View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by CURVE/open

# Aligning security and privacy: The case of Deep Packet Inspection

SARA DEGLI ESPOSTI, VINCENZO PAVONE AND ELVIRA SANTIAGO-GÓMEZ

**Published PDF deposited in Coventry University Repository**

**Original citation:**
Degli Esposti, S; Pavone, V. and Santiago-Gomez, E. (2017) Aligning security and privacy: The case of Deep Packet Inspection. In *Surveillance, Privacy and Security: Citizens' Perspectives,* Michael Friedewald, J. Peter Burgess, Johann Čas, Rocco Bellanova, Walter Peissl (eds), 71-90.

https://www.taylorfrancis.com/books/e/9781317213543

E ISBN: 9781317213543

Routledge

CC BY-NC-ND

**Copyright © and Moral Rights are retained by the author(s) and/ or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This item cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder(s). The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders**.

# 4 Aligning security and privacy

## The case of Deep Packet Inspection

*Sara Degli Esposti, Vincenzo Pavone and Elvira Santiago-Gómez*

## Introduction

When surveillance functionalities are embedded into security tools and systems the risk of facing a backlash, due to widespread privacy concerns, may increase dramatically. Speed enforcement cameras, for instance, have produced strong resistance in the UK since 2001 (Wells and Wills, 2009). By the same token, in 2008 the prospect of deploying body scanners in EU airports raised serious public concerns and produced strong public opposition (Bellanova and González Fuster, 2013). As explored by van den Broek *et al.* in this volume, on the one hand, individual privacy concerns may contribute to increase public resistance to surveillance technologies; on the other hand, the perceived trustworthiness of the institutions, or entities, in charge of managing the surveillance system may contribute to decrease public resistance. However, many other factors may also play a role. Thus, at the time of deploying a new surveillance-based security measure, it is hard for developers and product designers to imagine all end-users' reactions and to foresee the kind of concerns the technology will eventually trigger.

Understanding the reasons behind, and the manifestations of, public resistance to surveillance technologies is certainly a complex task. Resistance to surveillance technologies may produce a wide range of public reactions, from simple avoidance to active opposition (Marx, 2003). Cultural, historical, and sociological factors may also influence both public perceptions and privacy and security attitudes (Pavone and Degli Esposti, 2012). Resistance to surveillance is also often based on existing knowledge about technologies (Ball, 2002), which implies that people's educational level and the degree of familiarity with the technology may also contribute to orient public opinion. As pointed out by van den Broek *et al.* in this volume, citizens' political opinions may also play a role in the context of a political demonstration.

Finally, the prevailing tendency to frame privacy and security as antagonistic values in security policy discourses, as pointed out by Strauß in this volume, have also prevented the academic community from achieving a deeper understanding of individual privacy concerns, security attitudes and public resistance to surveillance. To overcome these limitations, the SurPRISE Project was designed to challenge the privacy–security trade-off framework by empirically investigating factors influencing public attitudes toward surveillance technologies, in line with previous exploratory studies (Pavone and Degli Esposti, 2012).

This chapter aims at shedding light on the complex phenomenon represented by public resistance to, or acceptance of, surveillance technologies used to ensure human security, by offering insights on a particular surveillance technology, which is Deep Packet Inspection (DPI). We rely on both quantitative data gathered in six European countries and qualitative data gathered in the UK to draw our conclusions. Based on the analysis of the data, we offer evidence of the detrimental effects that a technology's perceived degree of intrusiveness exercises on a technology's perceived effectiveness. In other words, we find empirical support for the claim that security and privacy, being part of a broader concept of human security, are compatible rather than antagonistic dimensions. In addition, we offer preliminary evidence of the negative effects caused by the adoption of blanket-surveillance security strategies on end-users' perceptions.

## Digital surveillance, individual privacy concerns and technological acceptance

For a long time, dominant interpretations of opinion pool data on individuals' privacy concerns have led the academic community to believe in the existence of a *privacy paradox*, which can be summarized in a simple statement: 'despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances' (Smith *et al.*, 2011, 993). However, recent studies have challenged this interpretation and questioned the assumption that people adopt a cost-benefit approach when it comes to privacy risky data sharing decisions (Turow *et al.*, 2015).

Frequently users do not fully understand they are sharing their personal data for free services and apps. Often users feel they have no choice but sharing their data and, as a result, they feel resigned (Turow *et al.*, 2015). Many people tend to believe that the regulatory system in place protects their right to privacy and intimacy (Hoofnagle and Urban, 2014), even in the absence of their active mobilization, as it happens in the case of food labelling or medical treatments. Very often people inaccurately believe that the law protects them from third-party data sharing activities (Hoofnagle and Urban, 2014). In the case of location apps, users are also often unaware of the monitoring functions embedded into the same device. When users become aware of the data processing functionalities of mobile apps they might feel betrayed and, as a result, outraged (Shklovski *et al.*, 2014, Xu *et al.*, 2011). This might be the reason why, when confronted with the prospect of losing control over their personal data, the vast majority of users of online services express their concerns. For instance, as reported by van den Broek *et al.* within this volume, lay people consider especially unacceptable that Internet Service Providers (ISPs) sell customer data. Therefore, the *privacy paradox* (Acquisti, 2010) not only appears to be an interpretation far too simplistic, unable to map the complex set of emotions generated by modern digital surveillance practices (Shklovski *et al.*, 2014), but it also shifts the responsibility of data and privacy protection to individual citizens, away from the corresponding public authorities.

When lay people discover dataveillance (Degli Esposti, 2014; Clarke, 1988), they tend to react in a negative way. Sometimes, they perceive digital surveillance as something inevitable, an intrinsic part of the digital revolution; as a consequence they feel resigned and tend to succumb to it just because they do not want to miss the relational and job opportunities the Web offers (Turow *et al.*, 2015). Without these opportunities, many individuals, and especially the 'digital natives', are likely to feel unable to achieve full integration in our society. A minority of people, nonetheless, try to avoid, evade or circumvent surveillance by adopting different strategies, from the intentional provision of inaccurate information, to the adoption of anonymization and privacy-preserving tools.

Recent scandals showing the ability of governments and private firms to constantly monitor citizens and consumers have exacerbated the situation making people feel even more powerless, vulnerable and exposed (Ball, 2009). From an organizational perspective, mass surveillance has become so cheap, and its applications so numerous, that it is just easier to find arguments to justify its adoption, and contribute to its proliferation, than to question it (Hoofnagle *et al.*, 2012). Digital technologies have transformed surveillance performed by security agencies from a time-consuming and expensive practice into a technological routine so convenient that the asymmetry of power between citizens and the State has increased dramatically (Bankston and Soltani, 2014).

