# Wanting it all – public perceptions of the effectiveness, cost, and privacy of surveillance technology

Cayford, Michelle; Pieters, Wolter; van Gelder, P. H.A.J.M.

**DOI**
10.1108/JICES-11-2018-0087

**Publication date**
2019

**Document Version**
Final published version

**Published in**
Journal of Information, Communication and Ethics in Society

**Citation (APA)**
Cayford, M., Pieters, W., & van Gelder, P. H. A. J. M. (2019). Wanting it all – public perceptions of the effectiveness, cost, and privacy of surveillance technology. *Journal of Information, Communication and Ethics in Society*, *18*(1), 20-37. https://doi.org/10.1108/JICES-11-2018-0087

# Wanting it all – public perceptions of the effectiveness, cost, and privacy of surveillance technology

Michelle Cayford, Wolter Pieters and P.H.A.J.M van Gelder
*Delft University of Technology, Delft, The Netherlands*

Received 16 November 2018
Revised 10 April 2019
Accepted 20 May 2019

## Abstract

**Purpose** – This study aims to explore how the public perceives the effectiveness of surveillance technology, and how people's views on privacy and their views on effectiveness are related. Likewise, it looks at the relation between perceptions of effectiveness and opinions on the acceptable cost of surveillance technology.

**Design/methodology/approach** – For this study, surveys of Dutch students and their parents were conducted over three consecutive years.

**Findings** – A key finding of this paper is that the public does not engage in a trade-off neither with regard to privacy-effectiveness (exchanging more effectiveness for less privacy and vice versa) nor with effectiveness-cost, but rather expects all three elements to be achieved simultaneously. This paper also found that the correlation between perceived effectiveness and perceived privacy was stronger for parents than for students.

**Research limitations/implications** – Participants for this study were exclusively in The Netherlands. Survey questions on the effectiveness of surveillance technology focused on one type of technology, and on private mobile device use in two scenarios.

**Social implications** – The public's perceptions of the effectiveness of surveillance technology potentially influence its acceptance of the technology, which, in turn, can affect the legitimacy and use of the technology.

**Originality/value** – Within the much-discussed privacy-security debate lies a less-heard debate – that of the effectiveness of the surveillance technology in question. The public is one actor in this debate. This study examines the public's perceptions of this less-heard debate.

**Keywords** Cost, Surveillance, Privacy, Effectiveness, Public views, Surveillance technology

**Paper type** Research paper

## 1. Introduction

Amidst the anguish and anger following terrorist attacks such as 9/11 and Charlie Hebdo, erupt calls for more government action to prevent such events. This, in turn, leads to increased surveillance by intelligence agencies. Months or years later, leaked classified documents, such as in the Snowden case, result in privacy advocates decrying the government's surveillance actions as a violation of privacy. A debate ensues in which security is pitted against privacy. Such is the current discussion on government surveillance, which turns around privacy versus security.

The public is one actor in this debate. On both sides, other actors claim to act in the public's interest, either accusing the government of privacy rights' violation and demanding a cessation of activities or defending these surveillance programs as necessary to keep citizens secure against current threats. Both sides seek to influence whether the public accepts these surveillance programs, basing their arguments in the context of the privacy versus security trade-off.

Within the privacy-security debate, there is a less-heard debate – that of the effectiveness of the surveillance programs in question. Is the surveillance technology effective in accomplishing a given security goal? Different actors hold different views, and how to

Journal of Information, Communication and Ethics in Society

1477-996X
DOI 10.1108/JICES-11-2018-0087

evaluate effectiveness is in itself a complex question (Cayford and Pieters, 2018). The public's perception of effectiveness has significant social implications, as this potentially plays a role in its acceptance of the technology; and judgments on acceptability may depend on judgments of effectiveness. This, in turn, could influence the legitimacy and continued use of such technology. In democratic societies, the public's view matters. Its views influence policy and the making of law.

This study explores how the public perceives the effectiveness of surveillance technology, and how people's views on privacy and their views on effectiveness are related. Likewise, is there a relation between perceptions of effectiveness and opinions on acceptable cost of surveillance technology? This paper analyzes the results of surveys completed by a group of Dutch undergraduate students and their parents. It is one of only two studies investigating views of the Dutch public in relation to surveillance, and the first known study to analyze public views regarding effectiveness and the correlations between effectiveness, privacy and cost. Findings show some significant differences between the parent and student generations, as well as correlations that suggest that the public does not engage in the trade-offs imbedded in the privacy-security debate. Rather, the public wants it all – effectiveness and privacy at a reasonable cost, all delivered simultaneously.

The paper is structured as follows: Section 2 presents related work, followed by methodology in Section 3. The study's results are then given accompanied by analysis in Section 4, followed by a discussion of the results in Section 5, and finally, conclusions in Section 6.

## 2. Related work

The question of the effectiveness of surveillance technology is closely linked to the debate over the values of security and privacy. On one side of this debate are those who argue that access to telecommunications is necessary for stopping organized crime and terrorism. On the other side of the debate are those who argue for the right to privacy. The privacy-security debate is expansive, and the literature reflects this, spanning discussions of privacy and security and technology (Friedewald and Pohoryles, 2013; Schneier, 2013), privacy and data retention law (Tene, 2011; Mitrou, 2007), the question of balance that should be struck between the two (Guerrier, 2016; Stalla-Bourdillon *et al.*, 2014), whether there is or should be a trade-off between the two (Verfaillie and van den Herrewegen, 2013; van Leishout *et al.*, 2013), ethics (Stahl, 2007; Landau, 2014), dealing with cryptology (Diffie and Landau, 2007) and the balance between liberty and security with regard to law (De Hert, 2005; Poullet, 2004).

This debate enters the political sphere as countries decide, which balance to strike and accordingly adopt laws that restrict or allow, as the case may be, intelligence agencies' access to communications (Mansfield-Devine, 2015). This is where the people come in, in democratic societies the people's view of intelligence agencies and the surveillance technology they use affects this debate. If the public perceives surveillance technologies as effective and the associated agencies as trustworthy, negative impacts on privacy are more likely to be accepted.

Public perception is a topic in and of itself, which includes actual versus perceived effectiveness and influences on perceptions such as politics, the media (Altheide, 2006), culture, place and situations (Orru, 2013). Here, the goal is neither to focus on these influences nor to enter into a discussion of perceived versus actual effectiveness. Rather, it is to continue previous research of investigating different stakeholders' views of effectiveness. All stakeholders perceive effectiveness in some way, and these various views influence the debate around the use of surveillance technology.

