Internet Surveillance after Snowden: A Critical Empirical Study of Computer Experts' Attitudes on Commercial and State Surveillance of the Internet and Social Media post-Edward Snowden

Fuchs, Christian and Trottier, D.

The final, published version in Journal of Information, Communication & Ethics in Society, 15 (4), pp. 412-444, 2016 is available at:

https://dx.doi.org/10.1108/JICES-01-2016-0004

Emerald Journal of Information, Communication and Ethics in Society

Internet Surveillance after Snowden: A Critical Empirical Study of Computer Experts' Attitudes on Commercial and State Surveillance of the Internet and Social Media post-Edward Snowden

Journal:	*Journal of Information, Communication & Ethics in Society*
Manuscript ID	JICES-01-2016-0004.R1
Manuscript Type:	Journal Paper
Keywords:	Edward Snowden, social media, Surveillance, Internet, Privacy, data protection

1. Introduction

Surveillance is an inherent feature of modern society: It involves activities of state institutions such as secret services and the police that monitor criminals, political activists, enemies of the state, as well as companies that track workers, customers, and competitors (Ball, Haggerty and Lyon 2012; Fuchs 2011, 2013a; Lyon 2007). Surveillance's purpose is not only to collect data, but also to use this data to exert social control. The rise of consumer culture and computing have in the 20th century brought about some qualitative changes of surveillance so that it has become more networked, ubiquitous, focused on everyday life and consumption, and organised in real time.

In June 2013, Edward Snowden revealed with the help of *The Guardian* the existence of large-scale Internet and communications surveillance systems such as Prism, XKeyscore, and Tempora. According to the leaked documents, the National Security Agency (NSA) in the PRISM programme obtained direct access to user data from seven online/ICT companies: AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, Yahoo![1]. The Powerpoint slides that Edward Snowden leaked refer to data collection "directly from the servers of these U.S. Service Providers"[2]. Snowden also revealed the existence of a surveillance system called XKeyScore that the NSA can use for reading e-mails, tracking web browsing and users' browsing histories, monitoring social media activity, online searches, online chat, phone calls, and online contact networks, and follow the screens of individual computers. According to the leaked documents, XKeyScore can search both meta- and content-data[3].

The documents that Snowden leaked also showed that the Government Communications Headquarter (GCHQ), a British intelligence agency, monitored and collected communication phone and Internet data from fibre optic cables and shared such data with the NSA[4]. According to the leak, the GCHQ for examples stores phone calls, e-mails, Facebook postings, and the history users' website access for up to 30 days and analyses these data[5]. Further documents indicated that in co-ordination with the GCHQ, also intelligence services in Germany (Bundesnachrichtendienst BND), France (Direction Générale de la Sécurité Extérieure DGSE), Spain (Centro Nacional de Inteligencia, CNI), and Sweden (Försvarets radioanstalt FRA) developed similar capacities[6].

---

[1] NSA Prism program taps in to user data of Apple, Google and others. *The Guardian Online.* June 7, 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[2] Ibid.

[3] XKeyscore: NSA tool collects "nearly everything a user does on the internet'. *The Guardian Online.* July 31, 2013. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[4] GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian Online.* June 21, 2013. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?guni=Article:in%20body%20link

[5] Ibid.

[6] GCHQ and European spy agencies worked together on mass surveillance. The Guardian Online. November 1, 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

The study presented in this paper is set in a British context. Snowden's revelations were first published in the British broadsheet newspaper *The Guardian* and therefore received high public attention in this country, which makes a study conducted in a UK context particularly relevant. As in many other countries, Britain has also experienced intensification and extension of surveillance after 9/11. This development has been based on governments' assumption that an augmented and expanded use of surveillance technologies can detect and prevent terrorism.

The Regulation of Investigatory Powers Act 2000 extended government bodies' capacity to monitor society, buildings, vehicles, telephone communication, Internet communication and postal communications. After 9/11, this Act was amended multiple times in order to extend surveillance power. The Prevention of Terrorism Act 2005 introduced the possibility of control orders that can ban citizens suspected of terrorist activities from undertaking certain activities or can put them under constant surveillance. After the London bombings that took place on July 7, 2006, the Terrorism Act 2006 was introduced. It enabled the police to detain suspected terrorists for up to 28 days without raising criminal charges. The EU Data Retention Directive mandated that communications corporations store all meta-data of communications for at least six month and a maximum of 24 months. After the European Court of Justice had found that this Directive violated the right to privacy, the UK Parliament passed the Data Retention and Investigatory Powers Act 2014 in order to keep up data retention in the UK. In November 2015, the Draft Investigatory Powers Bill was published. It aims at extending the government capacities for targeted and mass surveillance of communications.

What is the British public's opinion towards Snowden's revelations? A survey conducted by Angus Reid Global in 2013 showed that 60% of the 2,000 British respondents thought that Edward Snowden was a hero. They argued that he should be commended for letting the public know that governments are running electronic surveillance programmes that threaten people's privacy[7]. 64% said they did not trust the British government to be a good guardian of citizens' personal information. In a 2014 survey, the polling company Ipsos Mori found that 85% of the 1,958 British respondents said that it was essential or important that their Internet browsing behaviour remains private[8]. A YouGov poll[9] conducted in 2015 showed that 72% of the respondents familiar with the Snowden revelations distrusted that the police responsibly deals with data it gathers from the Internet. 51% distrusted intelligence services and 69% the Home Office and ministries.

Various scholars have worked on the critical analysis of Internet and social media surveillance (Andrejevic 2007, Andrejevic 2013; Fuchs, Boersma, Albrechtslund and Sandoval 2012; Fuchs and Trottier 2013, Mathiesen 2013, Trottier 2012, Trottier 2014, Trottier and Fuchs 2014). Given the intensification and extension of surveillance and law and order-politics after 9/11 (Ball and Webster 2003, Chomsky 2011, Lyon 2003, Mathiesen 2013, Rockmore 2011), Snowden's revelations did not

[7] More Canadians & Britons view Edward Snowden as "hero" than "traitor", Americans split. *AngusReidGlobal.* October 30, 2013. http://www.angusreidglobal.com/polls/48837/more-canadians-britons-view-edward-snowden-as-hero-than-traitor-americans-split/

[8] One year after Snowden drops NSA bomb, UK citizens demand more privacy. *RT Online.* May 30, 2014. http://rt.com/news/162496-nsa-gchq-snowden-internet/

[9] https://yougov.co.uk/news/2015/08/21/peering-through-prism-authorities-should-always-ob/

come as a surprise. Secret services' Internet monitoring uses forms of Deep Packet Inspection surveillance that have existed before Snowden's revelations (Fuchs 2013b). What came however as a surprise for many is the extent and dimension Internet surveillance has taken on. We can therefore without a doubt assert that 21st century information society is not just a capitalist society, but also a mass surveillance society.

The task of this paper is to study how data and computer professionals think about commercial and state surveillance of the Internet and social media in the age of Edward Snowden. It reports the findings of focus group research that was conducted in London in 2014, a year after Snowden's revelations. It is of particular interest to interrogate how data and computer experts think about Snowden and surveillance because they are the type of professionals who best understand how digital surveillance works technologically. They are themselves frequently confronted with issues concerning the processing of personal data, privacy and data protection.

Section 2 briefly discusses literature about surveillance after Snowden. Section 3 explains the study's empirical methodology. Section 4 presents the main findings. Section 5 provides an overall interpretation and draws conclusions.

2. Surveillance after Snowden

The Snowden revelations have become an important topic in the study of public opinion, privacy and surveillance, Internet communication, journalism and the public sphere.

First, there have been studies concerned with public opinion. Bakir, Cable, Dencik, Hintz and McStay (2015) report the findings of several empirical studies attitudes on surveillance after Snowden in Britain and the EU: In the UK and the EU, there are especially concerns about deep packet inspection (DPI) Internet surveillance (compare Fuchs 2013b for a critical analysis of DPI Internet surveillance). In the UK, especially younger people and ethnic minorities are concerned about state surveillance. All age groups, but especially citizens older than 55, are concerned about commercial surveillance.

Based on a Pew survey of attitudes towards surveillance in the USA, researchers in China, Germany, Japan, Mexico, New Zealand, Spain, Sweden and Taiwan conducted similar quantitative surveys and compared the results. In the US survey, 45% of the respondents said in 2014 that Snowden's revelations served the public good, whereas 43% said they caused harm. 56% said that the US government should prosecute Snowden[10]. Adams, Murata, Fukuta, Orito and Palma (2015) conducted an international comparison of the results. With the exception of Japan, a very clear overall majority of respondents in the other countries agrees that Snowden's revelation serve the public good. In Japan, the degree of agreement to questions about whether the respondents would emulate Snowden's actions was lowest. Agreement was in contrast very high in Spain, Mexico, and New Zealand.

Second, there have been analyses that focus on the Snowden revelations from the

[10] http://www.people-press.org/2014/01/20/obamas-nsa-speech-has-little-impact-on-skeptical-public/

perspective of privacy and surveillance. David Lyon (2015a) has published the book *Surveillance after Snowden*, in which he argues that Snowed revealed how "[b]ig government and big business" (Lyon 2015a, 13) together carry out mass Internet surveillance. The revelations also show that secret services co-operate internationally in data exchange and surveillance, as for example the five eyes partnership of secret services in the USA, the UK, Australia, Canada and New Zealand shows (Lyon 2015a, 8). Fuchs (2015b) argues that Snowden's revelations further support the conclusion that concepts of participatory and democratic surveillance are mistaken. In the post-Snowden era, it would be clear that we need a critical theory of surveillance.

David Murakami Wood and Steve Wright (2015) edited a special issue of the journal *Surveillance & Society* on the theme "Surveillance and Security Intelligence after Snowden": Garrido (2015) argues that a focus on the global political economy of surveillance is necessary after Snowden. van der Velden (2015) classifies the surveillance technologies used by the NSA and other secret services as devices that leak data and devices that are inserted into networks for collecting data. Keiber (2015) says that the Snowden revelations display the US hegemony in surveillance. Schulze (2015) with the example of the German government argues that the Snowden case shows that denial, the delegation of responsibility, rationalisation, authorisation, singularity, and securitisation are ideological strategies that governments use for legitimatising surveillance. As Murakami Wood and Wright indicate, these revelations point to only the most recent attempt by several governments to "attack the basis of what makes the Internet creative and free, in the name of all kinds of 'risks' (mainly terrorism, identity crime, intellectual property crime and paedophilia)" (2015, 135).

Third, there have been analyses of the Snowden revelations that stress the dimension of Internet communication. Lyon (2015b) argues that post-Snowden, the Internet and big data should be key focuses in the analysis of surveillance. He writes that "the Snowden revelations raise as a key issue the future of the internet" (Lyon 2015b, 147). Vincent Mosco (2014, 7) argues that the Snowden revelations show the rise of a military information complex that "promotes the power of a handful of companies and the expansion of the surveillance state". Fuchs (2015b) makes the point that Snowden's revelations show the existence of a surveillance-industrial Internet complex, in which capitalist and state interests partly converge. "In the surveillance-industrial complex, the world's most powerful state institutions have collaborated with the world's most powerful communications companies to implement totalitarian surveillance systems" (Fuchs 2015b, 8). Lyon (2014) argues that Snowden has shown the existence of a form of big data surveillance in which state and corporate agents play a role. Hintz (2014) says that the Snowden affair has demonstrated the crucial role that social media corporations play in policing the Internet.

