"Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Project acronym: **SurPRISE**

Collaborative Project

Grant Agreement No.: 285492

FP7 Call Topic: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start of project: February 2012

Duration: 36 Months

D 6.9 – Citizen Summits on Privacy, Security and Surveillance: Country report United Kingdom

Lead Beneficiary: OU

Author(s): Kirstie Ball (OU), Sally Dibb (OU) and Sara Degli Esposti (OU)

Due Date: June 2014

Submission Date: September 2014

Dissemination Level: Public

Version: 1.1

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.
The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD	

*APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Table of Contents

Executive Summary

SurPRISE re-examines the relationship between security and privacy, commonly positioned as a "trade-off". Where security measures and technologies involve the collection of information about citizens, questions arise as to whether and to what extent their privacy has been infringed. This infringement of individual privacy is sometimes seen as an acceptable cost of enhanced security. Similarly, it is assumed that citizens are willing to trade off their privacy for enhanced personal security in different settings. This common understanding of the security-privacy relationship, both at state and citizen level, has informed policymakers, legislative developments and best practice guidelines concerning security developments across the EU.

However, an emergent body of work questions the validity of the security-privacy "trade-off". This work suggests that it has over-simplified how the impact of security measures on citizens is considered in current security policies and practices. Thus, the more complex issues underlying privacy concerns and public skepticism towards surveillance-oriented security technologies may not be apparent to legal and technological experts.

In response to these developments, the SurPRISE project consulted with citizens from nine[1] EU member and associated states on the question of the security-privacy "trade-off" as they evaluate different security technologies and measures.

In this report the results from the United Kingdom are presented.

The United Kingdom is an ethnically diverse society and the third largest economy in Europe after Germany and France. It has a three-party parliamentary democracy enacting legislation in response to national and European priorities. It pursues a global approach to foreign policy and a comprehensive approach to national security which reflects its position in the EU but also its closeness to the United States of America. It also has a strong tradition of activism in the area of civil liberties and an active data protection regulator.

Public discourse about surveillance, privacy and security in the UK erupts following controversies or public outcries about the use of security technologies. Since the early 1990s, public debate has arisen around the spread of CCTV, a proposed national identity card scheme and other databases, the rise of the surveillance society and press intrusion. Opinion surveys have suggested that the British public do not hold widespread privacy concerns, have low trust in public institutions and are exorcised by the use of personal data by private companies.

Two citizen summits were held in Birmingham, UK on the 1st and 15th March 2014. A total of 214 citizens attended, 105 on the 1st March and 109 on the 15th. They were recruited by a market research company who ensured that the sample represented national demographics in respect of age, gender, ethnicity, educational attainment and occupation. The summits considered Smart CCTV and Deep Packet Inspection (DPI).

Preliminary analysis of the data reveals that the following views were expressed:

- The public would like more information to be made available about the benefits and risks of surveillance-oriented security technologies (SOSTs).
- Overall, there is support for the use of SOSTs, however, there are greater concerns about DPI than smart CCTV. It is likely that the British public are familiar with the presence of CCTV because of its widespread use in the country.
- There were deep seated concerns about the retention of data within the UK, rather than it being shared with other countries.
- There were also worries about who might see collected data/information or try to gain benefit from it.
- There were views that only the security services (and possible some areas of government) should be involved in operationalising SOSTs and handling information produced. There was a general mistrust of private organisations' involvement in national security matters.
- There was a call for greater regulation, legislation and oversight of the use of SOSTs.
- The UK participants do not seem to be particularly prepared to resist the use of SOSTs.

[1] Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and United Kingdom

- Individuals are more concerned about how SOSTs may affect them personally, rather than the wider community.
- There were relatively few suggestions about alternatives to technology, though worries about policing levels being reduced.

Overall, although there was broad support for SOSTs by the end of the citizen summit, the summits had prompted the citizens to consider privacy issues more closely. This was reflected in huge movements in the measures representing privacy concerns. The concerns that participants had about the privacy of the general public rose from 46% to 65%, while concerns that they had about their personal privacy increased from 35% to 69%. In addition it seems that the British participants were not willing to lose their privacy for better security: they wanted to have both. In contrast to previous indications from public opinion research, they demanded both enhanced security *and* enhanced privacy following their participation in the summits.

1 Introduction

This report summarises and describes the initial findings from the UK citizen summits, held in Birmingham on the 1st and 15th March 2015. It begins by offering a brief overview of the British national context, including information about its demographic make-up, economy, political, judicial and law enforcement systems. Then, an overview of its national security policy is presented. Controversies and public debates about security technologies are discussed to frame the preliminary data analysis. The debate in Britain is plural with different factions of the state, the data protection regulator, the press and activists representing a wide range of views. Information about the citizen summits themselves is provided and then the descriptive statistical results are presented. It is revealed that the results, as presented here, represent a similar range of opinions found in previous research. However it is also revealed that the British participants were particularly concerned about the involvement of private companies in the operation of surveillance-oriented security technologies (SOSTs) and demanded new forms of democratic oversight in respect of this operation. Participants also demanded more information about who used SOSTs and how, when and where SOSTs were used. Finally the citizen summit prompted citizens to consider their privacy much more carefully. During the summit their levels of reported privacy concern changed significantly. This could indicate that whilst policymakers frame security and privacy in terms of a trade off, the British public, at least, are not willing to make that trade off. They demand not only greater security and support the use of SOSTs, but they do so within enhanced frameworks of democratic scrutiny which simultaneously protect their privacy.

2 Privacy, security and surveillance in the national context

2.1 United Kingdom general national context

The United Kingdom (2001 census population: 58,789,194; total area: 244,110 sq. km) comprises the whole of the island of Great Britain—which contains England, Wales, and Scotland—as well as the northern portion of the island of Ireland. The name Britain is sometimes used to refer to the United Kingdom as a whole. The capital is London, which is among the world's leading commercial, financial, and cultural centres.

Economy

The UK is the third largest economy in Europe after Germany and France. Services, particularly banking, insurance, and business services, account by far for the largest proportion of GDP while manufacturing industry continues to decline in importance. In 2008, the global financial crisis hit the economy particularly hard, due to the importance of its financial sector.[2] Over the past two decades, public ownership has been reduced and the growth of social welfare programs has been contained. Agriculture is highly mechanized, producing about 60% of food needs with less than 2% of the labour force. The UK has large energy resources, but its oil and natural gas reserves are declining and the UK became a net importer of energy in 2005.

Society

The resident population of England and Wales on 27 March 2011 was 56.1 million, a seven percent (3.7 million) increase since 2001 with 55 percent (2.1 million) of this increase being due to migration.[3] Since World War II Britain has been a country of net immigration. After WWII, a need for labour resulted in migration from New Commonwealth countries as well as a period of active recruitment of European workers. Since then, it was attempted to match immigration to labour market needs through a work-permit and visa system.

In the last census, one in six people were aged 65 or over (16 percent, 9.2 million). With regards to ethnic groups, the majority of the usual resident population, 48.2 million people (86.0 percent of the population), reported their ethnic group as *White* in the 2011 Census. Within this ethnic group, *White British* was the largest, with 45.1 million people (80.5 percent), followed by *Any Other White* with 2.5 million people (4.4 percent). *Indian* was the next largest ethnic group with 1.4 million people (2.5 percent) followed by *Pakistani* (2.0 percent)[4]. The remaining ethnic groups each accounted for up to 2 percent of the population in 2011. There were two new tick boxes in the 2011 Census: Gypsy or Irish Traveller and Arab. Arab accounted for 240,000 usual residents (0.4 percent of the population). Gypsy or Irish Traveller accounted for 58,000 usual residents (0.1 percent of the population), making it the smallest ethnic category (with a tick box) in 2011.

British national government and local authorities

The United Kingdom is a constitutional monarchy and a parliamentary democracy. The country's head of state is the reigning king or queen and the head of government is the prime minister, who is the leader of the majority political party in the House of Commons. Sovereignty resides in Parliament, which comprises the monarch, the mainly appointive House of Lords, and the elected House of Commons. The sovereignty of Parliament is expressed in its legislative enactments, which are binding on all, though individuals may contest in the courts the legality of any action under a specific statute. In certain circumstances individuals may also seek protection under European law.

---

2 United Kingdom. (2012) in CIA World Factbook. URL: http://libezproxy.open.ac.uk/login?qurl=http%3A%2F%2Fsearch.credoreference.com.libezproxy.open.ac.uk%2Fcontent%2Fentry%2Fcia%2Funited_kingdom%2F0

3 Office for National Statistics (2012) "2011 Census: Key Statistics for England and Wales, March 2011", 11 December. URL: http://www.ons.gov.uk/ons/dcp171778_290685.pdf

4 Office for National Statistics (2012) "Ethnicity and National Identity in England and Wales 2011", 11 December. URL: http://www.ons.gov.uk/ons/dcp171776_290558.pdf

Each part of the United Kingdom has a distinct system of local government. Local governments have very few legislative powers and must act within the framework of laws passed by the central Parliament (and by the Scottish Parliament in Scotland). Nevertheless, they do have the power to enact regulations and to levy rates (property taxes) within limits set by the central government. They are funded by the rates that they levy, by fees for services, and by grants from the central government. Local governments in the United Kingdom are responsible for a range of community services, including environmental matters, education, highways and traffic, social services, firefighting, sanitation, planning, housing, parks and recreation, and elections.[5]

The British Constitution

The British constitution is uncodified; it is only partly written and is flexible. Its basic sources are parliamentary and European Union legislation, the European Convention on Human Rights, and decisions by courts of law. Matters for which there is no formal law, such as the resignation of office by a government, follow precedents (conventions) that are open to development or modification.

Political process and elections

All citizens aged 18 or older are eligible to vote in parliamentary and local elections as well as in elections to the European Parliament. All other public posts are filled by appointment. Each member of the House of Commons represents one parliamentary constituency.

A two-party system has existed in the United Kingdom since the late 17th century. Since the mid-1920s the dominant groupings have been the Conservative Party and the Labour Party. However, several smaller parties—e.g., the Liberal Democrats, the United Kingdom Independence Party, the Scottish National Party, Plaid Cymru (the Welsh Nationalist Party), and loyalist (unionist) and republican (nationalist) political parties in Northern Ireland—have gained representation in Parliament, especially since the 1970s.

The two-party system, together with uncertainty about the timing of a general election, has produced the British phenomenon of the official opposition. Its decisive characteristic is that the main opposition party forms an alternative, or "shadow," government, ready at any time to take office, in recognition of which the leader of the opposition receives an official salary.

International Relations

As one of five permanent members of the UN Security Council, the UK pursues a global approach to foreign policy. The United Kingdom retains also links with parts of its former empire through the Commonwealth. It also benefits from historical and cultural links with the United States and is a founding member of the North Atlantic Treaty Organization (NATO). The UK is also an active member of the EU, if a sometimes reluctant one, who chose to remain outside the Economic and Monetary Union.

The Police

The United Kingdom has no national police force or any minister exclusively responsible for the police. Each provincial force is maintained by a police authority, a committee elected by several local councils. One of its important tasks is to appoint and dismiss the chief constable. Once appointed, the chief constable has the sole right of appointment, promotion, discipline, and deployment of their force. The British police wear a uniform that is non-military in appearance and they do not routinely carry firearms.

Judicial System

Recruited from successful practicing lawyers, judges in the United Kingdom are appointed and virtually irremovable. The courts alone declare the law, but the courts accept any act of Parliament as part of the law. More than 90 percent of criminal cases in England and Wales are tried and determined by about 30,000 justices of the peace, who are unpaid laypersons, or by the more than 60 stipendiary (paid) magistrates, who are trained lawyers.[6] More serious crimes also come initially before a magistrate's court. The system is similar in Northern Ireland, but in Scotland district and sheriff courts try most criminal cases.

---

[5] Barr, Nicholas A. and Peter Kellner (n.d.) s. v. "United Kingdom", Encyclopædia Britannica Online. URL: http://www.britannica.com.libezproxy.open.ac.uk/EBchecked/topic/615557/United-Kingdom.

[6] Ibidem.

2.2 Major security policy and strategies

The current UK's approach to national security is overseen by the National Security Council and detailed in the *National Security Strategy* [NSS].[7] The implementation of that strategy is considered in the *Strategic Defence and Security Review* [SDSR].[8] The SDSR details decisions about key security capabilities and how they will be applied. The strategy assumes that UK interests can best be pursued through "a commitment to collective security via a rules-based international system and our key alliances, notably with the US; though an open global economy that drives wealth creation across the world; and through effective and reformed international institutions including NATO, as the anchor of transatlantic security, and our vital partnership in the EU" (NSS: p. 10). The pace of technology change is likely to continue, given states and other better access to a range of technologies and technological solutions. These have the potential to both enhance and threaten national security. The NSS acknowledges that the use of these approaches will need to be regulated, not least because (NSS: p. 17) "… society's complex response to improved surveillance, data-mining and profiling technologies is likely to challenge the balance between security and individual rights".

In the National Security Strategy, the British National Security Council has categorised risks into three groups on the base of their priority for UK national security, taking account of both likelihood and impact.

Tier one risks include: international terrorism; hostile attacks upon UK cyber space; major accidents or natural hazard; an international military crisis between states.

Tier two risks include: an attack on the UK or its Overseas Territories by another state or proxy using chemical, biological, radiological or nuclear (CBRN) weapons; risk of major instability, insurgency or civil war overseas which creates an environment that terrorists can exploit to threaten the UK; a significant increase in the level of organised crime affecting the UK; severe disruption to information received, transmitted or collected by satellites, possibly as the result of a deliberate attack by another state.

Tier three risks include: a large scale conventional military attack on the UK by another state resulting in fatalities and damage to infrastructure within the UK; a significant increase in the level of terrorists, organised criminals, illegal immigrants and illicit goods trying to cross the UK border to enter the UK; disruption to oil or gas supplies to the UK, or price instability, as a result of war, accident, major political upheaval or deliberate manipulation of supply by producers; a major release of radioactive material from a civil nuclear site within the UK which affects one or more regions; a conventional attack by a state on another NATO or EU member to which the UK would have to respond; an attack on a UK overseas territory as the result of a sovereignty dispute or a wider regional conflict; short to medium term disruption to international supplies of resources (e.g. food, minerals) essential to the UK.

It is acknowledged that the National Security Strategy needs to be delivered within the context of British values, as the following quote explains:

The UK has a proud tradition of protecting its citizens, promoting civil liberties and upholding the rule of law. … Our security and intelligence agencies play a vital role in protecting our country from threats to our way of life… Here too we must strike a balance, between the transparency that accountability normally entails, and the secrecy that security demands (SDSR: p. 23)

The *technological solutions* to security problems mentioned in the NSS and SDSR include: CCTV/ANPR cameras, drones, data mining and profiling technologies, interception of communications, cyber security technologies, and chemical/biological/radiological/nuclear science (see also Section 2: Current SOSTs in use in the UK). *Non-technological solutions* include: diplomacy, multilateral efforts through members of the UN Security Council, NATO, the EU, etc.; cross-government bilateral agreements; commitments to overseas development programmes to address poverty and support fragile states; conventional policing and military efforts; and citizen and community engagement. In addition, the UK Government seeks greater sharing of military and other capabilities with other governments, encompassing a range of technological and non-technological solutions.