A review of the existing literature treating surveys of the public related to surveillance reveals that they primarily focus on privacy issues, and that many are concentrated around the Snowden leaks. One such study surveyed students in various countries (Germany, Spain, Sweden, Japan, China, Taiwan, Mexico and New Zealand) regarding their views on privacy and state surveillance following the Snowden leaks (Adams *et al.*, 2017; Murata *et al.*, 2017; Kavathatzopoulos *et al.*, 2017; Gunasekara *et al.*, 2017). The study's questions probed general privacy attitudes and investigated knowledge and evaluation of Snowden's actions. The surveys found, among other things, that attitudes toward privacy varied in different countries and that most respondents approved of Snowden's actions and a majority would act as he had, except for those in China and Japan. A separate study surveyed students in Slovenia to understand public perception of cyber-surveillance pre and post-Snowden and found that more people felt threatened by domestic and foreign intelligence services post-Snowden (Zavrsnik and Levicnik, 2015).

The Pew Research Center in the US surveys public opinion and has produced several reports of survey results related to the National Security Agency (NSA) surveillance, privacy and Snowden. One such report revealed that a small majority (50 per cent) approved of the government surveillance programs collecting phone and internet data (Pew, 2013c). Another survey (Madden, 2014) indicated that Americans are concerned about government and businesses' surveillance of their communications. A Pew report focused on Americans' views of NSA surveillance and privacy and security (Gao, 2015) found that a majority do not believe they need to sacrifice privacy and freedom to be safe from terrorism, while also stating that anti-terrorism policies do not do enough to protect them. Additional Pew surveys polled Americans' views on NSA surveillance programs and of Snowden's actions (Desilver, 2014; Pew, 2013a, 2013b), of monitoring Allied leaders' phones (Pew, 2013d), whether they think the government is monitoring their calls and emails (Olmstead, 2017), and their concerns of security versus privacy (Doherty, 2013; Rainie and Maniam, 2016; Rainie, 2016).

Outside of student surveys and Pew surveys, Reddick *et al.* (2015) examine American public opinion related to NSA surveillance programs, studying the correlation between engagement in political discourse (and therefore, political efficacy) and approval of these programs. Brooks and Manza (2013) write about American public opinion on counterterrorism. Through surveys conducted in 2007, 2009 and 2010 covering ten counterterrorism policies and practices, their research found strong support for NSA surveillance of telephone conversations between US citizens and suspected terrorists, as well as for the Patriot Act, which was described as facilitating government access to phone and email records. The authors believe that the persistence of the high-intensity counterterrorism strategies put in place following 9/11 are in large part explained by high levels of public support.

In all the above studies and surveys, themes emerge of investigating views on privacy, acceptance of surveillance programs, and the impact of the Snowden leaks. They tend to be conducted within the context of and with an implicit understanding that citizens weigh and exchange their privacy versus their security. This is the notion of trade-off. This notion implies that to have more privacy some security must be given up and vice versa. A small set of studies probes this understanding, using surveys to examine how citizens assess surveillance technology, including whether they evaluate surveillance technologies according to the security-privacy trade-off model.

The first study (Pavone and Degli Esposti, 2012), suggests that the public's assessments are context-specific, reflecting their trust or distrust of the institution conducting the surveillance, and that the public does not perform a trade-off. Those who are distrusting see

their privacy being infringed upon by the surveillance technology without their security being increased, in other words, the technology is both ineffective and privacy-invasive – while those who are trusting considered the technology to be effective without infringing on their privacy. Through a citizen summit in Spain, Degli Esposti and Santiago-Gomez (2015) investigated the public's perceptions of CCTV and deep packet inspection (DPI), including whether they considered these two technologies effective national security tools. The study found that more participants (63 per cent) considered CCTV to be an effective security tool than DPI (43 per cent), and that half the participants held a security-privacy trade-off approach, considering these technologies to both enhance security and invade their privacy. The rest either viewed the technology as highly invasive and not really effective or as very effective without infringing on privacy. Finally, Degli Esposti *et al.* (2017, p. 72) report on surveys conducted in six European countries investigating public perceptions of DPI. They found that a technology's perceived intrusiveness negatively impacts its perceived effectiveness, and that security and privacy are "compatible rather than antagonistic dimensions."

Similar to the above studies, Van den Broek *et al.* (2017, p. 29) surveyed the EU citizens using real-life scenarios of security issues, but without explicit references to security or privacy. Among the authors' conclusions were that acceptance of surveillance and views of privacy intrusion depend on the security issue, that trust plays a role, and that those with a high degree of privacy awareness are less likely to be accepting of surveillance while those with a high level of security concerns are more accepting. The authors conclude that "EU citizens assess security and privacy aspects as rather independent values that both need to be secured."

This current research contributes to the work investigating the public's views on surveillance technology, zeroing in specifically on the question of effectiveness, and the relationship between perceptions of effectiveness and privacy. As with the notion of the privacy-security trade-off, it examines if the public engages in a privacy-effectiveness trade-off, exchanging more effectiveness for less privacy and vice versa. This study also investigates how the public views the cost of surveillance technology and if there is an effectiveness-cost relation in which the public is willing to spend more money if it considers the surveillance technology to be effective and vice versa.

In addition to governments, internet service providers (ISPs), businesses, users, advertising, social media and personal devices all introduce and perform forms of surveillance (Asghari *et al.*, 2012; Bendrath and Mueller, 2011; Trottier and Lyon, 2012; Trottier, 2012; Fuchs and Trottier, 2017). This study also explores whether people differentiate between types of surveillance – whether they feel differently about privacy and effectiveness with government surveillance versus commercial surveillance versus individuals' surveillance using mobile devices.

## 3. Methodology

This paper analyzes the results of a survey, designed to explore the public's views on surveillance technology in relation to effectiveness, privacy and cost. The survey polled a group of bachelor's students and their parents in 2014, 2015 and 2016. The students were part of safety, security and justice (SSJ) minor run jointly by the Delft University of Technology and Leiden University in The Netherlands. In 2014, SSJ minor students were enlisted to distribute surveys to non-SSJ minor students and their parents. Both 43 non-SSJ minor students and 43 of their parents completed the survey. In 2015, only students completed the survey. In total, over the three years, there were 359 respondents, of which

200 were students. Among the respondents, 164 were women and 195 were men. The survey was conducted in English.

The survey's first three questions explored how bothered people were by different parties – ISPs and internet companies; the Dutch intelligence services, Algemene Inlichtingen- en Veiligheidsdienst (AIVD); and the American NSA – potentially having access to their online activity. The aim was to explore differences and relations between how people felt about privacy intrusion by private companies versus domestic intelligence versus foreign intelligence services.

Two yes/no questions explored attitudes related to the effectiveness of surveillance technology. To learn more about why participants considered a particular NSA technology to be effective or not, we added a free text response. Three additional questions focused on privacy attitudes related to individuals' use of their mobile devices to record and report crime and speeding. Likert scale responses were used to gauge the degree to which respondents were bothered or comfortable with different surveillance actions.

Two years into conducting the survey, our research on the effectiveness of surveillance technology was indicating cost to be an important question with other stakeholders. A question on cost was, therefore, added in 2016 to explore attitudes of the public related to the cost of surveillance technology. The final two questions investigated expectations of security, with the intention of studying any correlations with this and perceptions of effectiveness.

