20.2
When ISP can allow continuous surveillance of its Internet users by the police		
Never	Reference level	
Any time without a warrant	−1.059***	−30.2
Only with a warrant	0.153***	5.4
Without a warrant but only under government declared state of emergency	−0.321***	−11.3
Services offered to improve online privacy		
ISP will not offer any service to improve your online privacy	Reference level	
ISP will advise on how to use the Internet anonymously without allowing websites to collect your personal data	0.763***	22.2
ISP will warn you which websites do not meet your desired level of privacy	0.779***	22.3
ISP will actively hide information on your Internet use from others	0.819***	21.2
Monthly cost or discount for Internet security and data management		
Discount * (all income levels)	−0.001***	−9.3
There is no impact on price * (all income levels)	0.389***	10.9
Cost if household income less than €500	−0.003***	−10.8
Cost if household income from €500 to €1500	−0.002***	−14.1
Cost if household income greater than €1500	−0.002***	−10.9
Discount * (missing income)	0.001***	3.3
There is no impact on price * (missing income)	−0.060	−0.6
Cost (missing income) for low/medium-income countries	−0.006***	−15.6
Cost (missing income) for high-income countries	−0.004***	−7.8

***: $p \leq 0.001$; **: $0.001 < p \leq 0.05$; *: $0.05 < p < 0.10$.

Table 5
Country-, age- and education-level-specific effects.

Model parameter	Country differences relative to the baseline group		Socio-demographic differences relative to the baseline group	
	Stronger preference	Weaker preference	Stronger preference	Weaker preference
Type of Internet-usage information stored				
No information will be stored	*Finland* (0.282**)	*Bulgaria* (-0.609***) *Latvia* (-0.682***) *Lithuania* (-0.887***)		*Females* (-0.112***) *Secondary education* (-0.130***)
Website you have visited			*18-24 year olds* (0.282***)	
All Internet activities		*Finland* (-0.353***) *Ireland* (-0.406***)		
How long Internet data are stored				
1 year	*Latvia* (0.346**)			
Who has access to Internet information				
Worldwide	*Slovenia* (0.495***)	*Luxembourg* (-0.241**)		
When ISP can allow continuous surveillance of its Internet users by the police				
Never		*Malta* (-0.811***)		*65+ year olds* (-0.122**)
Any time without a warrant		*Lithuania* (-1.061***)		
Only with a warrant	*Denmark* (0.374***) *Spain* (0.531***)			
Without a warrant but only under government declared state of emergency		*Lithuania* (-0.900***)		*55–64 year olds* (-0.122**)
Services offered to improve online privacy				
ISP will not offer any service to improve your online privacy	*Slovakia* (0.362***) *Czech Republic* (0.619***)	*Estonia* (-0.271***) *Belgium* (-0.305***)	*Males* (0.250***)	*65+ year olds* (-0.200***)
None of these options				18–24 year olds (-0.392***) 25–34 year *olds* (-0.153***) Primary education (-0.137***)

***: $p \leq 0.001$; **: $0.001 < p \leq 0.05$; *: $0.05 < p < 0.10$.

those who completed secondary education expressed significantly lower strength of preference for the "no information will stored" level and thus they were more likely to opt-in for scenarios that involved some type of internet-use storage. On the other hand, respondents aged 18–24 years were more likely to choose scenarios that involved storage of "websites visited" relative to the reference level ("no information will be stored").

5.2.2. How long information is stored

Similar to preferences regarding internet-use storage, respondents across the EU27 were on average less likely to choose an ISP that stored data on users' Internet activity for a period longer than one month, the reference level in the experiment. Only respondents in Latvia were in favour of an ISP retaining data on Internet-use for up to one year.

5.2.3. Who has access to your information (if seen needed by judge/court)

Relative to the reference level "information will not be shared with anyone else", respondents were averse to scenarios under which an ISP would share Internet-use data with "police departments in the home country" (coef: −0.144; $p < 0.001$), "police departments across Europe" (coef: −0.510; $p < 0.001$) or "police departments worldwide" (coef: −0.644; $p < 0.001$). Increasing absolute values of the coefficients for those attribute levels shows that respondents were increasingly averse as the geographic scale of access increased. The level of aversion for worldwide access to

