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