Fourth, there have been studies that focus on the Snowden revelations from the perspectives of journalism and the public sphere. Glenn Greenwald (2014), one of the journalists who covered the Snowden revelations in *The Guardian*, wrote the book *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. He argues for example that the Snowden affair shows that the purpose of whistle-blowing, activism and engaged political journalism is to promote "the human capacity to reason and make decisions" (Greenwald 2014, 253).

Scherman (2014) argues that Snowden's revelations show the relevance of civil disobedience today. Chadwick and Collister (2014) analyse the role of *The Guardian* as news organisation in the Snowden revelations. Qin (2015) shows that mainstream news media tend to frame Snowden as traitor and social media users as hero. Petley argues that the fact that the conservative press in Britain argued for prosecuting *The Guardian* shows that these media are not watchdogs, but part of the Establishment. Branum and Charteris-Black's (2015) discourse analysis of how the British press reported the Snowden affair confirms Qin's result. In respect to the role of the public in responding to Snowden's revelations, research has also given attention to aspects of activism (Bauman et al. 2014, Haunss 2014).

3. Empirical Research Methodology

The research presented in this paper was conducted as part of a European Union project, in which one of our tasks was to study how experts assess privacy and surveillance. Our specific case study focused on Internet and social media surveillance. We chose to conduct focus groups (for a methodological overview, see: Bryman 2012, chapter 21) with data and computer experts in London. Internet surveillance has been intensively discussed in the British public after Snowden revealed the role of GCHQ in mass surveillance. Some people consider London the world capital of surveillance due to its extensity of CCTV[11]. The Silicon Roundabout in East London has made the city an important hub for the computer and Internet industry in Europe. Likewise, Google's decision to build its £1 billion, 2.4 acre headquarters in Central London ensures that the city retains this status[12]. London is therefore particularly suited as the location for a case study on digital surveillance after Snowden.

We first developed a focus group guide that gave special significance to three topics: ethics and societal impacts of Internet surveillance, Internet surveillance in the light of Edward Snowden's revelations, and political responses to contemporary digital surveillance. The logic of choosing these three major topics was that we first wanted to know how computer professionals think about commercial and state surveillance in general independent of Snowden. Second, based on this general discussion, we wanted to engage the participants in conversations about the implications of Snowden's revelations. And third, given that we took a critical research approach, the question arose what could be done politically against mass surveillance. The focus group guide is documented in the appendix to this paper.

A pre-test was conducted in early August 2014 with two computer science experts. It resulted in some improvements of the focus group guide.

We invited digital data and computer experts to two focus groups that were conducted on September 8 and 9, 2014, at the University of Westminster in Central London. We defined "digital data and computer experts" as individuals whose working lives involve a significant amount of processing of personal data in digital form. Digital data experts are either people working in the computer and Internet industry as

[11] See for example: http://www.youtube.com/watch?v=OOIfzj5k8HA
[12] http://www.theguardian.com/technology/2013/jan/17/google-uk-headquarters-kings-cross

developers, managers, consultants, or technology officers or researchers who have studied computing and/or the Internet.

For sampling, we developed a list of 200 Internet and IT businesses that are headquartered in London. We searched for contact e-mails and phone numbers, contacted these businesses, and asked if we could get in touch with computer professionals working for them in the areas of privacy, data protection and security. In addition, we identified 20 mailing lists to which computer scientists, computer experts, and computer professionals are subscribed. This way of establishing contacts ensured that we only reach computer experts as potential participants. Sampling took place from the middle until the end of August 2014 by e-mail and telephone. The contacting and sampling process was continued until we had found 16 participants who volunteered, that is 8 for each focus group. We expected that some of those who agreed to participate would have to drop out in the last minute. Therefore we recruited more participants than required. Some participants indeed had to drop out, resulting in 5 participants in each of the two focus groups, which was our target size. Out of the 10 participants, four were digital data researchers and six worked in the digital data industry. Four women and six men participated.

Participants were asked to sign an informed consent form, by which they agreed that we recorded the focus groups and quoted from them in publications. We have anonymised all participants' names and institutional affiliations for this report. Table 1 provides a general overview of the focus group participants as well as their IDs (e.g. P1) that we use in the analysis.

Identification number	**Profession**	**Organisation, organisation type**
P1	Computer ethics expert	University
P2	Computer science student	University
P3	Chief operations officer	Company that is a global provider of Internet, voice and video services
P4	Founder of a wireless community project	Wireless community project
P5	Consultant on privacy, data control and security; researcher	Non-profit initiative
P6	Founder of an ICT consultancy	Company that provides business IT services
P7	PhD student in Internet studies	University
P8	User experience consultant	Single-person company
P9	Social scientist, who has been involved in research about social media	Research institution
P10	Chief Technology Officer	Company that provides online advertising solutions

Table 1: An overview of the participants in the 2 focus groups

Both focus groups lasted around 2.5 hours, which resulted in a corpus material of 5 hours as input for the analysis. We partially transcribed the data based on the audio- and video-recordings. The resulting data was used as input for a text analysis. We

conducted this analysis with the help of topical coding, a qualitative method of data analysis, in which each category represents an important theme in the material (Bryman 2012, 578-581). Thematic coding structures and in turn facilitates thematic analysis. As participants are considered experts and have different backgrounds and professional duties, we opted to present findings on an individual basis, rather than collapse them into quantified statements. As much as possible, we present key findings in the words of these experts.

The participants were asked to fill out a quantitative feedback questionnaire at the end of the focus group. On average, the participants considered themselves to have relatively high knowledge about privacy and data protection (mean=4.1, scale: 1=I do not have much knowledge of privacy and data protection issues … 5=I consider myself a privacy and data protection expert), which confirms that we had indeed invited computer and data experts.

4. Internet Surveillance in the Age of Edward Snowden: The Results of 2 Focus Groups

The focus groups had *three major topics:*
1) Privacy and surveillance in online advertising and the information economy as a case example for surveillance in general and ethical and societal dimensions of the Internet;
2) Edward Snowden's revelations about state surveillance of the Internet;
3) Political responses to mass Internet surveillance.

The reason for the focus on both commercial and political surveillance is that Snowden's revelations uncovered that in mass Internet surveillance major transnational companies such as Facebook and Google, for whom targeted online advertising is an important business mechanism, collaborate with secret services, which calls forth the question of what political responses are feasible. Snowden's new revelation is the existence of a surveillance-political-industrial Internet complex, in which big data business and big state institutions collaborate.

4.1. Corporate Surveillance in Social Media Advertising

The participants identified and discussed three issues that in their view were of particular concern for understanding the ethics of online advertising:
1) The contradiction of economic interests and the protection of employees, customers, and users' data.
2) Ideologies and complexity in the context of explicit consent given to online companies' processing of personal data.
3) The distinction between opt-in to VS. opt-out from targeted advertising.

The *first issue* is that there is a lack of concern among companies and little technical knowledge among users. Participant 6 (P6), who is founder of an ICT consultancy firm, said for example: "Very few people actually have the technical competence to be fully aware of all the consequences what they do on their devices and how easy it is to pull it out". P3, who is chief operations officer in a global communications company, argues that there is a strong lack of data protection in companies: "Most SMEs don't have any way to deal with sensitive personal data. They don't have any

procedures in place. They don't have any technical ability to deal with it. […] They just lock the data up. Anything they might come across – they just store it. Probably unencrypted. […] Also now more in the cloud".

The same participant says that also in respect to data retention, there are often problematic practices. S/he mentions the example of HR records: "The minute you leave that job, your employer should destroy it. And nobody does it". P6 reports from experience with clients that those who are under the jurisdiction of data processing and protection acts, "ignore it completely". P6 also discusses the example of solicitors: "They got vast amounts of historical data. What they would really want to do is to have all of the historical data in a sort of internal Google where they can search for everything that is relevant. So when I tell them they really can't do that and I rant before them, they are very irritated. Until I point to the solicitors' Law Society, which also says they can't do it. And then they have to conform".

The participants agree in principle that data protection and privacy laws are very important. Some of them point out specific examples of how capitalist reality contradicts data protection because companies have a vast appetite for and economic interest in collecting, storing, analysing, and keeping data on employees and customers. The focus group contributions indicate that economic surveillance seems to be an inherent feature of capitalism that contradicts employee and consumer privacy. Although laws are in place, they according to the focus group participants are hardly enforced so that the state tends to mainly support capitalist interests and does not support consumer and employee privacy.

A *second issue* of discussion was explicit consent to the processing of personal data, especially sensitive data. The UK Data Protection Act (and similar regulations in all EU countries) regulates that users must give "explicit consent" to the processing of sensitive personal data that concerns racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health conditions, sexual life, alleged or committed criminal offences (Article 2, Schedule 3).

The research participants criticise the complex, vague, euphemistic, and ideological language often used in online platforms' privacy policies. P1, a computer ethics expert, refers to such practices as "cleverly worded things" that one has to read multiple times to grasp. P3 argues: "Most consent documents and end user licenses are so convoluted anyway. Did you actually ever read an end user license agreement? The whole thing?". P5, a privacy consultant and researcher, points out that if Google changes its privacy policy, it assumes users automatically consent. This participant holds the view that this is not a true form of consent: "There is no real consent. They [Google] are very weak on this side of the argument".

P3 argues that privacy policies and questions if one accepts changes of it, often use loaded and deceptive questions and language that compel users into agreeing: "'Do you want us to make your experience better by tracking you?' […] 99% will go: Of course I do because it makes my experience better. […] Or: 'Do you want to improve your search experience by enabling search history?' 'Do you want to improve your location access services?'". Such questions mask the intention of these services because they do "not tell you that they are going to track everything you do".

P2, a computer science student, points out that consent is often not real consent because the alternative to not agreeing is to not use the technology: "Sometimes we don't want any of our information to be stored, but we just have to click on 'yes'", otherwise the service cannot be used. P2 said about the language used in privacy policies: "It's really vague, so making it simple would really be good".

P5 points out the complexity of data processing and consent in networked computing systems such as the Internet: "How do you know what people consent to? What is explicit consent? […] The individuals need to be more in control of their sensitive data". Other participants add that the issue of consent and legal responsibility has been further complicated by the fact that companies and individuals increasingly store data in the cloud. They also stress that data's contexts change over time. P6: "Several of our clients are moving over to the cloud. […] Microsoft is now being sued by the American government so that the information that is stored in the EU[13], in Ireland, should be given by Microsoft, which is an American company, to the American government, without European consent. And my solicitors have started waking up to the issues here and were wondering what on earth to do about the Microsoft cloud because they got an awful lot of client data in it". This respondent concludes by stating that Microsoft Cloud users effectively "have no privacy". P4, who founded an open wireless community network, identifies data collection in various contexts as risks because "increasing amounts of dimensions of data are now stored on us".