Within this scenario, it becomes especially urgent and necessary to renew current efforts to analytically explore how citizens interpret surveillance-oriented security technologies (SOSTs), i.e. those technologies that are being introduced in order to improve human, public or national security, and what, in the common pursuit of higher security, they expect from these technologies. If living in a surveillance society (Murakami Wood, 2009) might generate a sentiment of resignation and a sort of passive behaviour, we should nonetheless distinguish between those who actually support the adoption of certain surveillance measures, from those who are not happy with these solutions, but have not been able to demonstrate their dissent yet. Moreover, in current times characterized by a growing mistrust towards security agencies and public institutions (Gandy, 1989, Verble, 2014), understanding and rethinking the relationship between privacy, security and surveillance becomes extremely important for the future of democratic societies (Bauman *et al.*, 2014).

To shed light on these issues, this chapter focuses specifically on public perceptions of Deep Packet Inspection (DPI), and relies on both qualitative and quantitative data to investigate the complex articulation of arguments, factors and priorities influencing citizens' acceptance of surveillance measures used for security purposes.

## The distinction between public acceptance and acceptability of DPI

Within this study, we use quantitative data to study those factors influencing *public acceptance of DPI*, while we tried to use qualitative data to explore *public acceptability of DPI*. Unfortunately, within this study we could not gather enough qualitative data to fully explore the issue of public acceptability of DPI. Nevertheless, some considerations regarding this topic are included in the next section and a clear conceptual distinction between acceptance and acceptability is provided in the next paragraphs.

In order to clarify our terminology, a clear distinction between public acceptance and acceptability of technology needs to be made. We consider that a technology is accepted (i.e. *public acceptance of technology*) when it is received neutrally, or favourably, and the population of the region, or country, where the measure is adopted not only does not engage in any form of collective, or individual, action meant to create disruptions to the deployment and implementation of the technology by complaining, protesting, refusing to use the solution or opposing it in any way, but actively supports its deployment. According to this definition public acceptance is the opposite of public resistance.

In contrast, we say that a technology is acceptable (i.e. *public acceptability of technology*) when it has the potential of being endured, because the measure is tolerable, adequate and conforms to approved societal or ethical standards. While technological acceptability represents a forward-looking concept which entails some ethical criteria, which help us judge the appropriateness, or legitimacy, of a technology, acceptance is a backward-looking idea and can only be used to assess the extent to which a technology, which has been already adopted in a certain social and cultural context, has triggered public opposition or acquaintance.

Although in policy documents (EC, 2012), and in the academic literature (Siegrist, 2008, Venkatesh *et al.*, 2003), the construct most widely used is public acceptance, the idea of acceptability deserves to be further investigated as it may help identify controversial aspects of technologies in phase of design and as it may suggest criteria or guidelines for improving the design and management of technological systems. Nonetheless, we expect that technologies which are considered *acceptable* by the public are also technologies *accepted* by the public. Although acceptance and acceptability are two interrelated ideas, public acceptance does not necessarily imply acceptability from a legal or human rights perspective. Surveillance technologies may enjoy high public acceptance but still run contrary to established human rights, or national constitutional principles, or to existing regulation. Sometimes public acceptance can be the result of repression, lack of freedom of expression or simple inertia or lack of information.

Finally, we should remember that security technologies differ from consumer technologies because they are used to monitor and protect the public, but they are not chosen or operated by the public. In the case of security technologies, which are not chosen by citizens, but by security agencies and public authorities, we consider that the study of SOSTs' acceptability is especially important and should be developed further in future empirical studies. Although SOSTs are used to protect citizens and to prevent, or respond to, security threats, citizens are not involved in the design and selection of security measures. This lack of participation in the decision-making process reduces drastically the impact of public opinion on the development of security technologies. By better understanding the criteria lay people use to assess the acceptability of SOSTs, scholars could help governments and security agencies develop more sensible solutions (Hess, 2014).

## The data collection

Data presented in this chapter were gathered as part of the SurPRISE project, funded by the *Seventh Framework Programme for Research and Innovation*, between January and March 2014, during 12 citizen summits held in nine European countries, involving approximately 200 citizens per country. The SurPRISE citizen summits were full-day events. Participants received information before and during the event, discussed topics related to specific SOSTs in small groups of six to eight persons, and filled in an electronic questionnaire along the day. As concluding activity each group of citizens was asked to formulate recommendations for policymakers to be used. Summit participants had also the chance to write their thoughts on individual postcards, and participants' opinions were also annotated by table moderators and note takers. More information on the SurPRISE citizen summit methodology can be found in previous publications (Degli Esposti and Santiago-Gómez, 2015).

During each summit two out of three specific SOSTs were discussed. These SOSTs were: Smart CCTV, Deep Packet Inspection (DPI), and smartphone location tracking. Within this chapter we will rely on evidence related to the case of DPI. Qualitative data used in this chapter were gathered during the citizen summits held in England. In contrast, quantitative data here analysed come from six EU countries, which are Austria (sample size n = 220), Italy (n = 180), Norway (n = 113), Spain (n = 163), Switzerland (n = 204) and the UK (n = 244).

## Deep Packet Inspection

Given the importance of digital communications, interactions and relations, this article focuses on lay people's opinions of a specific surveillance technology, which is Deep Packet Inspection (DPI). DPI is a type of data processing that looks in detail at the contents of the data being sent. On the Internet, any information sent or received is collected into *packets*, which have a label on them called a *header* that describes what these packets are, who sent them, and where they are going: just like a letter flowing through a postal network. DPI is a method of *packet* filtering which allows examining the content of a packet rather than simply read its header by deeply analysing packet contents, including information from all seven layers of the *Open Systems Interconnection* (OSI) model. As DPI makes it possible to find, identify, classify, reroute or block packets with specific data or code payloads, it has been compared to a postman opening one's letters and reading their contents (SurPRISE, 2014).

As many ICT technologies, DPI has several applications. Internet service providers (ISP) can use DPI to allocate available resources to streamline traffic flow, or to apply different charging policies, traffic shaping, or offer quality of service guarantees to selected users or applications (Antonello *et al.*, 2012). DPI has been used by major network operators in the U.S. and Canada to block or restrict the speed of peer-to-peer file sharing traffic by their customers (Mueller and Asghari, 2012). In enterprises, it is used to ensure network security, and to support quality of service and terms of use, copyright enforcement, target marketing and behavioural advertising to online customers (Corwin, 2011). DPI represents a basic component of network security as it combines techniques such as protocol anomaly detection and signature scanning, traditionally available in anti-virus solutions (Anderson, 2007).