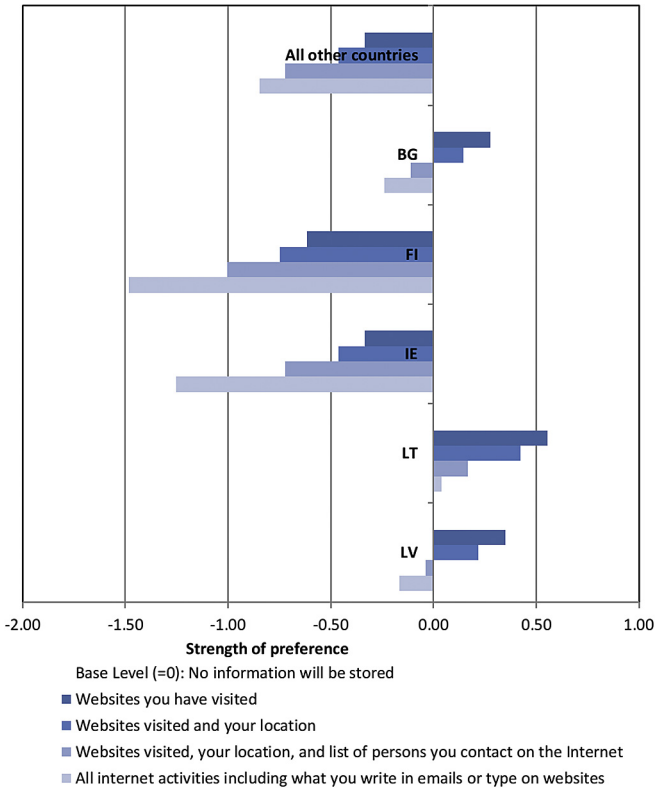


Fig. 4. Strength of preference for the type of information stored by ISP.

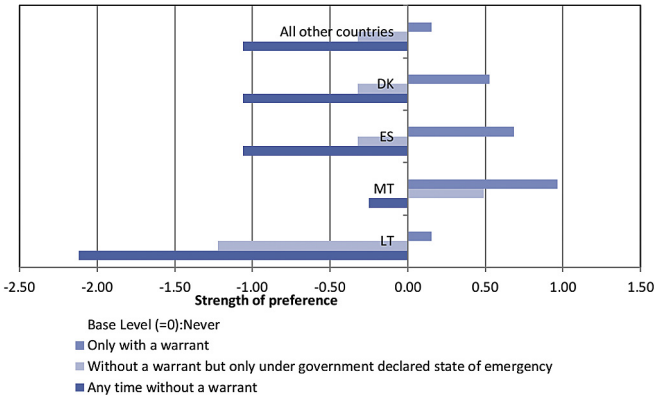


Fig. 5. Strength of preference for allowing continuous surveillance.

Internet use data was higher than the EU27 average in Luxembourg (coef: −0.241; $p < 0.05$). On the other hand, Slovenia was the only country where respondents were more likely to choose ISPs if the Internet-use data were to be shared with police departments worldwide (coef: −0.495; $p < 0.001$).

5.2.4. When an ISP can allow continuous surveillance of its internet users by the police

With regard to the conditions under which ISPs should allow continuous surveillance of Internet users, a different picture emerged. On average and across the EU27, respondents were more likely to choose ISPs that allowed continuous surveillance 'only with a warrant' (coef: −0.153; $p < 0.001$) over ISPs that would 'never allow continuous surveillance'. On the other hand, respondents were less likely to opt-in for an ISP that would either allow continuous surveillance 'without a warrant' (coef: −1.059; $p < 0.001$) or in the case of 'government-declared state of emergency or at any time without a warrant' (coef: −0.321; $p < 0.001$).

As shown in Table 4, model estimates showed that respondents across Denmark, Malta, Spain and Lithuania expressed significantly different preferences compared to the remaining EU countries. These patterns are shown in more detail in Fig. 5. Danish and Spanish respondents expressed a stronger than average positive preference for ISPs that 'allowed continuous surveillance only with a warrant'. On the other hand, respondents in Lithuania expressed stronger aversion to higher levels of oversight of Internet users than the EU average. Respondents in Malta were more likely to choose ISPs that would allow continuous surveillance either with a warrant or under government-declared state of emergency; the latter was contrary to the EU-average preferences.

Regarding differences in preferences based on the socio-demographic profiles of respondents, we found that respondents aged 65 years and over were overall less averse to continuous surveillance with or without warrant than other age groups. On other hand, those aged 54–64 years were less likely to choose ISPs that allowed continuous surveillance without a warrant under a government-declared state of emergency. Finally, respondents over the age of 65 years had overall stronger preferences across all attribute-levels relative to other age groups.

5.2.5. Services offered to improve online privacy

As shown in Table 4, respondents were generally in favour of ISPs that offered privacy enhancing services including 'advice on how to use the Internet anonymously' (coef: 0.763; $p < 0.001$), 'warning which websites do not meet users' desired level of privacy' (coef: 0.779; $p < 0.001$) and 'actively hiding information from others', which received the highest strength of preference among these offered services (coef: 0.819; $p < 0.001$).

The strength of preferences was significantly stronger than average across Belgium and Estonia, while respondents in the Czech Republic and Slovakia expressed weaker (though overall still positive) preferences for these services. All else being equal, significant differences in preferences were found according to gender and age. Males were more likely to opt-in for ISPs that offered no services to improve online privacy whereas respondents aged 65 or older were less likely to choose those options and were more likely to opt-in for ISPs that offered privacy-enhancing services compared to other age groups.

