THE IMPORTANCE OF BEING TRANSPARENT:
THE EVOLUTION OF TRANSPARENCY REPORT IN THE ICT INDUSTRY

By Alexandra Kulikova
MSc, Media and Communication Governance
London School of Economics and Political Science

Abstract

The paper looks at the transparency policies of the major ICT companies and Transparency Report as an emerging corporate accountability standard in the digital media sector. It presents a research carried out as a case study framed by the US NSA surveillance practices media leak in June 2013. The allegations against the major Internet-companies as colluding with the state put the issues of the transparency and compliance high on the agenda in the ICT industry reflecting new challenges in data protection and privacy policies that they face as aggregators of vast amounts of data, liable to lawful data disclosure requirements by state authorities. The study highlighted the increased salience of the transparency principle in the corporate privacy policies with enhanced focus on the commitment to user trust and the values of human right of privacy operationalised inter alia by Transparency Reports. It was suggested that as more companies adopt this practice, even though it's not comprehensive due to currently lawful limitations the ICT sector is fighting against, transparency report is also developing as a reflection of the ongoing debate between the governments and businesses on the issue of privacy in cyberspace and limits and trade-offs in how they access and use citizens' data. Interviews with companies highlighted the value of the report both as a trust-building instrument and a corporate lobbying tool as tested by the recent event. This has indicated that transparency reports have been developing as the ICT industry accountability standard further stimulated by the above-mentioned event.

This paper then builds on the original study which took place at the start of a new wave of debates around online privacy following shortly the above mentioned event (dissertation submitted to the Department of Media and Communications, London School of Economics, August 2013, for the MSc in Media and Communication governance). The identified trend was proved: shortly after the research completion Facebook and Yahoo published their transparency reports, and more ICTs followed suit. The revealed lobbying potential of the transparency agenda as the tech-giants are reciprocally seeking more granularity in reporting on national security information by state agencies as well as more openness in their own information disclosure, is attracting more ICT companies to join the transparency effort. With obvious PR benefits and controversial implications for legal reform, these developments still shape a new privacy-driven discourse in the public sphere and internal corporate and state narratives.

INTRODUCTION

Transparency report as a form of self-regulation is a recent trend, although it is deeply correlated with long existing corporate governance practices and accountability standards. The domination of the top internet-corporations in the new media world as well as the digital convergence have brought about the amalgamation in ICT companies' public policies of the self-regulatory efforts arising from the online environment of their operation with a broader range of corporate accountability and compliance issues through the human rights perspective.

The increasing aggregation of user data online has emphasised the importance of the information security, privacy and data protection issues. Therefore, this sets Internet development further in the human rights context, inevitably affecting the ICT industry, the operation of which is predicated on the Internet ecosystem.

In the framework of what Raab calls privacy governance (Raab, 2006), ICT companies' reports on user data disclosure to the state authorities could be considered as part of the 'social contract' existing between these companies and the users (Donaldson, 1982). This implies that the companies pledge to stand by the human rights protection by monitoring and reporting on the state surveillance, which is a way of the state performing its part of the social contract with the public in providing security. This complex triangular relationship means that the corporate sector becomes increasingly embedded into the system of state versus public relationship as data aggregators and – potentially – privacy rights watchdogs as intermediaries.

This self-assumed role is ambivalent. It does not only manifest their compliance with international human rights legal norms in the legal context of a given state as well as their compliance with state legitimate demands for data disclosure. By pushing the public interest agenda it also helps secure consumer confidence and trust as well as serves as a competitive advantage.

This ambivalence also testifies to the growing power and outreach of the mentioned companies, as their close to monopoly status allows them to gain much bargaining power in now key issues of security, privacy and data protection. Transparency in this area is limited by state regulation, on the one hand, and supported and encouraged by the human rights protection commitments, those of freedom of expression and privacy in particular, on the other.

In this context of complex power relations, transparency and accountability go beyond mere good corporate practices. This paper looks at Transparency Report (TR) as a specific manifestation of corporate policies in user data management, tracing the motivation for its publication, the development of its content and future fate – as perceived by the major Internet companies. The discussion is set against the background of the NSA leak about the surveillance programme PRISM, followed up by further revelations about state surveillance activities by governments in different countries gathering information of the citizens and the debate around lawfulness of their actions. Instead of going deep into the analysis of the event itself, the focus is on the way it highlighted for the first time the transparency agenda in the public policies of the biggest ICT companies, which had to make firm statements rejecting all allegations on cooperating with the authorities, and set a new trend in ICT accountability.

