Public Feeling on Privacy, Security and Surveillance

A Report by DATA-PSST and DCSS

November 2015

Contributors

Vian Bakir, Bangor University
Network for the Study of Media and Persuasive Communication (MPC)
ESRC Seminar Series: Debating & Assessing Transparency Arrangements - Privacy, Security, Surveillance, Trust (DATA - PSST!)
v.bakir@bangor.ac.uk

Jonathan Cable, Cardiff University
ESRC Digital Citizenship and Surveillance Society Project (DCSS)
cablej1@cardiff.ac.uk

Lina Dencik, Cardiff University
ESRC Digital Citizenship and Surveillance Society Project (DCSS)
DencikL@cardiff.ac.uk

Arne Hintz, Cardiff University
ESRC Digital Citizenship and Surveillance Society Project (DCSS)
HintzA@cardiff.ac.uk

Andrew McStay, Bangor University
Network for the Study of Media and Persuasive Communication (MPC)
ESRC Seminar Series: Debating & Assessing Transparency Arrangements - Privacy, Security, Surveillance, Trust (DATA - PSST!)
mcstay@bangor.ac.uk

Public Feeling on Privacy, Security and Surveillance
A Report by DATA-PSST and DCSS

Contents

Public Feeling on Privacy, Security and Surveillance
A Report by DATA-PSST and DCSS

Need for Report

Edward Snowden's revelations in June 2013 prompted major debates around the topics of privacy, national security, and mass digital surveillance. Within these debates, the British government and its intelligence agencies regularly invoke British public opinion as:

a) desiring greater security, and;
b) probably being prepared to give up privacy to enhance security.

For instance:

- '*we do not subscribe to the point of view that it is acceptable to let some terrorist attacks happen in order to uphold the individual right to privacy—nor do we believe that the vast majority of the British public would'* (Intelligence and Security Committee , *Privacy and Security: A Modern and Transparent Legal Framework*. House of Commons [12 March]. 2015: 36).
- '*To those of us who have to tackle the depressing end of human behaviour on the internet, it can seem that some technology companies are in denial about its misuse. I suspect most ordinary users of the internet are ahead of them: they have strong views on the ethics of companies, whether on taxation, child protection or privacy; they do not want the media platforms they use with their friends and families to facilitate murder or child abuse. They know the internet grew out of the values of western democracy, not vice versa. I think those customers would be comfortable with a better, more sustainable relationship between the agencies and the technology companies*.' (Robert Hannigan, Director of GCHQ, *The Financial Times,* Nov.2014, arguing that tech firms need to help security services monitor the internet)

Others recognise that while the public want more security, they don't want to sacrifice their privacy:

- '*There is a dilemma because the general public, politicians and technology companies, to some extent, want us to be able to monitor the activities of terrorists and other evil-doers but they don't want their own activities to be open to any such monitoring*.' (Sir John Sawers, ex-Director of Secret Intelligence Service (MI6) *The Telegraph*, January 2015)

However, what does the public actually think on privacy, security, and the Snowden leaks? Is the public prepared to give up privacy for security?

Studies Consulted

To answer these questions, this report draws on the following studies:

- The ongoing *Digital Citizenship and Surveillance Society Project* (DCSS) at Cardiff University into UK public opinion on the Snowden leaks, comprising analysis of opinion polls and in-depth focus groups with different demographics of the public in England and Wales.
- The published in-depth, participatory study, *Surveillance, Privacy and Security* (SurPRISE), of 2000 citizens from nine European countries (Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and United Kingdom) on attitudes towards surveillance-oriented security technologies and privacy (Pavone et al. 2015). This study involved large citizen summits conducted in 2014 to generate quantitative data and to explore public views on these complex matters in much more depth than opinion polls can deliver. Part of this project comprises a UK country study (Ball et al. 2015). These studies focused on three security-oriented surveillance technologies:

  (a) Smart Closed Circuit Television. This features digital cameras which are linked together in a system that has the potential to recognise people's faces, analyse their behaviour and detect objects.

  (b) Deep packet inspection. This detects and shapes how messages travel on a network. It opens and analyses messages as they travel, identifying those that may pose particular risks.

  (c) Smartphone location tracking. This analyses location data from a mobile phone, to glean information about the location and movements of the phone user over a period of time. NB UK participants were not asked to consider (c).
- Published advertising industry studies (opinion polls) on privacy and commercial surveillance.

Synthesising these studies, we provide the following observations and recommendations.

Observations

1. Unlike the UK government, the British public sees bulk data collection as constituting mass surveillance.
2. The topics of UK state surveillance of digital communications and online privacy matter to the British, and wider EU public. This is confirmed by opinion poll data since 2013 and in-depth studies.
3. The EU and UK public think some surveillance technologies are useful/effective for combating national security threats, and should be used, but acceptability varies according to whether the surveillance is of communications or bodies, and blanket or targeted. Surveillance of physical bodies (smart CCTV) and targeted surveillance of digital communications (smartphone location tracking) are more accepted than blanket surveillance of digital communications (deep packet inspection).
4. The EU and UK public think that although certain surveillance technologies are useful/effective for combating national security threats, they compromise human rights and are abused by security agencies. These concerns especially apply to deep packet inspection.

5. In the UK, those under 60 see UK state surveillance of digital communications as going too far, and an infringement upon the right to privacy. Over 60s do not. This finding is echoed by EU-wide studies.
6. In the UK, it is younger people & ethnic minorities who are most concerned about lack of transparency & consent when it comes to state surveillance of digital communications.
7. There are identifiable criteria for what makes security-oriented surveillance technologies acceptable for EU publics. Targeted rather than blanket surveillance is preferred, as are clear communications to citizens about what is going on, with strong regulatory oversight.
8. All age groups in the UK, especially those over 55, are strongly concerned about commercial surveillance, and increasingly take concrete steps to defend against intrusive behaviour by advertising companies. This suggests that if people *could* do more about state surveillance, they would.
9. There are a range of tools and behaviour change open to people to defend against state surveillance.

Recommendations

1. Given Observation 1, the UK government has more work to do if it wants to persuade the British public that Bulk Data Collection is different to mass digital surveillance.
2. Given Observation 2, the UK government should take into consideration public views on digital surveillance and privacy.
3. Given Observation 3, the UK government has a public mandate to use some surveillance technologies for combating national security threats. However this mandate is much weaker for blanket surveillance of digital communications (deep packet inspection) than more targeted surveillance of digital communications (smartphone location tracking) or surveillance of physical bodies (Smart CCTV).
4. Observation 4 shows that the UK government has more work to do if it wants to persuade the British public that its security agencies do not abuse their surveillance powers, especially concerning deep packet inspection. Observations 5 and 6 show that the least persuaded are those under 60 and ethnic minorities.
5. Given observation 7, governments seeking a popular mandate for digital surveillance should ensure that such surveillance is targeted rather than blanket, accompanied by strong regulatory oversight and clear communications to citizens about what is going on.
6. Given public concerns over blanket digital surveillance, observation 8 which shows people taking increasing action against commercial digital surveillance, and observation 9 which shows that there are things people can use and do to mitigate state surveillance, this suggests that unless the UK government provides a digital surveillance architecture that is acceptable to its people, it is quite possible that people will refuse this surveillance.