DPI is also used in the fight against major crimes such as child pornography, transnational organized crime and terrorism (Person, 2010). However, DPI has been also used by Libyan and Syrian Governments to spy and capture rebels, and it is used by the Chinese Government as a censorship tool (Fuchs, 2013). The Snowden's revelations also demonstrated that DPI has been used by the NSA to spy on both citizens and public authorities of several countries around the world (Lyon, 2014). It is important to consider that, by the time the citizen summits took place, DPI had begun to receive remarkable media attention, due to the NSA scandal and Snowden's revelations. For this reason, most users were aware of the existence of this technology.

## Summit participants' perceptions of Deep Packet Inspection

Citizen summit participants had the chance to learn about DPI before and during the events. They received a booklet before the event and watched a short documentary film on DPI during the event which helped them understand this specific technology. Most citizens in all the six countries where DPI was discussed were confident about their understanding of DPI functions and operations. Moreover, in all countries except the UK, more than half of the participants said to be fairly knowledgeable about the way DPI was used.

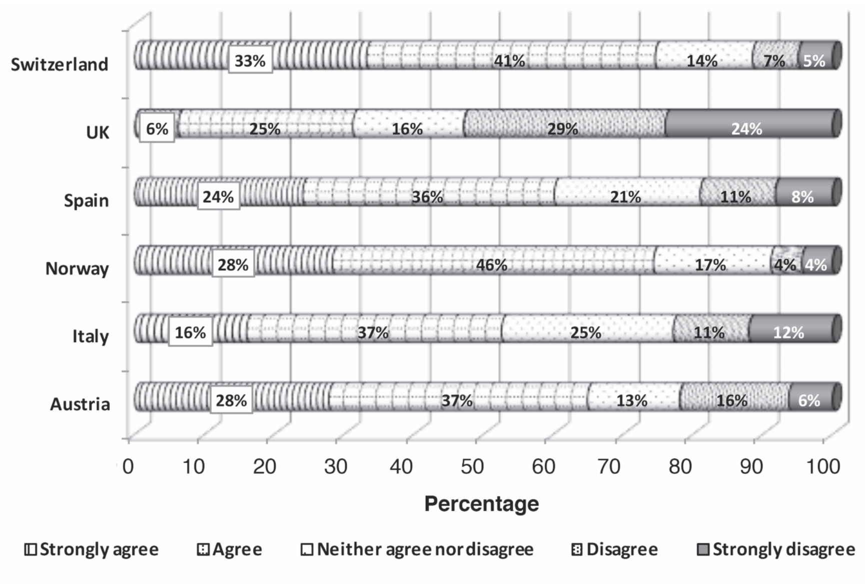

*Figure 4.1* Agreement with the statement 'I understand what DPI is'

Although British participants had some doubts about the functioning of DPI, they were able, nonetheless, to engage with the topic and discuss its advantages and drawbacks. As reported in the following quote, extracted from one table discussion, DPI was considered to have useful security applications, though also to be problematic in terms of regulation and accountability.

> *F4*: Overall it was felt that DPI would be useful against cyberbullying, child pornography, terrorist attacks and other security related issues. However, it's hard to regulate who uses this information and for what purposes and international agreement on how to regulate this seems impossible.
>
> (Table moderator's reflections)

Nearly half of the participants in all countries considered DPI an effective national security tool, even though regulatory instruments were considered in general insufficient to tackle the problem of preventing inappropriate uses of DPI. As shown in Table 4.1, only 19 per cent of respondents agreed with the statement 'laws and regulations ensure that DPI is not misused'. As expressed in the following statement made by a citizen participant, the main problem is that Internet users rely on services offered by organizations subject to different laws and regulations from the ones enforced in the user' country.

> *AbB30-C5*: National security. I'm happy to have it but it needs more control. How do I get junk mail when I don't give people my details? I noticed a difference when I started using Yahoo mail. Because of today I know this is because of the lack of rules or different rules in America.

Nevertheless, laws, regulations and legal procedures are interpreted by the public as a possible solution to ensure the correct adoption of SOSTs. As reported in the following statements, legal guarantees contribute to set standards for the acceptable use of SOSTs.

> *AbB11-C5*: There should have to be a warrant to hack into my email, a criminal investigation reason for it.
>
> *AbB28-C5*: None but there should be regulations about it to protect us.

Despite the fact that DPI was considered useful in improving national security by almost half of the participants (48 per cent), two third of them said DPI was nevertheless highly intrusive (71 per cent). Figure 4.2 highlights the difference between the perceptions of British and Austrian participants on the matter. A higher proportion of British respondents considered DPI an effective security measure (UK: 58 per cent; Austria: 28 per cent), while a higher proportion of Austrian people considered DPI intrusive (Austria 56 per cent; UK: 16 per cent). For a more in-depth discussion on the effect of culture on privacy and security attitudes see Budak, Rajh and Recher within this volume.

By looking at the data collected during the citizen summits, we can see that DPI

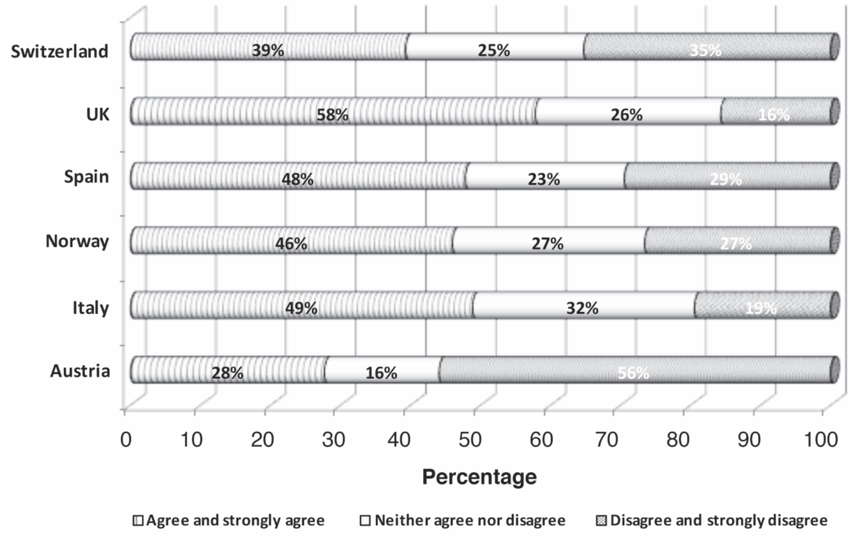

*Figure 4.2* Agreement with the statement 'In my opinion, DPI is an effective national security tool'