5.2.6. Surcharge on and reduction of monthly fees

As shown in Table 4, some of the ISP choice options were designed to include a premium to enhance users' Internet-security. Respondents' sensitivity to cost was modelled as a linear variable by estimating separate effects according to respondents' monthly household-income (after taxes) thus capturing decreasing cost sensitivity with increasing income. Adjacent income bands were grouped when the coefficients were not statistically different thus resulting into three income groups with significantly different cost sensitivity: (a) less than €500, (b) €500 to 1,500, and (c) over €1500.

A separate coefficient was also estimated for the group of respondents for whom income was not recorded ('missing income') who answered, 'prefer not to say' or 'don't know' to the income question. Respondents in the 'missing income' group were further split into two groups (low/medium and high income countries) to account for the wide range of average income across the EU27. Thus, our model captures cost sensitivity across five income-based population segments. The estimated coefficients indicate that

respondents were generally against paying for an additional surcharge to cover security and as shown in Table 4, respondents' sensitivity to cost decreased with increasing income.

The discount variable was also specified as a linear variable. However, no significant difference in sensitivity for discounts was observed for respondents with different income. For respondents who did not state their income, model specification tests were also undertaken to examine if the discount variable could be split into different categories based on the average income of the country of residence. The tests did not show a significant difference in sensitivity of the discount coefficient by the average income of the country. Hence only two discount coefficients are reported in Table 4; one for missing income and another for all other income levels.

All else being equal, respondents were more likely to choose ISPs that would not charge any security premiums, except those who did not report their income, and were more likely to prefer ISPs that offered discounts. The negative marginal utility placed on ISPs offering a discount by respondents who reported their income (coef: −0.001; $p < 0.001$) may be due to the disparity between willingness to accept payment to disclose personal information (discount) and willingness to pay to protect their personal information (Acquisti et al., 2013). Put differently, respondents might feel that the discount on offer may not have been enough for them to disclose their Internet activity and related aspects in the experiment. Finally, it is worth noting that the findings on premium/discount coefficients does not mean that the 'no charge' option dominated respondents' choices. If that were the case, it would not have been possible to estimate any significant coefficients for the remaining attributes in the experiment.

6. Discussion and conclusion

This pan-European study examined Internet-user privacy concerns and preferences for privacy, surveillance and privacy-enhancing services across the EU27. Using the Privacy Calculus concept, respondents were presented with alternative options of ISPs involving varying levels of data storage, retention and sharing of these data with authorities. Options also involved scenarios in which continuous surveillance of users' Internet activity might occur or ISPs might offer potential benefits such as privacy-enhancing advice or technologies to help users protect their privacy while using the Internet.

The findings showed that, on average, respondents across the EU27 were less likely to choose ISPs that retained data for more than one month and shared any type of data related to their Internet activity (e.g. websites, location, emails). These findings provide a robust evidence base that challenge recent policy initiatives to enable enforcement agencies to more easily access a user's Internet activity. For example, in 2015, the UK Home Office proposed a law, the Investigatory Powers Bill, which would require ISPs to store internet activity of all users in Britain and allow law enforcement agencies without a warrant to access information of websites users visited over the period of one year (BBC, 2015). The above findings regarding retention of data imply that EU Member States and subsequently ISPs should be transparent and should establish a 'right to be informed' when users are subject to such measures (de Hert & Boehm, 2012).

The analysis of preferences also uncovered significant effects of preference heterogeneity according to respondents' age, gender and education qualifications. For example, women were less likely to opt-in for ISPs that did not store any information relative to men – women were thus willing to disclose some of their Internet activity to ISPs. Although there were no significant gender differences in terms of respondents' willingness to allow ISPs to store emails, location and contacts, this finding is broadly in line with findings of a meta-analysis of 205 studies on gender differences and self-disclosure which showed that women disclose more information than men (Dindia & Allen, 1992). Gender differences in self-disclosure may arise from differences on how individuals socialise, gender-role expectations and the different criteria men and women use to define and control personal information (Petronio, 2002 cited in; Sheldon, 2013).

It is not straightforward to contrast differences in preferences according to age as most studies employ convenience samples targeting younger participants. In this study,18–24-year olds were more likely to choose ISPs that stored websites visited and 55–64-year olds were strongly against ISPs that would allow continuous surveillance without warrant. Confounding this prior evidence, it is worth highlighting that those aged 65 and over were less likely to choose ISPs that would never allow continuous surveillance. Broadly, these findings are consistent with previous studies that showed that privacy concerns may decrease with age (Bergström, 2015; Taddicken, 2014). The latter may arise from a general lack of trust in the Internet, stemming from different perceptions about the credibility of online information. This has been shown to be a factor in healthcare (e.g. Zulman, Kirch, Zheng, & An, 2011). A further potential explanation could lie in the fact that those over working age are more likely to read about and thus be appraised of government surveillance activities reported by the media.