Digital Citizenship and Surveillance Society (DCSS) Study: Quantitative Findings

Edward Snowden's revelations in June 2013 prompted major debates around the topics of privacy, national security, and mass surveillance. The evidence for this is that there have been approximately 40 UK public opinion polls on these subjects since June 2013. The results of these polls detail the level of concern within the population of the UK. Overall, we see an increase in concerns with online privacy since the revelations, and particularly amongst younger people there are also substantial concerns with levels of interception and existing surveillance powers of the state. In particular, issues regarding lack of transparency over what and how data is collected as well as the nature and level of public consent are prominent amongst the British public. This section provides a brief overview of some of these findings.

Importance of the Topic of Surveillance

There is a general sense that the topic of state surveillance matters to the British public. This is evidenced by public opinion of what Snowden did. From June 2013 to November 2013 there were 4 YouGov polls which asked the question "Do you think Mr Snowden was right or wrong to give this information to the press?" In all 4 of the polls a majority of the British public said Snowden was 'right' to do what he did (See YouGov polls 13/06/13, 14/06/13, 28/08/13 and 05/11/13). Taken together the 4 poll results average out to 49% thought Snowden was 'right' to do what he did, compared to 32% who believed Snowden was 'wrong' to leak the documents to the press.

The importance of this issue to the general public can also be seen in an Angus Reid Global poll from October 2013 which asked 'Overall, how important do you yourself consider this whole issue of government surveillance of the public's internet communications to be'? By a large majority 82% of respondents felt that this issue was either 'very' or 'quite important', and only 17% responded 'not that important' or 'not important at all'.

Concerns Over Privacy

Similarly, the level of public concern about online privacy is reflected in the yearly TRUSTe Privacy Index conducted by Ipsos-MORI. Each year the public is asked "How often do you worry about your privacy online?" in 2014 the total amount of people who worried either 'sometimes', 'frequently' or 'always' was 89%. In 2015 in answer to the same question the proportion of people who worried about their online privacy had risen to 92%. The public were also asked in 2014 if they were more worried about their online privacy than a year ago, and given that this particular poll was carried out one year after the Snowden revelations the result is quite telling. A total of 60% of the British public felt more worried about their online privacy than a year ago. The poll enquired about what the public's main concerns were online. This included concerns such as businesses sharing personal information, and companies tracking online behaviour. In both 2014 and 2015 20% of people cited government surveillance as one of their top causes for concern.

Also, when the public was asked specifically about the privacy of online and mobile data by Ipsos Mori in May 2014 they saw this being either 'essential' or 'important' by a very large margin. The results broke down as: the privacy of internet browsing records – essential/important 85%, not important 12%; content of emails – essential/important 91%, not important 6%; mobile phone location – essential/important 79%, not important 18%.

Concerns Over State Powers

Concerns over the levels of powers granted to state agencies are often framed along the lines of privacy vs. security. As outlined below, opinion polls show greater support for increased surveillance powers at the expense of privacy amongst older generations, particularly the 60+. All other age groups show a greater concern with surveillance as an infringement upon the right to privacy. The common thread running through these polls is the question of whether or not the security services should be allowed to intercept, store, and analyse digital data. The polls detailed below covers June 2013 to March 2015. (For the full statistics please see Appendix 1.) This demonstrates that the public's concern is not abating as time moves on from the Snowden revelations.

The first such poll of the post-Snowden era was published in June 2013 by YouGov. They asked if the security services should be given the powers to access the public's data such as web browsing, email and social media activities held by mobile phone companies and internet service providers. The question does however make it clear that this does not mean the content of social media and emails. That said, the proportion of people who said this would 'go too far' was 43% vs 38% who believed it was a 'good idea'.

The divide between the age groups is clear. The three categories between 18 and 59 came out in the majority stating this proposal went 'too far', and only the 60+ thought it was a 'good idea'. There were subsequent variations of this question in other polls but the proportions of people for and against remained consistently opposed to bulk data collection by the security services. The YouGov poll from October 2013 for instance asked whether the security services "should or should not be allowed to store the details (but not the actual contents) of ordinary people's communications" the top line results were 38% said they 'should be allowed', but the majority 46% said they 'should not'. In this instance every single age group came out against this data collection.

When YouGov repeated the question and answer options from the June 2013 poll in July 2014 the results were almost identical one year on. Overall 41% of people thought that granting the security services access to personal data went 'too far', and 37% believed this would be a 'good idea'. The spread of opinion across the age groups remained the same as the June 2013 poll. All three age ranges between 18 and 59 stating this power 'goes too far' and only the 60+ category came out in majority for 'is a good idea'.

Concerns Over 'Bulk' Data Collection

The second part of the polling data orientated around the clandestine nature of the interception of personal data. Following the Edward Snowden revelation in August 2013 that GCHQ had been accessing fibre optic communications cables in secret to capture and store peoples' data regardless of any wrongdoing YouGov asked the public whether or not they thought this was right or wrong. The overall results of the poll showed a public relatively evenly divided where 41% said what GCHQ did was 'right', compared with 45% who said that this was 'wrong'. It is in the age differences where a real divide showed itself. Only 24% of 18-24 year olds thought that this was 'right' compared to 39% 25-39 year olds, 43% 40-59, and 46% 60+. The 60+ age group was again the only segment which came out in the majority for 'it is right'.

In March 2015 YouGov asked the British public if GCHQ did have the resources and capability to intercept/collect the internet-based communications of everyone could they be trusted not to abuse this ability? A majority of 42% came out in favour of 'no' compared to 34% who said 'yes' they could trust GCHQ. Similarly, YouGov conducted a poll on behalf of Amnesty International where the public were asked if they thought that their government should or should not intercept, store and analyse internet use and mobile phone communications of all citizens living in the country. The majority of the British public again came out on the side of 'should not intercept' 44% versus 'should intercept' 36%. What is clear from the opinion poll results is that the total figures are heavily influenced by the 60+ age bracket. Their lack of concern with privacy is not shared by younger age groups. These polls also demonstrate that blanket mass collection of communications data is of real concern to vast sections of the population.

Digital Citizenship and Surveillance Society (DCSS) Study: Qualitative findings

In addition to analysing opinion polls, the DCSS project conducted a series of focus groups with different demographics of the public in England and Wales.

Younger People & Ethnic Minorities are most Concerned about Lack of Transparency & Consent

The results of these focus groups support data from opinion polls regarding concerns with online privacy and state powers, but particularly highlight concerns with a lack of transparency regarding the collection and use of data, as well as concerns with an absence of obtaining public consent. These concerns are more prominent amongst some demographics, relating to both age as well as ethnic background with minorities expressing greater concern.

Bulk Data Collection constitutes Surveillance

DCSS' focus groups explored definitions of surveillance, including the collection of metadata. UK intelligence agencies present their surveillance of digital communications as 'bulk data collection', Rejecting the term "surveillance", intelligence agencies state that rather than conducting blanket searches, as implied by press accounts of 'indiscriminate' or 'drag-net' surveillance, they only search for specific information (ISC 2015). The UK's intelligence oversight committee concludes that such 'bulk data collection' does not constitute mass surveillance since British intelligence agencies do not have 'the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the internet as a whole' (ISC 2015: 2). However, the general consensus from DCSS' focus groups was that the collection of metadata is seen as surveillance. The reasons given by members of the public centred around ideas such as giving consent for data collection, personal ownership of data, questions around why this data would need to be collected, the lack of anonymity and the ability to be identified by the collection of metadata.