*Table 4.1* Level of agreement with each statement

| | *DPI* | | *sCCTV* | | *SLT* | |
|---|---|---|---|---|---|---|
| | *Freq.* | *Per cent* | *Freq.* | *Per cent* | *Freq.* | *Per cent* |
| 1. Laws and regulations ensure that DPI is not misused | 195 | 19% | 260 | 24% | 278 | 28% |
| 2. I believe that DPI improves national security | 507 | 48% | 645 | 59% | 505 | 51% |
| 3. I believe that DPI is intrusive | 750 | 71% | 553 | 51% | 549 | 55% |
| 4. I think that the level of intrusiveness is acceptable given the benefits DPI offers | 372 | 35% | 517 | 48% | 483 | 49% |
| 5. None of the above | 22 | 2% | 28 | 3% | 25 | 2% |
| 6. DK/NA | 13 | 1% | 12 | 1% | 9 | 1% |
| Total number of respondents | 1050 | | 1087 | | 994 | |

was perceived to be the most intrusive measure (71 per cent), more than smart CCTV (51 per cent) or smartphone location tracking (55 per cent). One of the reasons behind this difference in perceptions is that people feel to have no control over the way Internet is governed and managed. We quote the following conversation as an evidence of this assertion.

> *AbB34-C5*: Of the two, DPI and Smart CCTV, I prefer the Smart CCTV. More control over that. Nearly everyone in this room uses the Internet and we have no control over it.
> *AbB35-C1*: There will be terms and conditions on websites.
> *AbB36-C5*: But nobody reads them and it's not enough. I think there should be a section for our own terms and conditions. No control.

At the time of balancing intrusiveness against effectiveness of DPI, only one-third of participants considered the level of intrusiveness of DPI acceptable (35 per cent). In contrast, nearly half of the participants said to consider the intrusiveness of smart CCTV (48 per cent), and smartphone location tracking (49 per cent), reasonable given the benefits these technologies offer. This variation may be explained by the fact that people tend to perceive the Internet as a private space, rather than as a public space. The fact that the activity is performed while people are at home, or at work, which are considered intimate spaces, wherein confidentiality is safeguarded, may generate some confusion and make people underestimate the risks of being online. The following reflection made by a note taker and the statement made by a study participant offer some insights into some lay people's perceptions on the matter.

> *RhBSum*: Interestingly, they saw a big difference between the privacy concerns with smart CCTV and DPI. They felt that when you are outside the house, you must expect to be watched by others. However, inside the house and online, people feel as though their actions are private and personal.
>
> (Note taker's reflections)

> *AbB9-C5*: I was naïve to think until today that some of my information on the Internet was private and now I know I can be hacked. This conference has made me realise. I can be compromised financially. There is no control.

Digital communications are also expected to resemble analog communications; which are characterized by attributes such as mail correspondence confidentiality. Because of these expectations, participants tended to perceive DPI as a more deceptive, subtle and invasive measure than the other technologies analysed. Compared to smart CCTV systems, which are positioned in public places, DPI operates in what are considered private spaces during activities, such as surfing the net or sending emails, that are also perceived as private (Degli Esposti and Santiago-Gómez, 2015). As any automated digital system, DPI goes also virtually undetected by users when it is used to spy on people.

> *F4*: [DPI] It's an unseen invasion of privacy, worse than CCTV because it is more personal (online banking, etc.) and open to fraud. There is very little public awareness. Worries were expressed about government covering up the use and purposes of DPI. Overall the pros do not outweigh the cons.
>
> (Table moderator's reflections)

The lack of transparency on the use and purpose of DPI generated a feeling of frustration and resignation among participants, as pointed out in other studies (Turow *et al.*, 2015). While the use of CCTV systems is advertised in public spaces, no information about when, how, and by whom DPI is operated is made available while users are surfing the Web. Even smartphone location tracking was perceived more favourably. Thus, DPI raises more concerns and generates negative reactions even among British participants, who were on average the more willing to support the adoption of surveillance measures.

> 'I don't know what I will do. I'm paranoid even though I do nothing wrong'.
> 'It is out of our hands, there is nothing we can do'.
> 'The majority will just have to accept it if they want to use the Internet'.
> 'Up until now, I didn't realize they monitor our Internet'.
> (Statements made by participants and reported by Note Taker no. R01)

These perceptions are exacerbated by the fact that everyone goes online (see Figure 4.3). The large majority of participants said they use the Internet 'all of the time' (minimum 39 per cent in Italy; maximum 70 per cent in the UK). In other terms, the Web is now a space of social and economic interaction which is constitutive of everyday life. It is increasingly difficult to try to live offline. This is an important consideration, because it implies that any problem produced by technologies that intrude our privacy and human rights in cyberspace can no longer be simply dismissed as something that can be solved by 'not going online'.

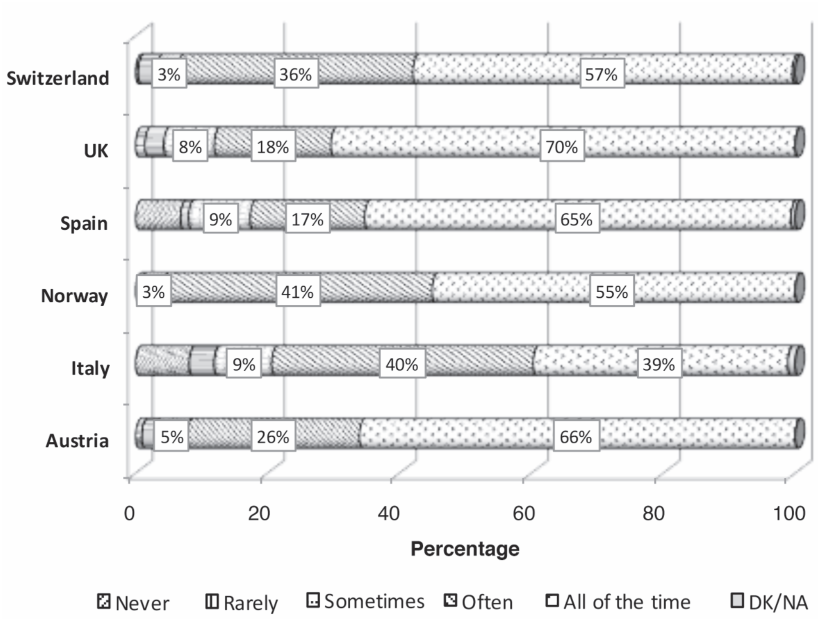

*Figure 4.3* Distribution of answers to the question 'How often do you use the internet?'