Concerning levels of educational attainment, our study showed that those who only completed secondary education (i.e., without a university degree) were less likely to choose an ISP that stored no data. This finding raises interesting questions: (a) was this preference due to implicit trust that the storage of information would be in line with privacy preferences? or (b) were people with lower levels of educational attainment less likely to question the need for surveillance and more likely to take at face value the necessity of the potential trade-offs between privacy and security as articulated by governments when disclosing surveillance practices? This finding is supported by the work of Davis and Silver (2004) who note the relevancy of educational levels when considering preferences regarding surveillance.

Findings also point towards significant country-level differences from the average preferences at the EU27 level. For example, respondents in Lithuania and Bulgaria were in favour of ISPs collecting information on websites visited and the location of users. Additionally, respondents in Latvia were more likely to opt-in to ISPs collecting all types of Internet activity including email communications and retaining these data for up to year. Respondents in Slovenia were content with ISPs sharing Internet usage activity with security authorities worldwide. There could be several reasons why preferences in some countries were contrary to the EU27 average. One such reason could be the history of surveillance and its place in culture. Bulgaria, Latvia, Lithuania, and Slovenia belonged to the block of Central and Eastern European countries where state surveillance was endemic for a number of years (Svenonius, Bjorklund, & Waszkeiwicz, 2014). From a cultural perspective and according to Hofstede's Dimensions of National Culture, Bulgaria, Latvia and Lithuania have similarities in terms of exhibiting quite low scores on the 'Indulgence' dimension implying that individuals' actions are 'restrained' by social norms (Hofstede, 2017). Slovenians' preferences towards sharing their Internet activity with security authorities worldwide may be part the country's tendency to follow the 'Western prototype' and globalisation, recognising that the 'security landscape is changing profoundly' and boundaries between security actors disappear (Zavrŝnik, 2013). These findings are in line with prior suggestions to researchers when conducting fieldwork to place emphasis on the consumers' cultural background due to its potential to moderate attitudes

towards online privacy (Pavlou & Chai, 2002). Another factor which may reflect significantly different preferences include possible media events on surveillance contemporaneous to the fieldwork. Nonetheless, the findings also demonstrate that heterogeneity of preferences across the EU27 has implications towards the development and implementation of European-level policy and legislation on data protection. The findings also point towards empowerment of the individual in terms of being able to control their data and thus addressing inequalities between individuals and global corporations such as ISPs (in 't Veld, 2012).

A related aspect which merits discussion is the public-private aspect to surveillance and the way in which the private sector, wittingly or unwittingly assists governments in performing surveillance. In the aftermath of the disclosures by Edward Snowden regarding government surveillance capabilities, the private sector were quick to point out the damage that such revelations would have upon their customer base, eroding trust (Amnesty International, 2015). Although this study implicitly considered the role of the private sector (in terms of ISPs that respondents were asked to choose from) we did not explore the legal obligations and behaviour of the ISP toward security authorities in respect of honouring requests for users' personal information (whether covered by a warrant or not). Similarly, we did not explore the ISPs willingness (or not) to install government surveillance technology on their own infrastructure.

Respondents did recognise that the Internet can be a platform for child pornography, terrorism and fraud. Thus, they do recognise that continuous surveillance of users' activity may be useful to law enforcement in tackling these types of misuse or malfeasance, but doing so requires a legal basis. Interestingly, the findings showed that, all else being equal and when compared to an ISP option that would not allow continuous surveillance under any circumstances, respondents were more likely to choose an ISP that would allow continuous surveillance providing it was suitably accountable (i.e., when a warrant was issued). This implies that individuals are able to make complex trade-offs when they set their own privacy against broader social benefits (e.g. tackling crime).

The finding that individuals were willing to opt-in for an ISP which offered privacy protections imply a nascent market for privacy enhancing services and PETs. Respondents were more likely to select an ISP that offered some level of privacy protection relative to the base scenario which did not offer any service to improve user privacy. These services were presented in the form of an ISP offering advice or warnings or actively helping users to protect their anonymity and preventing websites from collecting data. Technologies offering anonymization of records and logs have been introduced as 'countermeasures to surveillance' and include TOR, Free Heaven and Pretty Good Privacy (Shen & Pearson, 2011). Supply side aspects of the market for privacy enhancing technologies were historically assessed as being immature (London Economics, 2010) in part because companies saw little economic benefit in offering users ways to protect their privacy compared to the revenue available to them from exploiting it. By comparison, the findings indicated above imply that the economic potential has not yet been fully recognised.

Despite the uniqueness of this study as one of the largest exercises concerning preferences for online surveillance, privacy and security employing SPDCE and given the geographical scale of the fieldwork, several challenges were encountered. Firstly, significant time was spent in translating and validating terms into different languages, especially the terms 'privacy', 'surveillance' and 'security' which can be particularly ambiguous and sensitive. Risks that clumsy translation of such sensitive and context dependent terms would affect the validity of understanding and presentation of the survey instrument were mitigated through collaboration with an experienced and internationally accredited market-research firm who applied consistent, industry-recognised standards for interviewing and internet-based research across the EU27.