Transparency report, being a relatively new form of reporting on the relationship with the state authorities, is shaping into an industry standard of accountability in online privacy governance. This paper presents the original research undertaken in summer 2013 and looks at how companies initially conceptualised transparency report, whereby the mentioned event arguably set a context and testing ground for its viability and relevance and is used here to highlight the role of transparency and TR in the situation of user trust crisis. The results are then discussed in a follow-up context testifying to the accuracy of the identified trend.

When sunlight becomes searchlight it can be uncomfortable
and when it becomes torch it may be destructive
(Heald in Hood & Heald, 2006, p. 71)

The rapid development of the ICTs[1] and the domestication of new technologies (Silverstone & Haddon, 1996) have made us spend more time online and leave numerous digital traces in various types of data (Gellert, Gutwirth in Guagnin, Hempel, Ilten, Kroener, & Neyland, 2012). The stunning pace of technological innovation as highlighted by Moore's law on computing power growth, makes it increasingly easier for individuals, companies and governments to store, share and process vast amounts of personal and communications data (Brown & Marsden, 2013, p. 48). Cloud computing technologies have made access to data even more ubiquitous and their protection more challenging (Bennett in Guagnin et al., 2012, p. 37), to the extent that the applicability of the term 'surveillance state' might not necessarily have controversial connotations for everyone (Goold & Neyland, 2013, p. XV). This poses new challenges for the concepts of privacy, data protection and surveillance (Bennett in Guagnin et al., 2012, p. 48). These are much defined by the biggest corporate data holders – the major ICT companies: Google, Apple, Twitter, Yahoo, Microsoft, Facebook etc. The 'emerging Internet oligopoly' of most popular Internet services they form, shapes what Chris Freeman calls 'ICT paradigm' of the modern economy (Freeman in Mansell, 2007). This market power therefore boosts their role in how we know, define and tackle the issues of privacy, surveillance and user data protection online.

Privacy, Surveillance and Data Protection Revisited

The subtitle of David Brin's seminal "Transparent Society" asks *Will Technology Force Us to Choose Between Privacy and Freedom*, which is an "intentionally provocative" question (Brin, 1999, p. 13). Considering privacy as one of the fundamental human rights, Brin suggests that "whenever a conflict arises between privacy and accountability, people demand the former for

[1] For the purposes of this study under ICT companies/ICTs we understand collectively, unless specified otherwise, social media networks (e.g. Facebook, Twitter), content aggregators and search engines (e.g. Google. Yahoo), tech-companies (e.g. Microsoft, Apple) – in other words, the current major corporate players on the Internet market

themselves and the latter for everybody else" (Brin, 1999, p. 12). It is even more obvious now as digital technologies place all of us in almost constant visibility (Colburn, Nolin in Akrivopoulou et al., 2012, p. 5).

The idea of Panopticon, a prison where one *might* be observed at any moment of time – originated by Jeremy Bentham and taken further by Foucault – is often used as a vivid metaphor to describe the modern digitalised routines. It is 'a way of defining power relations in terms of everyday life of men' (Foucault, 1979, p. 197), which the advent of new technologies has made a reality. Twenty years ago, writing about information as 'a commodity in its own right', Oscar Gandy suggested that the 'panoptic sort, as the integrated control technology of the Information Age, depends for its operation on ready access to information about individuals' (Gandy Jr, 1993, p. 52).

The term of commodification of privacy through electronic surveillance, increasingly embedded in both corporate world and public institutions, has been adopted by later studies (Campbell & Carlson, 2002). At present behavioural advertising (Brown & Marsden, 2013, p. 56), corporate monitoring (Colburn, Nolin in Akrivopoulou et al., 2012, pp. 5-6), or administrative information gathering (Gandy Jr, 1993, p. 55) could all be conceptualised in surveillance terms. State monitoring for security purposes, increasingly reinforced by new technological advances, sparked a debate around CCTV creating a surveillance society with the Big Brother always watching and the 'myth of public security', thus revealing a difficult trade-off between security and privacy (Goold in Goold & Neyland, 2013, pp. 18-19) (Akrivopoulou in Akrivopoulou et al., 2012, p. 25).