---

[7] HM Government (2010) "A Strong Britain in an Age of Uncertainty: The National Security Strategy", Presented to Parliament by the Prime Minister by Command of Her Majesty, October. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[8] HM Government (2010) "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review", Presented to Parliament by the Prime Minister by Command of Her Majesty, October. URL: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr

2.3 Major privacy issues

There is neither a clear right to privacy in the UK nor a law such as the 1974 U.S. Privacy Act. The 1984 Data Protection Act [9]represents the first statutory protection for information privacy in the UK. Prior to the 1998 *Human Rights Act*[10] the only route to establishing privacy rights in the UK was to take out an action under breach of confidentiality of one's personal data. While the Human Rights Act incorporated into domestic law Article 8 of the European Convention on Human Rights (ECHR),[11] the 1998 Data Protection Act[12] defines UK law on the processing of data on identifiable living people, in line with the 1995 EU Data Protection Directive. Data Protection is regulated by the Information Commissioner's Office, which oversees and enforces the Freedom of Information Act 2000 and the Data Protection Act 1998, with the objective of promoting public access to official information and protecting personal information. The Information Commissioner reports annually to Parliament on the performance of his/her functions under the acts and has obligations to assess breaches of the acts. As of April 2010, the ICO has been able to fine organisations up to £500,000 for serious breaches of the Data Protection Act.[13]

2.4 Public discourse on surveillance-oriented security technologies and related practices

Public discourse on surveillance-oriented security technologies veers between strongly positive views based on their supposed ability to catch criminals and strongly negative views based on the challenges they pose to civil liberties. Public debates have included the expansion of CCTV, The Identity Card Scheme, The Surveillance Society and the Leveson Enquiry.

In the 1990s, **the expansion of CCTV systems** caused some interesting public debates. It was originally thought of by police and local authorities as the 'silver bullet' which would result in dramatically reduced crime figures. Eventually it was realized that the presence of CCTV in one area merely removed crime to an area where there was no CCTV. Public opinion tends to support CCTV if there have been major security or safety problems in the public realm. For example public opinion in favour of CCTV rose following the summer 2011 riots in many cities across the UK[14]. Police and Security Industry specialists were keen to promote its success in identifying many of the rioters, as CCTV images were checked against photographs on facebook, and on existing police databases, for example. However, despite its widespread ubiquity its effectiveness is questionable[15].

The same debate arose as a result of the proposed **National Identity Card Scheme** in the '00s. The scheme was eventually abandoned. In accordance with the Identity Cards Act 2006 the scheme comprised a plastic card[16] and behind the card was a database, which was supposed to hold the identity records of every citizen in the UK. The purposes for which the databases were to be used were unclear. Strong campaigning by the groups 'NotoID' and Privacy International, and a high profile report published by academics at the London School of Economics (LSE) meant that the project was eventually scrapped by the coalition government elected in 2010.

In August 2004 Richard Thomas, the UK's information Commissioner, made a comment in 2004 that the nation was **'sleepwalking into a surveillance society'**. His comments were made in response to government plans for two databases discussed above, databases which are now scrapped: Contact Point and the National Identity Register. In the light of the aforementioned one might argue that the ICO was successful in his campaign, but part of his agenda was to gain more powers to punish those who were in breach of the data protection act to deter others who possessed personal data from being negligent. In

---

9 Data Protection Act 1984 (repealed 1.3.2000). URL: http://www.legislation.gov.uk/ukpga/1984/35/contents

10 Human Rights Act (1998), retrieved from legislation.gov.uk. URL: http://www.legislation.gov.uk/ukpga/1998/42/contents

11 Raab, Charles and Benjamin Goold (2011) "Protecting information privacy", Equality and Human Rights Commission, Research report 69, First published Summer 2011. URL: http://www.equalityhumanrights.com/sites/default/files/documents/research/rr69.pdf

12 Data Protection Act (1998), retrieved from legislation.gov.uk. URL: http://www.legislation.gov.uk/ukpga/1998/29/contents

13 Whitaker's Almanack, published by A&C Black in October 2013. Retrieved from KnowUK.co.uk

14 URL: http://www.synx.com/index.php/News/public-attitudes-to-cctv-shift-following-riots.html

15 URL: https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf

16 URL: http://news.bbc.co.uk/1/hi/8175139.stm

2004, the UK ICO could only impose a £5,000 penalty on offending data controllers. As a result of his interventions since then fines of up to £500,000 can be imposed. His main intervention was to commission a consultancy report which detailed the different dimensions, consequences and issues associated with the Surveillance Society[17]. The report was launched in November 2006 and a carefully orchestrated media campaign resulted in worldwide media coverage for the Commissioner, the report and its contents. The raft of documentaries and media discussions which followed ensured that the term 'Surveillance Society' became common parlance in the UK. Furthermore, the government of the time took an interest, launching a Home Affairs Select Committee enquiry into the Surveillance Society, published in 2008 [18] and a House of Lords Constitution Committee enquiry entitled 'Surveillance: Citizens and the State'[19], published in 2009. As a result of the latter it was decided that the Information Commissioner report to Parliament on a biannual basis on the state of the surveillance society.

Finally, **the Leveson Inquiry** was a judicial inquiry set up by the current UK Prime Minister, David Cameron, to examine closely the ethics and practices of the press. The inquiry was split into two phases. The first phase concerned the press's relationships with the police, public and politicians. The second phase concerned the conduct of the paper *News of the World* and *News International* media group who have been alleged to encourage phone tapping in order to generate stories. As such one of the main issues considered in the enquiry is the question of press intrusion. Recent allegations of the press tapping the phones of celebrities as well as the victims of high profile crime and their families have raised questions about an individual's right to privacy in different situations. The issue of a trade off arises in that the press assert that because celebrities are seen to court publicity to further their careers they have less of a right to privacy. And yet evidence to date suggests that press intrusion, particularly unlawful phone tapping, causes harm to these individuals. More clear cut are the privacy issues surrounding press behaviour around victims of crime and their relatives. It is hoped that the inquiry will produce guidelines on how the press should be regulated and some insight into the privacy claims of those featured in stories. In 2012, the inquiry concluded that the press should be self regulated, but a new independent standards body be introduced which was supported by specific legislation.

Internet, or cyber, surveillance represents another highly controversial issue for Britons. In February 2008, Phorm, a digital technology company, announced it had signed deals with BT, TalkTalk and Virgin Media – the country's three largest ISPs – to install its contextual advertising system.[20] The system was designed to analyse all contents channelled through the three big ISP companies by means of deep packet inspection (DPI). The objective was to build customers profiles and deliver targeted advertisements online. Phorm, which was already known for having developed solutions labelled 'spyware' by security experts, sparked a privacy backlash when it became public that the companies were already testing the system on their customers without giving any notice or asking for consent.[21] Although none of the firms was prosecuted for internet traffic wiretapping,[22] they had to abandon the project and bear the market and reputational costs coming with the bad publicity.

Besides the proliferation of consumer surveillance sponsored by the private sector, British citizens, as other European citizens, worry about government cyber-surveillance. The revelation of whistleblower Edward Snowden in June 2013 on the US National Security Agency's (NSA) massive surveillance activities

17 URL: http://www.surveillance-studies.net/?page_id=3
18 URL: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf
19 URL: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm
20 Halliday, Josh (2011) "CPS under attack over BT and Phorm's covert online monitoring: Privacy watchdogs fear big corporations can violate UK internet users' rights with impunity", theguardian.com, Monday 11 April 2011 17.30 BST. URL: http://www.theguardian.com/technology/2011/apr/11/cps-bt-phorm-appeal
21 Williams, Christopher (2008) "How Phorm plans to tap your internet connection: Under the hood of BT's data pimping machine", The Register, 29 Feb 2008. URL: http://www.theregister.co.uk/2008/02/29/phorm_documents/
22 Williams, Christopher (2011) "BT and Phorm: how an online privacy scandal unfolded: The Crown Prosecution Service's decision not to prosecute BT and Phorm over their secret interception of internet traffic closes a chapter of Britain's biggest online privacy scandal", The Telegraph, 08 Apr 2011 4:32PM BST. URL: http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html

prompted an ongoing debate in the UK on information privacy.[23] The new climate has already produced changed in British legislation such as the new UK data retention laws.[24]

Opinion surveys of the British public's reactions to security and surveillance technologies have been mainly assessed as a response to public outcries. For example, in the context of the envisioned reform of the data protection directive, the European Commission has commissioned studies to understand citizens' opinions about data protection as part of the Eurobarometer initiative.[25] So we know that about one-third of Internet users in the UK (63%) use anti-spy software to protect their identities on the Internet, while in real life privacy concerns seems to be much lower and six out of ten respondents (59%) say they usually share old bills, bank statements, credit card receipts and the like. A considerable low number of British interviewees (47%), in comparison to citizens in other EU member states, say to have adapted their behaviour after reading privacy statements on the Internet. Yet British users of social networking or sharing sites (68%) are most likely to change the privacy settings on their personal profile to protect their privacy. Trust in national public authorities is lower (38%) than trust in bank and financial institutions (75%) in the UK, while trust in European institutions is astonishingly low (38%). In addition, British and Irish citizens are very concerned (both 80%) about their personal information used by private companies for purposes other than those for which they have been collected (e.g. for direct marketing or targeted online advertising), without being informed.

With regard to security and migration policies, in 2011, the European Commission Directorate-General for Home Affairs (DG HOME) commissioned a survey to understand European citizens' opinions about a number of themes, among which there are: awareness and attitudes in relation to border control inside the EU for both EU and non-EU citizens; non-EU labour migration within Europe; migration data; integration of non-EU immigrants; opinions about asylum seekers and illegal migrants, and labour or sexual exploitation; perceptions of public security, individual rights and freedoms.

According to this study, British respondents think that discussion about immigration in the EU is not based on reliable information (56%). Regarding immigration policies, 56% of British people think that the EU should not encourage labour migration from non-EU countries (against a 33% that think it should). Besides this, a relatively high proportions of respondents in the UK (25%) disagree that asylum should be offered to people in need and that national governments should work more closely together (87%).

The UK is also one among those countries with the least positive view on how secure the EU is (67%). In addition to this, the belief that fundamental rights and freedoms have been restricted in the EU because of the fight against terrorism and organised crime is the absolute majority view in UK (57%). Europe, then, is neither secure nor liberal in their view.

If at European level studies have been commissioned to monitor the degree of concern generated by certain societal issues, in the national context opinion pool research has been applied to observe the extent of potential dissent originated from some policy initiatives. For instance several surveys have been repeatedly undertaken as a result of the debate originated with the *2006 Identity Cards Act (c 15)* and ended with the approval of the provisions to reverse the identity cards scheme and to destroy information held on the *National Identity Register*, as foreseen by of the *Identity Documents Act 2010 (c. 40)*. Between 2003 and 2009, several pollsters – such as ICM, Ipsos MORI, Opinium, Populus, YouGov – asked their panel members whether or not they were in favour of the national ID card scheme.[26] Questions touches a bunch of themes related to ID cards: from implications of the introduction of ID cards for civil liberties, data security, to evaluation of their effectiveness in preventing terrorist attacks, tacking benefit frauds, controlling illegal immigration, or whether people would have been willing to pay for having an ID card.

---

23 theguardian (2014) "Edward Snowden: Latest on the computer analyst whistleblower who provided the Guardian with top-secret NSA documents leading to revelations about US surveillance on phone and internet communications", The Guardian. URL: http://www.theguardian.com/world/edward-snowden

24 Data Retention and Investigatory Powers Act 2014 URL: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

25 URL: http://ec.europa.eu/public_opinion/index_en.htm

26 UK Polling Report: survey and polling news from YouGov's Anthony Wells. URL: http://ukpollingreport.co.uk/issues/id-cards

	Institution	Title	Year	Sample size	Questionnaire available at:
1	Daily Telegraph YouGov	ID cards and the surveillance society	2006	1,979	http://d25d2506sfb94s.cloudfront.net/today_uk_import/YG-Archives-pol-dTel-SurveillanceSociety-061204.pdf
2	THE GALLUP ORGANIZATION European Commission	Data Protection in the European Union Citizens' perceptions	2008	1,001	http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf
3	TNS UK European Commission	Special Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union	2010	1,291	http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
4	TNS UK European Commission	SPECIAL EUROBAROMETER 380 - Awareness of home affairs	2011	1,306	http://ec.europa.eu/public_opinion/archives/ebs/ebs_380_en.pdf

Table 1: List of public opinion studies listed in this section.

3 Process design – the citizen summit in the UK

3.1 Organisational setting

Two citizen summits were organised in Britain on Saturday 1st and 15th of March 2014. Both meetings were held at the Crowne Plaza Hotel in the city centre of Birmingham. Birmingham is the second largest city in the UK, lying northwest of London in central England. It is the administrative headquarters of the West Midland's metropolitan county and a major manufacturing, engineering, commercial and service centre. The city has an international airport and its concert halls, theatres, and three universities make it an important cultural and educational centre. There are many miles of restored canal walks, with Birmingham known as 'Britain's Canal City'.[27] Birmingham was chosen as a location thanks to the multicultural diversity of its citizens, making it highly representative of today's ethnically rich Britain.

3.1.1 Citizen recruitment strategy

A market research company was sub-contracted to recruit the 200 citizens required for each event. They were recruited using a mixture of methods. People were approached face to face in a busy shopping street in central Birmingham. They also used telephone recruitment methods, approaching existing individuals in their contact database who matched the recruitment criteria. If a citizen was interested, they then followed up the contact with information about the project, the magazine and the consent form.

3.1.2 Seating plan

The recruitment company sorted citizens into tables of either 8 or 9 citizens. They put a mixture of ages, genders, educations, ethnicities and occupational levels on each table.

3.1.3 Incentives

Participants were paid an incentive of £100 for their attendance at the day. This was given to them in the form of a shopping voucher which could be used in all high street shops.

3.1.4 The venue

The UK summits were held at the 4* Crowne Plaza Hotel in Central Birmingham in its main plenary meeting room, 'The Vista Suite'. The hotel offered a high standard of meeting accommodation, service and refreshment for the participants.

3.2 Structure of the citizen panel

In total, the British citizen summit had 214 participants. 105 citizens attended the first summit on Saturday 1st of March 2014, while 109 participated on the 15th of March 2014. Although the large majority were British citizens (97% of respondents; N = 205), 25% of all respondents (N = 201) claimed they belonged to a minority ethnic group. British society is highly multicultural and ethnic groups such as Indian, Asian or Black African account for 14% of the total population of England and Wales (56.1 million). Although these groups were represented in our sample, some participants stated they would have preferred to see an even more diverse sample.

> "The sample of people surveyed today did not reflect the true background of our nation. There were a lack of people from ethnic backgrounds." [Postcard: 55]

A balanced panel of men and women (53% men and 47% women; N = 212) of different ages participated in the summits (see Figure 1).

[27] ' Birmingham (UK)' Hutchinson UK Gazetteer, Helicon Publishing, May 2012. Retrieved from http://www.knowuk.com/

The large majority live in urban (45%; N = 209) or metropolitan areas (39%), with only a small portion coming from rural areas (14%). 38% of respondents (N = 207) have children aged 16 or under at home.

In terms of education, the majority have vocational qualifications (39%; N = 206), 17% have a university undergraduate degree, with 9% having a postgraduate qualification. Only a very small proportion finished studying at the end of lower secondary school (1% primary school; 7% lower secondary).