Public Resignation, rather than Apathy or Consent, over State Surveillance

Overall, DCSS' focus groups highlighted a prominent concern with the collection of online data by a number of different actors, but also a lack of understanding or sense that it is possible to do much about it. In that sense, focus groups results indicate that *state surveillance is being carried out on the basis of public resignation rather than apathy or consent*.

Surveillance, Privacy and Security (SurPRISE) Study

An in-depth, participatory study, 'SurPRISE', of 2000 citizens conducted across the European Union (EU) in 2014 finds that the EU public want both better national security through surveillance *but that they also want better* privacy – they do not accept a trade-off between the two (Pavone et al. 2015).

EU Public (especially Younger People) Concern about State Surveillance

As with the DCSS study, SurPRISE finds that across the EU, age makes a difference. Age is positively correlated with the acceptability of security-oriented surveillance technologies.

EU Public think some Surveillance Technologies are Useful/Effective for Combating National Security Threats

Most people in the EU agree or strongly agree that security-oriented surveillance technologies are effective national security tools – especially Smart CCTV (64% agreement) and smartphone location tracking (54% agreement) (see Appendix 2.1). Furthermore, more people than not also feel that these are appropriate ways to address national security threats – especially Smart CCTV (51% agreement) although less so smartphone location tracking (42% agreement) and deep packet inspection (41% agreement) (see Appendix 2.2). Overall, more people than not support security-oriented surveillance technologies as a national security measure – especially Smart CCTV (63% agreement) and smartphone location tracking (58% agreement) (see Appendix 2.3).

EU Public think all Surveillance Technologies Compromise Human Rights and are Susceptible to Abuse by Security Agencies

Despite supporting security-oriented surveillance technologies as a national security measure, most people in the EU agree or strongly agree that security-oriented surveillance technologies could violate everyone's fundamental human rights – especially deep-packet inspection (82% agreement) and smartphone location tracking (72% agreement), followed by Smart CCTV (59% agreement) (see Appendix 2.4). Furthermore, more people than not disagree or strongly disagree that security agencies using these security-oriented surveillance technologies do not abuse their powers – especially deep-packet inspection (56% disagreement) although less so for Smart CCTV (48% disagreement) and smartphone location tracking (36% disagreement) (see Appendix 2.5).

To summarise, the EU public thinks that certain surveillance technologies are useful/effective for combating national security threats, but that all such technologies compromise human rights and are abused by security agencies. These concerns especially apply to deep packet inspection.

SurPRISE also demonstrates that while there are differences according to nation and security-oriented surveillance technology, on the whole:

- The public does not accept blanket mass surveillance. Security-oriented surveillance technologies that operate blanket surveillance are found significantly less acceptable than those that carefully focus on specific targets.
- The public demands enforced and increased accountability, liability and transparency of private and state surveillant entities.

Drilling down into the EU data, the UK's national study finds similar results (Ball et al. 2014).

SurPRISE: UK National Report

UK Public Concern about Privacy

UK participants were concerned about the privacy of the general public (63% express concerns) and about their own personal privacy (66% express concerns). 76% are afraid that too much information is collected about them, with many worried that the personal data held about them may be inaccurate (74%), shared without their permission (96%), or used against them (68%) (see Appendix 2.6).

UK Public think Surveillance-oriented Security Technologies Improve National Security and Should be Used

Despite their privacy concerns, 90% of UK participants think that surveillance-oriented security technologies improve national security, and 80% think that since these technologies are available, governments might as well use them (see Appendix 2.7). However, support for deep packet inspection (at 56%) is much less than support for Smart CCTV (88%) (see Appendix 2.8).

UK Public think all Surveillance Technologies Compromise Human Rights and are Susceptible to Abuse by Security Agencies

Over half of UK participants (55%) worry that once in place, surveillance-oriented security technologies might be abused (see Appendix 2.7). While 46% agree that security agencies using Smart CCTV have the welfare interests of citizens at heart, only 31% consider them competent, and only 29% viewed them as trustworthy, with large amounts undecided. Only 16% considered that these agencies would not abuse their power, with far more (41%) expressing doubts that such abuses would not occur, and similar amounts undecided (see Appendix 2.9).

The figures for deep packet inspection are similar, with 41% satisfied that agencies that implement this technology were focused on citizen welfare. Only 29% view agencies that implement this technology as competent, and only 30% consider them to be trustworthy, with large amounts undecided. Once again, participants were more cynical about the extent to which security agencies might abuse their power, with 45% expressing doubts that such abuses would not occur, and large amounts undecided (see Appendix 2.10).

General Policy Recommendations from UK Participants

Following the citizen summits, participants were asked to make policy recommendations. UK participants recommended the following (Ball et al. 2014: 32-33).

On Transparency and communication

- Raise citizen awareness about the use of security-oriented surveillance technologies.
- Provide greater clarity about whom, how and where gathered information/data is held and used.
- Give citizens access to information that the security services and others hold about them.

On Responsibility for regulating and implementing security-oriented surveillance technologies.

- They should be governed by transparent and understandable legislation.
- Establish an independent regulatory body with responsibility for overseeing use of security-oriented surveillance technologies, and which sets rules about handling the gathered information/data.
- Government should ensure that any information/data collected through security-oriented surveillance technologies is held within the UK and not sent elsewhere.
- Nationally control security-oriented surveillance technologies, but to an EU standard.
- Do not involve private companies in operating security-oriented surveillance technologies or give them access to the information/data produced.

EU Public Criteria for What Makes Security-Oriented Surveillance Technologies Acceptable

As with the findings on the UK, the wider SurPRISE study finds that a common criterion determining the acceptability of security-oriented surveillance technologies by the European public is that they are operated by transparent, accountable public agencies that inform citizens about their purposes and functions (Pavone et al. 2015).

The study's full list of criteria for what makes security-oriented surveillance technologies acceptable to EU citizens is as follows:

a) Operate under an international legislative framework, monitored by a data protection authority with sufficient powers at the European level;

b) Are operated by transparent, accountable public agencies that inform citizens about their purposes and functions;

c) Are cost-effective and allow citizens to access and control the data that security services retrieve and store;

d) Always target the least sensitive data, only in public spaces, whenever possible and be specifically orientated towards suspects and criminal activities;

e) Are deployed only after significant evidence has been collected and only after judicial authorities grant permission;

f) Incorporate Privacy-by-Design mechanisms and principles;

g) Do not replace but complement human intervention, as part of a broader, socially informed, security strategy that addresses also the social and economic causes of crime and violence.