Within this context, it is worth noticing that almost two-thirds of EU households have Internet access at home and that nowadays people are more likely to access the Internet through a combination of both home and mobile phone connections (EC, 2014); these considerations help us understand the extent to which Europeans are constantly exposed to the risk of Internet surveillance. As a result, the majority of participants in five countries out of six said to worry about Internet security, while most Hungarians were indecisive or not concerned (see Figure 4.4).

The rise in the number of activities performed on the Web makes it difficult for people to simply avoid the digital space as they would avoid going to a certain neighbourhood or to any other geographical space. Nonetheless only a small proportion of people (22 per cent) declared to be absolutely sure they were not willing to change their behaviour because of DPI, while a largest proportion of people said that, in principle, they would not change their online behaviour because of DPI (40 per cent). On the other hand, one-third of respondents were said to be willing to act in a different way when they were online (31 per cent), and some participants said they would even avoid going online (6 per cent). See results displayed in Figure 4.5.

Becoming aware of DPI and concerned about it, however, do not constitute *per se* sufficient conditions for people to actively oppose, or avoid, technologies such as DPI. As shown in Figure 4.6, obtaining more information on how to protect one's privacy is the top priority for the majority of participants (55 per cent). Only a small proportion of respondents would be willing to actively resist DPI (10 per cent), campaign against it (11 per cent), or support those who protest against its use

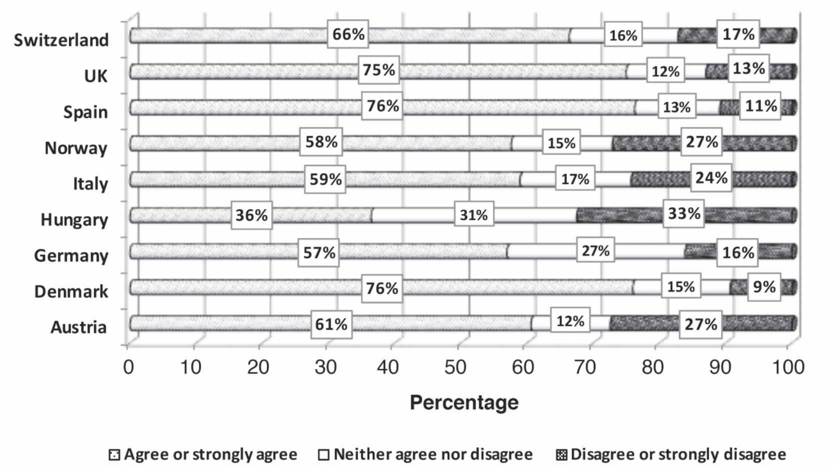

*Figure 4.4* Level of agreement with the statement 'I worry about security when I am online'

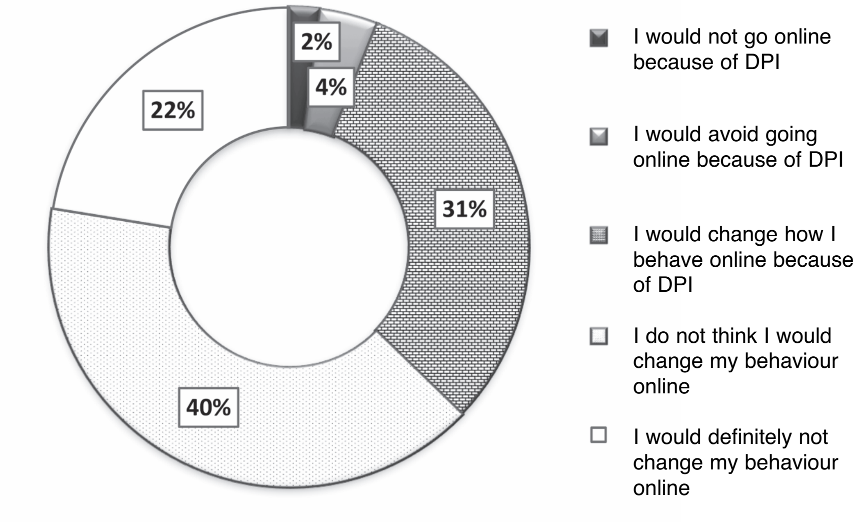

*Figure 4.5* Active avoidance of DPI

(13 per cent). The most likely form of resistance would probably be enacted through individual actions on personal digital devices (Lyon, 2007).

When it comes to the topic of the adoption of DPI as a national security measure, as shown in Figure 4.7, the public is divided between those who are in favour (46 per cent), those who are against it (34 per cent), and those who are undecided (19 per cent).