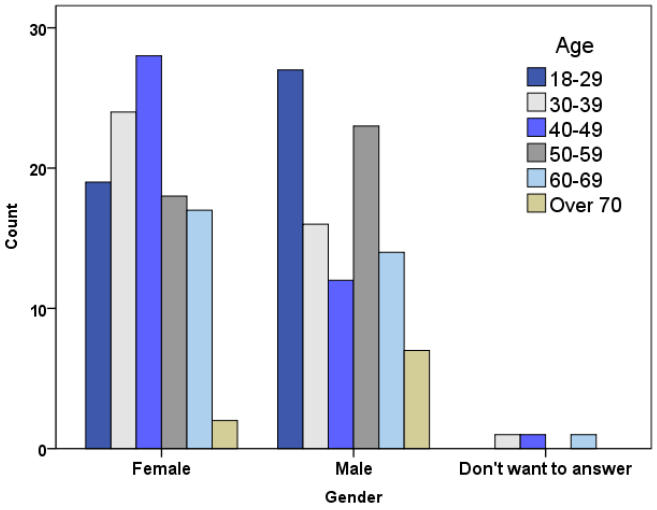


Figure 1: Age by gender

42% (N = 206) earn far less than the average annual British salary (£26,500 per year). These people included retired workers (21%) as well as employees (43%). In contrast, the 13% of citizens earning much greater than the average was composed of university postgraduates (37%), and also managers or senior officials (35%) or professionals (35%).

	Type of profession	*Valid Percent*	***Earnings compared to national average of £26,500 per year***	*Valid Percent*	***Employment Status***	*Valid Percent*
1.	Manager, legislator or senior official	18%	A lot more than the average	13%	Employed	54%
2.	Professional	29%	More than the average	11%	Self-employed	10%
3.	Technician and associated professional roles	13%	About the same as the average	4%	Unemployed	6%
4.	Clerical support worker	13%	Less than the average	22%	Stay-at-home parent or carer	6%
5.	Services and sales worker	11%	A lot less than the average	42%	Student	5%
6.	Skilled agricultural, fisheries or forestry worker	1%	Don't know/don't want to answer	8%	Retired	16%
7.	Craft and related trades-person	6%			Don't know/don't want to answer	1%
8.	Plant and machine operator or assembler	1%				
9.	Elementary worker	1%				
10.	Don't know/don't want to answer	7%				
	N	*207*		*206*		*203*

Table 2: Citizens characteristics: occupation, household income and current employment condition

3.3 How citizens assessed the summit

Citizens enjoyed participating in the citizen summits. 90% of participants considered the event to be an insightful and enriching experience. 70% believed that the opinions and reflections gathered during the summits will help policy-makers and politicians in designing better security policies. The ambience was friendly and welcoming, and people felt free to express and share their ideas; even when issues were highly controversial or it was difficult to find an agreement.

> "I have found today's event very enjoyable and informative. And it was a pleasure to meet some of your colleagues." [Postcard: 37]

		Total agree	Agree	Neither agree nor disagree	Rather disagree	Total disagree	NA
	N			**Percentages**			
I have gained new insight by participating in the citizen summit	202	40%	50%	8%	1%	1%	0%
I believe the citizen summit has generated valuable knowledge for the politicians	202	16%	54%	18%	5%	5%	2%

Table 3: Citizens' evaluation of citizen summits

The summits were also an opportunity for citizens to learn about SOSTs and express informed opinions in relation to both the privacy and security implications. At the beginning of the event only 15% of people considered themselves to be fairly or very knowledgeable about SOSTs, while at the end that figure rose to 58%.

		I was very knowledgeable	I knew a good amount	I had some knowledge	I knew little to nothing	DN / NA
	N		**Percentages**			
Before reading the SurPRISE information booklet how would you rate your knowledge of surveillance-oriented security technologies	199	2%	13%	60%	25%	1%
After watching the SurPRISE films, discussing with fellow participants and reading the information booklet how would you rate your knowledge of security technologies	209	11%	47%	40%	1%	0%

Table 4: Citizens' knowledge of SOSTs before and after the citizen summits

Becoming more knowledgeable of SOSTs does not seem to imply that citizens will automatically be more positive or negative about the use of surveillance technologies for security reasons. When we asked whether respondents had changed their opinions on SOSTs as a result of the citizen summit, the sample was divided into those whose views had changed - 31% were more positive while 39% were more negative -and 27% whose views remained the same. Among those who had changed their opinions, a larger proportion had become more negative than positive.

> "The last question of all should have included an additional option as an answer: being more aware has made me even more cynical!" [Postcards: 60]

The specific technologies being discussed at the British summits appear to have played a role in this change in views. Participants regarded Deep Packet Inspection (DPI) as a particularly shocking use of technology, expressing deep concerns about the existence and intrusiveness of this tool. As explained in

the next section, concerns about privacy increased at the end of the event. However, overall support for the implementation of SOSTs also rose. These results suggest a polarization effect which we cannot test at this stage, but that will be further investigated later in the project. A more in-depth analysis of the effect of the citizen summit on people's opinions will be conducted as part of the next project deliverables.

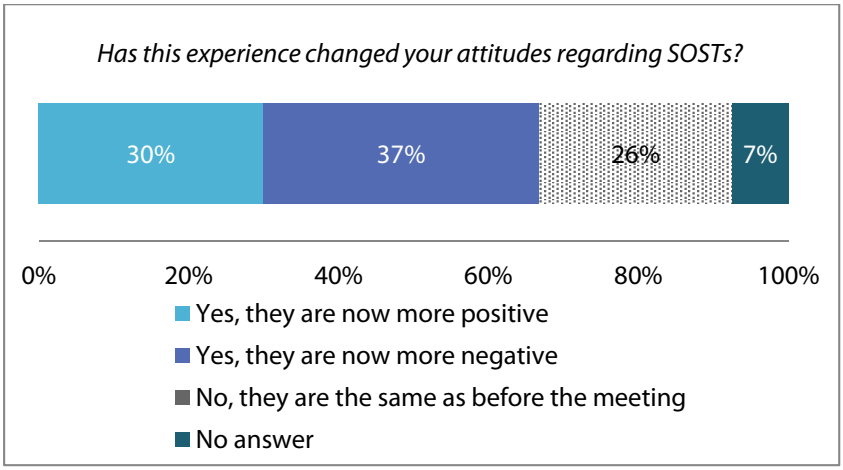


Figure 2: Participants' perceptions of how the citizen summit has influenced their opinions

4 Empirical results of the citizen summit

At the end of the citizen summit the number of people who thought that SOSTs should be routinely implemented to improve national security increased slightly from 74% to 82%. Yet, the demand for non-technology alternatives to SOSTs also increased from 35% to 40%. The concerns that participants had about the privacy of the general public rose from 44% to 63%, while concerns that they had about their personal privacy increased from 34% to 66%.

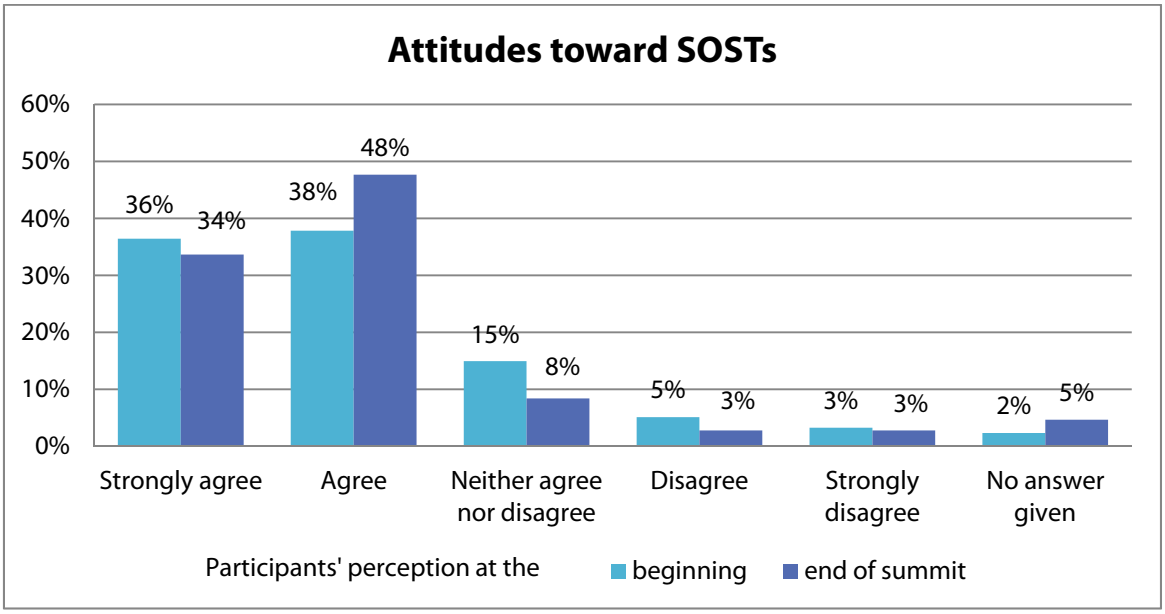


Figure 3: Overall I believe surveillance-oriented security technologies should be routinely implemented to improve national security (question asked at the beginning and the end of the event

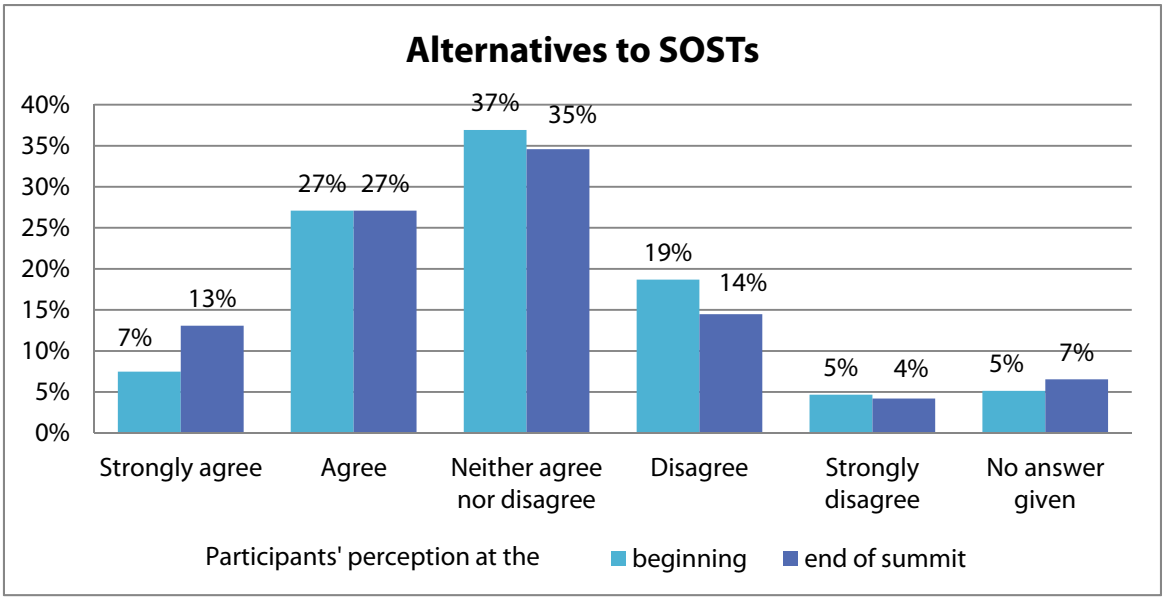


Figure 4: Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority

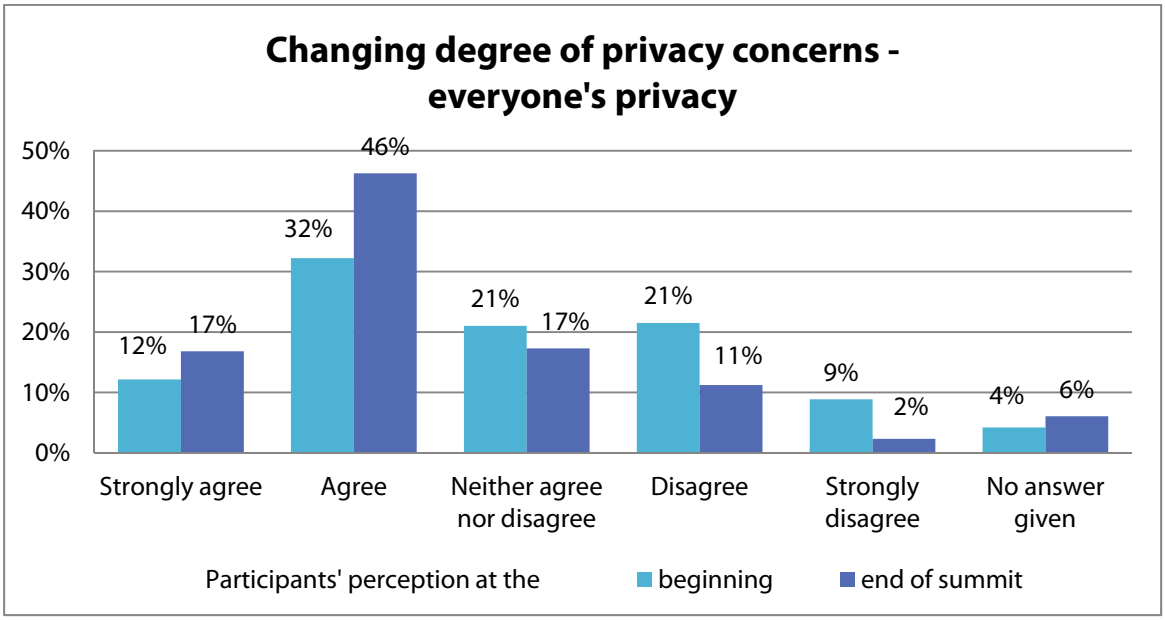


Figure 5: I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general (question asked at the beginning and the end of the event

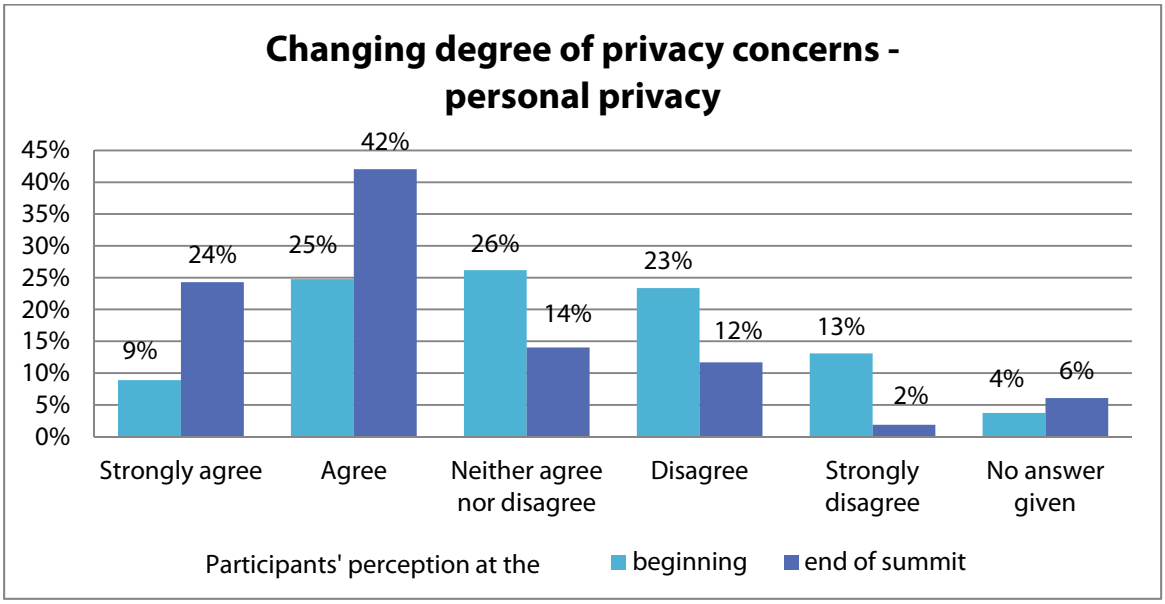


Figure 6: I am concerned that the use of surveillance-oriented security technologies is eroding my privacy (question asked at the beginning and the end of the event).

