UK Citizen Summits | 1 and 15 March 2014

Report for participants

surprise

surveillance
privacy
security

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

Introduction

It seems a long time since we ran our citizen summits in the Crowne Plaza Hotel, Birmingham on the 1 and 15 March 2014. Thanks again for your participation and enthusiasm. Since then, we have waited for the results to come in from the other citizen summits held across Europe, and we have been diligently number crunching to find out how everyone responded. We have now finalised the British results and, as you showed an interest in hearing more about what we found, this short report summarises the main findings. The British results have also been handed in to the European Commission and are available for all to view at www.surprise-project.eu

First of all, the good news (for us) was that you seemed to enjoy yourselves at the summit. 90% of you considered the event to be insightful and enriching. 70% of you believed the insights you generated would be useful for policymakers.

You also told us that you had learned something new. This is what the OU is all about! 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%.

Here are some of the things you told us about SOSTs, Surveillance, Security and Privacy:

> You would like more information to be made available about the benefits and risks of surveillance-orientated security technologies (SOSTs).

> Overall, you supported the use of SOSTs for national security purposes. However, you said that you had greater concerns about DPI than smart CCTV. We think that this is because the British public are familiar with the presence of CCTV as opposed to DPI. DPI also presents greater communications privacy concerns.

> You said that you would prefer surveillance data to be retained within the UK, rather than being shared with other countries.

> You were concerned about who might see data collected using SOSTs and who might try to exploit or profit from it.

> You suggested that only the security and law enforcement agencies (and possibly some areas of government) should be involved in using SOSTs and handling the information they produce.

> You had a general mistrust of private sector organisations' involvement in national security matters and concern about how security agencies would abuse their power when using SOSTs.

> You called for greater regulation, legislation and oversight of the use of SOSTs.

> You were not particularly prepared to resist the use of SOSTs.

> You were are more concerned about how SOSTs may affect you personally, rather than the wider community.

> By the end of the summit, you had much greater privacy concerns than at the beginning. Concern for privacy of the general public rose from 46% to 65%; while concerns for your personal privacy rose from 35% to 69%.

> You were not willing to trade off your privacy for better security, you wanted both privacy and security.

The vital statistics: views on security and privacy

Secure or not?

- 57% of you considered Britain to be a safe country and 80% of you feel safe in your daily life.
- But 75% of you worry about security when you are on line.
- 90% of you thought that the use of SOSTs improves national security.
- 80% of you support the idea that governments should use SOSTs for national security purposes.

But you expressed major privacy concerns:

- 76% of you are afraid that too much information is collected about you.
- 74% of you were concerned that your personal data are inaccurate.
- 96% of you worried that your information was shared without your permission.
- 68% of you were worried that it would be used against you.
- 55% of you were worried that once SOSTs were in place, they were likely to be abused.

Some of you suggested that technology should only be part of the solution to security problems, and that other, non-technological solutions were available. This person expressed their opinion on a postcard:

> "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 was important:

> "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. Bring 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

What you said about the SOSTs

You had very different views on the acceptability of Smart CCTV and DPI

- 88% of you supported the use of Smart CCTV for security purposes.
- 56% of you supported the use of DPI for security purposes.

This difference in opinion might partly be to do with the fact that DPI is a comparatively less well known technology when compared to Smart CCTV. In general, you knew more about Smart CCTV than you did about DPI. In spite of 88% of you regularly using the internet only 31% of you knew about DPI. And although only 28% of you regularly came into contact with CCTV cameras, nearly half (43%) of you knew what smart CCTV is.

When we explored your views in more depth, however, there were significant concerns about the intrusiveness of DPI when compared to Smart CCTV. The following participant sums up some views on the SOSTs we explored:

> **"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

More than half of you had concerns about both Smart CCTV and DPI, even if you were not specifically targeted. 58% of you were bothered by smart CCTV and 63% of you were bothered by DPI even if they only targeted criminals rather than the general public.

DPI also presented greater worries for the future. 81% of you were worried about how DPI would develop in future but only 53% of you were concerned about how Smart CCTV would develop.