Further complexity is added to the question if users consent to the processing of sensitive personal by the circumstance that meta-data can reveal a lot of personal data, including sensitive data. P7, a PhD student in Internet research, argues: "From a relatively small amount of data you can infer with very high accuracy most of these categories of sensitive personal data. And that may be done in a way that may not even personally identify people, but you might be able to categorise someone with such a high degree of accuracy. […] Sensitive data is then not collected in the first place, it is just inferred from statistical ones". P10, who is chief technology officer (CTO) in an online advertising company, talks about "the amount of data that we as individuals are transmitting […] just because we have mobile phones". He sees this data explosion as the most pressing issue because of the possibility for retrospective identification.

P4 provides an example of how meta-data can reveal a lot of sensitive personal data: "If you go to a mosque twice a day, and it is on GPS, at certain times of the days. Does that come under the religious believes and should be protected? How indirect does the information have to be to be sensitive personal data?". P1 adds another example of identifying people's religion or ethnicity based on CCTV footage.

P9, who is a social scientist in a research institution working a lot with personal data, argues that there is a difference between the way social scientists and online companies deal with data. The difference would be that social scientists first specify what data they collect and they ask for permission, whereas on the Internet "people just provide all sorts of data without being asked. And then that can be used and analysed and conclusions can be drawn from that. It's much harder to determine what

[13] See: http://www.cbc.ca/news/business/microsoft-and-other-tech-giants-fight-u-s-right-to-seize-cloud-data-1.2677688

makes that person identifiable and what information it is that makes them identifiable".

The participants generally feel that the way online companies obtain consent is often purely pseudo-consent, insufficient, and relying on deceptive and ideological language. They also have the overall impression that data protection laws do not reflect the complexity of online data processing caused by cloud computing, the global networking of data in the context of national data protection acts, meta-data, and changing contexts of personal data. As experts in this area, they are able to identify risks in current technologies based on professional experience as well as extrapolations from formerly unknown surveillance practices that Snowden and other whistle-blowers have revealed. Most participants' conclusion is, however, not that data protection is therefore outdated, but rather that it does not adequately protect users today and should be brought up-to-date.

A *third important discussion topic* was if there should be opt-in to or opt-out from targeted online advertising. It was the most controversially discussed issue in our focus groups.

Data protection experts and the advertising industry tend to hold different opinions on this issue: The Article 29 Working Party is a group of data protection commissioners and experts set up by the European Union. It publishes opinions and recommendations about privacy and data protection issues, including a 2010 report on online advertising[14]. Its view is that many users do not know about opting-out and that opt-out it does not amount to real consent because passivity of the user does not necessarily imply agreement. Active participation is therefore required for expressing agreement. The Article 29 Working Party concluded that ad network providers "should swiftly move away from opt-out mechanisms and create prior opt-in mechanisms" (23) and that mentioning "the practice of behavioural advertising in general terms and conditions and/or privacy policies can never suffice" (24).

The advertising industry tends to have a different, opposing opinion. So for example the European Advertising Standards Alliance and the Interactive Advertising Bureau argue that opt-in approaches are "disruptive for users"[15] and that such mechanisms "are not of comparable privacy value to users" and can have "severe negative economic impact on a legitimate business activity"[16] of advertisers. The ad industry prefers opt-out from targeted ads or no opt-in or opt-out at all.

P6, founder of an ICT consultancy who finds data protection issues to be of crucial importance, argues: "Opt-in. […] It has to be opt-in. Things ought to be set that they are by default secure. Otherwise you are making decisions for people. […] The default start has to be default secure. I don't think there is any other way it can be done if you are responsibly looking after people. Obviously, if the industry does not

[14] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171, Adopted on 22 June 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[15] http://www.iabeurope.eu/policy/oba-and-self-regulation/industry-offers-consumers-greater-transparency-and-control-o

[16] IAB Europe and EASA: Letter to Article 29 Working Party. January 17, 2012. http://www.iabeurope.eu/download_file/977/211

like that, it worries about its income. […] The default should be that one is opted out. That is my view". P7 supports P6's view: "For a certain category of settings there should always be opt-in because there are certain things that are categorically about security and categorically in the interest of the individual". This participant argues that there should be opt-out in some cases, where the basic functionality of an online platform would otherwise not be possible.

P8, who is a user experience consultant, also expresses some doubts about the privacy of targeted advertising, but adds that one has to think about how opting out effects user experience: "My gut feeling is that if I have to opt out of everything, there will be a lot of additional interaction". A problem would also be the complexity of explaining opt-in: "But how easy is it to explain what you are opting into? […] So it is the complexity of explaining to people what you are opting into and what could be done with it".

P10, who is the CTO of an online advertising company, supports P8's concerns about the convenience of usage: "The challenging part is how to convey that [opt-in information] in a way that is easy for consumers, for an end-user who has not an idea of what technology means, does not want to go through a hundred options or 200 options because they want something much easier but at the same time gives an amount of flexibility for advertisers to work with that user".

P10 adds that opt-in can have very negative impacts for companies: "They [representatives of the advertising industry in an example] mentioned about the immense economic impact that it would have on the Internet, the technology, not just the advertisers themselves, but the entire Internet. You need to think about what powers the Internet? […] It's advertising. Advertising makes it possible for all of us to consume services like Google Search. It allows us to connect to other people on Facebook. Facebook exists not because it is a benevolent entity of the connected people, it is doing that for advertising. It is the same thing with Twitter and e-mail. Why is it free for all of us? Why is information freely accessible as well?"

P7 responds to P10 and points out that the capitalist and targeted-ad model of the Internet is not the only possibility: "I agree that this is definitely how things work at the moment. But it would be a shame if every good that was produced in the economy would completely be holding to the current business model. We can imagine lots of different ways that all sorts of goods might be funded. And historically this is what has happened. […] So it would be a shame if we were to limit how run the Internet just based on its current most accepted model". P6 adds that in the earlier days of the Internet there was no advertising and things worked well. In referring to his experiences online in the late 1980s, he states that "[a]t that time there was no advertising on the Internet. We had perfectly working search engines and they all worked quite well. I agree this has changed completely. The difficulty is it is now being dominated by a group of American organisations who are in the capitalist part of the world dominant in every way. […] Many of the things around the ideas of privacy and what is not private, these are strictly Western hemisphere ideas".

P9 adds to the discussion the question how relevant ads are in the case of opt-in and opt-out: "And if I do opt out for Google to use those search terms wouldn't the adverts be just more random? Say I look for restaurants in London and I get constant

adverts from Pizza Express but I hate Pizza Express, that's a nuisance. But if I am opted out, then I might get results for restaurants in Swansea, which might be even less relevant to my sort of interest if I search the Internet". While non-targeted ads would be "less relevant", this statement also identifies targeted ads as largely ineffective as well as "a nuisance".

P10 argues: "Targeting advertising is the better option compared to non-targeted because if you get non-targeted advertising, an advertiser is wasting a lot of money because every time you show a person an ad, the advertiser incurs a cost". P6 strongly disagrees and argues that one has to see that capitalism is the context of advertising and that the question is in what kind of society we want to live in: "But what I don't want is to be targeted for adverts when I am not looking for products. And that is the default setting. […] It doesn't matter how much you turn off the search terms in your browser, your search history has been captured by Google, every detail of it is known and audited, and so forth. […] It seems to me the whole issue here is what's the relationship between capitalism and society. […] The defaults of society have to be to protect people. Otherwise, what's the point?"

This discussion is a very good example of discourses about advertising's advantages and disadvantages for individuals and society (see: Pardun 2014). A typical pro-advertising argument that could also be found in the focus groups is that advertising allows free and cheap access to culture, technology, and media and that without it, Internet, culture, and the media could not exist. Critics hold that such an argument confuses the dominant reality of the Internet and culture with how it could be different, i.e. the essence and potentials of the media world and its capitalist reality. Specifically, some of our focus group participants pointed out that there once was an Internet without advertising that worked and that there are non-advertising-based and non-commercial applications and platforms on the Internet. Some participants pointed out that opting into advertising might result in less convenience and a more difficult user experience. Further arguments in favour of targeted ads were that targeted ads would be more relevant than non-targeted ones and that opt-in would result in a waste of advertisers' money. The critics of online advertising pointed out that the issue at hand is a much larger one, having to do with capitalism and society and the question if we want to live in a society that is dominated by capitalism and advertising or if we shouldn't create alternatives to it and social spaces that are free from advertising and commodity logic.

The focus group participants' discussion showed nicely the range of diverse opinions and controversies about online advertising. The vast majority of people living in Western societies are confronted with different forms of advertisements every day. Advertising's ubiquity adds to the fact that discussions about its pros and cons tend to be fairly controversial. Whereas some think it lowers prices, gives helpful information to consumers, is all about liberal consumer choice, and that also children are sovereign consumers, others hold that it increases prices, tries to manipulate consumers, fosters the concentration of markets and the media, advances stereotypes and sexism, harms children, advances a surveillance society and the exploitation of employees and consumers, and fosters the financialisation and therefore proneness of the economy to crisis and bubbles. Our focus group showed that these controversies have in the age of the Internet and social media gained even more importance. Targeted advertising is at the heart of the capitalist Internet model that dominates

today. It is a capital accumulation model that some cherish as a new form of consumer choice and business opportunity, whereas others detest it as a form of manipulation and the colonisation of the lifeworld by commodity logic. Such controversies are an indication that social and ideological conflicts and struggles are at the heart of contemporary Internet politics.

Carol J. Pardun's (2014) book *Advertising and Society* presents controversies around advertising in such a form that a pro-advertising argument is opposed to a counter-argument. One chapter focuses on Facebook and social media. It shows that academic controversies about targeted online ads follow the same line of controversy as our focus groups. Whereas Joe Bob Hester argues in the pro-position that targeted online advertising "greatly reduces waste" (of money, time, attention) (in: Pardun 2014, 165), is "more relevant" (167), enables interfaces that are "less cluttered by advertising" (167) and "services free of cost to users" (167), Tom Weir holds against Hester that targeted ads are a "violation of individual privacy" (170), that they confirm an Orwellian vision of society (173), and that they display how freedom reduced to ownership and consumption turns into slavery (173). One can add to Weir's argument that theories of audience labour and audience commodification in the age of social media hold that the users of corporate social media constitute a class of unremunerated and exploited digital workers who produce value and a data commodity that is sold to advertisers (Fuchs 2014a, 2015a; Fuchs, Boersma, Albrechtslund and Sandoval 2012; Fuchs and Sandoval 2014, McGuigan and Manzerolle 2014). Both the academic debate and our empirical research confirm the controversial and antagonistic nature of social media advertising.

4.2. Edward Snowden and State Surveillance of the Internet

The second discussion topic was how participants think about Edward Snowden's revelations and secret services' state surveillance of the Internet with the help of systems such as Prism, XKeyscore, or Tempora.