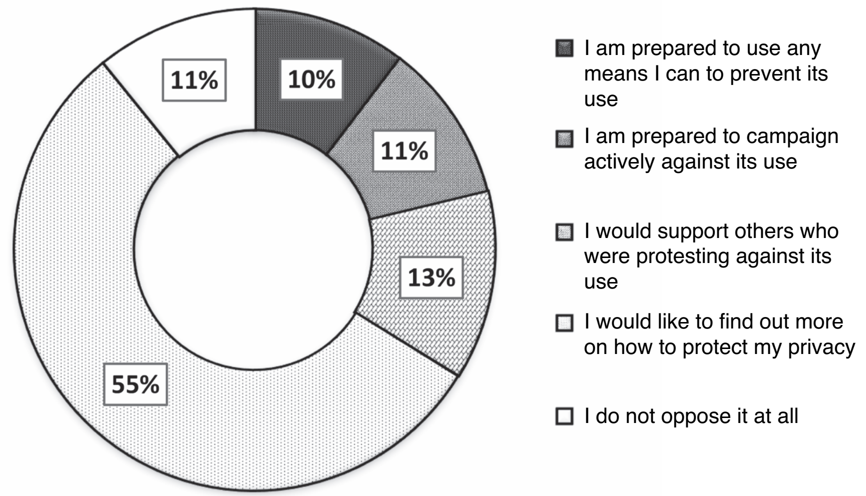

*Figure 4.6* Challenging the use of DPI for security purposes

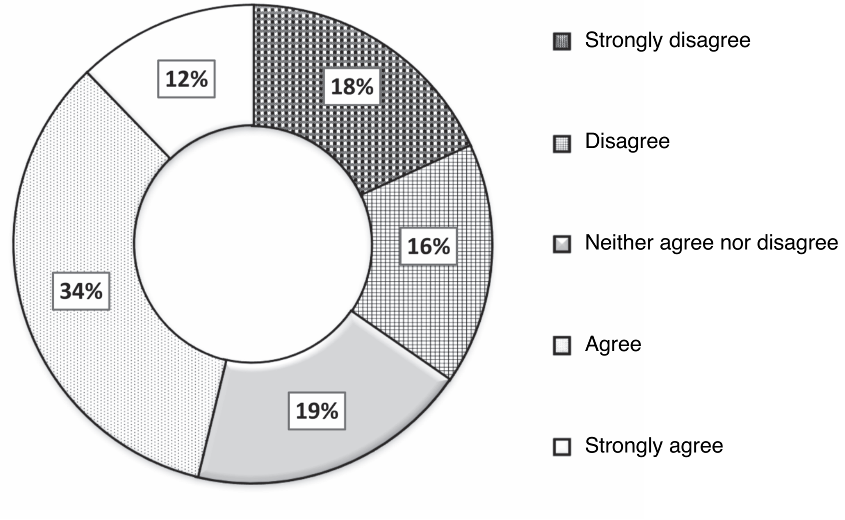

*Figure 4.7* Agreement with the statement 'Overall I support the adoption of Deep Packet Inspection as a national security measure'

To conclude, DPI can be considered a very ambiguous technology: Internet users recognise its benefits in the security area, but they are also concerned about online surveillance. For this reason, as shown in Figure 4.5, they would like to know more about how to protect their privacy online and would welcome more effective regulation on the matter. Nonetheless they do not succumb to the chilling effect (Askin, 1972) and tend to refuse to change the way they behave online because of DPI. The lack of information, knowledge and transparency contribute to the emergence of an apparently static scenario, which is characterized by frustrated users who are concerned about their privacy and feel powerless and resigned. As a result, considering that most of the times citizens are monitored by SOSTs without having a chance to opt out, assessing SOSTs' acceptability in advance becomes absolutely necessary. In fact, more qualitative studies are necessary to study under which conditions, and for what purposes, the use of technologies like DPI can be considered acceptable by the citizens. As previously said, we could not investigate DPI acceptability in depth because of limitations in the qualitative data gathered, so in the next section we move to explore and discuss factors influencing public acceptance of DPI.

## Factors influencing public acceptance of DPI

Within this section we analyse survey data gathered during the citizen summits. The aim is to investigate factors influencing public acceptance of DPI. We use the statement 'Overall I support the adoption of Deep Packet Inspection as a national security measure' to measure the dependent variable. We have taken into consideration the following independent variables:

- DPI's perceived effectiveness (EFF);
- DPI's perceived intrusiveness (INT);
- Social proximity (SPRO);
- Privacy risks (RISK);
- Security operators' degree of trustworthiness (THR).

Each independent variable has been measured with one or more questionnaire item. Exact formulation of the questions is reported in Table 4.2.

We have used median regression (Koenker and Bassett, 1978) to test the effect of the independent variables on public acceptance of DPI. Most notably, the outcomes show how DPI's perceived effectiveness and system operators' trustworthiness play a relevant positive role in determining public acceptance. The fact that DPI is used only to investigate criminal activity also increases the chances of supporting the use of DPI. In contrast, the fact that DPI is perceived to intrude into a person's life, and that it entails risks due to errors, such as misinterpretation of one's behaviour, decreases the likelihood of supporting its adoption. In other words, the perceived effectiveness of DPI in contributing to the fight against terrorism and other major crimes, contributes positively to the acceptance of DPI. However, and for the same reason, the perceived intrusiveness of the technology produces concern and rejection. In between these two basic relations, there exist other variables that also influence acceptance in one way or another. For instance, the trustworthiness of public authorities using DPI contributes positively to the acceptance of DPI, and so does the perception that DPI is being used against specific crimes, like child pornography and terrorism, and against a specific human target, i.e. criminals and suspects (SPRO). Conversely, the perceived risk of abuse, or misuse, negatively influences the acceptance of DPI.

*Table 4.2* Questions measuring perceived effectiveness, intrusiveness, social proximity, trustworthiness and various privacy risks

| *I. V.* | *Questionnaire item* |
|---|---|
| EFF1 | In my opinion, DPI is an effective national security tool |
| EFF2 | When I am online, I feel more secure because DPI is used |
| EFF3 | DPI is an appropriate way to address national security threats |
| INT1 | The idea of DPI makes me feel uncomfortable |
| INT2 | I feel DPI is forced upon me without my permission |
| SPRO | DPI does not bother me as long as it only targets criminals |
| RISK1 | DPI worries me because it could reveal sensitive information about me |
| RISK2 | DPI worries me because it could result in my behaviour being misinterpreted |
| RISK3 | DPI worries me because it could reveal the content of my communications |
| RISK4 | DPI worries me because it could violate my fundamental human rights |
| TRU1 | Security agencies which use DPI are trustworthy |

*Table 4.3* Median regression

| [D.V.] ACC1: 'Overall I support the adoption of Deep Packet Inspection as a national security measure' | *Coef.* | *Std. Err.* | *t* | *P>t* | *[95% Conf. Interval]* | |
|---|---|---|---|---|---|---|
| EFF1: 'In my opinion, DPI is an effective national security tool' | .465 | .034 | 13.65 | 0.000 | .398 | .532 |
| INT2: 'I feel DPI is forced upon me without my permission' | –.132 | .042 | –3.12 | 0.002 | –.215 | –.049 |
| SPRO: 'DPI does not bother me as long as it only targets criminals' | .153 | .029 | 5.26 | 0.000 | .096 | .210 |
| RISK2: 'DPI worries me because it could result in my behaviour being misinterpreted' | –.083 | .036 | –2.32 | 0.021 | –.154 | –.013 |
| TRU1: 'Security agencies which use DPI are trustworthy' | .305 | .035 | 8.82 | 0.000 | .237 | .373 |
| Constant | .597 | .168 | 3.54 | 0.000 | .266 | .928 |

Notes: Number of observations = 864
Pseudo R2 = 0.3574

Apart from studying the direct relationship between the independent variables and the dependent variable, we have also studied relationships among independent variables listed in Table 4.2, in order to explore whether they influence each other and in what ways. In doing this, we have used a non-parametric statistical technique called Kendall's rank correlation (Kendall, 1970), which provides a distribution free test of independence and a measure of the strength of dependence between two variables.