Secondly, the target sample in the study was adults aged 18 years and over with representative quotas for age, gender and geographic regions within each of the EU27. For reasons of speed and efficient use of human and financial resources, sampling, recruitment and data collection differed according to the country's Internet-access rates. Face-to-face interviews were conducted across countries with the lowest Internet-access rates and online surveys were administered across those countries with the highest Internet-access rates. However, Internet use was not part of the sampling-quota criteria and hence, Internet-use patterns observed in both the Internet and face-to-face samples were not necessarily representative of the country's Internet-user profiles and patterns. The use of mixed-mode methods, however, ensured that the study collected responses from both regular Internet users but also those that it is otherwise difficult to recruit via online surveys but do have some experience in using the Internet. These differences are controlled for in the results reported in this study.

As in the case with all experimental studies, respondents in the SPDCE expressed behavioural intentions and not actual choices, which may be different and change over time. However, this limitation is not prohibitive from revealing the *relative* importance individuals place on different levels of surveillance, data retention and privacy enhancing services or technologies. SPDCEs have been robust in providing evidence on the relative importance of different choice-related attributes and have had a long-standing application in other complex and difficulty to quantify subject areas such as transport (e.g. Hensher, 1994). Most importantly, the findings in this study provide a strong evidence base for comparison of individual preferences across the EU27 as well as across real-life situations. The latter is reported by Potoglou et al. (2014b) who discuss findings across the travel on metro/rail, healthcare data and Internet-use scenarios providing empirical evidence regarding the context dependent nature of preferences regarding privacy, security and surveillance. For example, in some situations, privacy is considered as a form of control of personal information and in others as control of physical space.

While on average preferences across Europe are broadly consistent, findings point toward the importance of accounting for the diversity in preferences across country and demographic groups when designing and deploying security and physical or digital surveillance infrastructure. Europeans' preferences relating to security and privacy are much more nuanced than a straightforward inverse relationship that assumes that enhanced security or surveillance must come at the cost of privacy and liberty. Country-specific models could provide an even greater insight into variations across the 27 Member States.

In conclusion, this work provides robust and consistent evidence from across the EU27, which points towards: the need for greater transparency and accountability regarding the surveillance of Internet use by law enforcement agencies, the need to empower individuals to set the right level of privacy for themselves and potential business opportunities through exploiting nascent demand for privacy enhancing services and technologies. Given better communication from governments about the reasons why security services must employ surveillance capabilities and clarity about the accountability and governance of these capabilities, coupled with greater availability of tools to help users better manage their preferences, the delicate task of managing the competing priorities of privacy, surveillance and security may be more actively addressed. Finally, evidence from this study serves to add another set of insights into the complex and broad picture that security authorities have to consider in their decision-making.

Funding

This work was supported by the European Commission's 7th Framework Programme Security [Grant Agreement no 285635].

Acknowledgements

The authors are grateful to the PACT consortium for their contribution in the development of the survey and the two anonymous reviewers for their constructive comments and suggestions.

Appendix A. Country codes

Code	Country
BE	Belgium
BG	Bulgaria
CZ	Czech Republic
DK	Denmark
DE	Germany
EE	Estonia
IE	Ireland
EL	Greece
ES	Spain
FR	France
IT	Italy
CY	Cyprus
LV	Latvia
LT	Lithuania
LU	Luxembourg
HU	Hungary
MT	Malta
NL	Netherlands
AT	Austria
PL	Poland
PT	Portugal
RO	Romania
SI	Slovenia
SK	Slovakia
FI	Finland
SE	Sweden
UK	United Kingdom