Being asked if they feel Snowden is a hero or a villain, the clear majority view of our focus group participants is that he did the right thing. P1 claims that Snowden "made a valuable contribution in coming out with" the revelations. Likewise, P10 says that "[h]e has certainly done something heroic by revealing to the world what's happening and just bringing that in front of people's minds so that they are reading about it and they are considering that governments can be evil. […] He is always gonna be a target for the Americans". P7 also agrees that Snowden is a hero, adding that "[t]here's this very complex world that very young people like Snowden are the experts on, for the most part. And a security community, people with experts in governments, clearly are not going to understand it. That disconnect kind of struck me at the time, seeing some of the discussion in the media and so on".

Some participants hold more ambivalent views about Snowden's actions. P2 says: "I think he did the right thing, but not in the appropriate way. […] He could have done it in a different way". P6 disagrees: "The question is if he could have done more to bring it to the authorities in America. It looks like the answer is 'no". In that case he has put his own life on the line, which makes him fairly heroic looking". P8: "Who knows what his motivation was. […] But it seems like this was a way out of a situation, which seems to be unjust and this was the only way he could talk about it.

[…] I think that's something that lots of people have a right to know".

The above findings indicate that the vast majority of participants feel Edward Snowden has done the right thing, even though he thereby broke US law, and that his revelations have been important for uncovering the extent of online mass surveillance.

Being asked how they feel about Snowden's revelation that the NSA, GCHQ, and other security agencies conduct large-scale surveillance of online communications, most participants express that they are outraged, that surveillance has gone too far, and that we live in a mass surveillance society with totalitarian potentials. They express a sense of urgency that things have to change.

P3 says: "It changed a lot, although many people suspected there were things like that going on. It really changed our belief in our security services being the white hats [ethical computer hackers] vs. the black hats [unethical computer hackers]. […] The NSA are malicious hackers and just like any other malicious [...] hackers and they do not follow the law necessarily. […] And the magnitude and the question whether we think the government is interested in specific data: I think they are interested in all data. […] They collect everything". P4 expresses a desire to participate in a collective response to these practices: "I believe that such access to surveilled data at the moment it is high and I wish to convince as many people as I can to be part of something that questions that".

The participants problematize warrantless surveillance that treats everyone as a terrorist until proven innocent and installs a system of categorical suspicion. P6 states that "[t]here is nothing new about monitoring. Anybody in the tech industry knows about Tinkerbell […], which enables the government to monitor any telephone phone call in Great Britain. […] The difficulty for them was that they could not monitor every phone, they had to target. […] I don't think many people object to the idea of targeting criminals, murderers, rapists, etc. […] The difficulty is feature creep and the ability with the speed of technology – […] tens of billions of operations per second – means you can monitor tens of billions of people. You can monitor everything they do at all times as a general process. And it is still easier to monitor everyone than it is not to".

Based on the above, P6 is especially concerned with "the feature creep: when it moves from begin a socially agreed consensus that certain behaviour should be monitored and discouraged to a political background, that people are being targeted for their political beliefs or their threat to the stability of the state not through terrorism, but through their opinions". S/he adds that feature creep "has always turned up in totalitarian states. And we don't want that here". P8 identifies a lack of oversight as troubling, noting that previously "you had to go and get permission if you wanted to monitor. And now you don't have to get permission. […] Who agreed to that?"

The participants consider the argument "If you have nothing to hide, then you have nothing to fear" as short-sighted and ideological. P1 believes that those who espouse this view "don't live in London and don't regularly see the variety of people I see […], many of whom would not agree with that statement. They are stopped and searched every day probably in on their way or something". P10 adds the subjective

element of secret service agents as a concern in this case and notes that "it becomes a problem if somebody in the government does not like me".

One participant expresses a somewhat different opinion, arguing that the mass of data generated in everyday life will not be of interest to secret services. P9: "I don't feel strongly about Snowden. […] As a normal user, I don't think I am important enough for the government to actually care about what I am looking at online. And I don't have enough money for it to be worth it to hack into my bank account and so on. So personally I am not too concerned about monitoring in a way". Also the quantity and complexity of available data would matter: "I can't even see how one would look at each individual in the UK, in the world, and what they are doing and all the output that is coming out of it without using tools that filter and monitor. […] It will always be a sample of the population".

Other focus group participants disagree with the view that it is unlikely that the everyday citizen will be targeted. They argue that mass surveillance results in false positives and that this is precisely the problem. P10 considers this to be "the scary part because if you look at filters: […] Out of a 100 people, it will catch 99 criminals and one innocent person". P6 refers to this as the "false positive/false negative-problem". P8 stresses the importance of the legal system for preventing such problems. P6 states in response that "[u]nfortunately the legal system has been circumvented by the [monitoring] systems". P10 fears that a "guilty until proven innocent" approach may be adopted. P6 identifies these issues as "the 'Who guards the guards?'-problem. It's nothing new".

There was a clear sense in the focus groups that surveillance in the age of Snowden's revelations is a huge problem that it is conducted on a mass scale without differentiation so that all citizens are treated as suspicious and as being potential terrorists. Besides categorical suspicion, warrantless blanket surveillance is according to the focus group participants also problematic. They mention that people's opinions are monitored, which contains a strong totalitarian potential. Most participants consider the argument "If you have nothing to hide, then you have nothing to fear" as short-sighted, one-dimensional, and ideological.

4.3. Political Responses to Mass Surveillance

The third discussion topic focused on how the participating experts felt about political responses to mass surveillance.

One possibility that some expert observers recommend in light of the existence of online mass surveillance systems such as Prism and XKeyscore are *technological counter-measures* so that code and technology become politics. Ann Cavoukian, a former Information and Privacy Commissioner in the Canadian province Ontario, is one of the main advocates of privacy by design and privacy-enhancing technologies. Privacy by design and privacy enhancement means according to Cavoukian that "privacy protections are engineered directly into the technology"[17].

[17] Ann Cavoukian, Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum. http://www.ipc.on.ca/images/Resources/trans-tech.pdf

One privacy-enhancing technology is that private users and organisations make their online communication anonymous. Edward Snowden commented on this issue in an interview: "What last year's revelations showed us was irrefutable evidence that unencrypted communications on the internet are no longer safe and cannot be trusted. Their integrity has been compromised and we need new security pro[grams] to protect them. Any communications that are transmitted over the Internet, over any networked line, should be encrypted by default"[18].

Snowden therefore argues that users should encrypt all of their online communications. One form of anonymisation is e-mail encryption. Available tools for email encryption include Pretty Good Privacy (PGP) and the GNU Privacy Guard. In these systems, both the sender and the receiver use public and private encryption keys. If they use these keys, then they are the only ones who can read the e-mail content. Another privacy-enhancing technology is anonymous browsing. The most well known tool for anonymous browsing is the Tor web browser that anonymises IP addresses.

We asked the focus group participants how they felt about privacy-enhancing technologies. They tend to think that privacy-enhancing technologies are an important response to mass surveillance. Yet P1 is concerned with "how realistic, manageable, or something similar it is, I don't know. Anonymising. Whether it will work or not, I don't know". P4 cites his experience training other: "on the use of a Linux system called Tails. Tor is part of it. It can also assist in protecting e-mails as far as that's possible". However s/he also point to "a steep learning curve", adding that [i]t is very difficult to train people".

Participants also point out that it is important that privacy-enhancing technologies have good usability and user experience. P8 notes that "[a] lot of things that would improve privacy are difficult to use. Most people can't manage their own Facebook privacy settings". Noting frustration with the fact that data is largely left under the control of those "who have a commercial interest in using it", this respondent hopes "to see better tools for people to have ownership of their own data and to choose what they do. And the default place where that data sits is in a place that I have control of. And I can then choose to share it with these services". P6 responds by adding that "[t]here have been suggestions along these lines […] setting up a citizen digital ID, where you say: This is me and this is what I am prepared to share with this class of access […] And I think even the EU is looking at that. And that could be an answer".

One concept that the participants point out as particularly relevant is to move away from centralised data storage as in Google, Facebook, or cloud hosting, towards decentralised data storage that allows more privacy controls. P5 argues in this context that "[o]ur data might be out there, but we also have some ability to control that data or to say 'That's my data'. […] The data that was put up there, we could give preferences for how it should be used in certain contexts." P4 anticipates that in the future, "we may have some mechanism by which we control the context of information we give and withdraw that consent at any time through such measures". P5 agrees and identifies such a feature as "contextual privacy". In describing a

[18] *The Guardian Online*, Transcript of an Interview with Edward Snowden. July 18, 2014 http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

decentralised Internet, P10 identifies "data that […] no government or no single entity can hold. Then there is nobody that can use it for a purpose. And anybody who accesses that data, there is an audit blog entry of why that company or why that government body accesses that information. That is again public. So if somebody asks for my data for some reason, I can go to a judge and say: Look, something happened there". P6 endorses this morphology that s/he terms "public justice".

One participant points also out that users should learn how to analyse data in order to address the monopolisation of this process by states, marketers, and online companies. The participant specifically discusses Maltego, an open source intelligence software that allows analysis and visualisation of open data, link analysis, and data mining. P4 supports "the idea of being able to start to use such tools for individuals because eventually, perhaps, you could start to see exactly where your position was regardless of where your data was on the planet. […] So I think there is some validity to the whole 'Take it back'-philosophy". Search engines and intelligence agencies would have far more complicated tools, but making these tools broadly available and offering the necessary education would nonetheless be a start.

One criticism of privacy-enhancing technologies is that not everyone has the time, skills, and interest in educating him- or herself and for using such technologies. Another criticism is that advocating privacy-enhancing technologies is a form of techno-determinism that tries to find technological solutions to societal and political problems. The argument is that such solutions are insufficient because they do not challenge the underlying surveillance conducted by secret services, companies, or criminals, but just operate on the surface without challenging the root causes.

The German public service broadcasting channels WDR and NDR revealed in July 2014 that the US National Security Agency used XKeyscore and other surveillance programmes in order to identify who searched on the WWW for encryption technologies such as Tor or who visited the Tor website[19]. The NSA classifies users of tools such as Tor as "extremists"[20]. It for example monitored the German computer science student Sebastian Hahn and his servers because he operates one of the 5,000 TOR encryption servers that are active on the WWW. The NSA tried to store all accesses to Hahn's servers.

This example shows that using privacy-enhancing technologies may encrypt the content of online communication, but that those who operate and use such technologies are considered as "extremists" by secret services and may therefore be put under surveillance . Moreover, the fact that they rely on these services can be a visible and discoverable fact, which undermines their intention to avoid scrutiny.