The new risks of terrorism and extremism, especially in the wake of the 9/11 attack in the US, created new insecurities and brought about new regulatory defence tools, granting the state easier access to citizens' data[2]. The development of the ICTs and the spread of cloud technologies allowing access to the data through an internet-based server network infrastructure, got in

[2] US Patriot Act 2001 and its extension in 2011 granting law enforcement authorities more intelligence power within the US; FISA Amendment Act 2008 to extend the foreign intelligence discretion in electronic surveillance outside the US to apply to non-Americans

spotlight due to the amount of data they process and store, thus offering efficient monitoring opportunities for national security through social sorting (Lyon, 2002, p. 20). This is facilitated by the increased concentration in the Internet markets and increased exit costs due to networking effects also mean high concentration of vast amounts of data in the hands of just a few companies (Birnhack & Elkin, 2008). In this context, the ICTs are bound both by legal compliance requirements on disclosure of user data under relevant legislation[3] and, in the US case, by legal limitations on some public disclosure of this compliance (gag orders, limited granularity of reporting on the number of national security letters etc). Thus, the simultaneous increase of security risks, state monitoring and ICT development, complicated by the overlap of jurisdictions in the cloud, puts much pressure on the private sector at the intersection of related but not identical debates around the fundamental right to privacy, secured by the European Convention on Human Rights (Article 8) and Universal convention of human rights (Article 12), and ensuring data protection[4] (Giannakaki in Akrivopoulou et al., 2012, pp. 12-13).

The variety of literature on privacy and data protection reveals the difficulty in defining and conceptualising these terms. It seems important to discriminate between the normative concept of privacy as a fundamental human right protected by national and international laws and data

[3] E.g. RIPA in the UK; FISA, FISAAA, Patriot Act in the US

[4] It is important to differentiate between users' personal and communications data as handled by the ICT sector. As follows from the UK Information Commissioner's Office guide to the UK Data Protection Act 1998, personal data means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of (Carey, 2009).

Communications data, meta-data or 'traffic data' as defined in the Council of Europe Convention on Cybercrime 2001, means 'any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service' ("Council of Europe Convention on Cybercrime," 2001).

Today search engines, social media and other data aggregators hold a wealth of both personal, meta-data as well as content data and can be seen as both processors and controllers. When combined together, as helped by the contemporary cloud technologies, these data could disclose potentially sensitive information about an individual (Nissenbaum, 2004; van den Hoven, 2008).

protection which offers lawful mechanisms of transparency for allowing for free flow of a limited amount of data (Gellert, Gutwirth in Guagnin et al., 2012, pp. 263, 267). The authors argue that although the development of ICTs poses challenges to privacy of individuals, the emphasis has been mostly on data protection.

Frimholz mentions this disparity in cultural and linguistic terms in her article on the existing EU and US legislation on privacy and data protection arguing that Americans focus just on the overarching right of privacy while Europeans conceptualise data protection in terms of the mechanisms of collecting and processing data (Fromholz, 2000, p. 470). While in Europe citizens' data are protected by the EU Data Protection Directive 95/46 (currently under revision) and domestic Data Protection Authorities (e.g. UK Data Protection Act 1998), there's no single piece of legislation on data protection in the US, where the US Constitution and the 4th amendment are the key guarantors of the right of privacy and data management is handled by industrial laws; this complicates the interoperability between the US and EU legislations in terms of privacy and data protection, given the mentioned acceleration of data exchange through cloud technologies (Brown & Marsden, 2013, pp. 59-63).

This distinction suggests that data protection does not necessarily guarantee privacy per se in a given jurisdiction (Gellert, Gutwirth in Guagnin et al., 2012, p. 263), and responsible attitude to these challenges in the private sector is reflected in the adoption of accountability approach to user data handling and transparency about their sharing with the state authorities.

Accountability, transparency and good governance

Accountability and transparency both in private and public sector are better understood though the concept of *social contract*. Originated by Jean-Jacques Rousseau, developed by Hobbes and taken further by Locke, the theory has it that the public exercise their civil rights while committing to respect and defend the rights of others and to give up some freedoms in order to do this (Locke, 1947).