You also expressed a lack of trust in the institutions which ran both Smart CCTV and DPI. We asked a number of questions about trust in the summit. First we asked if you thought institutions were trustworthy overall. Then we asked whether you thought they were competent, had the best interests of citizens at heart, and whether they were likely to abuse their power. The results were very similar in the case of both SOSTs. In particular, you were concerned about abuses of power in relation to SOSTs:

- Regarding overall trustworthiness: only 29% of you think that agencies using Smart CCTV and 30% of you think that agencies using DPI are trustworthy.
- Regarding competence: only 31% of you think that agencies using Smart CCTV and 29% of you think that agencies using DPI are competent.
- Regarding citizens' interests: 46% of you agreed that agencies using Smart CCTV and 41% agreed that agencies using DPI have the welfare of citizens' at heart.
- Regarding abuses of power: only 16% of you in relation to Smart CCTV and only 12% of you in relation to DPI thought that agencies wouldn't abuse their power.

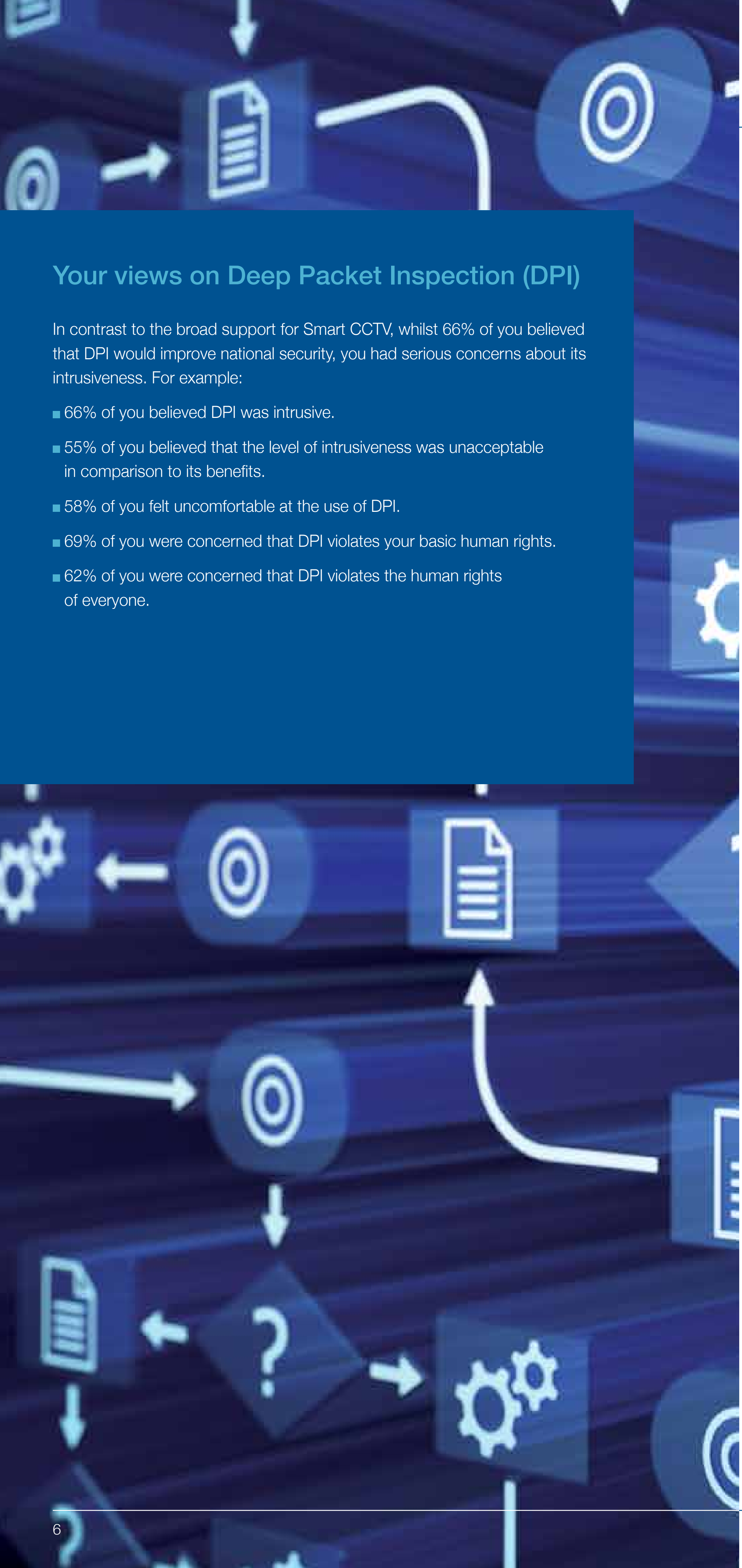
Your views on Smart CCTV

Generally you were supportive of the use of Smart CCTV. Britain is a country in which CCTV is commonplace, so it didn't surprise us that the idea of Smart CCTV was so widely accepted and supported.