As our data were not normally distributed, non-parametrical statistical tests were used to test the above hypotheses. Mann–Whitney tests were used to compare means between different groups of respondents. Spearman tests were used for correlations. Wilcoxon signed ranks test and sign test were used for pairwise comparisons. *Z*-tests were used for comparing population proportions, and a parametric Levene's test was used for comparing the variance between different subpopulations. The null hypothesis is rejected if the $p$-value (probability of rejecting the null hypothesis given that it is true) is less than a predetermined significance level of 5 per cent. Exact $p$-values will be reported, unless the $p$-value is below 1 per cent. In that case, the $p$-value will be reported as $p < 0.001$. Finally, to analyze the free-text responses, the responses were coded to identify themes.

## 4. Results and analysis

This section presents and analyzes the results, with the associated hypotheses presented at the beginning of each sub-section.

### *4.1 Privacy*

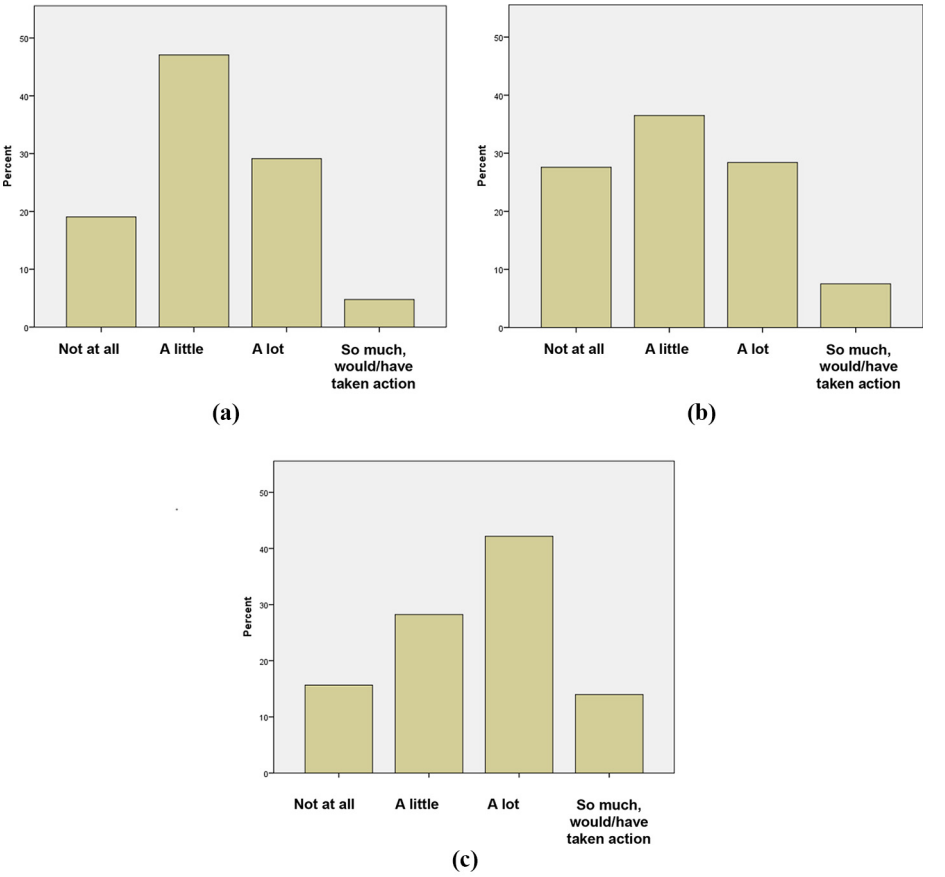
It was expected that attitudes regarding privacy would vary depending on who was accessing people's data. This is inherently linked to a question of trust – those who trust a given institution are more likely to be less bothered by potential privacy intrusion:

*H1.* People are more bothered by the NSA potentially accessing their online activity, than by the AIVD.

*H2.* People are more bothered by both the NSA and the AIVD potentially accessing their online activity, than by ISPs and internet companies.

*H3.* Parents, being closer to a pre-internet era and a time when intelligence agencies were more trusted, will be less bothered than students by potential NSA and AIVD access, and more bothered than students by ISP and internet companies' access.

The response results of the first three survey questions are shown in Figure 1. From left to right, the bars show respondents being least bothered ("not at all," corresponding to a Score 1) to most bothered ("so much that I would or have taken action," corresponding to a Score 4). For Q1 ($M = 2.20$, $SD = 0.797$) most respondents reported being "a little" bothered by ISPs and internet companies having access to their online information – 47 per cent. Q2 ($M = 2.15$, $SD = 0.916$) also showed the highest number of respondents being "a little" bothered by AIVD access 37 per cent. While the means for Q1 and Q2 were similar, the figure suggests that responses for the AIVD are more spread. Indeed, the standard deviation for Q1 was 0.797, and that for Q2 was 0.916, meaning that responses for Q2 tended more toward the extremes, with more people reporting that they were "not at all" bothered by the AIVD and that they were so bothered that they had taken action, such as using encryption, than those who reported the same for ISPs and internet companies. In regards to the NSA Q3 ($M = 2.54$,




**Notes:** (a) (Q1) To what extent are you bothered by ISPs and internet companies having access to all your online activity?; (b) (Q2) To what extent would you be bothered if the Dutch AIVD had access to all your online activity?; (c) (Q3) To what extent would you be bothered if the American NSA had access to all your online activity?

**Figure 1.**

*SD* = 0.918) most were bothered "a lot" – 42 per cent. As expected, respondents were significantly more bothered by the NSA than by both private companies and the AIVD ($p < 0.001$), according to a pairwise Wilcoxon signed rank test.

Mann–Whitney tests were run to test hypothesis *H3*. While there was no significant difference in the means between students and parents for Q1 and Q2, the standard deviation showed differences in variance. Related to internet providers and companies, the 197 students ($M = 2.18$) had a standard deviation of 0.726, while the 160 parents ($M = 2.21$) showed a higher standard deviation of 0.879 ($p < 0.001$). As regards the AIVD, 199 students showed, $M = 2.15$, $SD = 0.851$ and 160 parents also showed a higher standard deviation, $M = 2.17$, $SD = 0.992$ ($p < 0.001$).

One of the goals of this study was to investigate relationships between responses related to effectiveness, privacy and cost. This included correlations in responses to questions on the same subject, such as privacy (hypotheses *H1-H3*). This was done by using Spearman's correlation coefficients. These tests did indeed reveal some interesting correlations. There was a significant correlation between Q1 (ISPs) and Q2 (AIVD) ($r(357) = 0.467$, $p < 0.001$), as well as between Q1 and Q3 (NSA) ($r(357) = 0.460$, $p < 0.001$). The correlation of how people answered Q2 and Q3 was even stronger, $r(358) = 0.624$, $p < 0.001$. This suggests that those who are bothered by others having access to their online information tend to be bothered regardless of whether it is an ISP or internet company, a domestic government or a foreign government. And likewise, those that are more accepting, are accepting regardless of the party accessing the data.