Public Perceptions of Privacy from the Advertising Industry

While not ostensibly focused on the Snowden revelations it is instructive to look at poll findings about public perceptions of privacy from the advertising industry, such as the Internet Advertising Bureau (IAB), an organisation that champions the collective interests of the UK ad-tech industry. This is relevant because:

- The advertising industry has an interest in overcoming people's privacy concerns;
- Public concerns about online privacy from commercial and state surveillant entities arguably overlap;
- Because of the overlap, Snowden's revelations have dented the potential for trust in the online *environment*.
- People actively take steps to prevent commercial surveillance – and this could be an indicator of what they might be prepared to do regarding state surveillance, if only they could.

Everyone Wants More Online Privacy (this Pre-dates Snowden)

Pre-Snowden, in 2012, the IAB found that: 89% of people 'want to be in control of their online privacy'. While this is not surprising, their finding that 62% 'worry about online privacy' is notable. The findings in the IAB (2012) study differ here from poll findings on concern over state surveillance in that it is over 55s who most demonstrate a wish for online privacy (93%), although younger people also seek control (84%) (IAB 2012).

Post-Snowden, data from TRUSTe (2014) on UK perceptions also highlight high levels of concern about advertising with 89% of British internet users worried about their online privacy. Furthermore, due to privacy concerns, Britons are less likely to click on an online ad (91%), use apps they do not trust (78%) or enable online tracking (68%). More recent 2015 commentary from the IAB shows increased interest in privacy. This is in response to unequivocal consumer concern and the forthcoming new European framework for data protection in Europe. They suggest now is 'a real opportunity to create incentives for organisations to build privacy-enhancing measures and embrace a truly 'privacy by design' approach' (IAB 2015b).

People increasingly Defend Themselves against Intrusive Behaviour by Advertising Companies

It is interesting to also consider defences that people take against intrusive behaviour by advertising companies. Although deletion of browsing history remains the foremost means to avoid tracking cookies, in the commercial sectors adblockers and anti-trackers are used at rates that worry the advertising industry. PageFair (2014) found that in the UK 15 per cent of British adults online currently use adblocking software, while 22 per cent have downloaded the software at some point. Unsurprisingly this skewed towards the young, as 34 per cent of 18-24 year olds are most likely to block ads.

A recent IAB (2015a) report finds privacy concerns are cited as a reason for blocking ads (31% cite privacy concerns), although this is certainly not users' main concern. Ads are most likely to be blocked because: they are interruptive (73%); the design can be annoying (55%); and ads slow down users' web browsing experience (54%).

If People *Could* Mitigate State Surveillance, Would They, & What Would They Do?

From the studies consulted, it is clear that online privacy is important to people both in regards to state surveillance and commercial surveillance.

Furthermore, people can take steps regarding commercial surveillance – and increasingly they are doing so. Taking steps against state digital surveillance is less fine-tuned.

What Can People do to Mitigate State Surveillance

People can:

- Encrypt their communications (for instance, using services that encrypt end-to-end, like email *Ghostmail*, social media platform *Whatsapp* or web browser *Tor*);
- Choose to use digital communications platforms that do not track communications (eg Search Engines like *DuckDuckGo*);
- Try to obfuscate their information, individually or collectively, by adding noise to existing data collection to make its results ambiguous and hence less valuable. Examples include swapping store loyalty cards; utilising a *FaceCloak* plug-in that gives users a choice, on creating a *FaceBook* profile, as to who will see their personal data; and using plugin *TrackMe Not* that foils the profiling of users through their web searches by creating ghost queries that make users' pattern of real queries harder to discern (Brunton & Nissenbaum 2015);
- Reduce what is posted, shared and searched. They may even choose not to use digital communication platforms at all (going 'off-grid'), but as the Anderson Report (2015) notes, this means not participating in 21st century life).

Will People Act to Mitigate State Surveillance?

Given this range of tools and behaviour change open to people to defend against state surveillance, the crucial question for all concerned with such issues, including politicians, regulators, businesses and activists, is:

- Whether people will act to mitigate state surveillance;
- Whether technology companies will act on people's behalf to mitigate state surveillance, for instance, by making encryption a default mode.

Since Snowden's leaks, intelligence agencies have publicly lamented the internet 'going dark' (Comey 2015; ISC 2015: 9). The extent to which this becomes a widespread reality has yet to be seen. No doubt this will be determined by a range of factors – not least public feeling on privacy, security and surveillance.

Observations and Recommendations

Drawing on these studies, we make the following observations and recommendations.

Observations

1. Unlike the UK government, the British public sees bulk data collection as constituting mass surveillance.
2. The topics of UK state surveillance of digital communications and online privacy matter to the British, and wider EU public. This is confirmed by opinion poll data since 2013 and in-depth studies.
3. The EU and UK public think some surveillance technologies are useful/effective for combating national security threats, and should be used, but acceptability varies according to whether the surveillance is of communications or bodies, and blanket or targeted. Surveillance of physical bodies (smart CCTV) and targeted surveillance of digital communications (smartphone location tracking) are more accepted than blanket surveillance of digital communications (deep packet inspection).
4. The EU and UK public think that although certain surveillance technologies are useful/effective for combating national security threats, they compromise human rights and are abused by security agencies. These concerns especially apply to deep packet inspection.
5. In the UK, those under 60 see UK state surveillance of digital communications as going too far, and an infringement upon the right to privacy. Over 60s do not. This finding is echoed by EU-wide studies.
6. In the UK, it is younger people & ethnic minorities who are most concerned about lack of transparency & consent when it comes to state surveillance of digital communications.
7. There are identifiable criteria for what makes security-oriented surveillance technologies acceptable for EU publics. Targeted rather than blanket surveillance is preferred, as are clear communications to citizens about what is going on, with strong regulatory oversight.
8. All age groups in the UK, especially those over 55, are strongly concerned about commercial surveillance, and increasingly take concrete steps to defend against intrusive behaviour by advertising companies. This suggests that if people *could* do more about state surveillance, they would.
9. There are a range of tools and behaviour change open to people to defend against state surveillance.

Recommendations

1. Given Observation 1, the UK government has more work to do if it wants to persuade the British public that Bulk Data Collection is different to mass digital surveillance.
2. Given Observation 2, the UK government should take into consideration public views on digital surveillance and privacy.
3. Given Observation 3, the UK government has a public mandate to use some surveillance technologies for combating national security threats. However this mandate is much weaker for blanket surveillance of digital communications (deep packet inspection) than

more targeted surveillance of digital communications (smartphone location tracking) or surveillance of physical bodies (Smart CCTV).

4. Observation 4 shows that the UK government has more work to do if it wants to persuade the British public that its security agencies do not abuse their surveillance powers, especially concerning deep packet inspection. Observations 5 and 6 show that the least persuaded are those under 60 and ethnic minorities.
5. Given observation 7, governments seeking a popular mandate for digital surveillance should ensure that such surveillance is targeted rather than blanket, accompanied by strong regulatory oversight and clear communications to citizens about what is going on.
6. Given public concerns over blanket digital surveillance, observation 8 which shows people taking increasing action against commercial digital surveillance, and observation 9 which shows that there are things people can use and do to mitigate state surveillance, this suggests that unless the UK government provides a digital surveillance architecture that is acceptable to its people, it is quite possible that people will refuse this surveillance.