4.1 General attitudes on privacy and security

The majority of participants (57%) consider Britain to be a safe country, with four fifths of them indicated that they feel secure in their daily life. Nonetheless, three quarters of respondents worry about security when they are online. There were also major concerns about information privacy. 76% of citizens 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%). These concerns were intensified for participants when they considered the role that digital technologies play in young peoples' lives.

> "I used a PC at 10 – 11 years old. Children these days use it at 3 – 4 years old… protection and security is key for our children to stay safe. They are naïve." [Postcard: 64]

The importance of safeguarding data security becomes then paramount.

> "To put people's worries at ease about the process, I think it's important to have some control over when whoever is in control of the footage can access the footage itself. For example, you may only have access to footage from a certain camera if someone's behaviour has been flagged, so you can't abuse the technology and just look at any footage on any camera..." [Postcard: 67]

> "To keep the data secure. No selling of information, no call centre type users looking at the data." [Postcard: 36]

		Total agree	Agree	Neither agree nor disagree	Rather disagree	Total disagree	NA
	N			**Percentages**			
I generally feel safe in my daily life	208	18%	63%	13%	6%	18%	
I worry about security when I am online	208	34%	41%	12%	12%	1%	
I feel that this country is a safe place in which to live	211	9%	48%	20%	19%	4%	

Table 5: Perceived level of security threat

		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

These concerns surface the need for effective data protection approaches and reinforce the need for citizens to be reassured in this regard, as the following comments from participants show:

> "The problem I have with CCTV and DPI is who has access to all my information, where is it stored and how long for? Who accounts for it all?" [Postcard: 32]

> "DPI Feels really uncomfortable subject … Who 'owns' this DPI behaviour. Are the general public aware of DPI and how it's used?" [Postcard: 76]

4.2 How do participants perceive the use of surveillance-oriented security technologies?

In the following sections the attitudes of participants in the UK summits towards a range of issues relating to the use of SOSTs are explored. In section 4.2.1 the general attitudes of citizens towards these technologies are considered, capturing opinions about the appropriateness of these approaches, their likelihood to reduce crime, and the implications for intrusiveness. Section 4.2.2 reviews the responses to questions about specific SOSTS. The UK summits asked participants about two technologies: Deep Packet Inspection (DPI) and smart CCTV. After considering specific questions about the use of these technologies, the focus shifts to consider the social, temporal and spatial aspects associated with their use. Finally, some more substantive privacy concerns are considered. In section 4.2.3 the likelihood that citizens will avoid or resist the use of SOSTs is reviewed.

4.2.1 Perceived effectiveness vs. intrusiveness of SOSTs

The vast majority of participants (90%) consider that the use of SOSTs improves national security, and most (80%) also support the idea that governments should use these technologies for this purpose. Just under half of participants (43%) did not agree that SOSTs are used to give the impression that something is being done to fight crime. Over half of citizens (53%) were of the view that those who have done nothing wrong have nothing to fear from SOSTs. This view was aptly reflected in the following observation: "What I have learned today is that we are trying to make the world a better place and surveillance society will help." (Postcard 30)

"This is like when they introduced swipe cards at school. I remember this happens to my daughter, who is now 30. They did to avoid that anybody could get access to the school. There were people who complained. I thought it was a marvellous idea! I would love to have more light at night illuminating the cash machine and a camera watching me in case someone tries to mug me." (Statement made by a participant as reported in the facilitator's reflections no. F6)

"CCTV has replaced that caring eye of your anti or granny. You feel there is somebody looking after you when you are there alone in the darkness. People also tend to associate CCTV with security and safety because these systems are mainly administered and owned by public authorities for public security purposes, but they have different opinion when it comes to technologies which are equally used, accessed or managed by security agencies and private companies." (Interpretation given by table facilitator F6)

There were, however, concerns about the potential negative impacts of SOSTs, with over half of participants (55%) worried that once in place they might be abused; and 76% concerned about the amount of information being collected about them (see table 6). These comments from participants reflect these worries:

> "Smart CCTV and DPI concerns me. Who monitors this, what will be done with the information. What about privacy? We were never asked if it was OK in the first place. More public involvement." (Postcard 1)
>
> "I am against Smart CCTV, DPI. However I can see the need regarding terrorists/national security. I would be highly suspicious of usage and sharing information with 3rd parties. This area to me is of great concern." (Postcard 69)

Some individuals expressed the view that technology should only be part of the solution to security problems, and that other ways should be sought to improve safety. Others pointed out that in some circumstances technology is no substitute for the human mind: "As good as the idea is and as much as I support it, the mind of a man/woman cannot be put into a hard drive" (Postcard 46). Getting the right balance between the use of technology and other means to improve security was an important issue for some participants:

> "I feel that the new technology is a great idea if it is used correctly and for what it is intended for. Technology should not be the only resource though. The community spirit needs to be rekindled. If people look out for each other we will feel a greater sense of security knowing somebody is

watching out for us. Being back community centres and neighbourhood activities to bring communities back together again. A sense of awareness of what is going on around us." (Postcard 47)

		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

Questions were also asked about the effectiveness of SOSTs, with some participants seeking more insights into the costs and benefits.

> "I have no problems with smart CCTV but the use of it, the running costs, the legitimacy and the effectiveness of it needs to be carefully monitored. And the watchers made accountable." (Postcard 65)

> "DPI and Smart should work together – government to monitor DPI, when suspicious activity occurs, government should inform local police to monitor CCTV in suspicious area. Government to monitor companies who use DPI – enforce legal requirements." (Postcard 4)

> "I believe there should be stricter surveillance over high risk criminals and repeat offenders. I.e. maybe a chipping (micro) system for GPS purpose, so that crimes are caught out before they are committed." (Postcard 5)

> "Who monitors how many cameras or Smart CCTVs there are in a public location. I.e. (1) government agencies (2) private CCTV (3) or could it be possible to put up criminal CCTVs." (Postcard 6)

4.2.2 SOST-specific questions

Once the general questions about perceptions of SOSTs had been asked, participants were questioned about specific technologies. In the UK, questions were focused on two technologies: Deep Packet Inspection (DPI) and smart CCTV.

In general, summit participants were less knowledgeable about and more concerned with the use of DPI in security contexts than they were about Smart CCTV. Only 31% claimed to understand they know what DPI is, while nearly half (43%) of citizens claimed that they know what smart CCTV is. The following comment from one participant captures this difference in views about the two technologies:

> "Smart CCTV is a good improvement on CCTV, but must be properly regulated. DPI is a wonderful way of checking for potential crimes but the privacy of the individual is paramount." (Postcard 24)

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**Percentages**			
I understand what smart CCTV is	207	11%	32%	19%	26%	10%	2%
I understand what DPI is	210	6%	25%	16%	29%	24%	1%

Table 8: Knowledge of smart CCTV and DPI

Most citizens attending the summits had some familiarity with aspects related to these technologies though. 28% reported regularly seeing CCTV cameras in their local areas, with 29% noticing them some of the time. The vast majority (88%) often used the internet, with only 1% reporting that they never did.

		Never	Rarely	Sometimes	Often	All of the time	DN / NA
	N			**Percentages**			
In the area where you live, how often do you see CCTV cameras	210	7%	35%	29%	11%	17%	1%
How often do you use the internet	209	1%	3%	8%	18%	70%	0%

Table 9: Familiarity with SOST-related technologies

The adoption of smart CCTV for security purposes was overwhelmingly supported by 88% of participants; with only 5% disagreeing with its use. One participant remarked: "Install it everywhere and if you are doing nothing wrong you have nothing to worry about!" (Postcard 80). For example, there was support for the use of the technology in order to protect vulnerable groups or to counteract trouble caused by crowds:

> "Vulnerable people i.e. disabled, mentally ill can be identified through their behaviour and therefore protected. … The technology can be targeted to areas e.g. football matches/airports/ethnic groups where trouble is more likely to start." (Postcard 75)

Even so, this support was tempered by those who could see the costs of the SOSTs to their privacy, as one participant explained: "Do not like the fact that I am being monitoring constantly without my consent" (Postcard 33). The overall support for DPI adoption was slightly less, with 56% of citizens agreeing that it should be used to support national security, with 20% disagreeing. DPI was also perceived as a far more controversial and unintelligible technology than smart CCTV: 22% of respondents were unsure about being either in favour or against the adoption of DPI, while only 6% were indecisive in the case of smart CCTV.

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	DN / NA
	N			**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

Smart CCTV

76% of participants regard smart CCTV as an appropriate method for addressing national security threats, with 77% of them agreeing that this technology is an effective security tool and 68% of respondents selected the option "I think that the level of intrusiveness is acceptable given the benefits smart CCTV offers" (see table 11b). 36% of respondents also consider appropriate to say that "Laws and regulations ensure that smart CCTV is not misused". Even so, the degree to which citizens are personally comfortable with the use of this SOST varies, as does the extent to which people feel that their privacy may be affected as a result. While 63% claim to feel more secure when CCTV is being used, there were also some more negative views expressed. 45% of participants believe that the technology is forced on them without their permission, while 21% indicated that the used of smart CCTV actually makes them feel uncomfortable. There was also evidence that citizens were worries about the implications of these technologies for their human rights, with 37% agreeing that the possibility for Smart CCTV to violate their basic human rights was a worry. A slightly small number (30%) were also concerned about the potential for the technology to violate everyone's' human rights. The fact that more participants were worried about their own human rights, illustrates the personal dimension of some of these views.

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
PERCEIVED EFFECTIVENESS	**N**			**Percentages**			
In my opinion, Smart CCTV is an effective national security tool	207	27%	50%	15%	4%	2%	1%
I feel more secure when smart CCTV is in operation	208	20%	43%	27%	5%	4%	0%
Smart CCTV is an appropriate way to address national security threats	207	32%	44%	15%	4%	3%	1%
PERCEIVED INTRUSIVENESS	**N**			**Percentages**			
The idea of smart CCTV makes me feel uncomfortable	209	5%	16%	21%	35%	23%	5%
I feel that smart CCTV is forced upon me without my permission	207	19%	26%	28%	17%	10%	0%
Smart CCTV worries me because it could violate my fundamental human rights	207	14%	23%	23%	27%	13%	1%
Smart CCTV worries me because it could violate everyone's fundamental human rights	206	8%	22%	28%	24%	17%	0%

Table 11: Perceived effectiveness and intrusiveness of smart CCTV

Table 12 represents a range of statements and participants were asked to choose with which statement they agreed. Just over 80% of participants agreeing that smart CCTV improved national security. This acceptance was underpinned by only 23% of the sample indicating that they thought the technology was intrusive. Furthermore, 68% of the sample indicated that the level of intrusiveness was acceptable given the benefits. However there was less confidence in how effectively regulations were in preventing abuses of Smart CCTV, with only 36% agreeing with the statement in line 1.

Choose the options which better reflect your opinions..	N	Selected	Unselected
1. Laws and regulations ensure that smart CCTV is not misused	201	36%	64%
2. I believe that Smart CCTV improves national security	201	81%	19%
3. I believe that Smart CCTV is intrusive	201	23%	77%
4. I think that the level of intrusiveness is acceptable given the benefits smart CCTV offers	201	68%	32%
5. None of the four listed in case of smart CCTV	201	2%	98%
6. Don't know/don't want to answer	201	0%	100%

Table 12: Perceived effectiveness and intrusiveness of smart CCTV

DPI

In general, there was agreement that DPI has a role to play in preventing criminal activity, particularly in relation to certain crimes such as the dissemination of child pornography, though the majority (53%) also said they did not understand what DPI is. 19% admitted that they felt more secure when online as a consequence of DPI, with 57% agreeing that it is an effective security tool. Even so, most citizens (84%) were deeply uneasy by the fact that DPI was being used without their permission and that it can be used to monitor everyone, not just criminals, as this participant and others explained:

> "DPI should only be used if you have been charged with a crime not just to look at what your habits are" (Postcard 14).

> "DPI should only be implemented in cases where a person is a legitimate suspect in a criminal investigation where just cause can be established to a judge and a recorded warrant of execution is issued, and the record can be viewed by the public." (Postcard 15)

Just over half (58%) were made to feel uncomfortable by the use of DPI, with 22% disagreeing that this was the case.

> "DPI can be damaging to the public and cost a lot of money. Needs to be made clearer to users who and what is looking at their activities etc. and for what reason". (Postcard 10)

> "DPI should only be used for stopping of virus and spam mail. There are other methods of catching criminals such as paedophiles, phishing sites etc. This prevents the used of DPI unnecessarily and violation of privacy." (Postcard 44)

Once again, there were also concerns that basic human rights could be violated by the technology, with 69% expressing concerns about their personal rights and 62% about the fundamental rights of everyone. Only 46% of respondents agree with the statement "I think that the level of intrusiveness is acceptable given the benefits DPI offers", and a very small group (23%) believed that laws and regulations were able to ensure that DPI was not misused.

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
PERCEIVED EFFECTIVENESS	**N**			**Percentages**			
In my opinion, DPI is an effective national security tool	206	17%	40%	26%	11%	4%	1%
When I am online, I feel more secure because DPI is used	209	4%	15%	33%	31%	16%	1%
DPI is an appropriate way to address national security threats	209	23%	37%	22%	11%	4%	2%
PERCEIVED INTRUSIVENESS	**N**			**Percentages**			
The idea of DPI makes me feel uncomfortable	207	23%	35%	19%	15%	7%	1%
I feel DPI is forced upon me without my permission	205	51%	33%	9%	4%	2%	0%
DPI worries me because it could violate my fundamental human rights	204	36%	33%	14%	10%	7%	0%
DPI worries me because it could violate everyone's fundamental human rights	202	28%	34%	19%	11%	7%	1%

Table 13: Perceived effectiveness and intrusiveness of DPI

In contrast to table 12, table 14 shows that while participants believed that DPI would improve national security (line 2) they had serious concerns about its intrusiveness. Participants were given a choice of 6 items and they were to select the statements that they agreed with. 66% of the sample believed DPI improved national security and 66% also believed it was intrusive. 46% agreed that the level of intrusiveness was acceptable given its benefits. There was widespread scepticism about the ability of the laws and regulations to guard against the misuse of DPI (line 1) with only 23% believing that the laws prevented its misuse.