The participants in the focus groups were not naïve techno-determinists. They do not

[19] Quellcode entschlüsselt: Beweis für NSA-Spionage in Deutschland. *NDR Online*. July 3, 2014. http://daserste.ndr.de/panorama/archiv/2014/Quellcode-entschluesselt-Beweis-fuer-NSA-Spionage-in-Deutschland,nsa224.html. See also: Bruce Schneier: Attacking Tor: how the NSA targets users' online anonymity. *The Guardian Online.* October 4, 2013. http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

[20] XKeyscore: NSA beobachtet Anonymisierungs-Server von deutschem Studenten. *Spiegel Online*. July 3, 2014. http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaehte-tor-server-von-deutschem-student-mit-xkeyscore-aus-a-978914.html

think there are technological fixes to political problems. They see privacy-enhancing technologies as only one dimension of political resistance and counter-measures to mass surveillance. P4, who teaches others how to use privacy-enhancing technologies, sees such educational measures as just one step and a starting point: "I find that an interesting beginning. But it is not the end of it. […] How you break down the intelligence hangover we got really from the post-war era. […] We are not going to dismantle that over night. And we are just going to continue to have a culture of post 9/11 fear and control. So there don't seem to be an easy way out of this until we grow out of that fear and out of that control".

The participants discuss the limits and problems of privacy-enhancing technologies. P3: "Even if you're anonymised, you'll go to the same websites. And eventually given enough processing power – and the US government does have infinite computational power – if they want to know about you, they are going to know about you. […] If you're subject of a one-person NSA focus, they know everything about you. You have no chance". P10 argues that one could try to create a lot of noise and false information on the Internet, but that doing so may especially create attention and raise suspicions: "If I wanted to create a certain image about me on the Internet, I could write a lot, I could put a lot of data points out there. And if lots of individuals share this the same as I do, then it will be difficult for somebody to figure out that […] But again, doing all these things puts a red flag on: 'Why is he trying so hard to hide? There is something definitely wrong'".

P6 and P7 argue that governments aim to remove and break all encryption mechanisms by technological and legal measures:
P7: "It's a bit like if the government said: We are going to take away all the locks that people put on their own houses and we'll put a lock there that we have a key to and other people might get that key too".
P6: "Public key cryptography is broken. It is useless"
P7: "Snowden himself says that PGP [the encryption tool Pretty Good Privacy] still works".
P6: "Secure cryptography in the UK is not a problem for the state because you now got DRIP [the Data Retention and Investigatory Powers Act 2014: an emergency law passed by British parliament in July 2014], which means that you have to hand over your encryption keys. It is required. And if you don't, you go to prison. A couple of people have gone to prison".

The participants disagree on the question whether Tor is secure or not. P6 asserts that "Tor was written by the American navy. And it's a honeypot to catch people and their communications to be monitored". P7 and P8 disagree with P6's view. P7 says that "it's not insecure".

The law and the state constitute a realm of politics that goes beyond privacy-enhancing technologies. Many participants in the focus groups felt that although current governments and state institutions have implemented mass surveillance with totalitarian potentials, the right kind of government could change the situation and put legal protections of citizens and users' privacy into place and could limit the power of the police and secret services to conduct surveillance. P10 sees the need for legislation, they were concerned with the notion of "Who watches the watchers?". P1 also endorses the presence of laws, noting that while they may not always be

respected, they can at least "provide a benchmark and presumably hold somebody to account." P6 acknowledges social complexities: "[M]ost people really want a peaceful life and no trouble and a government that delivers that to as many people as possible with minimum pain for all." In his/her view, laws must be accompanied by "people in government that actually understand technology. […] The only way I can see to counter it is to put some legislative oversight by people who actually know what technologies mean". However, the focus group participant also acknowledges that s/he does not "know how you get technical expertise into the government or generally throughout the economy."

Overall, there was a feeling among the focus group participants that currently British and international laws tend to predominantly protect the interests of communications companies, the police, and secret services, but that it is possible to create "stronger legislation to protect people" (P6). They indicated that they are rather sceptical about the British government's reaction to Snowden's revelations. An example is the Data Retention and Investigatory Powers Act (DRIP) that was passed by British parliament in July 2014. P4 observed that suddenly "service providers such as social networking sites now come under the regards of telecommunications networks. So now they are required to give to whoever asks meta-data, whatever". The governments in place would typically have short-term interests, lack technical expertise, and further extend surveillance so that the protection of citizens' interests would be undermined. P10 believes that "[g]overnments pass a few laws to appease the masses. More than anything else they look at what can I do so that four or five years from now, when there is a general election". P10 is especially concerned with the long-term implications of supposedly short-term strategies: "And they can go back as far into the past as they want to. They have started to collect data from the early 2000s. […] If I am a teenager and I have done some stupid things in my past and if I am a different person now and it is 30 years after that happened. That shouldn't have an impact on if I want to become the Prime Minister".

Data storage and processing is a matter of power. Some citizens argue that one must reduce or take away the power of those who can monitor users and empower the users themselves as well as organisations, political parties, and social movements that want to protect users' data. A related opinion is that what we need most urgently are activism and protests against surveillance. An initiative called "Academics against Mass Surveillance" has for example initiated a petition, in which academics call for transparency and accountability of what secret services do. The Don't Spy On Us-coalition has "come together to fight back against the system of unfettered mass state surveillance that Edward Snowden exposed. Right now, the UK's intelligence services are conducting mass surveillance that violates the right to privacy of Internet users and chills freedom of expression". It is sceptical of the British government: "The current laws haven't stopped the intelligence services expanding their reach into our private lives. *Don't Spy On Us* is calling for an inquiry to investigate the extent to which the law has failed and suggest new legislation that will make the spooks accountable to our elected representatives, put an end to mass surveillance in line with our 6 principles and let judges not the Home Secretary decide when spying is justified"[21].

[21] https://www.dontspyonus.org.uk/about

In Summer 2014, the hacker group Anonymous called for a mass protest at a Cheltenham-based surveillance post of the GCHQ, the British secret service that according to Edward Snowden has collaborated with the NSA in conducting Internet surveillance and that apparently as part of the Tempora programme listens in on fibre-optic cables in order to extract personal data of Internet users and shares these data with the NSA[22]. Anonymous' call concluded: "The tyranny must end, 1984 was not an instruction manual. DEMAND YOUR FREEDOM BACK!!!"

We asked the participants in the focus groups how they feel about civil society and protest movements as responses to mass surveillance. P4 offers the one-word descriptor "[viable]", adding that "[i]t's bizarre that over the last few years, especially meetings such as the one of the Chaos Computer Club, who get together every year. Until recently in Berlin, there were 600-700 people, all men wearing black, with severe dietary malfunctions. Now, this year, the same event in Hamburg, and an explosion of different people, not white male geeks interested in Plan 9 or BSD". So one can now observe a much wider "scope of those who want to understand the impact of these subjects as well as technology and/or alternative ways of making, so the whole maker scene is blurring to this as well. I found a social interest in this area to have exploded. And I think that's great and we gotta keep going".

P5 notes that greater transparency will incite society to "push back." Likewise, P1 considers it a welcome change that citizens "are starting to stand up and anything that can give them the means to use technology to protest and make their voice heard is welcome". P3 argues that the general political climate in the world is conducive for mass protests: "In total there is properly popular uprising. And I am not talking about a hundred guys in Guy Fawkes masks. I am talking about truly popular uprising that forces governmental change. We are still fighting a losing battle when we are talking about privacy, no matter what. We talk about the government, any government, certainly any European government, […] has the power to figure out everything they want to know about you. They have the resources. Far more resources than you ever gonna have. […] People, […] even though they agree to what is being exchanged for terms of privacy or whatever else, they don't understand the scope of it. And it's that scope that we'll hopefully convince them that something is wrong and they can do something about it".

5. Discussion and Conclusion

Social media are convergent media in two respects (Fuchs and Trottier 2013): 1) They enable the *convergence of the social activities* of producing and sharing information, communicating, collaborating, and engaging with communities on single platforms. 2) They also reflect and further advance the convergence of different social roles: On social media like Facebook, we act in various roles. But all of these roles become mapped onto single profiles that are observed by different people who are associated with our different social roles. On Facebook, your "friends" are family members, people you are close with, colleagues from work, ephemeral acquaintances, and strangers.

Social media reflect complex changes of society that have resulted in a liquefaction

[22] http://en.wikipedia.org/wiki/Tempora

and blurring of boundaries between public/private, social/individual, labour/leisure, office/home, production/consumption, labour/play, etc. (Fuchs 2014c). Zygmunt Bauman (2002/2012, 2005) argues that liquidity is the main feature of life and society in modernity. Whereas it is an overarching claim to say that liquidity is *the* central feature of modernity, it is certainly one of its aspects (Fuchs 2014c) that has also affected the way communication is organised. In respect to surveillance, Bauman and Lyon (2013) therefore speak of the emergence of liquid surveillance. "Surveillance spreads in hitherto unimaginable ways, responding to and reproducing liquidity. Without a fixed container, but jolted by 'security' demands and tipped by technology companies' insistent marketing, surveillance spills out all over" (Bauman and Lyon 2013, 9).

Technologies are not the cause of these changes, but a field, where these changes and resulting contradictions unfold. The convergence of social activities and roles on social media results in the fact that the processed data reveals close pictures of most aspects of our lives. The access to a mass of data about converging activities in converging social roles is the reason why both Internet companies such as Facebook and Google (the world's largest advertising agencies) as well as repressive state institutions have such a huge interest in monitoring social media data. The focus groups we conducted discussed both corporate and state surveillance of social media as well as another form convergence that Edward Snowden uncovered: the convergence of state and corporate surveillance of the Internet and social media.

The focus groups conducted with data and computer experts showed that these professionals are highly sceptical of Internet and social media surveillance. They argue that data protection is an important principle that profit-driven companies often disregard; that many terms of use and privacy policies are complex, vague, euphemistic, ideological, loaded, and deceptive; and they pointed out that giving informed and explicit consent to data processing and the processing of sensitive personal data has become more difficult because of the global and networked nature of data, cloud computing, changing contexts of data, and inferences that algorithms draw from meta-data. Targeted online advertising is at the heart of many large social media companies' capital accumulation model. The focus groups showed the controversial and contradictory nature of targeted online advertising.

The vast majority of the focus group participants feel Edward Snowden has done the right thing, even though he thereby broke US law, and that his revelations have been important for uncovering the extent of mass surveillance of the Internet that has been going on. Many of them indicate that Snowden's revelations have shown that we live in a mass surveillance society with totalitarian potentials. There was a sense in the focus groups that it is a huge problem that surveillance is conducted as mass surveillance without differentiation, that surveillance is not just targeted at actual criminals and terrorists who are under suspicion, but that everyone is treated as suspicious and as being a terrorist. Besides categorical suspicion also blanket surveillance of single individuals without a warrant would be very problematic. The participants mentioned that people's opinions are monitored, which would have a strong totalitarian potential. Most participants considered the argument "If you got nothing to hide, then you got nothing to fear" as short-sighted, one-dimensional and ideological.