In the private sector context, the integrative social contracts theory (ISCT), first developed by Donaldson (Donaldson, 1982) and Dunfee (Dunfee, 2009), holds it that corporations enjoy limited liability and freedom of operations in return for efficient services and goods provision with fair treatment of the community which trusts them and offers them this right, e.g. their staff and customers. The moral underpinning to this contract is the premise that the consent is well informed and there is a right to exit the community. However, businesses as intermediaries in many instances between the citizens and the state, have to live up to the contract with the public by fulfilling these conditions and by successfully doing so they get greater legitimacy to magnify the needs of its stakeholders (Fort, 2001, pp. 143-144). In other words, viability of business depends on this performance on its social contract with the public, as well as grants companies more power in relations with the state – and a competitive advantage among peers.

User trust, which once lost is hard to win back, is predicated on the good governance practices like accountability and transparency which underpin company's responsibility. Bennett argues that accountability goes beyond mere responsibility implying 'a process of transparent interaction, in which [an external body] seeks answers and possible rectification' (C. J. Bennett, 2010, p. 21). Transparency in its turn has become 'a standard component of corporate governance', supporting trustworthy performance (O'Neil in Hood & Heald, 2006, pp. 75-76).

Interestingly, transparency in contemporary political sense was developed by the inventor of Panopticon Jeremy Bentham, who explained the need for what he called "publicity" by the following main reasons: "to constrain the members of the assembly to perform their duty", "to secure the confidence of the people, and their assent to the measures of the legislature" and "to enable the governors to know the wishes of the governed" (Bentham & Bowring, 1843). For Bentham a society is based on a "system of *distrust"* [author's emphasis] since "whom ought we to distrust, if not those to whom is committed great authority, with great temptations to abuse it?" Indeed, corporate transparency emerged as a response to corporate failures and information asymmetry around the data flows around corporations (Hood & Heald, 2006, pp. 16-18).

However, while classic corporate governance approach requires total transparency as a key to better corporate accountability (Hölmstrom, 1979), it might go against the entrenched corporate interests (Prat in Hood & Heald, 2006, p. 94). Heald similarly points outs the difference between effective and nominal transparency, or “transparency illusion” which, he argues, obfuscates the message by information overload (Heald in Hood & Heald, 2006, pp. 34-35). Moreover, transparency by increasing trustworthiness does not necessarily boost trust, since it takes care of disseminating the message by disclosure without taking much care of the public response (O'Neil in Hood & Heald, 2006, p. 78). O’Neil goes on in her critique of transparency as a ‘fifth wheel on the wagon of public, commercial and professional accountability’ by arguing that it benefits mostly the public image of the company and is essentially ‘a form of defensive risk management’ (O'Neil in Hood & Heald, 2006, pp. 87-89), protecting not the public/customers, but service providers proper by transferring any liability. In other words, transparency per se is not a panacea in securing public trust, but it is, nevertheless, crucial in maintaining it.

This is even more apparent for the ICT companies’ user data handling. First, secret services in most countries have tools to access vast amounts of publicly and privately owned information for security reasons, and in the recent years these practices have intensified due to above mentioned perceived risks and technological advances in cyberspace. Security as a part of social contract provided at the cost of loss of privacy through surveillance is thus in conflict with the understanding of privacy as a degree of personal security. Therefore, the balance between surveillance practices for social security and transparency about it, is not easy to demonstrate as it also would involve disclosure of classified information (Bulow, Wester in Akrivopoulou et al., 2012, pp. 41-43). It has been, however, much lobbied for now by both businesses and civil society groups.

Second, there is some asymmetry of understanding between the individuals and the ICTs, whereby the users are not fully aware of the potential ‘re-purposing’ of their data submitted in one context for other uses and therefore cannot assess properly the potential damage that can be incurred to them (Bulow, Wester in Akrivopoulou et al., 2012). The user agreement terms and the right of exit from the ICT platforms are still a controversial point as the consent is rarely truly informed (MacKinnon, 2012) and the exit, even though free, is not always easy to exercise because of network effects, which affect users’ switching power (Arsenault & Castells, 2008).

Essentially, ICT technologies have a “Hotel California Impact” on individuals: “They can check out any time they like but they can never leave” (Giannakaki in Akrivopoulou et al., 2012, p. 13).

Finally, despite the increasing attention drawn to cyberspace regulation and the operation of the big Internet companies, there’s still relatively little understanding by the public of the implications of failure in discriminating between private and public, as the rapid domestication of digital technologies has diluted the notion of privacy. With the ICT accountability being still a niche issue, there is little meaningful public response to transparency efforts. This, however, can be expected to change as the topic evolves in a more mainstream discourse.