	Choose the options which better reflect your opinions..	N	Selected	Unselected
1.	Laws and regulations ensure that DPI is not misused	200	23%	78%
2.	I believe that DPI improves national security	200	66%	34%
3.	I believe that DPI is intrusive	200	66%	34%
4.	I think that the level of intrusiveness is acceptable given the benefits DPI offers	200	46%	55%
5.	None of the four listed in case of DPI	200	3%	97%
6.	Don't know/don't want to answer	200	1%	99%

Table 14: Perceived effectiveness and intrusiveness of DPI

Social, temporal and spatial proximity of SOSTs

Overall, the concerns of participants about the social, temporal and spatial proximity of SOSTs were greater for DPI than they were for Smart CCTV. In relation to Smart CCTV, participants' views appeared to be affected by the extent to which the technology was likely to be implemented close to where they live or to have an effect on them personally. 58% agreed that if Smart CCTV only targets criminals they do not need to be bothered by it, though 23% disagreed with this viewpoint. Around half of citizens (53%) expressed concerns about how Smart CCTV might develop in the future. One participant considered that

the "next generation will be more accepting of surveillance" (Postcard 53). Some questioned the extent to which monitoring security using this kind of technology is cost effective.

Overall, much greater concerns were expressed about DPI, with 81% of participants worried about how DPI might be used in the future, and 80% questioning the potential of this SOST to reveal sensitive information about them. The personal implications of DPI were also evident in what citizens felt about it being used to track them personally, with 52% being anxious about the potential for using the technology in this way. As one citizen explained: "I would like to add that intrusion of privacy in DPI is unacceptable, records of personal details should not be kept" (Postcard 34). Another expressed fears about the possible manipulation of DPI:

> "DPI – open to manipulation? Who is funding this and who is the information sold to? This is a deep intrusion to privacy when targeting a whole population. How do you discriminate genuine errors from intentional use?" (Postcard 79)

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**Percentages**			
Smart CCTV does not bother me as long as it only targets criminals	208	26%	32%	18%	16%	7%	0%
I worry about how the use of smart CCTV could develop in the future	204	22%	31%	20%	19%	8%	0%
Smart CCTV only bothers me if it is used in the areas where I live and work	210	3%	8%	23%	37%	30%	0%

Table 15: Proximity dimensions – smart CCTV

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**Percentages**			
DPI does not bother me as long as it only targets criminals	205	29%	34%	16%	12%	8%	1%
I worry about how the use of DPI could develop in the future	204	40%	41%	10%	7%	3%	0%
DPI only bothers me if it is used to track my online activities	203	23%	29%	18%	19%	10%	1%

Table 16: Proximity dimensions – DPI

Substantive Privacy Concerns

Deeper insights into participants' privacy concerns were revealed through a series of questions about different aspects of privacy and the potential of SOSTs to affect them. In the case of Smart CCTV, people were particularly concerned that its use might result in their behaviour being misinterpreted in some way. Similar views were found in relation to the use of DPI, but for this technology the anxieties about privacy being invaded were deeper.

In relation to Smart CCTV, views were divided about whether the technology might reveal sensitive information, with 39% agreeing that this could be the case and 41% disagreeing. A larger number of participants (64%) feel that Smart CCTV could lead to their behaviour being misinterpreted. There were also worries about how 'normal' behaviour was defined, with one person commented about the dangers of misinterpreting the behaviour of those with learning disabilities:

> "Who decides what is classed as 'normal' behaviour for the auto behaviour recognition due to people having learning disabilities etc. that may not seem 'normal' or do 'normal things'." (Postcard 58)

40% of those involved in the summits were concerned that the technology might let strangers know their location.

The questions about DPI revealed a similar pattern, with 80% fearing that the technology might lead to sensitive information being revealed about them, 74% being concerned that it might reveal their location to others; 73% worried that their behaviour might be misinterpreted in some way; and 80% being concerned that it might reveal the content of their communications.

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**Percentages**			
Smart CCTV worries me because it could reveal sensitive information about me	207	14%	25%	20%	31%	10%	0%
Smart CCTV worries me because it could let strangers know where I am	207	18%	32%	17%	24%	9%	0%
Smart CCTV worries me because it could result in my behaviour being misinterpreted	208	31%	33%	16%	15%	4%	1%

Table 17: Substantive Privacy Concerns Scale – smart CCTV

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**Percentages**			
DPI worries me because it could reveal sensitive information about me	202	44%	36%	9%	7%	3%	1%
DPI worries me because it could let strangers know where I am	202	44%	30%	15%	7%	4%	0%
DPI worries me because it could result in my behaviour being misinterpreted	207	36%	37%	11%	14%	2%	0%
DPI worries me because it could reveal the content of my communications	204	42%	38%	9%	8%	3%	0%

Table 18: Substantive Privacy Concerns Scale – DPI

In Figures 7 and 8, concerns about trade-off between the potential risks and benefits of the two technologies are elaborated. In summary, these findings shows that half (50%) of participants consider Smart CCTV to be 'useful and not very intrusive', with 41% regarding the technology as 'useful but highly intrusive'. In relation to DPI, the picture is rather different, with the vast majority (85%) seeing DPI as 'useful but highly intrusive'. This tension between the potential costs and benefits was clearly evident in some of the comments made by participants:

> "I think the use of DPI is far too intrusive into personal emails etc. also bank details etc. It could be useful for targeting terrorists, child pornography etc." (Postcard 89)

"DPI. This is currently being used for the benefit of government and security agencies. Citizens suffer ID fraud, spam mail etc. on a daily basis but are not defended by DPI. The use/benefit from it is derived by government etc. to fulfil your own agenda. This needs to be changed. If everyone does not benefit on a daily basis the premise of DPI must be challenged and changed." (Postcard 92)

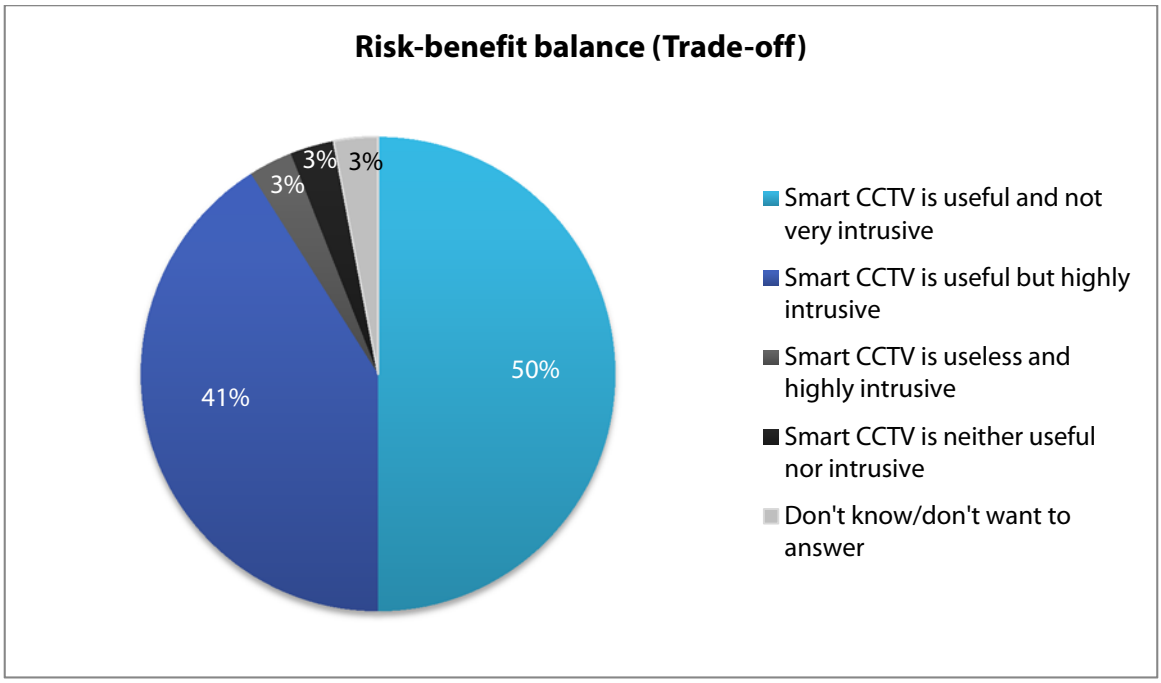


Figure 7: Risk-benefit analysis – Smart CCTV

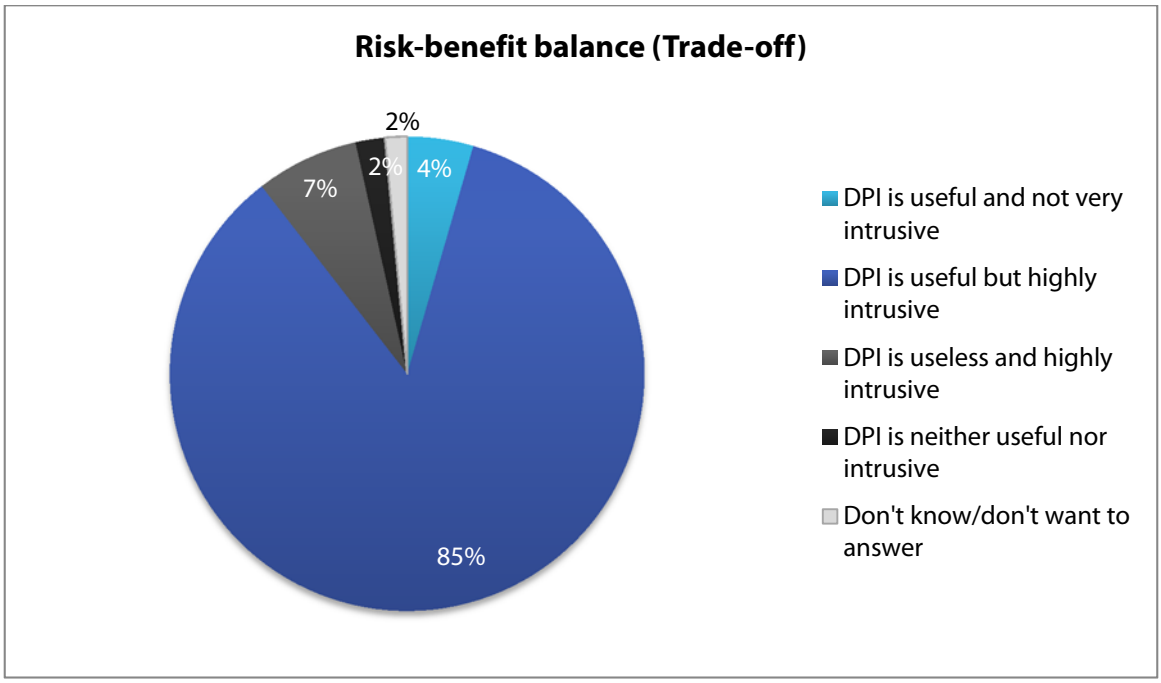


Figure 8: Risk-benefit analysis – DPI

4.2.3 Avoidance, resistance against surveillance

The next questions examine the ways in which citizens might respond to the use of SOSTs, with a particular focus on actions taken to avoid or resist the surveillant aspects of the technologies. Very few of those participating (3%) suggested they would actively avoid areas where smart CCTV was being used, with 91% indicating that they would not change their behaviour because of the technology. There was, however, a view that smart CCTV was more suitable for public than residential locations: "No smart CCTV in residential areas! This is too intrusive. But excellent in public areas" (Postcard 62).

The figures for DPI avoidance were also low, with only 4% indicating they would avoid going online as a result and 78% saying that it would not alter their behaviour. Some participants openly expressed concerns that they did not understand enough about how the technology worked, with some acknowledging that knowing more about it could influence whether they would decide to avoid or react against it:

> "I don't think I fully understand the ins and outs of DPI and I feel that even if I spent a whole day researching about it I would still be just as confused as I am now. I do think DPI could be useful but there needs to be more rules and regulations put into place to control who can get hold of this information." (Postcard 88).

		I would never go into areas where smart CCTV is used	I would avoid going into areas where smart CCTV is used	I would change my behaviour in areas where smart CCTV is used	I do not think I would change my behaviour because of it	I would definitely not change my behaviour because of it	NA
	N	**Percentages**					
These questions concern whether you would actively avoid CCTV	207	1%	2%	5%	27%	64%	1%

Table 19: Avoidance dimension – smart CCTV

		I would not go online because of DPI	I would avoid going online because of DPI	I would change how I behave online because of DPI	I do not think I would change my behaviour online	I would definitely not change my behaviour online	NA
	N	**Percentages**					
These questions concern whether you would actively avoid DPI	206	2%	2%	17%	45%	33%	1%

Table 20: Avoidance dimension – DPI

Actively resisting the surveillance imposed by SOSTs is a more extreme form of response to these technologies than avoidance. Only 5% of citizens said that they personally would be prepared to actively challenge the use of Smart CCTV, with a further 10% prepared to support others protesting against its adoption. The figures for DPI were higher, with 10% indicating they would do what they could to prevent its use, with 15% suggesting they would support others who were doing so. There was further evidence of concern about the detrimental effects of SOSTs to citizens' privacy, with 37% and 59% respectively, prepared to find out more about how to protect their privacy.

		I am prepared to use any means I can to prevent its use	I am prepared to campaign actively against its use	I would support others who were protesting against its use	I would like to find out more how to protect my privacy	I do not oppose it at all	NA
	N	**Percentages**					
These questions concern whether you would actively challenge the use of CCTV for security purposes	204	2%	3%	10%	37%	47%	1%

Table 21: Resistance dimension – smart CCTV

		I am prepared to use any means I can to prevent its use	I am prepared to campaign actively against its use	I would support others who were protesting against its use	I would like to find out more how to protect my privacy	I do not oppose it at all	NA
	N	**Percentages**					
These questions concern whether you would actively challenge the use of DPI for security purposes	205	6%	4%	15%	59%	13%	2%

Table 22: Resistance dimension – DPI

4.3 Trustworthiness of security authorities and the role of alternative security approaches

In this section the extent to which participants regard security authorities as trustworthy is considered and some reflections are presented on the role of alternative security approaches.

The degree to which citizens are prepared to accept the use of SOSTs is influenced by the views they hold of the security agencies and other bodies that are responsible for implementing the use of these technologies. A number of questions addressed the extent to which participants believed these agencies to be trustworthy, competent, to have the best interests of citizens at heart, and to not abuse their power. While 31% participants consider security agencies using Smart CCTV to be competent, 29% viewed them as trustworthy, and 46% agreed that they have the welfare interests of citizens at heart. However, only 16% considered that these agencies would not abuse their power with a substantial number (41%) expressing doubts that such abuses would not occur. The figures for DPI are broadly similar, with 29% viewing agencies that implement this technology as competent, 30% considering them to be trustworthy, and 41% satisfied that they were focused on the welfare of citizens. Once again, participants were more cynical about the extent to which security agencies might abuse their power, with 41% agreeing that this was likely.