Computing is based on a deterministic logic, in which reality is always calculable and has at each point of time a clear, one-dimensional binary status (either zero or one). Georg Lukács (1971, 131) argues that with the rise of capitalism, "human relations (viewed as the objects of social activity) assume increasingly the objective forms of the abstract elements of the conceptual systems of natural science and of the abstract substrata of the laws of nature". The economy thereby became "transformed into an abstract and mathematically orientated system of formal 'laws'" (105) that is governed by "the abstract, quantitative mode of calculability" (93). Max Horkheimer (1947) termed such thought instrumental reason. Herbert Marcuse (1964) spoke of technological rationality. The one-dimensional logic of calculability makes engineers prone to define society in terms of machine logic, to neglect contradictory thought that does not define the world in the logic of either/or, and to advocate technological fixes to political problems. An important result of the conducted study was that it provided indications that computer professionals do not view surveillance after Snowden as a technological, but a political problem and that they do not advocate technological fixes (the use privacy enhancing technologies), but political changes.

Overall, the participants in the focus groups feel it is important that there are political responses to the totalitarian potentials of mass surveillance that Edward Snowden revealed. They do not favour an approach that only relies on a single political dimension such as technology, law, or social movements' protests, but rather take an "anything goes" approach that advocates that any measure, strategy, and initiative that questions and aims at driving back mass surveillance is important, should be attempted and supported.

Two focus groups are not a large enough sample for generalising the findings. However, the research results show some very clear tendencies, which are an empirical indication that many computer and data experts are highly political and critical when it comes to questions of surveillance. The participating data and computer experts question the combination of corporate and state power that has resulted in a system of mass surveillance. They support the combination of various levels of resistance against such surveillance. They are not naïve techno-determinists and therefore do not simply propagate technological solutions, such as a sole focus on privacy-enhancing technologies. They see that there are no technological fixes to political problems. At the same time they also believe that it is very important not to neglect the technological dimension and that technological expertise is important for questioning and struggling against the surveillance-industrial complex.

The participants point out the limits of privacy-enhancing technologies such as secret services' vast computing power that is used to break encryption, the legal requirements to reveal encryption keys, and the suspicion that using privacy-enhancing technologies creates suspicion so that such users may especially be subject to surveillance. At the same time they feel that educating users on how to use privacy-enhancing technologies and open data analysis is an important form of empowerment in the struggle against the surveillance-industrial complex.

The participants in the conducted research think that it is important to strengthen laws that truly protect citizens, watch and limit the powers of the watchers, prohibit categorical surveillance, and only allow surveillance of single individuals who are under suspicion and with the help of a judicial warrant. At the same time they feel that

many governments' reactions to Snowden's revelations, including the British government, included the implementation of even more surveillance and further limitation of citizens' rights. In particular, they discussed the UK Data Retention and Investigatory Powers Act 2014. This scepticism towards the state does not mean that the focus group participants think that the law and the state cannot be reformed. To the contrary, the respondents feel that a government that truly cares about citizens can bring constructive change. They simply have the impression that many governments at the moment fall completely short of protecting citizens and only protect security agencies' interests in implementing conservative law and order politics that are based on the ideology that more policing and more surveillance is a solution to complex political and socio-economic problems such as crime and terrorism. One participant for example remarks in the feedback questionnaire: "Valuable discussion. How does this get into government?". This participant thereby expresses that citizens getting together, as in the focus groups, generate viable ideas for solutions, but governments at the moment do not take these citizen interests into account. The participant stresses the importance of civil society action and protest movements that aim at creating public awareness and exert pressure for political change.

Edward Snowden's revelations about the existence of surveillance systems such as Prism, XKeyScore, and Tempora have shed new light on the extension and intensity of state institutions' Internet and social media surveillance. But these are not just phenomena of state power, but also of corporate power. The concept of the military-industrial complex stresses the existence of collaborations between private corporations and the state's institutions of internal and external defence in the security realm. C. Wright Mills argued in 1956 that there is a power elite that connects economic, political, and military power: "There is no longer, on the one hand, an economy, and, on the other hand, a political order containing a military establishment unimportant to politics and to money-making. There is a political economy linked, in a thousand ways, with military institutions and decisions. […] there is an ever-increasing interlocking of economic, military, and political structures" (Mills 1956, 7-8).

Edward Snowden has confirmed that the military-industrial complex contains a surveillance-industrial complex (Hayes 2012), into which social media are entangled: Facebook and Google each have more than 1 billion users and have likely amassed the largest collection of personal data in the world. They and other private social media companies are first and foremost advertising companies that appropriate and commodify data on users' interests, communications, locations, online behaviour and social networks. They make profit out of data that users' online activities generate. They continuously monitor usage behaviour for this economic purpose. Since 9/11 there has been a massive intensification and extension of surveillance that is based on the naïve technological-deterministic surveillance ideology that monitoring technologies, big data analysis and predictive algorithms can prevent terrorism. The reality of the murder of a soldier that took place in the South-East London district of Woolwich in May 2013 shows that terrorists can use low-tech tools such as machetes for targeted killings. High-tech surveillance will never be able to stop terrorism because most terrorists are smart enough not to announce their intentions on the Internet. It is precisely this surveillance ideology that has created intelligence agencies' interest in the big data held by social media corporations. Evidence has shown that social media surveillance not just targets terrorists, but has also been

directed at protestors and civil society activists[23]. State institutions and private corporations have long collaborated in intelligence, but the access to social media has taken the surveillance-industrial complex to a new dimension: It is now possible to obtain detailed access to a multitude of citizens' activities in converging social roles conducted in converging social spaces.

Yet the profits made by social media corporations are not the only economic dimension of the contemporary surveillance-industrial complex: The NSA has subcontracted and outsourced surveillance tasks to approximately 2,000 private security companies[24] that make profits by spying on citizens. Booz Allen Hamilton, the private security company that Edward Snowden worked for until recently, is just one of these firms that follow the strategy of accumulation-by-surveillance. According to financial data[25], it had 24 500 employees in 2012 and its profits increased from US$ 25 million in 2010 to 84 million in 2011, 239 million in 2012, 219 million in 2013, 232 million in 2014, and 233 million in 2015. Surveillance is big business, both for online companies and those conducting the online spying for intelligence agencies.

Users create data on the Internet that is either private, semi-public and public. In the social media surveillance-industrial complex, companies commodify and privatise user data as private property and secret services such as the NSA driven by a techno-determinist ideology obtain access to the same data for trying to catch terrorists that may never use these technologies for planning attacks. For organising surveillance, the state makes use of private security companies that derive profits from organising the monitoring process.

User data is in the surveillance-industrial complex first externalised and made public or semi-public on the Internet in order to enable users' communication processes, then privatised as private property by Internet platforms in order to accumulate capital, and finally particularised by secret services who bring massive amounts of data under their control that is made accessible and analysed worldwide with the help of profit-making security companies.

The UK focus groups provided indications that many computer and data professionals are outraged and feel deep unease about the existence of the surveillance-industrial complex. They do not want an Internet that is controlled by companies and state institutions. Many of them rather argue for an alternative Internet that is controlled by civil society and the users and citizens themselves. Participant P7 for example concludes that "[i]f this is the way that governments and intelligence agencies want to go, it is a race to the bottom, the bottom being everyone spying on everyone else and no one being secure. The rational thing to do is to invest in […] creating secure systems that are public infrastructures […] Investment in public digital infrastructure that anyone can use, that is open source, that is decentralised, etc. That would be a good way to go. That should be coupled with regulation and new laws as well".

---

[23] Spying on Occupy activists. *The Progressive Online.* June 2013. http://progressive.org/spying-on-ccupy-activists

[24] A hidden world, growing beyond control. *Washington Post Online*. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/

[25] SEC Filings, http://investors.boozallen.com/sec.cfm

The alternative to a politically-economically controlled Internet is a commons-based Internet (Fuchs 2014b).

References

Adams, Andrew, Kiyoshi Murata, Yasunori Fukuta, Yohko Orito and Ana María Lara Palma. 2015. The view from the gallery: International comparison of attitudes to Snowden's revelations about the NSA/GCHQ. *SIGCAS Computer & Society* 45 (3): 376-383.

Andrejevic, Mark. 2013. *Infoglut. How too much information is changing the way we think and know.* New York: Routledge.

Andrejevic, Mark. 2007. *iSpy: Surveillance and power in the interactive era.* Lawrence, KS: University of Kansas Press.

Bakir, Vian, Jonathan Cable, Lina Dencik, Arne Hintz and Andrew McStay. 2015. *Public feeling on privacy, security and surveillance. Research report*. Cardiff: Cardiff University.

Ball, Kirstie, Kevin Haggery and David Lyon, eds. 2012. *Routledge handbook of surveillance studies.* Abingdon: Routledge.

Ball Kirstie and Frank Webster, eds. 2003. *The intensification of surveillance. Crime, terrorism and warfare in the information age.* London: Pluto.

Bauman, Zygmunt. 2000/2012. *Liquid modernity.* Cambridge: Polity Press.

Bauman, Zygmunt. 2005. *Liquid life.* Cambridge: Polity.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R.B.J. Walker. 2014. After Snowden: Rethinking the impact of Snowden. *International Political Sociology* 8 (2): 121-144.

Bauman, Zygmunt and David Lyon. 2013. *Liquid surveillance*. Cambridge: Polity.

Branum, Jens and Jonathan Charteris-Black. 2015. The Edward Snowden affair: A corpus study of the British press. *Discourse & Communication* 9 (2): 199-220.

Bryman, Alan. 2012. *Social research* methods. Oxford: Oxford University Press. Fourth edition.

Chadwick, Andrew and Simon Collister. 2014. Boundary-drawing power and the renewal of professional news organizations: The case of *The Guardian* and the Edward Snowden national security leak. *International Journal of Communication* 8: 2420-2441.

Chomsky, Noam. 2011. *9-11: Was there an alternative?* New York: Seven Stories Press.

Fuchs, Christian. 2015a. *Culture and economy in the age of social media.* New York: Routledge.

Fuchs, Christian. 2015b. Surveillance and critical theory. *Media and Communication* 3 (2): 6-9.

Fuchs, Christian. 2014a. *Digital labour and Karl Marx.* New York: Routledge.

Fuchs, Christian. 2014b. *Social media: A critical introduction.* London: Sage.

Fuchs, Christian. 2014c. Social media and the public sphere. *tripleC: Communication, Capitalism & Critique* 12 (1): 57-101.

Fuchs, Christian. 2013a. Political economy and surveillance theory. *Critical Sociology* 39 (5): 671-687.

Fuchs, Christian. 2013b. Societal and ideological impacts of Deep Packet Inspection (DPI) Internet surveillance. *Information, Communication and Society* 16 (8): 1328-1359.