### *4.2 Effectiveness*

This study anticipated that attitudes concerning privacy invasion would correspond with perceptions of effectiveness of the institution or technology involved:

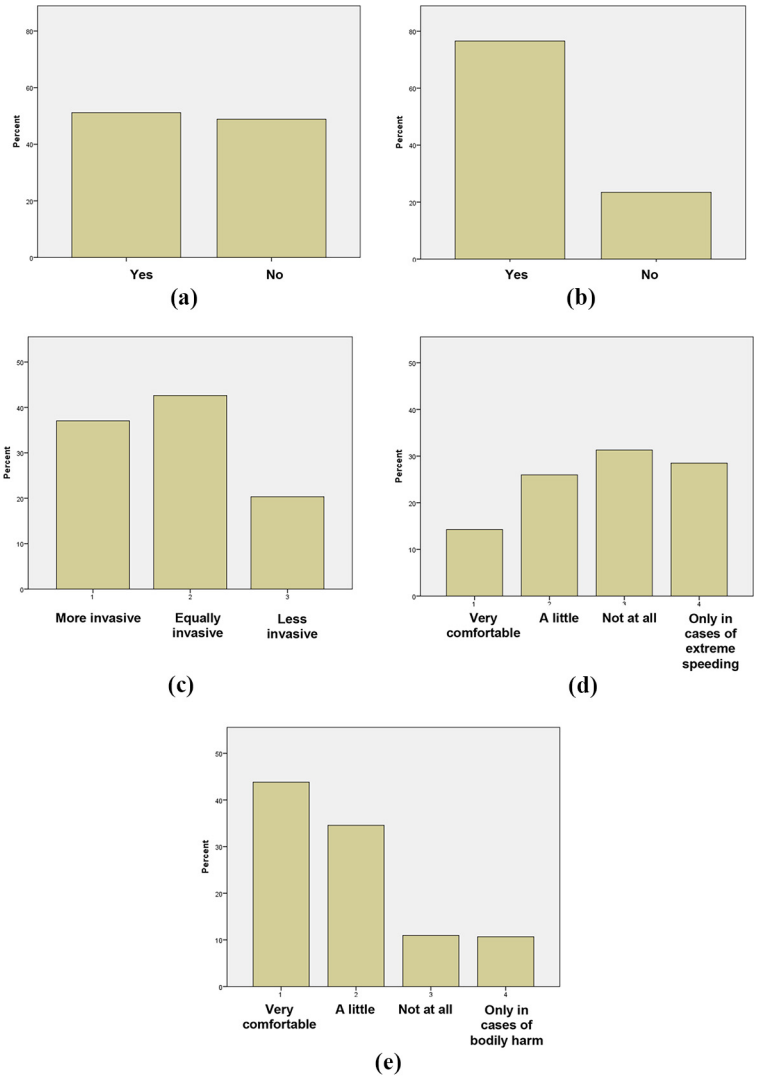
*H4.* Those who find NSA surveillance to be effective are less bothered by potential NSA access to their online activity.

*H5.* Those who find NSA surveillance to be effective are less bothered by potential AIVD access to their online activity.

*H6.* Those who consider using private mobile devices to record crime scenes and speeding vehicles to be effective for security find this action to not be particularly invasive.

*H7.* Those who consider using private mobile devices to be effective for security are more comfortable with the police using such recordings to issue speeding fines and investigate the crime.

The two survey questions specifically addressing the question of effectiveness produced fairly different results [Figure 2(a) and (b)]. Respondents were nearly equally divided regarding whether NSA wiretaps with wide filters were an effective form of surveillance technology, with 50 per cent responding "yes," and 47 per cent responding "no" (3 per cent gave no answer). However, many more thought that use of mobile devices by individuals to record crime and infractions was an effective use of technology for security purposes. Close to 80 per cent responded "yes," with a bit over 20 per cent saying "no." Most people found this to be less or as equally invasive as CCTV ($M = 1.83$, $SD = 0.740$). Only 20 per cent reported it was more invasive [Figure 2(c)]. There was considerable difference, however, between how comfortable people were with police using videos from private individuals to issue speeding fines versus investigating crime [Figure 2(d) and (e)]. A comparison of means




**Notes:** (a) (Q4) The NSA collects vast amounts of data by setting the filters wide for their wiretaps. Do you consider this to be an effective form of surveillance?; (b) (Q5) Using mobile devices, individuals can now take photos and films of crime scenes, speeding vehicles, etc. Do you consider this to be an effective use of technology for security purposes?; (c) (Q6) Do you consider the above activity (see Q5) to invade your privacy more than, for example, a CCTV camera in a public space?; (d) (Q7) How comfortable are you with police using videos from private individuals to issue speeding fines?; (e) (Q8) How comfortable are you with police using videos from private individuals to issue speeding fines?

**Figure 2.**

showed a strong significant difference with $p < 0.001$. Only 14 per cent were "very comfortable" and 26 per cent "a little comfortable" with police using private videos to issue speeding fines. The rest were closely divided between using such videos "only in cases of extreme speeding," or "not at all." In contrast, regarding police using private videos to investigate crime, a strong majority was "very comfortable" at 44 per cent and 34 per cent were "a little comfortable." The remainder were equally split at 11 per cent each, with being comfortable only in cases of bodily harm or not at all. A difference in the spread of responses between students and parents emerged related to police using private videos to issue speeding fines with parents showing more variance than students ($p = 0.045$): 198 students ($M = 2.78$, $SD = 0.998$) and 160 parents ($M = 2.76$, $SD = 1.103$). This same difference in variance did not emerge related to police using private videos to investigate the crime.

It was anticipated that those who considered NSA wiretapping surveillance technology to be effective would also be less bothered by NSA access to online activity (hypothesis *H4*). Indeed, there was a significant correlation between the responses, although this correlation appears to be associated with age/generation. Parents showed a strong correlation, $r(151) = 0.278$ and $p < 0.001$, while the student population had no significant correlation. Although the question on effectiveness was specifically related to the NSA, we hypothesized that there would still be a correlation between this question and that dealing with privacy related to the domestic intelligence agency (hypothesis *H5*). This was, in fact, the case, with those who consider wiretaps to be non-effective, also being more likely to be bothered by AIVD access to their online activity ($r(348) = 0.120$, $p = 0.026$). Once again, this correlation is associated with age – when looked at separately, students had no significant correlation, while their parents showed a strong correlation, $r(151) = 0.229$, $p = 0.005$. Although there was not expected to be a correlation between views on the effectiveness of NSA surveillance technology and ISP access to online activity, this same pattern was found of there being no significant correlation with students, but a significant correlation existing with their parents, $r(151) = 0.165$, $p = 0.043$.