By looking at rank correlation coefficients, four major results emerge. First, and contrary to what one would expect, perceived intrusiveness and perceived effectiveness are negatively related. We had imagined that DPI would be considered effective precisely as a result of its intrusiveness. In contrast, people who perceive DPI as highly intrusive are less willing to consider the technology to be effective, probably because they do consider that DPI is more effective when it is used to tackle specific crimes, and not when it is implemented as part of a massive surveillance strategy. As a matter of fact, and this is the second confirmed result, if DPI were used just to monitor and investigate criminal activity, rather than being used to screen the communications of all online users, summit participants would be more inclined to consider DPI as an appropriate security measure. Third, it is precisely the privacy risks associated with DPI, such as misinterpretation of users' online behaviour, human right violation, and unauthorized disclosure of confidential communications that make people consider DPI as highly intrusive. Finally, the fact that security agents who manage DPI are considered to be trustworthy by citizens plays an important role not only vis-à-vis its acceptance, but also in relation to its perceived intrusiveness. Agents' trustworthiness contributes to both increase

*Table 4.4* Kendall's rank correlation

| | *EFF1* | *EFF2* | *EFF3* | *INT1* | *INT2* | *SPRO* | *RISK1* | *RISK2* | *RISK3* | *RISK4* | *TRU1* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *EFF1* | 0.774 | | | | | | | | | | |
| *EFF2* | 0.279★ | 0.725 | | | | | | | | | |
| *EFF3* | 0.445★ | 0.344★ | 0.776 | | | | | | | | |
| *INT1* | –0.279★ | –0.300★ | –0.291★ | 0.730 | | | | | | | |
| *INT2* | –0.142★ | –0.200★ | –0.169★ | 0.269★ | 0.518 | | | | | | |
| *SPRO* | 0.281★ | 0.244★ | 0.326★ | –0.224★ | –0.104★ | 0.782 | | | | | |
| *RISK1* | –0.154★ | –0.179★ | –0.191★ | 0.258★ | 0.187★ | –0.138★ | 0.642 | | | | |
| *RISK2* | –0.136★ | –0.143★ | –0.181★ | 0.208★ | 0.144★ | –0.102★ | 0.245★ | 0.668 | | | |
| *RISK3* | –0.157★ | –0.191★ | –0.192★ | 0.272★ | 0.193★ | –0.131★ | 0.342★ | 0.264★ | 0.628 | | |
| *RISK4* | –0.180★ | –0.194★ | –0.226★ | 0.237★ | 0.187★ | –0.126★ | 0.273★ | 0.287★ | 0.331★ | 0.631 | |
| *TRU1* | 0.233★ | 0.210★ | 0.257★ | –0.221★ | –0.148★ | 0.257★ | –0.211★ | –0.159★ | –0.178★ | –0.185★ | 0.765 |

Note: ★ Significance level 1%

the likelihood of accepting DPI and of reducing its perceived privacy risks and, thus, its perceived intrusiveness.

## Discussion and conclusion

Surveillance-based security measures are conceived and designed to fight crime and reduce violence. Despite this legitimate purpose, these technologies bring new risk of human rights infringement, or potential negative consequences for citizens, which have to be taken into consideration at the time of assessing these solutions. Human rights risks and potential externalities can be reduced by means of organizational and procedural measures, and through the investigation of public perceptions and understanding of these measures.

Drawing from the quantitative data proceeding from 12 citizen summits, and from the qualitative data proceeding from the UK citizen summit, this study has explored the topic of public acceptance of Deep Packet Inspection (DPI). According to our results, study participants express deep concerns about the widespread use of DPI by security agencies, but, at the same time, acknowledge the potential contribution of DPI in the fight against major crimes. In general, DPI is considered a very intrusive technology, especially because it operates in what it is perceived to be a private space. The lack of transparency and information on the use of DPI on the Internet contribute to transform DPI in the least accepted technology among the SOSTs assessed during the Surprise citizen summits. Although the perceived trustworthiness of security operators, and the perceived effectiveness of DPI, contributes positively to increase its acceptance, the risk of abuse, or misuse, makes it a very controversial technology. This is an especially relevant issue, because DPI operates on the Web, where people perform most of their activities and communications nowadays. However, online users enjoy their freedom on the Web and are not willing to give up their rights to free expression and self-determination because of the potential chilling effect produced by technologies like DPI.

The more citizens become aware of the existence of online surveillance, the more likely they are to realize that they need to know much more about how to protect their privacy online. The complexity of the situation people face – on one side the need to be online, and on the other one, a certain feeling of frustration, or resignation, generated by the perceived lack of knowledge and control over digital technologies and personal data – is misleadingly described by the so-called 'privacy paradox'.

On the base of our analysis we argue that technology assessment, especially in the security area, needs to go beyond cost-benefit analysis and take into consideration the interplay between technological attributes, such as accuracy and effectiveness, and non-technological considerations related to system operators' level of competence and integrity. Technological systems, in fact, operate always within specific socio-cultural contexts and the characteristics of the context influence not only the way technology is operated and regulated, but also the way it is perceived and judged. This is why the societal knowledge offered and used by study participants should not be neglected: their concerns often reflect the reality of specific socio-cultural contexts, wherein the technology is implemented and regulated. When assessing a technology social, economic, and institutional features are crucial to properly assess the impact and benefits of a given technology. For instance, in the view of the citizens participating in this study, DPI is intrusive as much as it is effective: to the contrary, the degree of intrusiveness of this technology is considered an indicator of its lack of effectiveness. A more focused, and therefore less intrusive, use of interception of Internet traffic would make citizens perceive the latter as more effective.

In many ways, these considerations suggest that the trade-off between privacy and security is, in fact, a false one. The right to the integrity of our communications, relations and information is a key element of human security, and citizens consider it as important as the right to physical integrity and protection from violence. This understanding of security, which involves both digital security and physical security, suggests that framing our right to the integrity of our communication, relations and personal information as 'privacy' in opposition to 'security' is effectively diverting attention from the fact that governments are giving priority to the protection of physical security at the expenses of other, equally fundamental, elements of human security. Moreover, the approach prevents public scrutiny and hides the fact that current approaches prioritize the territorial integrity of the State and the physical security of the citizen, at the expense of other conceptions of security.

Following this way of reasoning, more security (in terms of investments, technologies, etc.) can sometimes results in less security (in terms of perceived public security). For instance, the effectiveness of DPI is often assessed against more traditional security measures, such as the number of police officers infiltrated or police intelligence fieldwork, from a cost-benefit perspective. In this way, DPI is not being assessed on the basis of the impact it has on other aspects of human security, such as, the integrity of people's movements and relations or the risk of data leaks. The societal knowledge offered by the citizens participating in this study, can help question current approaches to security precisely along these lines. There is a clear need to develop new security approaches that do not rely on the trade-off, and, rather, approach security from a systemic perspective, i.e., a view that considers simultaneously the totality of security needs of the society and that approaches individual security from a more sophisticated and comprehensive human security perspective where all aspects of individual security are taken into account and where every security measure introduced is assessed against the overall security balance of the society (Pavone *et al.*, 2016).