> "I believe that 'human rights' is allowed too easily and broadly to be used to debate certain issues such as the use of smart CCTV etc. amongst other things. However I think that public should always be fully informed in the implementation, purpose and users of such technologies. There should be a body, selected randomly from different sources to 'audit' security agencies in their use of technologies." (Postcard 8)

Citizens knew very little about the work of security agencies: both in the case of smart CCTV (47%) and DPI (45%) respondents were unable to express a clear view on their level of competence. There was also uncertainty regarding the integrity of agents: most respondents could not clearly say if agents would or would not abuse they power (40% in the case of smart CCTV and 39% in the case of use of DPI). There was also a sense that citizens wanted to know more about how the collected information would be used, by whom, and how long it would be kept. Some felt that gathered information should only be used by law

enforcement agencies, and that greater transparency is needed about its gathering and use. As the following comments reflect, citizens feel that agreement is needed on controls and where the limits of acceptability lie:

> "There should be some way that DPI and government do not misuse the data they obtain. I would like more clarification on what is being viewed and shared. World wide laws or agreement for clarification is needed." (Postcard 56)

> "More legislation for DPI; regulations for companies on gaining personal information. Permissions for data to be used." (Postcard 42)

In some cases, participants worried about DPI leading to personal information about them being accessible to third party companies which might use it in other ways or for other purposes. In particular, there were also worries about the involvement of profit making businesses in the implementation of security involving SOSTs, with one participant commenting that "No security services should be outsourced to private (profitmaking) companies" (Postcard 54).

Similar sentiments were expressed by other citizens:

> "I agree there should be DPI but the public should have the right to opt out of your private details being accessed by a third company without your permission. Then getting endless emails and calls from companies you do not wish to hear from." (Postcard 18)

> "Let us know if our data is going to be given to third parties, ask for our permission first. Create a law/legislation that protects our personal information from being used without us being informed." (Postcard 43)

There was also a strong sense among participants that data relating to the UK should only be gathered by and handled within the UK. One citizen argued that: "The British government should be more strict in controlling who accesses the info" (Postcard 96); and called for them not to "…be dictated by other countries i.e. the United States". However, there was also a recognition among citizens that in relation to DPI, the UK does not have control over the actions that are taken; as one participant explained: "With most internet traffic passing through USA we in Europe have little control over DPI" (Postcard 73).

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**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

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N			**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

Although the questions in this section focused on the agency or organisation responsible for using the SOSTs, citizens were also concerned about the role of individuals within the process and the extent to which they were competent or could be trusted. As one participant commented "I would really like to know who watches the people that are watching us" (Postcard 23). Another participant expressed similar worries: "I am concerned that a stranger has information about me and could use it for personal means. Who checks the operator?" (Postcard 7); while a third asked: "What qualifications and security checks to CCTV operators have?" (Postcard 93). According to one citizen, a solution might be to have: "New data police to be enforced and accessible to the public" (Postcard 59).

Others, however, found the notion of a human element within security systems to be what is needed: "Even with a continually developing security system I don't want it to replace the human element. Police officers should not be replaced by smart CCTV." (Postcard 61).

4.4 Citizens' recommendations to policy makers

In this section the recommendations that summit participants made to policy makers are considered. Those attending the summits enthusiastically embraced the opportunity to make recommendations for policy makers; addressing the task in a diligent and serious manner. A wide range of recommendations was produced, the content of which closely reflect the responses to the quantitative questions. In this section these recommendations are reported in several thematic sections: (a) transparency and communication; (b) responsibility for implementing SOSTs; (c) provision of evidence; (d) smart CCTV; (e) DPI; and (f) non-technological solutions to security. These thematic sections reflect the areas in which the recommendations were focused. Although the recommendations are stated in summary bullet point form, some quotes from the table groups are provided for illustrative purposes. A summary table drawing all of these recommendations together is provided at the end of this section, with the original table containing all of the recommendations from the table groups presented in the Appendix.

(a) Transparency and communication

The need for greater transparency about the use of SOSTs and the implications for the privacy and human rights of citizens was a recurring theme throughout the UK summits. Many citizens explained that they had been unaware of these issues prior to being invited to the summits. There was a feeling that levels of understanding about the use of SOSTs are low among the general public, and that a much better understanding of these issues needs to be developed. As one table group reported, the "majority of people are unaware of the depth of intrusiveness that occurs". Consequently there were demands for more user-friendly and accessible information to be made available. Areas in which greater clarity is deemed necessary include the following: the nature of the information/data being collected; details about who holds, uses, and is responsible for that information/data; and more transparency about whether there is access to it beyond those in the security agencies. The need for appropriate regulation

of SOSTs was also raised, a point which is explored further in the next sub-section. As one table group stated:

> "Who has access to our information beyond security agencies? We are uncomfortable about how the information is used and who it is passed on to".

Several recommendations emerged in relation to these views about transparency and the need for better communication about the use of SOSTs:

- Awareness about the use of SOSTs should be raised, through appropriate communication which presents information about these technologies in a way that can be readily understood by citizens.
- There should be greater clarity about who, how and where gathered information/data is held and used.
- In the interests of transparency, citizens should have access to information that the security services and others hold about them.

(b) Responsibility for regulating and implementing SOSTs

Strong views were expressed about the institutions that are responsible for operating the SOSTs and for handling the information/data that is produced as a result. Participants were supportive of operational responsibility taking place at a national (UK) level, with some approving of such responsibility overseen by European law and regulations. They were keen to know 'who would be watching the watchers?' Citizens were very resistant, for example, to the idea of private organisations being involved in operating any aspect of SOSTs. Several suggestions were made about how regulatory bodies might be constituted: one suggestion was to allow MPs from each political party to be represented; another was that those appointed should be publicly elected. There was a feeling that such a body should be directly accountable to the public, in order that individual privacy and human right would be respected. These sentiments are captured in the following comments:

> "Form a publicly elected independent either national or worldwide body/team who monitor and control the security agencies. Report findings to the public so that we can see who is accessing our data and they are using it for and we the public can make recommendations to that body".

These views translate into several recommendations in relation to regulating and implementing SOSTs for policy makers:

- The use of SOSTs should be governed by transparent and easy to understand legislation.
- In order to ensure accountability, an independent regulatory body should be established that has responsibility for overseeing the use of SOSTs, and which sets rules about handling the gathered information/data.
- Government should ensure that any information/data that is collected through the use of SOSTs is held within the UK and not sent elsewhere.
- SOSTs should be controlled nationally but to an EU standard.
- Private companies should not be involved in operating SOSTs or have access to the information/data that is produced.

(c) Provision of evidence

Some citizens were suspicious about the effectiveness of using SOSTs to solve security problems. These concerns were linked with the view that the general public may not be being kept fully informed about the costs and benefits associated with using these technological security solutions. Some participants argued that details of the costs should be made available and that evidence for the efficacy of these solutions should be gathered and shared. The following comment from one table group illustrates this theme:

> "The government and security forces to be more open with statistics showing how DPI has benefited us. How many interceptions have taken place?"

In light of these concerns, the following recommendations for policy makers about the provision of evidence emerge:

- Details about the costs of SOSTs should be made available in the public domain.
- Efforts should be made to gather information about the efficacy of SOSTs, which is open to scrutiny.

(d) Smart CCTV

The recommendations presented in this sub-section relate specifically to the use of smart CCTV. Participants were generally supportive of the need for smart CCTV and for its use as a tool to protect citizens in their daily lives. However, they were more supportive of the use of this technology in public areas – particularly where public order problems might be encountered - and less happy about its use or intrusion in residential locations. They were very much against the idea that this technology might 'see' into peoples' homes. In the words of one participant: "Do not let CCTV get too advanced so that we end of 1984, big brother watching you!" (Postcard 71). These worries were reflected in calls to ensure that CCTV does not become too intrusive. There was also a concern that this technology might be used as a substitute for police on the streets, which was t seen as a bad thing.

Some participants wondered about the extent to which smart CCTV technology could be developed so that its effectiveness could be improved and the likelihood of the human rights of innocent s being reduced.

From these concerns, a number of policy recommendations in relation to the implementation of smart CCTV are made:

- Only 'trusted operators' should be involved in implementing smart CCTV and handling the information that is generated.
- The use of smart CCTV should be increased in rural and public areas where public order problems were likely, but restricted in areas where the privacy of individuals in their homes could be affected.
- The use of smart CCTV should not detrimentally affect the level of policing on the streets; instead it should be used in conjunction with existing policing.
- Further investments should be made in smart CCTV technologies to improve its effectiveness; for example, to develop the technology's ability to identify suspect individuals in crowded areas.

(e) DPI

There was a widespread recognition among citizens that DPI is needed to ensure national security, to reduce crime, and to prevent websites that promote child pornography or certain kinds of propaganda. However, there were also major concerns about potential abuses of this technology. In particular, there was a sense that the monitoring of web traffic ought to go no further than is strictly necessary, and should be targeted as much as possible on criminals. Proof of the approach's effectiveness was seen as essential. As one table group explained:

> "DPI is essential for our personal, national and international security, this should continue. But with the government and security forces proving how it has helped us".

Citizens expressed substantial concerns about the intrusiveness of this SOST to those who are not doing anything wrong. These fears were exacerbated by the fact that DPI is not visible to the general public who are unlikely to know that it is going on: "We don't have enough information on who is watching us or what information is being collected and where and how long is the information stored".

One table group suggested that 'pop ups' or emails could be triggered upon visiting web pages that are monitored so that individuals would know that their behaviour was being watched. There were also concerns that data could fall into the wrong hands, or that it might be passed onto third parties for other uses (including financial gain). In the words of one table group, there should be: "Targeted use of DPI for security purposes (including criminal activity) supported by transparent/open regulations and consistent monitoring of data usage, only government agencies, not commercial companies".

These fears resulted in a large number of recommendations about guidelines and regulations for controlling DPI:

- A better understanding of DPI in the public domain needs to be promoted, ensuring that everyone is aware of the rules which govern it.
- There should be a centralised policy for the control and operation of DPI technologies.
- Laws and guidelines are needed to set the limits of acceptable data gathering under DP and data storage; to bring greater transparency about what is allowed and what is not. These laws must be regularly updated to reflect future technological developments. The following issues should be covered:
    - Where the data can be stored, under what conditions, who/which institutions have access to it, and for what purposes.
    - Set limits in relation to the allowable time period for the retention of information.
    - Only data on criminals should be stored.
- Only government and security agencies should be involved in gathering and analysing DPI data.
- An independent regulatory body should be established to monitor data usage and prevent the commercial use of DPI.
- The targeting of the most harmful activities should be prioritised, such as identifying terrorists and those responsible for child pornography.
- Options should be considered for notifying web users about sites that are monitored and providing guidance on how they can complain.
- If misleading information about citizens is stored, individuals must be fully informed about what recourse they have to get it removed.

(f) Increase non-technological solutions to security

A recurring theme in the recommendations was that the adoption of SOSTs should not replace non-technological solutions to security. However, ideas one what forms these other solutions might take were quite limited. Citizens were especially concerned that levels of policing on the streets should not fall, while others suggested the reintroduction and strengthening of neighbourhood watch schemes in local communities.

Two recommendations for policy makers are associated with issues relating non-technological solutions to security:

- Smart CCTV should supplement rather than replace the presence of police on the streets.
- The developments of local neighbourhood watch and other community schemes to promote security should be supported.

Transparency and communication

- Awareness about the use of SOSTs should be raised, through appropriate communication which presents information about these technologies in a way that can be readily understood by citizens.
- There should be greater clarity about who, how and where gathered information/data is held and used.
- In the interests of transparency, citizens should have access to information that the security services and others hold about them.

Responsibility for regulating and implementing SOSTs

- The use of SOSTs should be governed by transparent and easy to understand legislation.
- In order to ensure accountability, an independent regulatory body should be established that has responsibility for overseeing the use of SOSTs, and which sets rules about handling the gathered information/data.
- Government should ensure that any information/data that is collected through the use of SOSTs is held within the UK and not sent elsewhere.
- SOSTs should be controlled nationally but to an EU standard.
- Private companies should not be involved in operating SOSTs or have access to the information/data that is produced.

Smart CCTV

- Only 'trusted operators' should be involved in implementing smart CCTV and handling the information that is generated.
- The use of smart CCTV should be increased in rural and public areas where public order problems were likely, but restricted in areas where the privacy of individuals in their homes could be affected.
- The use of smart CCTV should not detrimentally affect the level of policing on the streets; instead it should be used in conjunction with existing policing.
- Further investments should be made in smart CCTV technologies to improve its effectiveness; for example, to develop the technology's ability to identify suspect individuals in crowded areas.

DPI

- A better understanding of DPI in the public domain needs to promoted, ensuring that everyone is aware of the rules which govern it.
- There should be a centralised policy for the control and operation of DPI technologies.
- Laws and guidelines are needed to set the limits of acceptable data gathering under DP and data storage; to bring greater transparency about what is allowed and what is not. These laws must be regularly updated to reflect future technological developments. The following issues should be covered:
  - Where the data can be stored, under what conditions, who/which institutions have access to it, and for what purposes.
  - Set limits in relation to the allowable time period for the retention of information.
  - Only data on criminals should be stored.
- Only government and security agencies should be involved in gathering and analysing DPI data.
- An independent regulatory body should be established to monitor data usage and prevent the commercial use of DPI.
- The targeting of the most harmful activities should be prioritised, such as identifying terrorists and those responsible for child pornography.
- Options should be considered for notifying web users about sites that are monitored and providing guidance on how they can complain.
- If misleading information about citizens is stored, individuals must be fully informed about what recourse they have to get it removed.

Non-technological solutions

- Smart CCTV should supplement rather than replace the presence of police on the streets.
- The developments of local neighbourhood watch and other community schemes to promote security should be supported.

Table 25: Summary List of Recommendations to Policy Makers.

5 Summary and Conclusions

The United Kingdom's views on surveillance, security and privacy reflect its unique position in Europe. It is subject to and affiliated with European countries in terms of regulation and law, but has a close relationship with the United States, which is also reflected in its security policies. It has a strong history of activism in the civil liberties arena, and a data protection regulator for whom the surveillance society is strongly on the agenda. Government policy, media debates and public opinion thus reflect the broad range of positions on the topic. The data reflect these patterns and also reveal general concern over who has access to personal data for security purposes, and a concern for accountability and transparency in relation to information use for security-related surveillance activities.

Among the British participants a widely held view was that the public do not know enough about the uses of and risks associated with surveillance-oriented security technologies. There were many calls for more information to be made available over what is being used both by the state and by private companies. Having said that, the participants supported the use of SOSTs, having been exposed to both the benefits and issues associated with them. The participants expressed greater concern for DPI than they did for Smart CCTV. We would suggest that this reflects the long standing, normalised use of CCTV in Britain and the recent (at the time) media coverage of NSA and GCHQ communications surveillance. Reflecting issues considered at European level the British participants raised deep seated concerns about data retention in the UK and whether and how personal data was shared with other countries. They were worried that data may fall into the wrong hands, that individuals or organizations would exploit their data without their knowledge in order to profit or benefit from it. The British participants were particularly adamant that only the state should be involved in national security matters involving SOSTs and handling the information which was produced. They were unanimous in their higher trust of security agencies such as the police and there was a general mistrust of the involvement of private institutions, which is perhaps not surprising given the negative feelings expressed about private companies. Greater regulation over the use of SOSTs was called for as was accountability. Whilst the public were concerned about the use of SOSTs, requesting greater democratic scrutiny of technology selection, implementation and use by security services on behalf of the public, they were not wholly opposed to their existence and use. Moreover they were not particularly prepared to resist their use in terms of taking action or protesting. In Britain the public were more concerned about how SOSTs would affect them as individuals, rather than the community in general. Reflecting broader debates about police resourcing, participants expressed a concern that policing levels would be reduced and police would be replaced by technologies.