References

Anderson, D. 2015. *A question of trust: Report of the investigatory powers review*. OGL. Retrieved from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Ball, K. et al. 2014. *Citizen Summits on Privacy, Security and Surveillance: Country report United Kingdom.* *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*. Retrieved from http://surprise-project.eu/

Comey, J. 2015. Encryption, Public Safety, and "Going Dark". *Lawfare*. Retrieved from https://www.lawfareblog.com/encryption-public-safety-and-going-dark

Brunton, F. & Nissenbaum, H. 2015. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge: MIT Press.

IAB 2012. *Consumers and Online Privacy 2012 - Bitesize Guide*. Retrieved from http://www.iabuk.net/sites/default/files/Consumers%20and%20Online%20Privacy%202012%20-%20Bitesize%20Guide.pdf

IAB 2015a. *15% of Britons online are blocking ads*. Retrieved from http://www.iabuk.net/about/press/archive/15-of-britons-online-are-blocking-ads

IAB 2015b. IAB believes in PRIVACY. Retrieved from http://www.iabuk.net/blog/the-iab-believes-in-privacy

ISC. 2015. *Privacy and Security: A Modern and Transparent Legal Framework*. House of Commons [12 March]. Intelligence and Security Committee. Retrieved from http://isc.independent.gov.uk/

Pavone, V., Esposti, S.D. and Santiago, E. 2015. *D2.4 – Key factors affecting public acceptance and acceptability of SOSTs. SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*. Retrieved from http://surprise-project.eu/

PageFair 2014. Adblocking Goes Mainstream. Retrieved from http://blog.pagefair.com/2014/adblocking-report/

TRUSTe 2014. 2013 UK Consumer Data Privacy Study: Advertising Edition. Retrieved from https://www.truste.com/resources/privacy-research/uk-consumer-confidence-index-2014/

Appendix 1. Polls Studied by DCSS

<table>
<tr><th>Poll</th><th colspan="6">Question</th></tr>
<tr><td>YouGov June 2013</td><td colspan="6">It has been suggested that the law should be changed to give police and security services access to the records kept by mobile phone and internet service provider companies. These would include individuals' web browsing, email and social media activity, though not the content of emails or social messages. In principle do you think this proposal...</td></tr>
<tr><td></td><td><b>Answers</b></td><td><b>Total</b></td><td><b>18-24</b></td><td><b>25-39</b></td><td><b>40-59</b></td><td><b>60+</b></td></tr>
<tr><td></td><td>Goes too far: it undermines our right to privacy</td><td>43</td><td>50</td><td>44</td><td>47</td><td>36</td></tr>
<tr><td></td><td>Is a good idea, given the way technology is evolving</td><td>38</td><td>28</td><td>31</td><td>38</td><td>49</td></tr>
<tr><td></td><td colspan="6"><b>Question</b></td></tr>
<tr><td>YouGov August 2013</td><td colspan="6">As you may know, Edward Snowden, a former US intelligence officer, has disclosed that GCHQ, a British intelligence agency, has been secretly accessing fibre-optic cables carrying internet and communication data. It can tap into and store anybody's phone calls and emails for up to 30 days, regardless of whether they are suspected of doing anything wrong. Which of these views comes closer to yours?</td></tr>
<tr><td></td><td><b>Answers</b></td><td><b>Total</b></td><td><b>18-24</b></td><td><b>25-39</b></td><td><b>40-59</b></td><td><b>60+</b></td></tr>
<tr><td></td><td>It is right: the secret service should have access to this information in order to protect the nation</td><td>41</td><td>24</td><td>39</td><td>43</td><td>46</td></tr>
<tr><td></td><td>It is wrong: the secret service should not have the power to eavesdrop into innocent people's private affairs</td><td>45</td><td>58</td><td>42</td><td>45</td><td>43</td></tr>
<tr><td></td><td colspan="6"><b>Question</b></td></tr>
<tr><td>YouGov October 2013</td><td colspan="6">Do you think the security services should or should not be allowed to store the details (but not the actual contents) of ordinary people's communications, such as emails and mobile phone calls?</td></tr>
<tr><td></td><td><b>Answers</b></td><td><b>Total</b></td><td><b>18-24</b></td><td><b>25-39</b></td><td><b>40-59</b></td><td><b>60+</b></td></tr>
<tr><td></td><td>Should be allowed</td><td>38</td><td>32</td><td>38</td><td>39</td><td>41</td></tr>
<tr><td></td><td>Should not be allowed</td><td>46</td><td>47</td><td>48</td><td>47</td><td>45</td></tr>
<tr><td></td><td colspan="6"><b>Question</b></td></tr>
<tr><td>Ipsos Mori May 2014</td><td colspan="6">How important, if at all, do you think it is to maintain the privacy of each of the following?</td></tr>
<tr><td></td><td><b>Answers</b></td><td colspan="2"><b>Essential / Important</b></td><td colspan="3"><b>Not Important</b></td></tr>
<tr><td></td><td>Internet browsing records</td><td colspan="2">85</td><td colspan="3">12</td></tr>
<tr><td></td><td>Content of emails</td><td colspan="2">91</td><td colspan="3">6</td></tr>
<tr><td></td><td>Mobile phone location</td><td colspan="2">79</td><td colspan="3">18</td></tr>
<tr><td></td><td colspan="6"><b>Question</b></td></tr>
<tr><td>YouGov July 2014</td><td colspan="6">It has been suggested that the law should be changed to give police and security services access to the records kept by mobile phone and internet service provider companies. These would include individuals' web browsing, email and social media activity, though not the content of emails or social messages. In principle do you think this proposal...</td></tr>
<tr><td></td><td><b>Answers</b></td><td><b>Total</b></td><td><b>18-24</b></td><td><b>25-39</b></td><td><b>40-59</b></td><td><b>60+</b></td></tr>
<tr><td></td><td>Goes too far: it undermines our right to privacy</td><td>41</td><td>51</td><td>43</td><td>44</td><td>32</td></tr>
<tr><td></td><td>Is a good idea, given the way technology is evolving</td><td>37</td><td>24</td><td>30</td><td>38</td><td>46</td></tr>
<tr><td></td><td colspan="6"><b>Question</b></td></tr>
<tr><td>YouGov March 2015</td><td colspan="6">If indeed they DID [GCHQ] have the resources and capability to intercept/collect the internet-based communications of every British citizen, would you trust them not to abuse that capability?</td></tr>
<tr><td></td><td colspan="5"><b>Answers</b></td><td><b>Total</b></td></tr>
<tr><td></td><td colspan="5">Yes</td><td>34</td></tr>
<tr><td></td><td colspan="5">No</td><td>42</td></tr>
</table>

	Question	
YouGov March 2015	Do you think the [your country] Government should or should not intercept, store and analyse internet use and mobile phone communications of all [your country] citizens living in the [your country]	
	Answers	**Total**
	Should intercept, store and analyse internet use and mobile communications	36
	Should not intercept, store and analyse internet use and mobile communications	44