Security measures, both technological and non-technological, need to foster public safety both in objective terms, by reducing crime, and in subjective terms, by helping people feeling secure and protected. With this chapter, we hope to contribute to this long awaited transition from the old privacy–security trade-off model, to the development of a new win-win security paradigm, where surveillance is minimized and where all aspects of human security, including those today presented as part of the privacy dimension, are intimately aligned.

## Bibliography

Acquisti, A. (2010) Background Paper #3: The Economics of Personal Data and the Economics of Privacy. The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, December 1, 2010, 9:30–18:00 2010 OECD Conference Centre. OECD.

Anderson, R. (2007) 'Deep packet inspection technologies', in Tiptin, H.F. and Krause, M. (ed.) *Information Security Management Handbook,* 6th edn, Boca Raton, FL and New York: Auerbach Publications.

Antonello, R., Fernandes, S., Kamienski, C., Sadok, D., Kelner, J., Gódor, I., Szabó, G. and Westholm, T. (2012) 'Deep packet inspection tools and techniques in commodity platforms: Challenges and trends', *Journal of Network & Computer Applications,* 35: 1863–1878.

Askin, F. (1972) 'Surveillance: The Social Science Perspective', *Columbia Human Rights Law Review,* 4: 59–88.

Ball, K. (2002) 'Elements of surveillance: A new framework and future directions', *Information, Communication & Society,* 5: 573–590.

Ball, K. (2009) 'Exposure', *Information, Communication & Society,* 12: 639–657.

Bankston, K. S. and Soltani, A. (2014) 'Tiny constables and the cost of surveillance: Making cents out of *United States v. Jones', The Yale Law Journal Online,* 123: 335–357.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R. B. J. (2014) 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology,* 8: 121–144.

Bellanova, R. and González Fuster, G. (2013) 'Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices', *International Political Sociology,* 7: 188–209.

Clarke, R. (1988) 'Information technology and dataveillance', *Communications of the ACM,* 31: 498-512.

Corwin, E. H. (2011) 'Deep packet inspection: Shaping the Internet and the implications on privacy and security', *Information Security Journal: A Global Perspective,* 20: 311–316.

Degli Esposti, S. (2014) 'When big data meets dataveillance: The hidden side of analytics', *Surveillance & Society,* 12: 209–225. Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/analytics (accessed 21 December 2016).

Degli Esposti, S. and Santiago-Gómez, E. (2015) 'Acceptable surveillance-orientated security technologies: Insights from the SurPRISE Project', *Surveillance & Society,* 13: 437–454. Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/acceptable_technologies (accessed 21 December 2016).

European Commission (EC) (2012) 'Security Industrial Policy: Action Plan for an innovative and competitive Security Industry', COM (2012) 417 final, Brussels. Online. Available at: www.statewatch.org/news/2012/jul/eu-com-security-industry-com-417-12.pdf (accessed 19 December 2016).

European Commission (EC) (2014) 'E-Communications and Telecom Single Market Household Survey', Special Eurobarometer 414, Brussels. Online. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_414_en.pdf (accessed 19 December 2016).

Fuchs, C. (2013) 'Societal and ideological impacts of Deep Packet Inspection surveillance', *Information, Communication & Society,* 16: 1328–1359.

Gandy, O. H. (1989) 'The surveillance society: Information technology and bureaucratic social control', *Journal of Communication,* 39: 61–76.

Hess, D. J. (2014) 'Publics as threats? Integrating science and technology studies and social movement studies', *Science as Culture,* 24: 69–82.

Hoofnagle, C. J. and Urban, J. M. (2014) 'Alan Westin's privacy homo economicus', *Wake Forest Law Review,* 49: 261–317.

Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J. and Ayenson, M. D. (2012) 'Behavioral Advertising: The offer you cannot refuse', *Harvard Law & Policy Review,* 6: 273–296.

Kendall, M. G. (1970) *Rank Correlation Methods,* London: Griffin.

Koenker, R. and Bassett, G. J. (1978) 'Regression quantiles', *Econometrica,* 46: 33–50.

Lyon, D. (2007) *Surveillance Studies: An Overview,* Cambridge: Polity Press.

Lyon, D. (2014) *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, Cambridge: Polity Press.

Marx, G. T. (2003) 'A tack in the shoe: Neutralizing and resisting the new surveillance', *Journal of Social Issues,* 59: 369–390.

Mueller, M. L. and Asghari, H. (2012) 'Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States', *Telecommunications Policy,* 36: 462–475.

Murakami Wood, D. (2009) 'The "surveillance society": Questions of history, place and culture', *European Journal of Criminology,* 6: 179–194.

Pavone, V. and Degli Esposti, S. (2012) 'Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security', *Public Understanding of Science,* 21: 556–572.

Pavone, V., Santiago Gómez, E. and Jaquet-Chifelle, D-O. (2016) 'A systemic approach to secu- rity: Beyond the trade-off between security and liberty', *Democracy and Security,* 12: 225–246.

Person, A. N. (2010) 'Behavioral advertisement regulation: How the negative perception of deep packet inspection technology may be limiting the online experience', *Federal Communications Law Journal,* 62: 435–464.

Shklovski, I., Mainwaring, S. D., Skladttir, H. H. and Borgthorsson, H. (2014) 'Leakiness and creepiness in app space: Perceptions of privacy and mobile app use', in *Proceedings of the 32nd annual ACM conference on Human factors in Computing Systems, Toronto, Canada*, New York: ACM Press.

Siegrist, M. (2008) 'Factors influencing public acceptance of innovative food technologies and products', *Trends in Food Science & Technology,* 19: 603–608.

Smith, H. J., Dinev, T. and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *MIS Quarterly,* 35: 980–1015.

SurPRISE (2014) SurPRISE Documentary Film: DPI (Deep Packet Inspection).

Turow, J., Hennessy, M. and Draper, N. (2015) *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*, Philadelphia, PA: The Annenberg School for Communication, University of Pennsylvania.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) 'User acceptance of information technology: Toward a unified view', *MIS quarterly*, 27: 425–478.

Verble, J. (2014) 'The NSA and Edward Snowden: surveillance in the 21st century', *SIGCAS Computers & Society,* 44: 14–20.

Wells, H. and Wills, D. (2009) 'Individualism and identity: Resistance to speed cameras in the UK', *Surveillance & Society,* 6: 259–274. Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3284/0 (accessed 21 December 2016).

Xu, H., Luo, X., Carroll, J. M. and Rosson, M. B. (2011) 'The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing', *Decision Support Systems,* 51: 42–52.