The study's second question on effectiveness concerned the effectiveness of recordings on private mobile devices for security purposes. As expected (hypothesis *H6*), those who consider private recordings of crime to be effective for security, found this action to not be particularly invasive – less invasive than CCTV ($r(358) = 0.124$, $p = 0.019$). Likewise (hypothesis *H7*), those who considered it effective were more likely to be more comfortable with police using private videos to issue speeding fines ($r(357) = 0.205$, $p < 0.001$) and investigate crime ($r(356) = 0.226$, $p < 0.001$).

### *4.3 Cost*

Perceptions of effectiveness and expectations of security influence how much money citizens are willing for the government to spend on surveillance technology; and attitudes related to privacy may also influence attitudes toward cost:

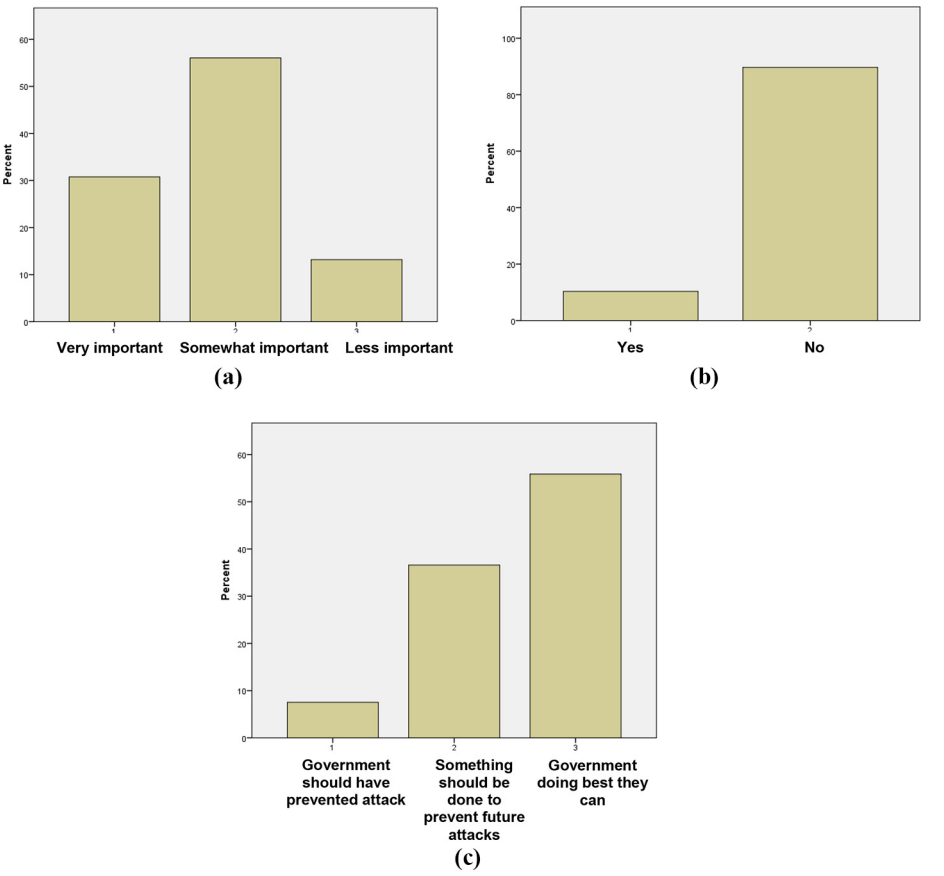
*H8.* Those who find NSA wiretaps to be effective place less importance on the cost of surveillance technology, and those who find NSA wiretaps to be ineffective place more importance on cost.

*H9.* Those that expect the government to prevent every possible terrorist attack place less importance on the cost of surveillance technology.

*H10.* Those that place more importance on the cost of surveillance technology are more likely to be bothered by potential AIVD and NSA access to their online activity.

Responding to how important the cost of surveillance technology is in relation to security [Figure 3(a)], 31 per cent said that cost is "very important" (that is, surveillance technology should only be deployed if the costs are reasonable), while 56 per cent said it is "somewhat important" (surveillance technology that improves security can be somewhat costly). Only 13 per cent responded that cost was "less important," and that any surveillance technology that improves security should be deployed ($M = 1.82$, $SD = 0.643$). Here again, a difference in variance between students and parents manifested itself, with parents having a wider distribution ($p = 0.038$): 46 students ($M = 1.87$, $SD = 0.582$) and 45 parents ($M = 1.78$, $SD = 0.704$).

Respondents were pragmatic in not expecting the government to be able to prevent every possible terrorist attack [only 10 per cent said yes – Figure 3(b)], and in their reaction when a terrorist attack occurs – only 8 per cent said their response is that the government should




**Notes:** (a) (Q9) As a taxpayer, how important is the cost of surveillance technology to you in relation to security?; (b) (Q10) Do you expect the government to be able to prevent every possible terrorist attack?; (c) (Q11) When a terrorist attack occurs what is your reaction?

**Figure 3.**

have been doing a better job and prevented it [Figure 3(c)]. A majority (56 per cent) said that their reaction when a terrorist attack occurs is that the government is doing the best they can, while the remainder (37 per cent) said their reaction is that something should be done to prevent this from happening again.

To test hypothesis *H8* we calculated the correlation in the responses to the question concerning the effectiveness of NSA surveillance technology and that investigating the importance of the cost of surveillance technology. That is, are those who considered NSA surveillance to be effective also willing for more money to be spent on surveillance technology. Contrary to our hypothesis, no significant correlation was found. However, the expected correlation between privacy and cost did appear (hypothesis *H10*), with those who were more bothered with AIVD surveillance of their online activity being more likely to say that cost is very important and surveillance technology should only be deployed if costs are reasonable ($r(91) = -0.280$, $p = 0.007$). Interestingly, though, there was only a significant correlation between the cost question and the question related to domestic intelligence, not between cost and foreign intelligence.

A final correlation related to cost was identified: those who expected the government to prevent every possible attack were also more likely to consider cost as very important and that surveillance technology should only be deployed if the costs are reasonable ($r(91) = 0.222$, $p = 0.035$). This is contrary to hypothesis *H9*, which anticipated that those who expect the government to prevent every possible attack would be more likely to consider cost to be less important and that any surveillance technology that improves security should be deployed.

### *4.4 Minor versus non-minor students*

In 2014, there were two groups of students surveyed – one group were students in the SSJ minor and the other group were not in the minor. It was anticipated that there would be some differences in the responses of these two groups. Those in the minor studied security and privacy issues surrounding surveillance technology, which we anticipated would make a difference in their responses.

*H11.* There will be a difference in the responses of SSJ minor students versus students not in the minor.