- 77% of you agreed that Smart CCTV is an effective security tool.
- 80% of you thought that it actually improved national security.
- 68% of you thought the level of intrusiveness was acceptable given its benefits.
- 63% felt more secure when CCTV is being used.

However your degree of comfort with this SOST varied and there were some negative views expressed. For example:

- Only 36% of you considered that laws governing smart CCTV were effective.
- 45% of you believed that the technology is forced on you without your permission.
- 1 in 5 of you (21%) indicated that the use of smart CCTV actually made you feel uncomfortable.
- 37% of you were worried about it violating your basic human rights. A slightly smaller number (30%) were worried about the potential for Smart CCTV to violate everyone's human rights.



Your views on Deep Packet Inspection (DPI)

In contrast to the broad support for Smart CCTV, whilst 66% of you believed that DPI would improve national security, you had serious concerns about its intrusiveness. For example:

- 66% of you believed DPI was intrusive.
- 55% of you believed that the level of intrusiveness was unacceptable in comparison to its benefits.
- 58% of you felt uncomfortable at the use of DPI.
- 69% of you were concerned that DPI violates your basic human rights.
- 62% of you were concerned that DPI violates the human rights of everyone.

There was widespread scepticism about the ability of the laws and regulations to guard against the misuse of DPI with 78% believing that the law did not prevent its misuse. 84% of you were deeply uneasy that DPI was being used without your permission and that it can be used to monitor everyone. We received some strong views on DPI in the postcards. Here are some examples:

> “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 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 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

> “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

> “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

Recommendations for policymakers

You made a range of suggestions to policymakers, which we grouped under the following six headings:

Transparency and communication

You made several recommendations in relation transparency and the need for better communication about the use of SOSTs, as follows:

- 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 the data gathered by SOSTs is held and used.
- In the interests of transparency, citizens should have access to information that the security services and others hold about them.

One table group reported:

> "The majority of people are unaware of the depth of intrusiveness that occurs."

Another questioned:

> "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"

Responsibility for regulating and implementing SOSTs

Many of you expressed strong views about the institutions which were responsible for operating SOSTs, and wanted to know who exactly it was who watches the watchers. You recommendations were that:

- 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.

By way of illustration, one table group commented:

> "Form a publicly elected independent either national or worldwide body who monitors 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."

Evidence about the effectiveness of SOSTs

You also wanted to know more about the costs and benefits of SOSTs. You felt that information about their effectiveness at fighting crime and terror should be made available. In light of these concerns, the following policy recommendations were made:

- 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.

A table group commented:

> "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

A number of policy recommendations were made specifically in relation to 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 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.

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

DPI

In relation to DPI you recognised its importance for national security and to prevent and detect crimes such as child pornography. 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."

However you also had major concerns about its intrusiveness, whether the information gathered would be shared with unauthorised third parties or would fall into the wrong hands.

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 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.

Increase non-technological solutions to security

You made two recommendations for policy makers associated with 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.

Some conclusions

We can't emphasise enough how thrilled we were when we held the events in March. Having spent the majority of time in the last two years designing, writing and producing the questionnaire, films and magazine, they were a huge achievement for us. We were moved by the way in which you engaged with the issues we presented.

By the time we reached the end of the summit, it seems that there was still broad support for the use of SOSTs. However we felt that the summits had prompted you to consider privacy issues more closely. This was partly reflected in the recommendations you made which concerned calls for greater transparency, more effective regulation, a limitation of SOST-use to 'trusted partners' rather than its widespread use. It was also reflected in the 'before and after' measurements we made of your views about privacy, surveillance and security. You were keen to learn more about the issues and wanted to be better informed all round and your calls for greater democratic scrutiny of the watchers were well judged and well made. In contrast to some high level governmental and policy figures encouraging people to 'give up a little privacy for greater security' it appears that you were not prepared to do that. You demanded both enhanced security and enhanced privacy following your participation in the summits.

Thanks once again,

Professor Kirstie Ball, Sara Degli Esposti, Professor Sally Dibb

surprise

surveillance
privacy
security

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