Appendix 2. SurPRISE Results

2.1. Pavone et al (2015: 115)

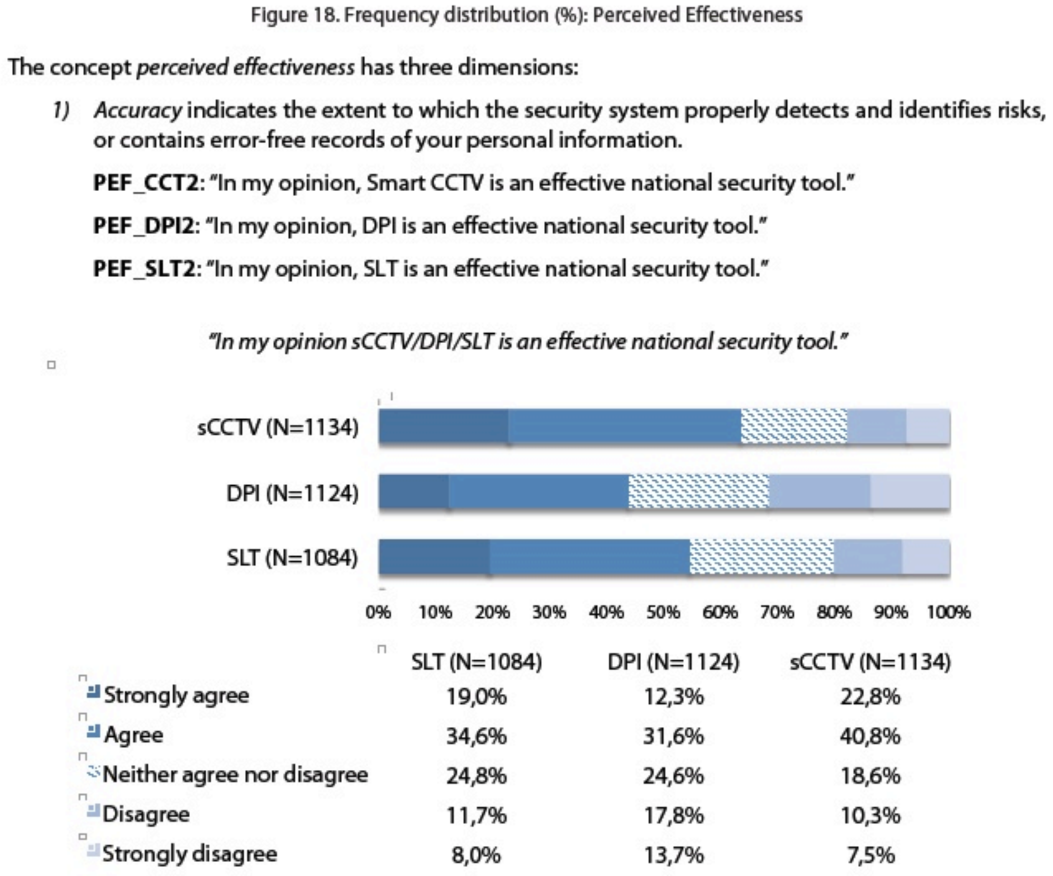


Figure 18. Frequency distribution (%): Perceived Effectiveness

The concept *perceived effectiveness* has three dimensions:

1) *Accuracy* indicates the extent to which the security system properly detects and identifies risks, or contains error-free records of your personal information.

PEF_CCT2: "In my opinion, Smart CCTV is an effective national security tool."

PEF_DPI2: "In my opinion, DPI is an effective national security tool."

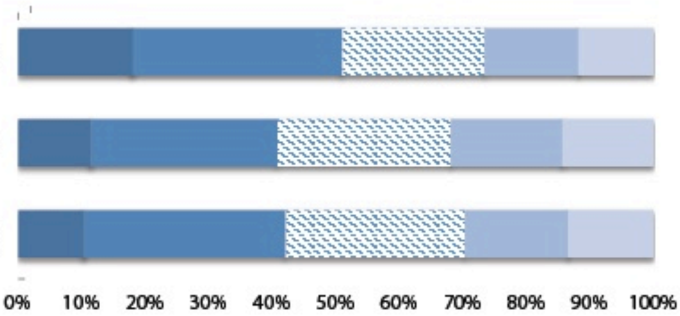
PEF_SLT2: "In my opinion, SLT is an effective national security tool."

"In my opinion sCCTV/DPI/SLT is an effective national security tool."

	SLT (N=1084)	DPI (N=1124)	sCCTV (N=1134)
Strongly agree	19,0%	12,3%	22,8%
Agree	34,6%	31,6%	40,8%
Neither agree nor disagree	24,8%	24,6%	18,6%
Disagree	11,7%	17,8%	10,3%
Strongly disagree	8,0%	13,7%	7,5%

2.2 Pavone et al (2015: 117)

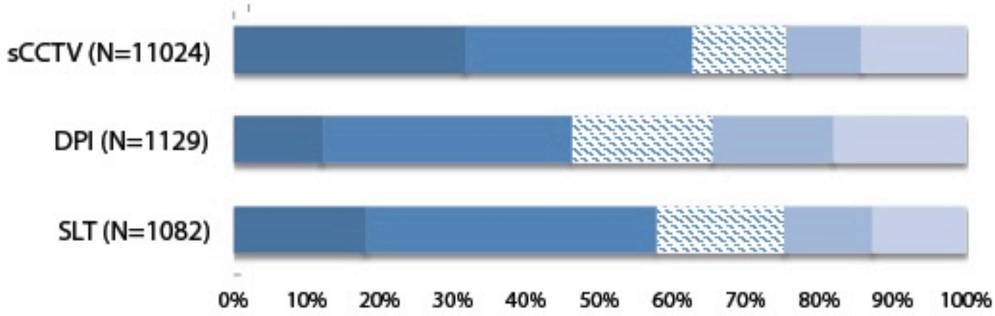
"sCCTV/DPI/SLT is an appropriate way to address national security threats."



	SLT (N=1064)	DPI (N=1115)	sCCTV (N=1134)
▪ Strongly agree	10,4%	11,5%	18,0%
▪ Agree	31,7%	29,3%	33,0%
▨ Neither agree nor disagree	28,3%	27,4%	22,4%
▪ Disagree	16,2%	17,5%	14,8%
▪ Strongly disagree	13,4%	14,3%	11,8%

2.3. Pavone et al (2015: 110)

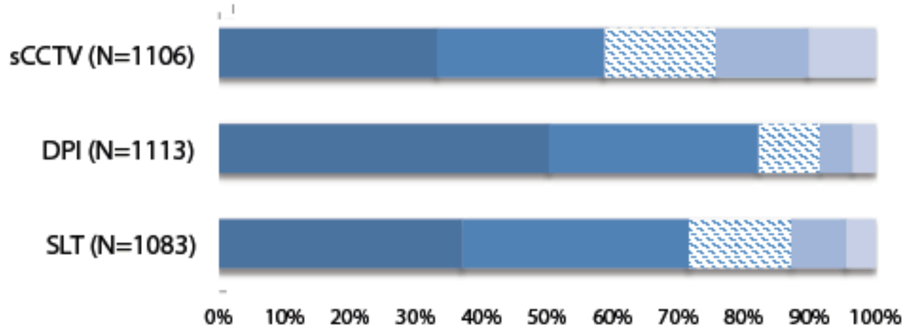
"Overall I support the adoption of sCCTV/DPI/SLT as a national security measure: overall results."