This turned out to be the case with several of the questions. Among the 68 SSJ students far more found private mobile devices recording crime and speeding to be effective for security purposes than not (82 per cent found it to be effective and 18 per cent not). A smaller majority of the 43 non-SSJ students found it to be effective (65 per cent). According to a *z*-test for two population proportions (two-tailed), the difference between 82 and 65 per cent is significant ($p = 0.042$). The reverse was found regarding the effectiveness of NSA surveillance technology with 60.5 per cent of non-SSJ students considering it to be effective, while only 46 per cent of SSJ students considered it effective, although this difference is not significant ($p = 0.136$). A significant difference between the two groups was found regarding whether they expected the government to be able to prevent every possible terrorist attack ($p < 0.001$). A quarter (26 per cent) of the students not in the minor expected the government to stop every attack versus only two students (3 per cent) in the minor. The difference in means to responses to the next – and related – question mirrored these responses. In total, 9 per cent of SSJ students said the government should have been doing a better job versus 16 per cent of non-SSJ students, although this difference is not significant ($p = 0.262$). The opposite end of the spectrum for this question was that the government is doing the best it can – an occasional terrorist attack will always get through. In total, 62 per cent of SSJ

students gave this answer, while only 40 per cent of non-minor students gave this response, which is significantly different ($p = 0.0394$). Interestingly, differences that were expected in views of privacy invasion related to ISPs, the AIVD and the NSA, did not appear.

*4.5 Qualitative data*

Respondents were asked to give free text responses as to why they considered NSA wiretapping surveillance technology with wide filters to be effective or not. We analyzed these responses by categorizing them according to themes. Strikingly, one of the most commonly stated reasons – a lot of data are collected – was given as an explanation both for why the technology was effective and ineffective. This was the number one reason that respondents gave for why they considered NSA wiretapping technology with wide filters to be effective – this technique yields a lot of information (30 per cent gave this response). These answers stated that it is necessary to monitor all this information to find the crucial information you are seeking – only by monitoring the haystack will you find the needle. For this same reason, many considered the technology to be ineffective – too much data are collected to be effective (15 per cent). Two particular responses that underline the same reason given for both sides of the argument were:

> *Only by collecting vast amounts of potentially relevant data, will you end up with having that one phone call on tape that you happen to need.*
>
> *It is like looking for a needle in a haystack.*

The second response implies that the haystack should not be collected as it is so much information just to try to identify one small needle. While the first response argues that the only way to find that needle – that one important piece of information – is to collect the haystack.

Additional frequently given responses for why this technology is effective were that collecting information with wide filters allows the NSA to find what or who it is looking for, and that it is a preventative measure against crime and attacks. Interestingly, preventing crime and attacks was the second highest reason given for effectiveness in 2014 and 2015, but in 2016 not one person gave this as a reason for effectiveness.

Other reasons people gave for considering the technology to be effective was that it allows the NSA to see everything and it identifies and predicts patterns. Several gave security as a reason, with some saying that anything that might increase security should be used: "if there's a 1 per cent chance that it would stop a terrorist attack or something like that, it is worth it." A small number reported that it was fast and easy and one person said the technology was cheap.

A number of respondents gave qualified "yes" responses. That is, this technology is effective, but [. . .] It is effective, but not ethical or it is effective but it invades privacy or whether it is effective depends on how it is used or on the analysis of the data. Others said it was maybe or a little effective.

The first reason for ineffectiveness was that it invades privacy (18 per cent). The second reason was that it collects too much data. The final reason given for it not being effective was that it yields a lot of unnecessary data (13 per cent). (Note that we created two categories – "too much data" and "unnecessary data" – but if the two were combined "too much data" would also be the number one reason for ineffectiveness.)

Other reasons that a significant number of people gave were that targeted surveillance is more effective, that criminals can work around filters and wiretaps, that it takes too much resource (time, money and manpower) and that it makes it more difficult to find the important data. A smaller number of people said that such a large amount of data cannot be

effectively analyzed, that this technique is not productive, and that it yields irrelevant information, which results in false leads.

## 5. Discussion

The results from the three questions treating how bothered people were by private companies, the AIVD, and the NSA may point to matters of trust and politics. While not having all the capabilities of the NSA, the AIVD appears to be fairly advanced in their surveillance techniques and in cooperating and sharing information (van Riezen and Roex, 2012; Derix *et al.*, 2013; Kraan, 2017). Given the AIVD's capabilities, it does not seem likely that the difference in response toward the two agencies is related to surveillance powers. Rather, the fact that fewer respondents were bothered by the AIVD than by the NSA may indicate more trust in the Dutch AIVD, which would be expected – one would trust one's own country's intelligence agency more than a foreign one, particularly with all the bad press for the NSA around the Snowden leaks. The difference in variance between the AIVD and the ISPs might point to the AIVD being more of a political issue, and thereby evoking stronger feelings in both directions. More people being "not at all" bothered by the AIVD (28 per cent) than by ISPs and internet companies (19 per cent) could indicate more trust in the AIVD or could again point to a difference in trust in domestic versus foreign as some internet companies are foreign and even based in the USA (e.g. Google, which was mentioned in the survey as an example of an internet company). An alternative explanation could be that people feel they have no choice but to accept ISP access to their data. Based on their decision to accept this reality, people will adapt their values to view their decision positively (Adams, 2014). Thus, they would be only a "little bothered," as most respondents were. All the post-Snowden discussion around privacy may also give people the impression that, contrary to ISP access, they do not have to accept AIVD access to their data, but can limit it through the democratic process (in reality, this could also be done for ISP access).

The correlations we discovered between responses related to effectiveness and privacy – e.g. those who considered NSA technology to be effective were also less bothered by potential NSA access to online activity and vice versa – are similar to a finding of Pavone and Degli Esposti (2010) that people tend to be divided into two groups of being either trusting or concerned. Their study found that those who were trusting (of the institutions concerned and the technology's legitimacy) believed both that the surveillance technology was effective in increasing security and that their privacy was not infringed upon. Those who were concerned saw the technologies as an invasion of privacy without increasing security. Our findings suggest that those who are concerned about privacy (and perhaps, see no added security value) are concerned regardless of who is looking at the data. And conversely, those who do not see a privacy invasion hold this view regardless of the institution involved. The Pew surveys cited earlier in this paper indicate American youth (ages 18-29) are more concerned about privacy and more disapproving of NSA surveillance programs than older adults. These reports, however, did not look for correlations between responses related to privacy and effectiveness. Our findings may suggest that the categories of being trusting or concerned, and therefore, viewing surveillance technology as either both effective and non-privacy invasive or the reverse, may be age-related; and that students are not yet divided into groups of being trusting or concerned across the board, while their parents are. This could be because students are still forming and developing their views on issues and in politics, and are, as yet, not polarized. Their parents, on the other hand, have well-formed views and furthermore, some of these questions around security may be politicized, resulting in more polarization. This could also be an explanation for the

difference noted above in the spread of responses between students and parents for Q1, Q2, Q7 and Q9.