Privacy governance in ICT industry: limitations of transparency and self-regulation

With these caveats in mind, the ICT sector, nevertheless, engages in online privacy governance through accountability and transparency to avert the threats to social contract through legal regulation (with national and transnational instruments), self-regulation or technological solutions (privacy by design) (C. C. J. Bennett & Raab, 2003; Guagnin et al., 2012). Legal regulation is first point of appeal in the context of privacy and data protection in commercial use, whereby the private sector is complying with state requirements by being transparent on how citizens’ data are used for profit-driven activities of the companies, thus accountable both to the state and the public. However, while legal regulation compels companies to disclose user data upon lawful requests, their accountability to the public on complying with those requests is essentially self-regulation, as companies voluntarily commit to doing so in respect to the fundamental human right of privacy and ultimately in pursuit of user trust. With more ICT companies, including telecoms, join this effort, we can observe the self-regulatory mechanism taking shape in the conditions of trust crisis.

Raab quotes Peter Hustinx, head of the Netherlands Data Protection Authority, who presented a paper in 1991 to the Conference of Data Protection Commissioners in Strasbourg in which he argued that there are four purposes of self-regulation for privacy: to avoid legislation, to anticipate legislation, to implement or to supplement it (Raab, 2006, p. 121). Raab argues that these are achieved by developing industry codes, standards, guidelines etc to shape out the benchmarks for corporate behaviour with better publicity, competitive advantage, and international pressures as major incentives for adopting them. A number of the Council of Europe recommendations to member-states suggest developing ‘codes of conduct guaranteeing the protection of individuals’ fundamental rights ("Recommendation of the Committee of Ministers to member-states on the protection of human rights with regard to search engines," 2012).

Gunningham and Rees differentiate define self-regulation as ‘a regulatory process whereby an industry-level (as opposed to a governmental or firm-level) organisation sets rules and standards (codes of practice) relating to the conduct of firms in the industry’ (Gunningham & Rees, 1997, pp. 364-365). This highlights the role of the Global Network Initiative as a human rights advocate: this multi-stakeholder group, with Google, Microsoft and Yahoo as founding companies (Facebook joined in 2013), includes civil society organisations, academics and businesses and focuses on working out mechanisms of safeguarding human rights in the ever growing complexity of interests and conflicting rights in the digital space. It emerged much in response to the criticism from the civil society when it appeared that due to the ICTs’ compliance with the Chinese law, ‘the modern “Great Wall of China” is, in effect, built with American bricks’ (Goldsmith & Wu, 2006, pp. 93-95). As it was argued at the time, these companies did not have enough legal justification for doing so, according to the UN ("Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights," 2003). The companies faced a dilemma of having to ‘respect international laws protecting rights and, at the same time, abide by national laws that protect the interests of the State’ (Dann & Haddow, 2008, pp. 222-223).

Thus, the GNI, as a self-regulating membership group initiated by the private sector to set ethical standards for its operations and allow fighting off the state attempts at censorship and filtering, expanded to oversee other norms and values such as online privacy and transparency. These are in special focus now due to the NSA surveillance leak discussed further and are part of the formal audit that all the members undergo as part of their own self-regulatory privacy and transparency policies based on respect for the right to privacy.

Transparency reporting

In spring 2010, the first among the ICT companies, Google published what it called ‘Transparency report’ (TR), and since then has been releasing the product biannually. Over time the report has evolved to provide statistics on user data requests from government agencies and courts, content removal requests from governments and copyright holders and (now real time) traffic data and statistics on detected malware and phishing sites (Transparency Report, Google).

Since then more companies came up with their reports, whereby the shared feature is the data they provide on lawful requests by the government about the data of the users of their services. Twitter was the first to follow suit in 2012 with its own Transparency report (Transparency report,Twitter) designed along similar lines; Microsoft in March 2013 released its Law Enforcement Requests Report (Law Enforcement Requests Report, Microsoft) focusing online on lawful requests on user data as the name suggests; a few smaller ICT companies came up with theirs later. The progress can be tracked from the Electronic Frontier Foundation annual analysis of online service providers’ privacy and transparency practices regarding government access to user data ("Who Has Your Back?," 2013).