	SLT (N=1082)	DPI (N=1129)	sCCTV (N=11024)
▪ Strongly agree	18,1%	12,2%	31,5%
▪ Agree	39,6%	34,0%	31,0%
▨ Neither agree nor disagree	17,4%	19,1%	12,9%
▪ Disagree	12,0%	16,5%	10,2%
▪ Strongly disagree	12,9%	18,2%	14,3%

2.4. Pavone et al (2015: 120)

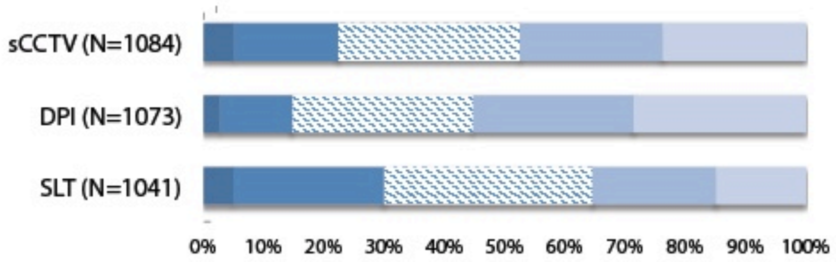
"sCCTV/DPI/SLT worries me because it could violate everyone's fundamental human rights."



	SLT (N=1083)	DPI (N=1113)	sCCTV (N=1106)
Strongly agree	37,0%	50,2%	33,2%
Agree	34,5%	32,0%	25,5%
Neither agree nor disagree	15,6%	9,3%	16,9%
Disagree	8,4%	5,0%	14,2%
Strongly disagree	4,4%	3,5%	10,2%

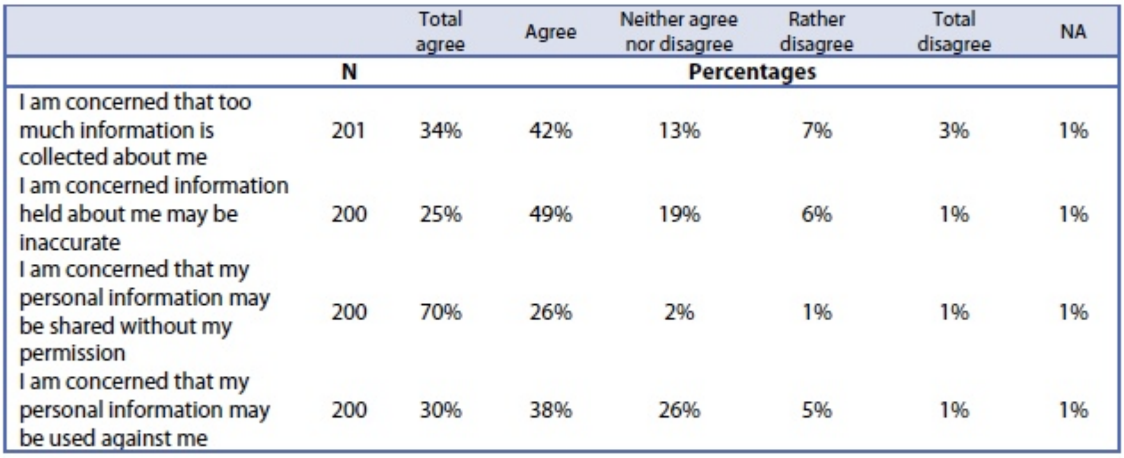
2.5 Pavone et al. (2015: 128)

"Security agencies which use sCCTV/DPI/SLT do not abuse their power."



	SLT (N=1041)	DPI (N=1073)	sCCTV (N=1084)
Strongly agree	4,9%	2,7%	5,0%
Agree	25,1%	12,0%	17,4%
Neither agree nor disagree	34,6%	30,0%	30,1%
Disagree	20,5%	26,7%	23,7%
Strongly disagree	15,0%	28,6%	23,8%

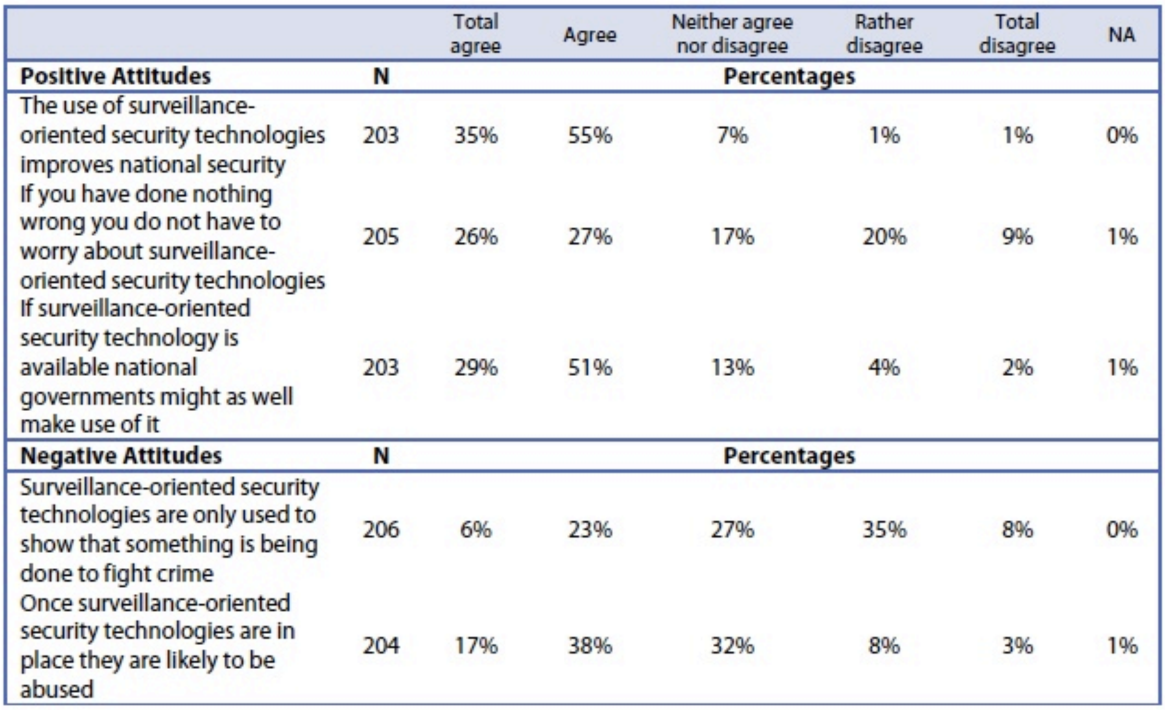
2.6 Ball et al (2014: 15)



		Total agree	Agree	Neither agree nor disagree	Rather disagree	Total disagree	NA
	N	Percentages					
I am concerned that too much information is collected about me	201	34%	42%	13%	7%	3%	1%
I am concerned information held about me may be inaccurate	200	25%	49%	19%	6%	1%	1%
I am concerned that my personal information may be shared without my permission	200	70%	26%	2%	1%	1%	1%
I am concerned that my personal information may be used against me	200	30%	38%	26%	5%	1%	1%