Overall, although there was broad support for SOSTs by the end of the citizen summit, the summits had prompted the citizens to consider privacy issues more closely. This was partly reflected in the recommendations they made which concerned calls for greater transparency, more effective regulation, a limitation of SOST-use to 'trusted partners' rather than its widespread use. They were keen to learn more about the issues and wanted to be better informed all round. Furthermore, there were huge movements in the measures representing privacy concerns as well as calls for greater democratic scrutiny of the watchers. Therefore, whilst this research was framed in terms of a trade off between privacy and security, it seems that the British participants were not willing to make this trade off. In contrast to previous research into public opinion, they demanded both enhanced security *and* enhanced privacy following their participation in the summits.

6 Bibliography

A Strong Britain in an Age of Uncertainty: The National Security Strategy, (October 2010), Crown Copyright 2010, ISBN: 9780101795326.

Barr, Nicholas A. and Peter Kellner (n.d.) s. v. "United Kingdom", Encyclopædia Britannica Online. URL: http://www.britannica.com.libezproxy.open.ac.uk/EBchecked/topic/615557/United-Kingdom.

BBC News (2009): UK's national ID card unveiled. URL: http://news.bbc.co.uk/1/hi/8175139.stm

'Birmingham (UK)' Hutchinson UK Gazetteer, Helicon Publishing, May 2012. Retrieved from know UK.co.uk

Data Protection Act (1998), retrieved from legislation.gov.uk. URL: http://www.legislation.gov.uk/ukpga/1998/29/contents

Data Protection Act 1984 (repealed 1.3.2000). URL: http://www.legislation.gov.uk/ukpga/1984/35/contents

Data Retention and Investigatory Powers Act 2014 URL: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

Ditton, J. (2000). Crime and the city: Public attitudes towards open-street CCTV in Glasgow. *British Journal of Criminology*, **40**, 692 - 709.

European Commission. URL: http://ec.europa.eu/public_opinion/index_en.htm

Halliday, Josh (2011) "CPS under attack over BT and Phorm's covert online monitoring: Privacy watchdogs fear big corporations can violate UK internet users' rights with impunity", theguardian.com, Monday 11 April 2011 17.30 BST. URL: http://www.theguardian.com/technology/2011/apr/11/cps-bt-phorm-appeal

HM Government (2010) "A Strong Britain in an Age of Uncertainty: The National Security Strategy", Presented to Parliament by the Prime Minister by Command of Her Majesty, October. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

HM Government (2010) "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review", Presented to Parliament by the Prime Minister by Command of Her Majesty, October. URL: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr

House of Commons/Home Affairs Committee (2008): A Surveillance Society?. Fifth Report of Session 2007–08. Vol. 1. URL: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf

House of Lords (2009): Surveillance: Citizens and the State. Constitution Committee - Second Report URL: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

Human Rights Act (1998), retrieved from legislation.gov.uk. URL: http://www.legislation.gov.uk/ukpga/1998/42/contents

Gil, Martin & Spriggs Angela (2005): Assessing the impact of CCTV. Home Office Research, Development and Statistics Directorate. February 2005. URL: https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf

Office for National Statistics (2012) "2011 Census: Key Statistics for England and Wales, March 2011", 11 December. URL: http://www.ons.gov.uk/ons/dcp171778_290685.pdf

Office for National Statistics (2012) "Ethnicity and National Identity in England and Wales 2011", 11 December. URL: http://www.ons.gov.uk/ons/dcp171776_290558.pdf

McCahill, M (2012) Surveillance, Crime and the Media in Ball, K, K Haggerty and D Lyon (2012) *The Routledge Handbook of Surveillance Studies*. London: Routledge

Raab, Charles and Benjamin Goold (2011) "Protecting information privacy", Equality and Human Rights Commission, Research report 69, First published Summer 2011. URL: http://www.equalityhumanrights.com/sites/default/files/documents/research/rr69.pdf

Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, (October 2010), Crown Copyright 2010, ISBN: 9780101794824. URL: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr

Surveillance Studies Network. URL: http://www.surveillance-studies.net/?page_id=3

Surveillance Studies Network (2010) An Update To 'A Report on the Surveillance Society'. Wilmslow: Information Commissioners Office. URL: http://www.ico.gov.uk/SearchResultAsHtml.aspx?cid=LzpZ9YU_gKsJ&page=http://www.ico.gov.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/surveillance_report_for_home_select_committee.ashx&keywords=an update to a report on the surveillance society Accessed 5th October 2012

theguardian (2014) "Edward Snowden: Latest on the computer analyst whistleblower who provided the Guardian with top-secret NSA documents leading to revelations about US surveillance on phone and internet communications", The Guardian. URL: http://www.theguardian.com/world/edward-snowden

United Kingdom. (2012) in CIA World Factbook. URL: http://libezproxy.open.ac.uk/login?qurl=http%3A%2F%2Fsearch.credoreference.com.libezproxy.open.ac.uk%2Fcontent%2Fentry%2Fcia%2Funited_kingdom%2F0

UK Polling Report: survey and polling news from YouGov's Anthony Wells. URL: http://ukpollingreport.co.uk/issues/id-cards

Whitaker's Almanack, published by A&C Black in October 2013. Retrieved from KnowUK.co.uk

Williams, Christopher (2011) "BT and Phorm: how an online privacy scandal unfolded: The Crown Prosecution Service's decision not to prosecute BT and Phorm over their secret interception of internet traffic closes a chapter of Britain's biggest online privacy scandal", The Telegraph, 08 Apr 2011 4:32PM BST. URL: http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html

Williams, Christopher (2008) "How Phorm plans to tap your internet connection: Under the hood of BT's data pimping machine", The Register, 29 Feb 2008. URL: http://www.theregister.co.uk/2008/02/29/phorm_documents/

URL: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy

URL: http://www.synx.com/index.php/News/public-attitudes-to-cctv-shift-following-riots.html

7 List of Figures

8 List of Tables

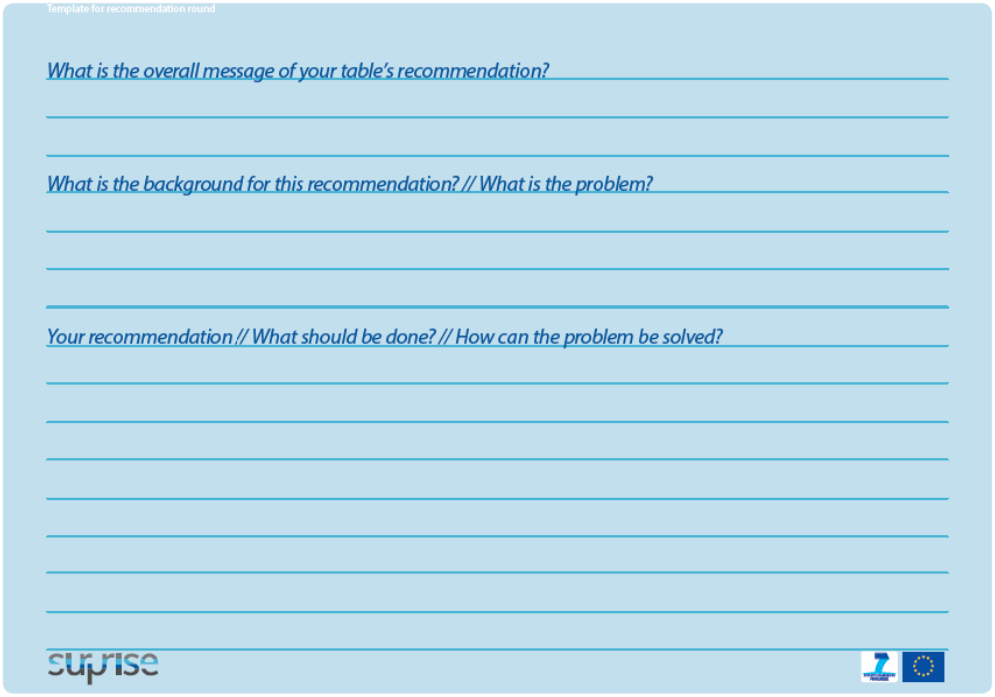
9 List of Abbreviations

Abbreviation	Definition
CCTV	Closed circuit television
DPI	Deep Packet Inspection
ECHR	European Convention on Human Rights
EU	European Union
GCHQ	Government Communications Headquarters
ICO	Information Commissioner
ID	Identity
LSE	London School of Economics
NSS	National Security Strategy
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
SDSR	Strategic Defence and Security Review
SOST	Surveillance-oriented security technology

10 Annex

10.1 Table recommendations

Template[28]



Recommendations – content 1st summit

Recommendation forms, 1st March 2014		
Overall message	*Background*	*What should be done?*
What is the core statement of the table's recommendation?	**What is the background of the recommendation?/ what is the problem?**	**The recommendation in detail/What should be done/how to address the problem?**
We need to be aware of who is looking at our data and to what purposes	WE need to know who is gathering the information and for what purpose	Regulated international body and constant policing. The problem cannot be solved only minimalised
Tighter regulation of technologies and greater transparency about these technologies especially how they are used so the public can make informed decisions	Lack of awareness about the extent of intrusion amongst the public and who/why their information can be accessed. Particularly, the lack of regulation of these technologies' users	EU level legislation, work towards international agreement Governments to focus on criminalisation of private data distribution, in their own jurisdiction or amongst private organizations, with responsibility being placed on the organization to get the consent of the individual about that data being shared Individual responsibility of the data gathering individual, if they are not working on behalf of an organization to gain consent (e.g. independent journalist etc.)

[28] This recommendation sheet was filled in by each table.

We agree to both systems being implemented	The information we have viewed today – who is watching, where is the data being viewed/stored. Who has access	Both systems should be overseen by a regulator. Information to the public needs to be in simple terms
Control, guidelines, what do they do with information? Data protection, where does it come from? Smart CCTV is a good idea as long as strict guidelines are adhered to	Problem=data falling into the wrong hands or data protection being compromised	Properly regulated and transparent. Set guidelines for how far it can go/what is deemed acceptable/ After a set period of time information should be made public, not hidden. How long for and where is this data being held?
DPI is a good idea as long as it is controlled with strict rules It's a good idea to catch the bad guys, however very intrusive, who has access and what is it being used for? Who is monitoring them?	Problem =-information is being taken without consent, and what information is where and whose hands does it fall into?	Properly regulated and transparent Set guidelines with how far it can go/what is deemed acceptable? At a set period of time information should be made public, not hidden. How long is data kept for and where is this data being held? Information what is being accessed/who has access to this?
DPI is acceptable for certain things i.e. monitoring National Security and prevention of child pornography and screening certain sites	Personal information can be accessed at any time and we don't know by who, and infringement of your human rights. Records being held by third parties for financial gain.	Block websites that promote child pornography and propaganda sites. Personal details to be limited to only that site, to be kept securely and not to readily available to third parties
Smart CCTV: Who holds and has access to recorded information for smart CCTV? Public should be fully informed of who owns information	Identity is misused and where and how long is this information	Independent bodies to inspect, monitor and audit all security companies to see how smart CCTV is used. Data and information is stored and for public to have access to public reports and findings
We demand a high standard of security with controls to respect public privacy	Security is a necessary evil in our advancing technological society. Problem = pack of personal privacy. The choice of who holds and uses our information, especially in the business world and the criminal world	Form a publicly elected independent either national or worldwide body/team who monitor and control the security agencies. Report findings to the public so that we can see who is accessing our data and what they are using it for and we the public can make recommendations to that body
An overall lack of communication by all agencies involved	Lack of consistency between agencies and their procedures and poor response to incidents	A centralised policy of control and a co-operation between technologies and monitoring of DPI activities. Keeping proactive rather than reactive
More clear information given to the public which is user friendly and made available to all. This should be provided by anyone using personal information	Majority of people are unaware of the depth of intrusiveness that occurs`	Stricter legislation which is open to the public and easily available Easy access to any personal record used by any organization Use of public service announcements through media and TV
(majority of table) The overall opinion is that smart	Problem = not kept fully informed and potential cost	Open policies for use of information

CCTV and DPI have a positive impact providing it is properly regulated and monitored, and how and by who it is used is made publicly available	Background = majority of table feel better protected by CCYV, but feel more vulnerable with DPI	DPI potentially breaches data protection Regulatory body could comprise from one MP from each party to promote fairness and transparency Neighbourhood watch and other similar schemes could be reintroduced in local communities, protect and serve
We feel SOST is good to protect children, combat crime and for national security. However we feel there is a lack of clarity	We are unclear about who has access to our information beyond security agencies. We are uncomfortable about how the information is used and who it is passed on to	Laws and policies are made crystal clear to society and they are strictly regulated
Accountability and control	Central access	Monitor the monitors
In favour of use of smart CCTV and DPI, however concerns have been raised about the central body, its leadership and when/how it could be stopped	Regulation and information needs to be more apparent	Regulation should be developed to ensure that the intelligence gathered through smart CCTV and DPI is not used beyond that intended: to protect citizens against acts of terrorism and breaches of national security More awareness to be accessible to the general public National control but EU standardised
DPI is essential for our personal, national and international security, this should continue. But with the government and security forces proving how it has helped us	Concerns raised about who can access our information and how safe we are. Citizens know we are being watched but who by?	The government and security forces to be more open with statistics showing how DPI has benefited us. How many interceptions have taken place?
Smart CCTV is a positive told for not only gathering evidence but preventing crime. It is technology that allows citizens to feel safer in their everyday lives and should be developed further.	We believe this technology has limitations currently. This must be developed further to ensure the system is effective. We are also concerned about the handling of data and innocent citizens' human rights	Technology – invest in developing so reliable and can identify suspects in crowds Data – data and tracking of citizens should only be stored on people of concern, not the nation Human rights – independent regulatory body to oversee this initiative.