We are focusing here on the case of transparency reports (or otherwise called reports for the same purpose) and more specifically the part covering user data disclosure to the state authorities, as a self-regulating practice of accountability on preserving the fundamental human right of privacy online. Therefore, the study presented in this paper stems from the understanding of transparency practices in terms of user data handling as a best practice among ICT companies, and transparency report is one of the ‘genres’ of accountability self-regulation. As more companies face the challenge of privacy issue in handling user data in their relations with the state authorities, they tend to follow the format introduced by Google.

The increasingly open environment of social interactions, technological process, convergence and new media integration into people’s daily practices dilutes the notion of privacy and renders new meaning to the notion of surveillance – both in commercial use by the key ICT companies or government’s’ inquiries into user data of particular citizens. Given the increased interest to and worries about safeguarding the right of privacy online, the Internet companies, holding vast amounts of personal and communication data of their users, undergo pressure from the civil society groups and NGOs to come up with ways of accountability both to the governments and the citizens about handling these data. Besides, their combined market power emphasises the salience of user trust, the loss of which does not only potentially mean reputational damage and business failure, but might have significant economic and political consequences.

In June 2013 a US National Security Agency contractor Edward Snowden leaked secret documents revealing the existence of the so-called PRISM programme, which gives the NSA access to user personal, metadata as well as the communications content of non-US persons through the databases of the ICT companies – Google, Microsoft, Yahoo, Facebook, PalTalk, Apple, AOL also YouTube and Skype as independent companies at the moment of being involved (Greenwald & MacAskill, 2013). The original story suggested that this access was gained with the consent of the named companies, which was immediately and vigorously denied in official corporate statements, saying that the companies never granted direct access to the user data.

The story is used here as a discretionary event to contextualise the ICT industry response, because:

a) It suggested a global threat to the security of user data online by disclosing the scale of electronic surveillance;
b) It set the spotlight on the major ICT companies, which hold those data.
c) The fact that there are secret user data requests that the companies can’t include into their reports (e.g. FISC requests in the US - at the time of the initial research), thus making data-sets incomplete, became known for broader audience.

These factors created a context of potential trust loss and related reputational risks for the companies involved, therefore, the leak was a useful background for testing the role and relevance of the transparency agenda in the public policies of the companies in dealing with the user data in their relationship with the state authorities; as well as to look at the role and use of transparency report in a trust crisis situation and implications for this format in future.

As transparency practices around user data came into focus, more companies got interested in releasing the data. However, the reporting limitations questioned the actual degree of transparency of the transparency reports and their meaningfulness. The original research undertaken in summer 2013 looked at the initial NSA leak event as trigger for the development of ICT transparency reports as a new format of accountability in the Internet industry on its compliance with the state requests on user data, despite these transparency limitations. The event also gave good grounds for pushing against them, and the potential loss of user trust served as a sort of litmus test on the actual relevance of transparency report for online privacy governance.

The study thus provided an early 'snap-shot' examination of the immediate policy reaction of the ICT companies to the situation of trust crisis around the privacy of user data. The questions in focus were as follow:

- How is transparency conceptualised in the public policies of the major Internet companies as a self-regulatory accountability tool?
- What is the company's view on TR as a form of accountability? What is the rationale for its publication?
- What effect did the NSA surveillance leak have on the approach to transparency policies and/or the transparency report in the companies which featured in the scandal (whether they already issue it or not)?

RESEARCH DESIGN AND METHODOLOGY

The research tracks the development of the transparency policies in user data disclosure in the ICT industry sector within the framework of the case study of transparency reports of major Internet companies as a form of accountability that they have recently started to employ. It adopts elements of process-tracing approach and thematic analysis in the discussion of to the material obtained from the interviews with the employees of the selected companies. The case is discussed against the backdrop of the NSA surveillance leak in June 2013 which foregrounded the public debate around the issues of surveillance, data protection and the right to privacy.

Case study, as 'an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident', allows more flexibility within a relatively under-researched field (Yin, 1994, p. 13). This study looks at the transparency reporting, and as the hypothesis suggests, the event framing this case study accelerated the evolution of privacy policies of the ICT companies related to the user data disclosure to the governments (Hakim, 2000, pp. 60-61, 68-69) (Hakim, 2000, p. 70). Looking at the change the companies' approach to privacy policies in terms of commitment or non-commitment to publication of transparency report also allows some instances of process tracing inferences about the development of the TR as a transparency accountability tool (A. Bennett & George, 2005, p. 147).