As multiple authors have found (Pavone and Degli Esposti, 2010; Van den Broek *et al.*, 2017; Anderson, 2015), and as these results suggest, trust is a core issue in surveillance. Trust in government institutions appears to equate to both trusting them with one's privacy and trusting that their surveillance technology is effective; and distrust results in the reverse. The differing results according to age, perhaps, also speak to trust in political parties – a trust or distrust in the current governing political party.

At first review, there was no correlation between effectiveness and cost. However, this might have been due to the effectiveness question zoning in on NSA surveillance technology, and the respondents being Dutch, and therefore, being no link between their taxpayer money and NSA technology. This interpretation is supported by the correlation found between cost and privacy as concerns the AIVD, while no correlation was found between cost and privacy related to the NSA. Further, there was a correlation between cost and expectations that the government would prevent every terrorist attack.

Expecting the government to prevent every possible terrorist attack points to respondents' expectations of effectiveness. The correlation this study discovered – that those who held this expectation were also more likely to consider the cost of surveillance technology as very important – is noteworthy. Although the sample size, in this case, is too small to make generalizations (the cost question only appeared in 2016), it merits further exploration to examine whether the public holds similar views related to cost and effectiveness as related to privacy and effectiveness/security (Van den Broek *et al.*, 2017). That is, citizens do not treat the two as a trade-off, but as two independent elements, which both need to be attained.

Expectations that the government prevents every terrorist attack were significantly higher among non-SSJ students versus SSJ students. One possible explanation is that, as a result of their studies, students of the minor were more conscious of the difficulties of preventing every possible terrorist attack, leading them to more realistic expectations. Of course, it is also possible that students who already held these views were more inclined to take the minor, and thus, the differences are not the result of the studies. If this difference is a result of their studies, however, it is noteworthy that these studies did not significantly influence results in views on privacy and the effectiveness of NSA surveillance technology.

Among the whole respondent population, 56 per cent said that their reaction when a terrorist attack occurs is that the government is doing the best they can. This majority could reflect a cultural aspect (e.g. the Dutch are a pragmatic people) and/or could be a result of there being no recent terrorist attacks in The Netherlands.

The contrast of respondents being considerably less comfortable with private videos being used to issue speeding fines than to investigate crime could indicate a consideration of more serious offenses meriting more invasive measures. An alternate explanation is that people are more averse to surveillance that touches them personally versus surveillance that does not concern them – i.e. we are probably all guilty of speeding, while few have committed a crime.

Limitations of this study include that its participants were exclusively in The Netherlands. Some of these findings, therefore, might only hold true for the Dutch. One study examining Dutch attitudes toward privacy and surveillance immediately following the Snowden leaks found them to be similar to attitudes in the UK (Mols and Janssen, 2017). Obviously, many national factors can influence attitudes toward privacy and surveillance, such as surveillance law, history, scale of terrorist attacks, etc. Future research could compare this paper's findings with similar studies in other countries.

Survey questions on the effectiveness of surveillance technology focused on one type of technology, and on private mobile device use in two scenarios. Other types of surveillance technology or different scenarios might yield different results. Although the results related to SSJ minor students versus non-minor students indicate significant differences in some areas and not others, further studies are needed to confirm these findings and to determine to what degree student findings across all years might be influenced by most students being in security studies. As previously mentioned, the cost question only appeared in one year. The results related to participants' views on the acceptable cost of surveillance technology merit further research to investigate if the lack of trade-off between cost and effectiveness holds true with a larger sample size.

## 6. Conclusion

Surveying the public on the effectiveness, cost and privacy implications of surveillance technology yielded some noteworthy results. This study's findings support other studies, which have found that people tend to be either trusting (believe surveillance technology to be effective and non-invasive) or concerned (find surveillance technology to be ineffective and invasive), and do not engage in a privacy-security trade-off. This paper found that this non-trade-off extends from privacy-security to privacy-effectiveness. It also suggests that the public being divided into groups of either trusting or concerned is age/generation dependent – students are not yet either trusting or concerned across the board, and show no correlation between effectiveness and privacy. Another key finding is that as with privacy-effectiveness, also with effectiveness-cost – the public does not engage in a trade-off here either, but rather expects both to be achieved.

Only one significant difference revealed itself between SSJ minor and non-minor students, with the first group having lower expectations of effectiveness. Finally, respondents gave the same top reasons for both why NSA surveillance technology was effective and ineffective – collection of a lot of data.

This study's findings contribute to the surveillance debate in investigating these questions and correlations for the first time. They support recent literature in the privacy-security debate, which shows that the public does not engage in trade-offs between the different values involved, but rather, wants it all. The results merit further investigation, particularly as regards the age-correlation. It is a significant finding that groups of trusting or concerned people appear to be age-related. The differences between parents and students, and between students in and outside the minor also suggest that this is an age when views on security matters are shaped and with time are increasingly solidified. To have real and inclusive dialogue, policymakers should move away from a trade-off mentality and engage in dialogue with the public sooner rather than later.

## References

Adams, A.A. (2014), "Facebook code: SNS platform affordances and privacy", *Journal of Law, Information and Science*, Vol. 23 No. 1.

Adams, A.A., Murata, K., Fukuta, Y., Orito, Y. and Lara Palma, A.M. (2017), "Following Snowden around the world: international comparison of attitudes to Snowden's revelations about the NSA/GCHQ", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. 311-327.

Altheide, D.L. (2006), *Terrorism and the Politics of Fear*, AltaMira Press, Lanham, MD.

Anderson, D. (2015), "A question of trust – report of the investigatory powers review", available at: https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Asghari, H., Van Eeten, M. and Mueller, M. (2012), "Unravelling the economic and political drivers of deep packet inspection", in Baku.

Bendrath, R. and Mueller, M. (2011), "The end of the net as we know it? Deep packet inspection and internet governance", *New Media and Society*, Vol. 13 No. 7, pp. 1142-1160.

Cayford, M. and Pieters, W. (2018), "The effectiveness of surveillance technology: what intelligence officials are saying", *The Information Society*, Vol. 34 No. 2, pp. 88-103.

De Hert, P. (2005), "Balancing security and liberty within the European human rights framework", *Utrecht Law Review*, Vol. 1 No. 1, pp. 68-96.

Degli Esposti, S., Pavone, V. and Santiago-Gómez, E. (2017), "Aligning security and privacy: the case of deep packet inspection", In Michael, F. (Ed.), *Surveillance, Privacy and Security: Citizens' Perspectives*, PRIO New Security Studies, Routledge, London, pp. 71-90.

Degli Esposti, S. and Santiago-Gomez, E. (2015), "Acceptable surveillance-orientated security technologies: insights from the SurPRISE project", *Surveillance and Society*, Vol. 13 Nos 3/4, pp. 437-454.

Derix, S., Glenn, G. and Huib, M. (2013), "Dutch intelligence agency AIVD hacks internet forums", *nrc.Nl*, November 30, 2013, available at: www.nrc.nl/nieuws/2013/11/30/dutch-intelligence-agency-aivd-hacks-internet-fora-a1429280

DeSilver, D. (2014), "Most young Americans say Snowden has served the public interest", Pew Research Center, available at: www.pewresearch.org/fact-tank/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/

Diffie, W. and Landau, S.E. (2007), *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, Mass.