Recommendations – content 2nd summit

Saturday 15th March 2014		
Overall message	*Background*	*What should be done?*
What is the core statement of the table's recommendation?	**What is the background of the recommendation?/ what is the problem?**	**The recommendation in detail/What should be done/how to address the problem?**
Happy with CCTV in public areas to reduce crime. Not happy looking in house, private settings	Don't want it to become too intrusive e.g. google maps, see registration number on cars, and accessible to everyone. Operators know not in house	More policing in streets, more security does not replace the police. Major powercut, CCTV down. Lady standing around on film – came up on video as she was loitering

	have to trust the operators. Would council operate?	
More smart CCTV in rural and public areas, and more police presence in residential areas. Also think it could be more cost effective, CCTV sees a crime and sends a message to police who can go straight there – increase efficiency	This will increase security in rural and public areas and maintain a level of privacy in residential areas by changing laws and regs so that you can't have smart CCTV within a certain amount of metres from a house or residential area. This would be replaced by more police officers dedicated to residential areas	
Transparency by government	At present there are no guidelines for information to the public	Information to be available to the public
The government should maintain the goings on regarding the information obtained through new technologies. Not companies and not external to the country unless international threats	Unknown to where the information is being sent and how the information is being used	Government should use the data collected within the country and not have it sent elsewhere. Therefore there would be someone held accountable for any wrongdoing occurring
That the information is not … and to know how this is monitored. To be used for identifying criminals/terrorists	It's already here and intrusion into our privacy has begun. Innocent people get caught up in this	Control needs to be implemented in computer systems to eliminate span etc., so personal data
Both systems are good ideas – the issue is who controls the surveillance, storage and action based on the data collected	All information used and collected must be kept and governed by the UK, NOT EU and other countries	No private company should be involved in the implementation or running of any systems. Who watches the watchers?
Both services should be available only to government security agencies	Personal security has been compromised due to privatisation of security services	Both services should only; - Transparency - More accountability - Tighter legislation to restrict access of services to government security
Ensuring use for the greater good – infiltration of the most harmful illegal activity such as terrorism and child pornography	Problem; underground internet. Material motivates perpetrators to carry actual real-life acts (how to deal with accidental usage)	Increased intelligence; decode vocabulary used to tag images. More effective monitoring; tougher laws and punishment – public awareness of the consequences. How to police the worldwide web – where does the punishment lie? Complete block of such information
See below	Lack of transparency, mistrust of government and companies	Targeted use of DPI for security purposes (including criminal activity) supported by transparent/open regulations and consistent monitoring of data usage, only by government

		agencies, not commercial companies
A non political, independent, regulating body to prevent the commercial use of DPI	Companies can get private information from citizens to promote sales, spam, cold calling	Completely independent regulating body
Data should be kept secure and governed by effective legislation	WE have concerns about the way data is collected, handled and monitored	All aspects should be overseen by independent regulators. All aspects, including regulation, should be updated in line with future technological developments
TO make DPI more visible to the general public and let us know who is being monitored and who is monitoring us	We don't have enough information on who is watching us or what information is being collected and where and how long is the information stored	Creating a pop up on controlled pages make us aware we are being monitoring. Potentially send an email advising that our history is being monitored, how we can make a complaint and who to go to. We also think that any misleading information should be removed
To make DPI more understandable with rules/regulations accessible to all	Understanding and transparency of DPI	For a clear explanation of who is running DPI
In relation to DPI more information, transparency and laws. Not to be used for commercial purposes only government agencies	Not enough information in the public domain	Damage is done, more laws and regulations, accountability, who's watching the watchers?

10.2 Postcards

Template

Postcards – content 1st summit

Postcards, 1st March 2014	
No	**Content**
1	Smart CCTV and DPI concerns me. Who monitors this, what will be done with the information. What about privacy? We were never asked if it was OK in the first place. More public involvement.
2	If Smart CCTV is to be implemented, then a QUANGO should be set up to monitor the government's use of the images and data
3	Honesty is key. Don't install systems and tell a web of lies and half truths about why. Share information – get value for money. Information gathered should be acted on proactively
4	DPI and Smart should work together – government to monitor DPI, when suspicious activity occurs, government should inform local police to monitor CCTV in suspicious area. Government to monitor companies who use DPI – enforce legal requirements.
5	I believe there should be stricter surveillance over high risk criminals and repeat offenders. I.e. maybe a chipping (micro) system for GPS purpose, so that crimes are caught out before they are committed.
6	Who monitors how many cameras or Smart CCTVs there are in a public location. I.e. (1) government agencies (2) private CCTV (3) or could it be possible to put up criminal CCTVs.
7	I am concerned that a stranger has information about me and could use it for personal means. Who checks the operator?
8	I believe that 'human rights' is allowed too easily and broadly to be used to debate certain issues such as the use of smart CCTV etc. amongst other things. However I think that public should always be fully informed in the implementation, purpose and users of such technologies. There should be a body, selected randomly from different sources to 'audit' security agencies in their use of technologies.
9	Remove online banking from everyday internet because of the risk of control of personal assets, when cash is abolished in the future.
10	DPI can be damaging to the public and cost a lot of money. Needs to be made clearer to users who and what is looking at their activities etc. and for what reason.
11	CCTV is a great idea. DPI I do not agree with. I don't want my mail or contacts being observed.
12	I have no problem with DPI if used for the correct purposes. I think that retail companies or businesses should be prevented from passing information for profit making activities. The use by national security agencies for the correct reasons, I feel is acceptable.
13	Birmingham shutting down CCTV due to cost, will EC fund smart CCTV?
14	DPI should only be used if you have been charged with a crime not just to look at what your habits are. The only people who do not like it have something to hide.

15	DPI should only be implemented in cases where a person is a legitimate suspect in a criminal investigation where just cause can be established to a judge and a recorded warrant of execution is issued, and the record can be viewed by the public.
16	I would like to know that DPI cannot fall into the wrong hands or have it used for the wrong purpose.
17	Please allow the UK to leave the European Union. As an organization (EU) you are as bad as the corporations and national governments who use our data to oppress us. We are not fooled!
18	I agree there should be DPI but the public should have the right to opt out of your private details being accessed by a third company without your permission. Then getting endless emails and calls from companies you do not wish to hear from. Tighter security.
19	All types of surveillance is necessary to protect us from criminals, paedophiles and terrorises. However it needs to be monitored and regulated officially by security officials such as governments, police etc. Far more so than is being done at present, to protect people's privacy.
20	Smart CCTV – does it work? It may help catch criminals but I don't think it 'prevents' crime. Keep police on the streets! I think security is necessary however public need to feel safe and that their info is not being misused. Maybe introduce requiring a 'warrant' to access someone's internet. Thanks – good interesting day.
21	Let public know what is happening.
22	Keep the information simple so the public can understand in simple forms how smart CCTV and DPI works.
23	I would really like to know who watches the people that are watching us. And how long is all this in the data base.
24	Smart CCTV is a good improvement on CCTV, but must be properly regulated. DPI is a wonderful way of checking for potential crimes but the privacy of the individual is paramount.
25	Low level monitoring is acceptable but must have a cost associated. Is it cost effective? Very concerned about the future.
26	Good idea but it needs good monitoring to protect people, and good regulations.
27	Good idea but needs careful monitoring at all times.
28	Happy holidays!
29	Wish you were here! Weather is great, food good, company fantastic.
30	What I have learned today is that we are trying to make the world a better place and surveillance society will help.
31	Hello! ☺
32	The problem I have with CCTV and DPI is who has access to all my information where is it stored and how long for? Who accounts for it all?
33	DO not like the fact that I am being monitoring constantly without my consent.
34	I would like to add that intrusion of privacy in DPI is unacceptable, records of personal details should not be kept.
35	Keep the public more aware that all our information is kept and we don't know where or who uses the information.
36	To keep the data secure. No selling of information, no call centre type users looking at the data.
37	I have found today's event very enjoyable and informative. And it was a pleasure to meet some of your colleagues.
38	Keep the public more informed on what is going on.
39	I feel more transparency needs to be given to CCTV and DPI as the information been collected could be used for many purposes and not for what is intended. Many people are not aware of DPI and should be as it is an infringement of people's rights and liberty.
40	Security agencies which use DPI are trustworthy – strongly agree. Surveillance privacy and security – trustworthy and to comply by law; CCTV technology for security purpose spotting crime and identifying suspicious behaviour, strongly agree.
41	More regulation and control information only to be used by law enforcement agency.

42	More legislation for DPI; regulations for companies on gaining personal information. Permissions for data to be used.
43	Let us know if our data is going to be given to third parties, ask for our permission first. Create a law/legislation that protects our personal information from being used without us being informed.
44	DPI should only be used for stopping of virus and spam mail. There are other methods of catching criminals such as paedophiles, phishing sites etc. This prevents the used of DPI unnecessarily and violation of privacy.
45	Legislation should be put in place so that the innocent people of the world can't have their data, email etc. However ex criminals, people on trial etc. can have their data/messages checked based on security purposes. Normal innocent people's emails/data does not need to be checked. Violation of privacy and trust.
46	Do not overestimate the capabilities of a computer system (you can't program human judgement). As good as the idea is and as much as I support it, the mind of a man/woman cannot be put into a hard drive.
47	I feel that the new technology is a great idea if it is used correctly and for what it is intended for. Technology should not be the only resource though. The community spirit needs to be rekindled. If people look out for each other we will feel a greater sense of security knowing somebody is watching out for us. Being back community centres and neighbourhood activities to bring communities back together again. A sense of awareness of what is going on around us.
48	Concerned at where the security level starts and finished i.e. national. Europe and at what level of crime i.e. terrorism or vehicle crime.
49	Not enough chocolate on the profiteroles!

Postcards – content 2nd summit

15th March 2014	
No	**Content**
50	More targeted use of DPI for security purposes supported by transparent open regulations and consistent monitoring of data usage (including criminal activity).
51	Who watches the watchers?
52	DPI – already in use but is being abused i.e. so much unwanted spam etc. Very strict controls should be put in place which can't be beyond the capabilities of technology.
53	Smart CCTV – consensus on our table that next generation will be more accepting of surveillance. Currently we are at a crossroads in advancing technology.
54	NO security services should be outsourced to private (profitmaking) companies.
55	The sample of people surveyed today did not reflect the true background of our nation. There were a lack of people from ethnic backgrounds. DPI is too intrusive! When surveying people more information should be given to get better responses.
56	There should be some way that DPI and government do not misuse the data they obtain. I would like more clarification on what is being viewed and shared. World wide laws or agreement for clarification is needed. More important it the penalty/punishment that is given. I strongly believe the death penalty should be reinstated – this will do more prevention than any surveillance.
57	The annual average salary is £26,500. I would like to ask why I know no-one who is on this average annual salary. Prices have gone up but salaries never seem to increase, Also don't like the privacy of smart CCTV and online DPI but definitely agree that these should be used in public areas for crime etc.
58	Who decides what is classed as 'normal' behaviour for the auto behaviour recognition due to people having learning disabilities etc. tat may not seem 'normal' or do 'normal things'.
59	New data police to be enforced and accessible to the public.
60	The last question of all should have included an additional option as an answer: being more aware has made me even more cynical!

61	Even with a continually developing security system I don't want it to replace the human element. Police officers should not be replaced by smart CCTV.
62	No Smart CCTV in residential areas! This is too intrusive. But excellent in public areas.
63	DPI – the most important thing to me is honesty and transparency.
64	I used a PC at 10 – 11 years old. Children these days use it at 3 – 4 years old… protection and security is key for our children to stay safe. They are naïve.
65	I have no problems with smart CCTV but the use of it, the running costs, the legitimacy and the effectiveness of it needs to be carefully monitored. And the watchers made accountable.
66	DPI I have never heard of. But it does make sense when national security is involved. But once again it is all about control and usage. Simple answer is don't discuss sensitive subjects on the net!
67	To put people's worries at ease about the process, I think it's important to have some control over when whoever is in control of the footage can access the footage itself. For example, you may only have access to footage from a certain camera if someone's behaviour has been flagged, so you can't abuse the technology and just look at any footage on any camera, Bruce K 07923 829180 I would love a job with you!
68	When thinking about these proposals consider Crimea. Would you rather be watched as a Ukrainian or a Russian? Who controls these systems? Are the only fit for a true democracy?
69	I am against Smart CCTV, DPI. However I can see the need regarding terrorists/national security. I would be highly suspicious of usage and sharing information with 3rd parties. This area to me is of great concern.
70	Smart CCTV should not replace police presence on our streets. Use of CCTV should not only be used for capturing terrorist activity but be used to monitor other criminals such as known rapists, paedophiles etc.
71	DO not let CCTV get too advanced so that we end of 1984, big brother watching you!
72	To fully consider the implications of Smart CCTV for individuals/groups of people/rights of the individual - Ensure effective policing of information gathered and who it is shared with - Appropriate consultation - Skills of the interpreters – what is and who determines 'normal' behaviour - Is it cost effective? - Publish data highlighting the pros/cons - Use it to enhance the human factor not replace - All in all 'let's keep it'
73	With most internet traffic passing through USA we in Europe have little control over DPI. Court order to put an individual under suspicion. Can we get the Kinnock family out of European Politics!
74	DPI – data protection? Health care workers emailing each other! Patient confidentiality at risk. Who's looking at the emailing. Is confidentiality being breached?
75	Smart CCTV – there are no rights without responsibility. Privacy is a privilege not a right. Using computer models takes operator error and prejudice out of the equation. Vulnerable people i.e. disabled, mentally ill can be identified through their behaviour and therefore protected. The technology can be targeted to areas e.g. football matches/airports/ethnic groups where trouble is more likely to start.
76	DPI Feels really uncomfortable subject. Data protection –effective in some areas i.e. illegal activity. Very intrusive if used in all email, web browsing etc. Who 'owns' this DPI behaviour. Are the general public aware of DPI and how it's used?
77	Smart CCTV – laws and regulations must be continually assessed as technology moves on. DPI supports national security and tracking of international criminals worldwide The price of quick communication and access to almost unlimited information is constant surveillance Terrorism, paedophiles, trolls, suicide sites, all need close supervision Do not tell the general public too much as criminals find out and try to circumnavigate the checks

78	Smart CCTV – must be used correctly. Reacted upon. Data protection respected. Not mis-interpreted. Accepted by all groups. Ends justifying the means. Must be cost effective. DPI – who has control over the system. Need to stay ahead of those who abuse the system. Data protection respected. Used with prior intelligence, not carte blanche.
79	DPI – open to manipulation? Who is funding this and who is the information sold to? This is a deep intrusion to privacy when targeting a whole population How do you discriminate genuine errors from intentional use?
80	Smart CCTV. Install it everywhere and if you are doing nothing wrong you have nothing to worry about!
81	IN total agreement with Smart CCTV bit concerned about DPI. Where will it stop?
82	Smart CCTV should only be used in areas of high public usage e.g. airports, train stations etc. as a measure of national security.
83	I hope smart CCTV helps prevent and solve crime in the future. DPI seems like a complete invasion of privacy.
84	If you have nothing to hide both DPI and smart CCTV aren't a problem. Very good ideas in fact… increases security and safety
85	DPI – would like to know who or what controls it. CCTV in placed into rural areas, parks – more quiet places!
86	Scrap Deep Packet Inspection!
87	If you have nothing to hide, why not? Need more info, should be open book policy.
88	I don't think I fully understand the ins and outs of DPI and I feel that even if I spent a whole day researching about it I would still be just as confused as I am now. I do think DPI could be useful but there needs to be more rules and regulations put into place to control who can get hold of this information.
89	I think the use of DPI is far too intrusive into personal emails etc. also bank details etc. It could be useful for targeting terrorists, child pornography etc.
90	The laws controlling surrounding DPI need to be strengthened. DPI is used by criminal organisations to trade on individual personal details etc.
91	DPI is a hugely complex area that many people (the majority) will struggle to fully understand. Therefore, clear laws have to be made around how it will be used.
92	DPI. This is currently being used for the benefit of government and security agencies. Citizens suffer ID fraud, spam mail etc. on a daily basis but are not defended by DPI. The use/benefit from it is derived by government etc. to fulfil your own agenda. This needs to be changed. If everyone does not benefit on a daily basis the premise of DPI must be challenged and changed.
93	What qualifications and security checks to CCTV operators have?
94	DPI is a very intrusive procedure. May be using your information when you don't know.
95	We need more public awareness about things like smart CCTV and DPI. Before coming along to this event I knew nothing about what the entailed and how much my privacy has been affected by them. Everyone should be aware of this.
96	The British government should be more strict in controlling who accesses the info. They should not be dictated by other countries i.e. united states. Law should be passed that controls the accessibility to information