Fuchs, Christian. 2011. How to define surveillance? *MATRIZes* 5 (1): 109-133.
Fuchs, Christian, Kees Boersma, Anders Albrechtslund and Marisol Sandoval, eds. 2012. *Internet and surveillance. The challenges of web 2.0 and social media.* London: Routledge.
Fuchs, Christian and Marisol Sandoval, eds. 2014. *Critique, social media & the information society.* New York: Routledge.
Fuchs, Christian and Daniel Trottier. 2013. The Internet as surveilled workplayplace and factory. In *European data protection. Coming of age*, ed. Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet, 33-57. Dordrecht: Springer.
Garrido, Miguelángel Verde. 2015. Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden. *Surveillance & Society* 13 (2): 153-167.
Greenwald, Glenn. 2014. *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Metropolitan.
Haunss, Sebastian. 2014. Privacy activism after Snowden: Advocacy networks or protest? In *Cultures of privacy,* ed. Karsten Fitz and Bärbel Harju, 227-244. Heidelberg: Universitätsverlag Winter.
Hayes, Ben. 2012. The surveillance-industrial complex. In *Routledge handbook of surveillance studies*, ed. Kirstie Ball, Kevin D. Haggerty and David Lyon, 167-175. Abingdon: Routledge.
Hintz, Arne. 2014. Outsourcing surveillance – Privatising policy: Communications regulation by commercial intermediaries. *Birkbeck Law Review* 2 (2): 349-367.
Horkheimer, Max. 1947. *Eclipse of reason.* NewYork: Continuum.
Keiber, Jason. 2015. Surveillance hegemony. *Surveillance & Society* 13 (2): 168-181.
Lukács, Georg. 1971. *History and class consciousness.* London: Merlin.
Lyon, David. 2015a. *Surveillance after Snowden*. Cambridge: Polity.
Lyon, David. 2015b. The snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society* 13 (2): 139-152.
Lyon, David. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1 (2)
Lyon, David. 2007. *Surveillance studies: An overview*. Cambridge: Polity.
Lyon, David. 2003. *Surveillance after September 11*. Cambridge: Polity.
Marcuse, Herbert. 1964. *One-dimensional man.* Boston: Beacon Press.
Mathiesen, Thomas. 2013. *Towards a surveillant society. The rise of surveillance systems in Europe.* Hook: Waterside Press.
McGuigan, Lee and Vincent Manzerolle, eds. 2014. *The audience commodity in a digital age. Revisiting a critical theory of commercial media*. New York: Peter Lang.
Mills, C. Wright. *The power elite.* Oxford: Oxford University Press.
Mosco, Vincent. 2014. *To the cloud: Big data in a turbulent world.* Boulder, CO: Paradigm.
Murakami Wood, David and Steve Wright, eds. 2015. Surveillance and security intelligence after Snowden. *Surveillance & Society* 13 (2): 132-217.
Pardun, Carol J., ed. 2014. *Advertising and society.* Chicester: Wiley Blackwell.
Petley, Julian. 2014. The state journalism is in: Edward Snowden and the British press. *Ethical Space* 11 (1/2).
Qin, Jie. 2015. Hero on Twitter, traitor on news: How social media and legacy news frame Snowden. *The International Journal of Press/Politics* 20 (2): 166-184
Rockmore, Tom. 2011. *Before and after 9/11: A philosophical examination of globzliation, terror, and history.* New York: Continuum.

Scheuerman, William E. 2014. Whistleblowing as civil disobedience: The case of Edward Snowden. *Philosophy and Social Criticism* 40 (7): 609-628.

Schulze, Matthias. 2015. Patterns of surveillance legitimization: The German discourse on the NSA scandal. *Surveillance & Society* 13 (2): 197-217.

Trottier, Daniel. 2014. *Identity problems in the Facebook era.* New York: Routledge.

Trottier, Daniel. 2012. *Social media as surveillance. Rethinking visibility in a converging world.* Farnham: Ashgate.

Trottier, Daniel and Christian Fuchs, eds. 2014. *Social Media, politics and the state: Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*. New York: Routledge.

van der Velden, Lonneke. 2015. Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance. *Surveillance & Society* 13 (2): 182-196.

Appendix: Focus Group Interview Guide

Before the Start

The moderator and his/her assistant welcome the participants, assign a seat to them, provide a name tag to them that stands in front of them on the table and besides their names also shows their institutions. The ideal setting is that a round-table can be used.

An informed consent form and an information sheet containing basic information about PACT is distributed to each participant after arrival. S/he is asked to read the material, if s/he has any questions or comments on it, and to sign the form.

[Distribution of two information sheets]

Explain to each participant that refreshments are available and they are welcome to take drinks and food.

Explain also to each participant that the focus groups will be audio- and video-recorded and that this makes the analysis easier.

Part 1: Start/Introduction

Welcome to this focus group. Thanks a lot for agreeing to participate. We much appreciate that you took time out of your surely busy schedule to come here and contribute. We welcome your contributions and inputs to our research.

My name is Christian Fuchs and I will be moderating this group discussion. I am a professor of digital and social media research here at the University of Westminster. I will be assisted by Daniel Trottier, who will take notes and take care of technology.

Our session will take about two hours with a short refreshment break after about one hour. Since we will be audio and video-recording the discussion, I would kindly ask you to speak in a clear voice; your opinions, experiences and suggestions are very important to this research, and we do not want to miss any of your comments.

We will audio- and video-record the discussion, but these recordings are for internal use by the research team only, which makes it easier for us to analyse the results. We will not publish the audio and video recordings.

In the research reports we publish, we want to quote from what you say in the discussion. But this will be fully anonymous. We will not mention your names, the names of the organisations you work for, or any other identifiable details. We will only say what kinds of organisations have participated, i.e. the fields or industries they come from. So the recorded comments might be used in scientific publications and reports, but only as anonymous quotes. There will be no possible way to identify you on the basis of the documented information. In order to ensure the latter, you will be assigned a number or letter in the report (e.g. respondent A), and only this symbol will be used in the reports.

The research we are conducting is part of the European Union research project

"PACT: Public Perception of Security and Privacy", in which 10 research teams study the role of privacy and surveillance in Europe. You can get further information about the project and read some of its reports by visiting its website http://www.projectpact.eu.

As a token of appreciation for your participation, we will give to each of you at the end of the focus group a printed version of three of our research reports that we hope can help your organisation to make better sense of issues that relate to privacy and personal data. You will be among the first people from the public getting access to them and we hope your organisations can benefit from the information obtained.

[Bound hard copies of the PACT deliverable reports D1.4, D5.1 and D5.2 are distributed to the participants at the end of the focus group]

A focus group is a structured discussion on a specific topic, in our case privacy and security. There are a couple of simple, but important rules, that we should observe in order to make it a good discussion:

- We are interested in the opinion of each individual and we would therefore like to hear from all the people in the group.
- There are no wrong or right answers. There are only different opinions. Consequently, it is important that we mutually respect each other's opinions. At the same time, it is unlikely that everyone agrees on the issues discussed. You are encouraged to articulate disagreements with what others say on specific issues we discuss.
- It is important for us that only one person speaks at a time. Each opinion is important and I would kindly request that you don't speak when others are speaking, otherwise it will be difficult for us to capture all of your opinions.
- I would also kindly request that you silence your mobile phones and thus provide for an uninterrupted discussion.
- In the focus group discussion, we are interested both in your personal opinions and in the actual practices and opinions you have encountered in organisations and companies you have worked in or with.

Do you have any comments or other suggestions or general questions before we start?
….

So, let us start with all members of the group briefly introducing themselves. I will start and we'll then go around the table. Maybe we can say our names, a bit about your work or studies, your organisations or universities, and what you do. All of you have a common interest in computing and the Internet.

Let me start by introducing myself

….

[Go around the table and let the participants introduce themselves]

Part 2: Ethical Values and Societal Dimensions

One important aspect of assessing information technologies has to do with ethics. Ethics discusses what principles we can use for deciding what appropriate and inappropriate actions are in contemporary society. We have tried to identify and

specify ethical values that are important to be respected in the design, implementation and use of information technologies. We want to now present some of these values to you, discuss with you how they relate to technology, and how they matter.

Part 2.1. Sensitive Personal Data

One issue that is important when dealing with the ethics of digital data is so-called sensitive personal data. Our research has identified the ethical importance of handling sensitive personal data in responsible manner.

We have prepared an information sheet that shows you the legal definition of sensitive personal data that is used in the United Kingdom. The same kind of definition is used in all European Union countries. Let's have a look at the definition.

[Distribution of an information sheet to the participants. The moderator reads and explains the definition]

So for example the information "He lives in the United Kingdom" is not sensitive personal data. The information "He is an HIV-positive, Protestant man who supports the Labour Party" is sensitive personal data because it contains health-related, religious and political data.

Part 2.1.1. Sensitive Personal Data in the Participants' Organisations

Sensitive personal data involves data about a person's ethnicity, political opinions, religious and other beliefs, membership in trade unions and political groups, health data, sexual orientations and interests, biometrical identifiers, and criminal convictions.

ICT professionals and scientists studying computing and data often develop or use information technologies that process personal data. I am wondering if you have been confronted by users with the question if and how to store or process sensitive personal data. Which approaches do you or your organisations take in respect to this issue? We are interested in both your personal and your organisations or research group's (where applicable) opinions and experiences on this issue.

… (Discussion)

Part 2.1.2. Google and Sensitive Personal Data in Targeted Advertising

Let us assume I want to market the University of Westminster's website on Google in order to try to get more students. So I use behavioural advertising on Google for this purpose to target specific groups. Behavioural advertising is advertising that makes use of specific behaviours of users, for example which keywords they type into Google.

We have prepared a video that shows how such ads are set up. Let us have a look at it.

[The moderator shows a prepared video and explains what the participants can see there]

So my aim is to target the ad at people who are interested in the Labour Party, Protestantism, or HIV. These are issues relating to politics, religion, and health. So they are quite sensitive. It is just a hypothetical example. In reality the University of Westminster does not run such ads.

What are your opinions: Should it be possible for me to run such an ad? Should I be allowed to do so or rather not? Why or respectively why not? How do you think about this issue?

… (Discussion)

2.1.3. Google's Privacy Policy and Privacy Regulations in Respect to Targeted Advertising: The Role of Opt-Out

Let's have a look at how Google regulates such issues in its privacy policy. You also find this information on another information sheet we have prepared.

[The moderator distributes an information sheet]

Google's current privacy policy (version from March 31, 2014) says:
"When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health".
Cookies are small files stores on users' computers in order to identify that they have visited specific websites. Anonymous identifiers are similar to cookies, but used on specific technologies, for example particular mobile phones.

So Google says it does not store cookies if I visit a sensitive website. It does however not rule out to use sensitive keywords for targeted ads.
The privacy policy also specifies:
"People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:
 Review and control certain types of information tied to your Google Account by using Google Dashboard.
 View and edit your ads preferences about the ads shown to you on Google and across the web, such as which categories might interest you, using Ads Settings. You can also opt out of certain Google advertising services here".

So there seem to be mechanisms that can enable me to opt out so that Google does not use my interests that I reveal in keywords for advertising.
Let us have a look at how this works. We have prepared another video for this purpose.

[The moderator shows the participants a prepared video and explains what they see there]

So the video shows us how I can delete certain searches from my search history and that I can disable Google to use my search keywords for advertising. How do you feel

about these so-called opt-out mechanisms? Do you feel the availability of such a deletion function and an opt-out is a sufficient privacy protection or rather not? How do you think about this topic?

…. (Discussion)

Part 2.1.4. Targeted Advertising: Opt-In or Opt-Out – What is Better?