Doherty, C. (2013), "Balancing act: national security and civil liberties in post-9/11 era", Pew Research Center, available at: www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/ (accessed 31 January 2018).

Friedewald, M. and Pohoryles, R.J. (2013), "Technology and privacy", *Innovation: The European Journal of Social Science Research*, Vol. 26 Nos 1/2, pp. 1-6.

Fuchs, C. and Trottier, D. (2017), "Internet surveillance after Snowden: a critical empirical study of computer experts' attitudes on commercial and state surveillance of the internet and social media post-Edward Snowden", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 4, pp. 412-444.

Gao, G. (2015), "What Americans think about NSA surveillance, national security and privacy", Pew Research Center, available at: www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ (accessed 19 January 2018).

Guerrier, C. (2016), *Security and Privacy in the Digital Era*, John Wiley & Sons, Hoboken.

Gunasekara, G., Adams, A.A. and Murata, K. (2017), "Ripples down under: New Zealand youngsters' attitudes and conduct following Snowden", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. 297-310.

Kavathatzopoulos, I., Asai, R., Adams, A.A. and Murata, K. (2017), "Snowden's revelations and the attitudes of students at Swedish universities", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. 247-264.

Kraan, J. (2017), "Achtergrond: dit moet je weten over de 'aftapwet' en het referendum", *Nu.Nl*, October 9, 2017, available at: www.nu.nl/internet/4956455/achtergrond-moet-weten-aftapwet-en-referendum.html

Landau, S. (2014), "Security and privacy: facing ethical choices", *IEEE Security and Privacy*, Vol. 12 No. 4, pp. 3-6.

Madden, M. (2014), "Public perceptions of privacy and security in the post-Snowden era", Pew Research Center, available at: www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (accessed 19 January 2018).

Mansfield-Devine, S. (2015), "The privacy dilemma", *Network Security*, February, pp. 5-10.

Mols, A. and Janssen, S. (2017), "Not interesting enough to be followed by the NSA: an analysis of Dutch privacy attitudes", *Digital Journalism*, Vol. 5 No. 3, pp. 277-298.

Murata, K., Adams, A.A. and Lara Palma, A.M. (2017), "Following Snowden: a cross-cultural study on the social impact of Snowden's revelations", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. 183-196.

Olmstead, K. (2017), "Most Americans think the government could be monitoring their phone calls and emails", Pew Research Center, available at: www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails/ (accessed 31 January 2018).

Orru, E. (2013), "Review of European level studies on perceptions of surveillance", *Deliverable 3.2*, SURVEILLE.

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 (Bristol, England)*, Vol. 21 No. 5, pp. 556-572.

Pew Research Center (2013a), "Majority views NSA phone tracking as acceptable anti-terror tactic", available at: www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/ (accessed 31 January 2018).

Pew Research Center (2013b), "Public split over impact of NSA leak, but most want Snowden prosecuted", available at: www.people-press.org/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted/ (accessed 13 February 2018).

Pew Research Center (2013c), "Few see adequate limits on NSA surveillance program", available at: www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/ (accessed 30 January 2018).

Pew Research Center (2013d), "Most say monitoring allied leaders' calls is unacceptable", available at: www.people-press.org/2013/11/04/most-say-monitoring-allied-leaders-calls-is-unacceptable/ (accessed 31 January 2018).

Poullet, Y. (2004), "The fight against crime and/or the protection of privacy: a thorny debate!", *International Review of Law, Computers and Technology*, Vol. 18 No. 2, pp. 251-273.

Rainie, L. (2016), "The state of privacy in Post-Snowden America", Pew Research Center, available at: www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (accessed 1 February 2018).

Reddick, C.G., Chatfield, A.T. and Jaramillo, P.A. (2015), "Public opinion on national security agency surveillance programs: a multi-method approach", *Government Information Quarterly*, Vol. 32 No. 2, pp. 129-141.

Riezen, B.V. and Roex, K. (2012), "Counter-terrorism in The Netherlands and the United Kingdom: a comparative literature review study", *Social Cosmos*, Vol. 3 No. 1, pp. 97-110.

Shelton, M., Lee, R. and Madden, M. (2015), "Americans' privacy strategies post-Snowden" Pew Research Center, available at: www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ (accessed 19 January 2018).

Stahl, B. (2007), "Privacy and security as ideology", *IEEE Technology and Society Magazine*, Vol. 26 No. 1, pp. 35-45.

Stalla-Bourdillon, S., Joshua, P. and Ryan, M.D. (2014), *Privacy vs. Security. Springer Briefs in Cybersecurity*, Springer, London.

Tene, O. (2011), "Privacy: the new generations", *International Data Privacy Law*, Vol. 1 No. 1, pp. 15-27.

Trottier, D. (2012), *Social Media as Surveillance: Rethinking Visibility in a Converging World*, Ashgate, Surrey.

Trottier, D. and Lyon, D. (2012), "Key features of social media surveillance", in *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, Routledge, New York, NY, pp. 89-105.

van den Broek, T., Ooms, M., Friedewald, M., van Lieshout, M. and Rung, S. (2017), "Privacy and security: citizens' desires for an equal footing", In *Surveillance, Privacy and Security: Citizens' Perspectives*, Michael, F. (Ed.), PRIO New Security Studies, Routledge, London, pp. 15-35.

## Further reading

Dillon, T.W. and Thomas, D.S. (2015), "Exploring the acceptance of body searches, body scans and TSA trust", *Journal of Transportation Security*, Vol. 8 Nos 3/4, pp. 51-67.

Lieshout, M.V., Friedewald, M., Wright, D. and Gutwirth, S. (2013), "Reconciling privacy and security", *Innovation: The European Journal of Social Science Research*, Vol. 26 Nos 1/2, pp. 119-132.

Madden, M. and Rainie, L. (2015), "Americans' attitudes about privacy, security, and surveillance", Pew Research Center, available at: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf (accessed 19 January 2018).

Mitrou, L. (2008), "Communications data retention: a Pandora's box for rights and liberties?", in *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, pp. 409-433.

Schneier, B. (2014), *Carry on: Sound Advice from Schneier on Security*, John Wiley & Sons, Hoboken, NJ.

Verfaillie, K. and Herrewegen, E.v.d. (2012), "Public assessments of the security/privacy trade-off: a criminological conceptualization", *Deliverable 4.1*, PRISMS.

Završnik, A. and Levičnik, P. (2015), "The public perception of cyber-surveillance before and after Edward Snowden's surveillance revelations", *Masaryk University Journal of Law and Technology*, Vol. 9 No. 2.

## Corresponding author

Michelle Cayford can be contacted at: m.r.cayford@tudelft.nl