Appendix B. Country and socio-economic effects on scales and the constant

	Coef.	t-ratio
Country effects		
Austria	1.000	n/a
Belgium	0.853	20.9
Bulgaria	0.693	10.3
Cyprus	0.484	8.4
Czech Republic	0.740	11.6
Denmark	0.855	19.1
Estonia	1.000	n/a
Finland	0.871	17.0
France	0.895	21.1
Germany	1.000	n/a
Greece	0.538	9.9
Hungary	0.684	11.2
Ireland	0.758	17.9
Italy	0.719	15.8
Latvia	0.689	11.0
Lithuania	0.496	8.5
Luxembourg	1.000	n/a
Malta	0.429	7.8
Netherlands	1.000	n/a
Poland	0.523	10.2
Portugal	0.528	9.3
Romania	0.434	8.4
Slovakia	0.764	11.9
Slovenia	0.634	11.1
Spain	0.723	17.8
Sweden	0.908	20.1
UK	0.911	21.1
Survey method effects		
Online	1.0000	n/a
Face to Face	0.8156	15.7
None constant		
Italy (Face-to-face)	−0.207	−1.8
Italy (Online)	0.099	1.1
UK	−0.049	−0.8
Sweden	0.464	6.6
Spain	0.214	2.7
Slovenia	0.166	1.7
Slovakia	0.009	0.1
Romania	−1.253	−7.3
Portugal	0.599	4.0
Poland	0.448	3.5
Netherlands	−0.057	−1.0
Malta	−2.294	−8.5
Luxembourg	0.190	3.0
Lithuania	−2.246	−10.1
Latvia	−3.284	−14.9
Ireland	0.005	0.1
Hungary	0.451	4.3
Greece	−0.987	−7.9
Germany (Face-to-face)	0.517	5.4
Germany (Online)	0.343	4.9
France	0.299	4.5
Finland	0.229	2.8
Estonia	−0.133	−2.1
Denmark	0.346	4.5
Czech Republic	0.048	0.5
Cyprus	0.321	2.2
Bulgaria	−1.490	−12.0
Belgium	−0.117	−1.8
Austria	0.212	3.5

References

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *Journal of Legal Studies, 42*(2), 249–274. http://dx.doi.org/10.1086/671754.

Allenby, G. M., Shively, T. S., Yang, S., & Garratt, M. J. (2004). A choice model for packaged Goods: Dealing with discrete quantities and quantity discounts. *Marketing Science, 23*(1), 95–108. http://dx.doi.org/10.1287/mksc.1030.0022.

Amnesty International. (2015). *Two years after Snowden: Protecting human rights in an age of mass surveilance*. https://www.privacyinternational.org/sites/default/files/Two Years After Snowden_Final Report_EN.pdf, 01/12/2016.

Angriawan, A., & Thakur, R. (2008). A parsimonious model of the antecedents and consequence of online Trust: An uncertainty perspective. *Journal of Internet Commerce, 7*(1), 74–94.

Bateman, I. J., Carson, R. T., Day, B., Hanemann, M., Hanley, N., Hett, T., et al. (2002). *Economic valuation with stated preference techniques: A manual*. Cheltenham, UK: Edward Elgar.

BBC. (2015). *Details of UK website visits to be stored for year*. http://www.bbc.co.uk/news/uk-politics-34715872, 22/12/2016.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly: Management Information Systems, 35*(4), 1017–1041.

Ben-Akiva, M., & Lerman, S. R. (1985). *Discrete choice Analysis: Theory and application to travel demand*. Cambridge: MIT Press.

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. http://dx.doi.org/10.1016/j.chb.2015.07.025.

Berkman. (2016). *Don't Panic: Making progress on the 'going dark debate'*. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf, 03/01/2017.

Bliemer, M., & Rose, J. M. (2009). Designing stated choice Experiments: State of the art. In R. Kitamura, T. Yoshii, & T. Yamamoto (Eds.), *The expanding sphere of travel*