Four semi-structured in-depth interviews between 45 min and 110 min long were conducted with relevant policy officials from the major ICT companies to address the research questions as well as to reveal some potential discrepancies between stated attitudes, approaches and actual behaviour of interviewees (Hakim, 2000, pp. 36-37). For this study, whereby for ethical reasons of the topic sensitivity the names and exact positions of the interviewees are not disclosed, we loosely apply the term 'elite interviewing', meaning that the sample consists of people in top positions relevant to public policy in the corresponding companies. This gives the advantage of getting first-hand testimony about decisions and actions behind an event or series of events (Tansey, 2007, pp. 766-767).

In-depth interviewing embedded in the case study approach, was expected to make a ‘probe’ into the corporate stance on the debate around transparency policies of ICT companies as intensified by the event framing the case study (Berger, 1998, p. 55). However, the returns should be assessed with understanding of corporate bias (Berry, 2002, p. 680) and account mitigation (A. Bennett & George, 2005, p. 102). Also interviewees could blend their official corporate stance with personal views (Hakim, 2000; Richards, 1996), and given the sensitivity of the topic, non-consent to be quoted was expected (Ruebhausen & Brim, 1965, p. 1189).

Non-probability, focused sampling was chosen for this project, not intended at achieving representativeness (Hakim, 2000, p. 36) but rather at exploring the ‘best practices’ of the ‘trend-setters’ in terms of transparency policies. It serves the goal ‘to obtain information about highly specific events and processes’ and uncover the causal mechanisms underlying decision-making at the elite level (Tansey, 2007, p. 768). For this study four companies were selected – Google, Microsoft, Facebook and Yahoo – which, with the caveat of offering different services (social networking, data aggregation, online search, software) and operating in different jurisdiction set-ups (e.g. Google is run along the US law around the world, while Yahoo tailors its legal base to the local market), are grouped together for the following considerations:

a) These are the ICT industry leaders in their respective sub-categories, ‘sovereigns of the Internet’ (MacKinnon, 2012), and handle huge amounts of user personal and communications data, to which the state authorities can have lawful access;
b) Google and Microsoft already publish transparency reports; Yahoo publicly announced its intention to release its own report in summer 2013[5] while Facebook made public its intention to follow suit after getting a permission to publish the data on US requests including FISA requests, and reiterated this in the interview. Therefore, one of the aims of the interviews was to see if the mentioned event had affected the importance of the TR

[5] Not released by the date of the original research completion on 30 August 2013

for both the companies which did publish it and for those which didn't, thus tracking the development of a corporate self-regulation accountability trend in ICTs.[6]

c) They all incurred reputational damages and had to refute allegations of allowing governments direct access to citizens' data after the NSA surveillance leak and talk to the public about the nature of their relationship with the authorities.

d) All four companies are members of the Global Network Initiative, which Facebook was the latest to join in 2013 and where the three other companies are founding members. The context of the GNI human rights commitments helps in understanding the development of TR as an industry self-regulation standard.

An interview guide was compiled to:
- take the interviewees through a general discussion about the role and development of transparency policies within the company as related to the disclosure of user data to the government to map out the corporate context and internal attitude to them;
- discuss TR and its value as a specific tool of accountability in this area, in particular, if the company produces one, the reasons for (not) having it;
- discuss the above mentioned issues in the post-NSA leak context in terms of further policy changes/development; interviewees were asked to reflect on how the transparency policies in their companies might or already have changed in response to the event, more specifically on the role of transparency report in the wake of the event.

Some questions got evasive answers or answers which then could not be reported here in full for ethical reasons. The findings of this study discuss only the information obtained upon the interviewees' written consent. The data then were analysed to answer the research questions, while the first question was addressed thematically in order to reveal the concepts, corporate values and aspirations related to transparency in the respondents' companies as a context from which the interviewees stem in their approach to transparency policies, TR in the framing of a particular event (Boyatzis, 1998).

[6] Twitter was not included in the sample, even though it was the first after Google to publish their TR in 2011, since the company was not mentioned in the scandal, therefore not running a reputational risk as big as did the others.

VOICE OF THE INDUSTRY: INTERVIEW RETURNS

Transparency in the public policies of the major Internet companies as a self-regulatory accountability tool

The analysis of the discussion of the role of transparency in user data disclosure in the public policies of the companies participating in the research revealed the following themes which underlie their understanding of this issue, its goals, measurement and the challenges it poses to the company:

1. *User trust*

   User confidence and comfort with the product is seen as one of the goals of the companies' accountability and transparency about user data handling with the governments 'to make sure that our users are able to enjoy a degree of privacy and security' (Yahoo).