Various surveys have shown that users feel quite uncomfortable about targeted advertising.

[do not read, just as additional information for the moderator: In 2011, the European Union carried out at a European-wide survey. It focused on how citizens think about data protection. One question was how comfortable they were with the fact that there are websites that "use information about your online activity to tailor advertisements or content to your hobbies and interests?"[26]. 54% of the respondents felt uncomfortable about it, 39% comfortable, 7% had no clear opinion. A survey carried out by Razorfish in 2014 shows that 78% of the UK respondents feel that targeted ads on the mobile Internet are a privacy invasion[27].]

The Article 29 Working Party is a group of data protection commissioners and experts set up by the European Union. It publishes opinions and recommendations about privacy and data protection issues. In 2010 it consulted on the topic of online advertising and then published its opinion and some recommendations[28]. Its opinion is that many users do not know about opting-out and that opt-out is not a real consent because passivity of the user does not necessarily imply agreement and is not an active participation in expressing agreement. The Article 29 Working Party concludes that ad network providers "should swiftly move away from opt□out mechanisms and create prior opt□in mechanisms" (23) and that mentioning "the practice of behavioural advertising in general terms and conditions and/or privacy policies can never suffice" (24).

The advertising industry has a different opinion. The European Advertising Standards Alliance and the Interactive Advertising Bureau argue that opt-in approaches are "disruptive for users"[29] and that such mechanisms "are not of comparable privacy value to users" and can have "severe negative economic impact on a legitimate business activity"[30] of advertisers. They prefer opt-out, as e.g. in the case of Google that we saw.

I am wondering what your opinions are on opt-in to vs. opt-out of targeted online

[26] Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[27] http://www.thedrum.com/news/2014/06/30/three-quarters-mobile-users-see-targeted-adverts-invasion-privacy-says-razorfish
[28] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171, Adopted on 22 June 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[29] http://www.iabeurope.eu/policy/oba-and-self-regulation/industry-offers-consumers-greater-transparency-and-control-o
[30] IAB Europe and EASA: Letter to Article 29 Working Party. January 17, 2012. http://www.iabeurope.eu/download_file/977/211

advertising. Should it better be organised as an opt-in, where the standard setting is that sensitive and other personal data is not used for targeted advertising, or opt-out, where the standard setting is that such data is used for targeted ads, and the users can go to a page, where they can deactivate such usage? Can you please also try to give reasons for your opinions.

….. (Discussion)

Part 3. Edward Snowden

Can you for a minute think about which personal data that is stored by an IT system, application or platform that you use in your organisation, for work, for your studies, or in private life, or that you study in your research and write down a list of stored data onto the notepad that lies in front of you.

So I think you all have now written down some of specific personal data. Let's maybe go around the table so that everyone can report about the system she has chosen and what s/he has written down.

[Go round the table and let everyone present briefly]

…. (Discussion)

In June 2013, Edward Snowden has with support of the *Guardian* revealed the existence of the global Internet surveillance system Prism that is operated by secret services such as the NSA in the USA and GCHQ in the UK in collaboration with communication companies such as AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, and Yahoo!. He also revealed the existence of a surveillance system called XKeyScore that the NSA can use for reading e-mails, track web browsing, phone calls, and online contact networks, and follow the screens of individual computers.
Here are short video excerpts, in which Snowden explains what Prism and XKeyScore are:

[Display of a 5 minute video, in which Snowden explains his leaks and revelations]

Let us now assume that a security agency actually demands that it gets access to the ICT system you have chosen before and to some or all of the personal user data stored in it. Let us assume they use the systems that Snowden talks about. How severe a privacy violation do you think the users would consider this monitoring if they knew about it? How do you in general assess Snowden's revelations?
I suggest that we again go round the table and that each of you tells us something about how you expect your users would react if they heard about the state monitoring of their data that is stored by your company.

… (Discussion)

Part 4. Control of Privacy Threats

If one has identified data protection and other risks for users, then the question arises

what can be done about it. The literature on the control of privacy threats identifies technical and organisational measures that can be taken.

Let us first discuss some possible technical measures.

Part 4.1. Privacy-Enhancing Technologies

One possibility that some experts recommend in light of the existence of the Prism and XKeyscore surveillance technologies are technological counter-measures. Ann Cavoukian, a former Information and Privacy Commissioner in the Canadian province Ontario, as well as many other data protection experts advocate the concepts of privacy by design and privacy-enhancing technologies. Privacy by design and privacy enhancement means according to Cavoukian that "privacy protections are engineered directly into the technology"[31].

One privacy-enhancing technology is that private users and organisations make their online communication anonymous. Edward Snowden commented on this issue in an interview:

"What last year's revelations showed us was irrefutable evidence that unencrypted communications on the internet are no longer safe and cannot be trusted. Their integrity has been compromised and we need new security pro[grams] to protect them. Any communications that are transmitted over the internet, over any networked line, should be encrypted by default. That's what last year showed us"[32].

So Snowden argues that users should encrypt all of their online communication. One form of anonymisation is e-mail encryption. Available tools for email encryption include Pretty Good Privacy (PGP) and the GNU Privacy Guard. In these systems, both the sender and the receiver use public and private encryption keys and if they use them, then they are the only ones who can read the e-mail content.

Another privacy-enhancing technology is anonymous browsing. When users browse the WWW, they are identifiable by their IP address. Data protectionists consider an IP address to be personally identifiable information. The most well known tool for anonymous browsing is the TOR web browser that anonymises IP addresses.

We have prepared a handout that shows how TOR works.

[The moderator distributes a handout]

So TOR generates random paths over encrypted servers in order to reach WWW pages.

TOR describes its benefits the following way: "Journalists use Tor to communicate

[31] Ann Cavoukian, Transformative Technologies Deliver
Both Security and Privacy:
Think Positive-Sum not Zero-Sum. http://www.ipc.on.ca/images/Resources/trans-tech.pdf
[32] *The Guardian Online*, Transcript of an Interview with Edward Snowden. July 18, 2014
http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript

more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization. […] Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online. Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers"[33].

I am wondering what opinions you have about privacy-enhancing technologies? Do you think that they are a good means for overcoming surveillance threats posed by secret services and other organisations or people monitoring the Internet. Can you think of specific advantages and risks of such technologies?

Discussion (…)

Do you or your organisations use specific forms of privacy-enhancing technologies? If so, which ones? Or did you have discussions in your organisations or with friends, colleagues, students about adopting privacy-enhancing technologies?

Discussion (…)

Are privacy-enhancement mechanisms something that you think Internet users care about?

…. (Discussion)

Part 4.2. Criticisms of Privacy-Enhancing Technologies

Hackers dedicated to privacy protection organise so-called crypto parties, which are public events, where computer experts teach lay users how to use encryption tools. CryptoParty London regularly organises such events.

One criticism of privacy-enhancing technologies is that not everyone has the time, skills and interest in educating him- or herself and using such technologies. Another criticism is that advocating privacy-enhancing technologies is a form of techno-determinism that tries to find technological solutions to social and political problems. The argument is that such solutions are insufficient because they do not challenge the underlying surveillance conducted by secret services, companies, or criminals, but just operates on the surface without challenging the root causes.

The German public service broadcasting channels WDR and NDR have in July 2014 revealed that the US National Security Agency used the XKeyScore and other surveillance programme in order to identify who searches on the WWW for encryption technologies such as TOR or who visits the TOR website[34]. The NSA

[33] https://www.torproject.org/about/overview.html.en

[34] Quellcode entschlüsselt: Beweis für NSA-Spionage in Deutschland. *NDR Online*. July 3, 2014. http://daserste.ndr.de/panorama/archiv/2014/Quellcode-entschluesselt-Beweis-fuer-NSA-Spionage-in-Deutschland,nsa224.html. See also: Bruce Schneier: Attacking Tor: how the NSA targets users' online anonymity. *The Guardian Online.* October 4, 2013. http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

classifies users of tools such as TOR as "extremists" and especially monitors them[35]. It for example monitored the German computer science student Sebastian Hahn and his servers because he operates one of the 5,000 TOR encryption servers that are active on the WWW. The NSA tried to store all accesses to Hahn's servers.

The example shows that using privacy-enhancing technologies may encrypt the content of online communication, but that those who operate and use such technologies are considered as "extremists" by secret services and may therefore especially be monitored.

I am wondering how you feel about these criticisms that privacy-enhancing technologies are just technocratic attempts that do nothing against the existence of surveillance and may put users and operators at new risks?

…. (Discussion)

Part 4.3. Political and Organisational Alternatives to Privacy-Enhancing Technologies

An alternative to privacy-enhancing technologies that is being discussed is to change the whole organisation and regulation of how data is being stored. Data storage and processing is a matter of power. So some argue that one must reduce or take away the power of those who can monitor users and empower the users themselves and organisations, political parties and social movements who want to protect users' data. Some privacy advocates therefore argue that what we need most urgently are activism and protests against surveillance. They argue that we need political and organisational solutions.

An initiative called "Academics against Mass Surveillance" has for example initiated a petition, in which academics call for transparency and accountability of what secret services do.

The hacker group Anonymous has called for a mass protest at a Cheltenham-based surveillance post of the GCHQ, the British secret service that according to Edward Snowden has collaborated with the NSA in conducting Internet surveillance and that apparently as part of the Tempora programme listens in on fibre-optic cables in order to extract personal data of Internet users and shares these data with the NSA[36].

The protest call said: "Between the 29th of August and the 1st of September 2014 the people will be holding a mass protest out side of GCHQ in Cheltenham, England to continue their campaign against the mass public surveillance employed by many of the worlds Governments, including the UK's. While we are told this measure worthy of Orwell is for our own protection we feel that this is simply another lie spun to us and that this massive invasion of privacy is nothing but a method of gathering intelligence to allow greater control of the worlds civil population. The tyranny must end, 1984 was not an instruction manual. DEMAND YOUR FREEDOM

[35] XKeyscore: NSA beobachtet Anonymisierungs-Server von deutschem Studenten. *Spiegel Online*. July 3, 2014. http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaehte-tor-server-von-deutschem-student-mit-xkeyscore-aus-a-978914.html

[36] http://en.wikipedia.org/wiki/Tempora

BACK...!!!"

In the end, such protests aim at forbidding legally that certain data are monitored by secret services. They argue for restrictions on or the outlawing of the development and use of specific surveillance technologies. They argue that citizens should only vote for parties that support privacy and oppose surveillance measures. They argue for a stronger political control of secret services by independent authorities or for the abolishment of secret services. And they speak in favour of changing data protection laws so that they require maximum privacy protection, storage of a minimum of data for a minimum period of time, i.e. only to the extent necessary for operating IT services, the decentralisation of data storage, etc.

I am wondering what your opinions are about such political movements, protests and demands?

…. (Discussion)

When you consider the measures we have discussed – privacy-enhancing technologies, changing existing laws, political protests, outlawing surveillance technologies, abolishing secret services: Which ones do you think are most relevant ((for you or your organisations in order to try to guarantee privacy of users))?

…. (Discussion)