behaviour Research: Selected papers from the 11th international conference on travel behaviour research (pp. 499–538). Bingley, United Kingdom: Emerald Group Publishing Limited.
Boyd, D., & Heer, J. (2006). Profiles as Conversation: Networked identity performance on friendster. In *Proceedings of the 39th annual Hawaii international conference on system sciences (HICSS'06)* (Vol. 3). pp. 59c-59c.
Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157–165. http://dx.doi.org/10.1002/asi.20459.
Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*, 291–302. http://dx.doi.org/10.1016/j.chb.2017.01.003.
ChoiceMetrics. (2010). *Ngene 1.0.2 User Manual and Reference Guide: The cutting edge in experimental design*. http://www.choice-metrics.com/, 15/12/2016.
Crump, C. (2003). Data retention: Privacy, anonymity and accountability online. *Stanford Law Review, 56*(1), 191–229.
Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*, 28–46. http://dx.doi.org/10.1111/j.0092-5853.2004.00054.x.
Dindia, K., & Allen, M. (1992). Sex differences in self-disclosure: A meta-analysis. *Psychological Bulletin, 112*, 106–124.
Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information System Research, 17*(1), 61–80. http://dx.doi.org/10.1287/isre.1060.0080.
Efron, B., & Tibshirani, R. J. (1994). *An introduction to the bootstrap*. Boca Raton, FL: CRC Press.
Eurostat. (2013). *Households - level of internet access*. http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database, 20/12/2016.
Eurostat. (2016a). *Digital economy and society statistics - households and individuals*. http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals - Internet_access, 26/12/2016.
Eurostat. (2016b). *E-commerce statistics for individuals*. http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals, 26/12/2016.
Hall, J., Viney, R., Haas, M., & Louviere, J. (2004). Using stated preference discrete choice modeling to evaluate health care programs. *Journal of Business Research, 57*(9), 1026–1032. http://dx.doi.org/10.1016/S0148-2963(02)00352-1.
Heirman, W., Walrave, M., Ponnet, K., & Van Gool, E. (2013). Predicting adolescents' willingness to disclose personal information to a commercial website: Testing the applicability of a trust-based model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(3), Article 3.
Hensher, D. (1994). Stated preference analysis of travel choices: The state of practise. *Transportation, 21*, 107–133.
Hensher, D. A., Rose, J. M., & Greene, W. H. (2005). *Applied choice analysis - a primer*. New York: Cambridge University Press.
de Hert, P., & Boehm, F. (2012). The rights of notification after surveillance is over: Ready for recognition? In J. Bus, M. Crompton, M. Hilderbrandt, & G. Metakides (Eds.), *Digital enlightment yearbook 2012* (pp. 19–39). Amsterdam: IOS press.
Hess, S., Daly, A., Dekker, T., Cabral, M. O., & Batley, R. (2017). A framework for capturing heterogeneity, heteroskedasticity, non-linearity, reference dependence and design artefacts in value of time research. *Transportation Research Part B: Methodological, 96*, 126–149. http://dx.doi.org/10.1016/j.trb.2016.11.002.
Heurix, J., Zimmerman, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers and Security, 53*, 1–17.
Hofstede, G. (2017). *Cultural Dimensions: Country comparison*. https://geert-hofstede.com/countries.html, 31/03/2017.
Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology, 63*(6), 597–606. http://dx.doi.org/10.1086/222355.
Home Office. (2015). *Draft investigatory powers Bill: Guide to powers and safeguards*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf, 01/09/2016.
Huber, J., & Zwerina, K. (1996). The importance of utility balance in efficient choice designs. *Journal of Marketing Research, 33*(3), 307–317. http://dx.doi.org/10.2307/3152127.
Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.
in 't Veld, S. (2012). Talkin' about a revolution. In J. Bus, M. Crompton, M. Hilderbrandt, & G. Metakides (Eds.), *Digital enlightment yearbook 2012* (pp. 9–17). Amsterdam: IOS press.
Inayatullah, S., & Milojević, I. (2015). Power and the futures of the internet. In J. Winter, & R. Ono (Eds.), *The future Internet: Alternative visions* (pp. 59–73). Cham: Springer International Publishing.
Internet World Stats. (2016). *Internet usage in the European union*. http://www.internetworldstats.com/stats9.htm, 26/12/2016.
ISTR. (2016). *Internet security threat report* (Vol. 21). https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, 13/12/2016.
Johnson, A., & Lucica, E. (2013a). *Sampling report*. http://www.projectpact.eu/deliverables/wp3-fieldwork/d3.2.
Johnson, A., & Lucica, E. (2013b). *Survey technical report*. http://www.projectpact.eu/deliverables/wp3-fieldwork/d3.3.
Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin's studies*. http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf, 28th October 2014.
London Economics. (2010). *Study on the economic benefits of privacy-enhancing technologies (PETs)*. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf, 30/01/2017.
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. http://dx.doi.org/10.1287/isre.1040.0032.
McFadden, D. (1974). Conditional logit analysis of qualitative choice behaviour. In P. Zerembka (Ed.), *Frontiers in econometrics* (pp. 105–142). New York: Academic Press.
Netten, A., Burge, P., Malley, J., Potoglou, D., Towers, A. M., Brazier, J., et al. (2012). Outcomes of social care for adults: Developing a preference-weighted measure. *Health Technology Assessment, 16*(16), 1–165. http://dx.doi.org/10.3310/hta16160.
Nissembaum, H. (2010). *Privacy in context. Technology, policy and the integrity of social life*. Stanford: Standford University Press.
Patil, S., Fuchs, C., Potoglou, D., & Robinson, N. (2013a). A note on PACT's survey. http://www.projectpact.eu/deliverables/wp2-survey-design/d2.4, 25/03/2016.
Patil, S., Hui, L., Patruni, B., Potoglou, D., & Robinson, N. (2012). Report on the analysis of pilot data. http://www.projectpact.eu/deliverables/wp2-survey-design/d2.3, 25/03/2016.
Patil, S., Lu, H., Saunders, C. L., Potoglou, D., & Robinson, N. (2016). Public preferences for electronic health data storage, access, and sharing – evidence from a pan-European survey. *Journal of the American Medical Informatics Association, 23*(6), 1096–1106. http://dx.doi.org/10.1093/jamia/ocw012.
Patil, S., Patruni, B., Potoglou, D., & Robinson, N. (2016). Public preference for data privacy – a pan-European study on metro/train surveillance. *Transportation Research Part A: Policy and Practice, 92*, 145–161. http://dx.doi.org/10.1016/j.tra.2016.08.004.
Patil, S., Robinson, N., & Potoglou, D. (2012). *Knowledge consolidation report*. http://www.projectpact.eu/deliverables/wp2-survey-design/d2.1, 25/03/2016.
Patil, S., Robinson, N., Potoglou, D., Burge, P., & Hellgren, T. (2013b). *Design and survey questionnaire*. http://www.projectpact.eu/deliverables/wp2-survey-design/d2.2, 25/03/2016.
Patruni, B., Lu, H., Patil, S., Robinson, N., Potoglou, D., & Fox, J. (2014). *Headline findings*. http://www.projectpact.eu/deliverables/wp4-data-analysis/d4.1, 25/03/2016.
Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly: Management Information Systems, 35*(4), 977–988.
Pavlou, P., & Chai, L. (2002). What drives electronic commerce across the cultures? A cross-cultural empirical investigation of the theory of planned behavior. *Journal of Electronic Commerce Research, 3*(4), 240–253.
Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.
Politico. (2015). *The Belgian intelligence gap*. http://www.politico.eu/article/two-paris-attackers-were-questioned-freed-this-year-isil-terrorism-attacks/, 15/12/2016.
Potoglou, D., Palacios, J. F., & Feijóo, C. (2015). An integrated latent variable and choice model to explore the role of privacy concern on stated behavioural intentions in e-commerce. *Journal of Choice Modelling, 17*, 10–27. http://dx.doi.org/10.1016/j.jocm.2015.12.002.
Potoglou, D., Patil, S., Gijón, C., Palacios, J., & Feijóo, C. (2013). The value of personal information Online: Results from three stated preference discrete choice experiments. In *The UK. ECIS 2013 completed research* (p. 189). http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1412&context=ecis2013_cr.
Potoglou, D., Robinson, N., Hellgren, T., Kobzar, S., & Patil, S. (2014a). *Literature review of approaches for measuring preferences with respect to privacy, security and surveillance*. http://www.projectpact.eu/privacy-security-research-paper-series/privacy-security-research-paper-series/PACT_ResearchPapers_10_FINAL.pdf, 25/03/2016.
Potoglou, D., Robinson, N., Patil, S., Dunkerley, F., Fox, J., & Lu, H. (2014b). *Privacy, security and Surveillance: New insights into preferences of European citizens*. Available at SSRN: https://ssrn.com/abstract=2418346, 14/03/2017.
Preibusch, S. (2015). Privacy behaviours after snowdon. *Communications of the ACM, 58*(5), 48–55.
Sheldon, P. (2013). Examining gender differences in self-disclosure on Facebook versus face to face. *The Journal of Social Media in Society, 2*(1), 88–105.
Shen, Y., & Pearson, D. (2011). *Privacy enhancing technologies: A review*. http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf, 27/01/2017.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196. http://dx.doi.org/10.2307/249477.
Solove, D. (2010). *Understanding privacy*. Cambridge, MA: Harvard University Press.
Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs, 92*(5), 1079–1105. http://dx.doi.org/10.1111/1468-2346.12706.
Svenonius, O., Bjorklund, F., & Waszkeiwicz, P. (2014). Introduction: Histories of state surveilance in Europe and beyond. In K. Boersma, R. van Brakel, C. Fonio, & P. Wagenaar (Eds.), *Histories of state surveillance in Europe and beyond* (pp. 95–117). New York: Routledge.
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. *T J Comput-Mediat Comm, 19*, 248–273.