Table 6: Information privacy concerns

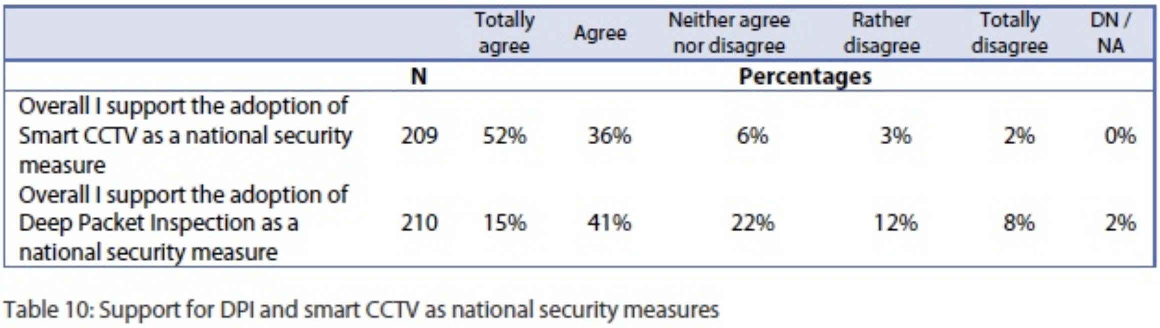
2.7 Ball et al (2014: 17)



		Total agree	Agree	Neither agree nor disagree	Rather disagree	Total disagree	NA
Positive Attitudes	**N**	**Percentages**					
The use of surveillance-oriented security technologies improves national security	203	35%	55%	7%	1%	1%	0%
If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies	205	26%	27%	17%	20%	9%	1%
If surveillance-oriented security technology is available national governments might as well make use of it	203	29%	51%	13%	4%	2%	1%
Negative Attitudes	**N**	**Percentages**					
Surveillance-oriented security technologies are only used to show that something is being done to fight crime	206	6%	23%	27%	35%	8%	0%
Once surveillance-oriented security technologies are in place they are likely to be abused	204	17%	38%	32%	8%	3%	1%

Table 7: General attitudes toward technology to foster security

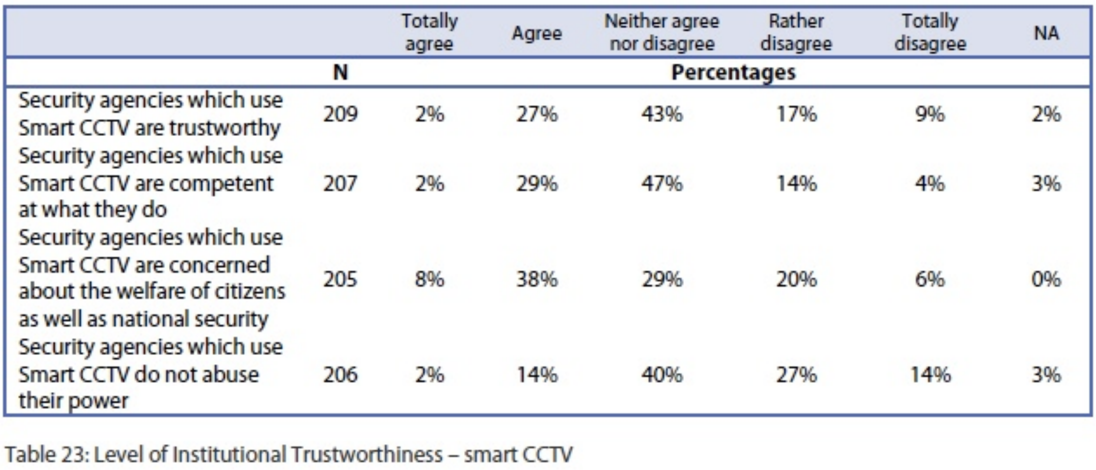
2.8 Ball et al (2014: 18)



	N	Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	DN / NA
		Percentages					
Overall I support the adoption of Smart CCTV as a national security measure	209	52%	36%	6%	3%	2%	0%
Overall I support the adoption of Deep Packet Inspection as a national security measure	210	15%	41%	22%	12%	8%	2%

Table 10: Support for DPI and smart CCTV as national security measures

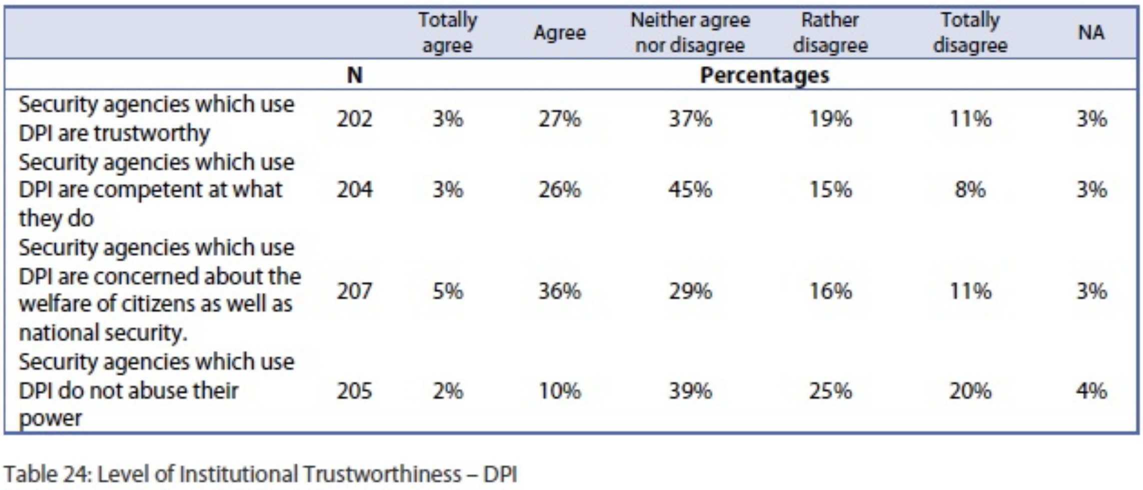
2.9 Ball et al (2014: 27)



	N	Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
		Percentages					
Security agencies which use Smart CCTV are trustworthy	209	2%	27%	43%	17%	9%	2%
Security agencies which use Smart CCTV are competent at what they do	207	2%	29%	47%	14%	4%	3%
Security agencies which use Smart CCTV are concerned about the welfare of citizens as well as national security	205	8%	38%	29%	20%	6%	0%
Security agencies which use Smart CCTV do not abuse their power	206	2%	14%	40%	27%	14%	3%

Table 23: Level of Institutional Trustworthiness – smart CCTV

2.10 Ball et al (2014: 28)



	N	Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
		Percentages					
Security agencies which use DPI are trustworthy	202	3%	27%	37%	19%	11%	3%
Security agencies which use DPI are competent at what they do	204	3%	26%	45%	15%	8%	3%
Security agencies which use DPI are concerned about the welfare of citizens as well as national security.	207	5%	36%	29%	16%	11%	3%
Security agencies which use DPI do not abuse their power	205	2%	10%	39%	25%	20%	4%

Table 24: Level of Institutional Trustworthiness – DPI