http://dx.doi.org/10.1111/jcc4.12052. Journal of Computer-Mediated Communication, 19(2).
The Guardian. (2016). *Paris attacks inquiry finds multiple failings by French intelligence agencies*. https://www.theguardian.com/world/2016/jul/05/paris-attacks-inquiry-multiple-failings-french-intelligence-agencies, 15/12/2016.
Thierer, A. (2013). The pursuit of privacy in a where information control is failing. *Harvard Journal of Law and Public Policy, 36*(2), 409–455.
Train, K. (2003). *Discrete choice with simulations*. Cambridge: Cambridge University Press.
Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2010). The effect of online privacy information on purchasing Behavior: An experimental study. *Information Systems Research, 22*(2), 254–268. http://dx.doi.org/10.1287/isre.1090.0260.
Viney, R., Lancsar, E., & Louviere, J. J. (2002). Discrete choice experiments to measure consumer preferences for health and healthcare. *Expert Reviews of Pharmaeconomics and Outcomes, 2*(4), 89–96. http://dx.doi.org/10.1586/14737167.2.4.319.
Waldron, J. (2003). Security and Liberty: The Image of Balance. *Journal of Political Philosophy, 11*(2), 191–210. http://dx.doi.org/10.1111/1467-9760.00174.
Završnik, A. (2013). Blurring the line between law enforcement and Intelligence: Sharpening the gaze of surveillance? *Journal of Contemporary European Research, 9*(1), 182–202.
Zulman, D. M., Kirch, M., Zheng, K., & An, L. C. (2011). Trust in the Internet as a health resource among older adults: Analysis of data from a nationally representative survey. *Journal of Medical Internet Research, 13*(1), e19. http://dx.doi.org/10.2196/jmir.1552.