   All respondents stated that their companies want to 'be clear' on terms and conditions with the users and follow formal procedures which are outlined in their publicly available privacy policies on how and on what grounds companies might have to 'disclose your data as a result of law enforcement requests' (Facebook). Two companies made a special point that they handle requests manually and 'push back on a lot', never handing over information 'automatically'.

   Not explicit in all the interviews, it was pointed out openly in two of them that transparency is about user loyalty and readiness to 'switch off' if their confidence is failed, which is a competitive advantage for the companies:

   'Transparency is explained best in terms of how users make choice for themselves, how they are comfortable with the product, because if you don't get transparency into your policy, the consumers will start backing off, and you will suffer from it as a company'. (Microsoft)

This reliability and trust through transparency is built over time. As Google pointed out, people are 'just starting to understand Internet, how it all works'.

2. *Accountability as good governance practice*

All respondents spoke of transparency as a 'good' or 'right' thing to do, as part of their accountability practices both with the users whereby the latter have an opportunity to hold companies accountable on handling their data in relationships with the state:

"…transparency for us in that sense is about trying to lift the lid a little, or at least demonstrate to users what we do with their data" (Yahoo)

and with the governments whereby companies are legally compliant with the local regulator:

'We as a company recognise that government and law enforcement agencies have a legitimate interest in maintaining law and order, and in particular serious criminal activities' (Facebook)

3. *Privacy as a human right*

Respect of privacy as a human right is deemed as an instance of 'best practices', set out by GNI inter alia as one of the key values for ICT companies. Respondents mostly view transparency as helpful but not exclusive in securing users' privacy:

'.. you need to protect personal information, you can't solve that by transparency alone, there has to be an active respect of the fundamental principles of privacy and data protection' (Yahoo)

Facebook mentioned the need to balance ‘the legitimate expectation of the public and the government that they should be able to maintain law and order to investigate crime and deter crime’ against the privacy of individuals.

The difference in expectations around privacy in different countries and parts of the world was pointed out by Yahoo and Facebook. The interviewee from Yahoo highlighted the ‘transatlantic divide’ whereby European users are much more comfortable with the governments accessing their private data while the opposite is more characteristic of the US where there is less anxiety about businesses having this access.

In terms of GNI standards on transparency and respect of human rights, the Yahoo respondent admitted that the company has been ‘lagging behind on transparency relationships with law-enforcement agencies’, while ‘the expectations bar was raised by the emergence of transparency reports’.

4. *The role of media*

Facebook mentioned among the goals of being transparent the need to influence ‘how the media talk about these issues’: ‘We also seek to use our engagement with the media to tell our positive and constructive story about these issues’.

Microsoft remarked that it’s useful to have a public debate around transparency now to get the message to the audience, since ‘there’s been a lot of talk but not enough media reporting what the internet companies are saying’.

It is important that respondents are aware that ‘there won’t be transparency automatically from the industry - it’s more about people being aware of their rights and the law’ (Microsoft). The transparency efforts can only be meaningful is there’s a ‘degree of understanding’ (Facebook) on the user side. All respondents indicated the goal to ‘spread the message’ but found it difficult to cite any specific internal tool to measure user understanding apart from measuring the amount of clicks/time spent on a relevant page and feedback forms/forums. This revealed the limitations of transparency efforts as a one-way exercise in the absence of a measured response in changing attitudes.

On the other hand, there's a perception that while being concerned about privacy and surveillance, people have 'confidence that their data are of no interest to governments' (Yahoo). At the same time, long-term, and especially in the wake of the NSA leak, the companies expect more interest, sensitivity and attention to the topic which is no more niche and could translate in the long run into deeper reputational risks for the companies interviewed as well as for other players in the sector.

Both Microsoft and Facebook pointed out the freedom of the users 'to switch off and go', since 'there is no contract' (Facebook) if their confidence is undermined by failure in the company's transparency over time. However, Yahoo admitted, in relation to the NSA leak scandal in particular, that although there's a lot of suspicion towards cloud services, people won't stop using them, especially in the UK: 'We live in a country where significant amount of people have never changed their electricity or gas supplier or broadband provider'. This difficulty of switch, better seen over time, is recommended for future studies in this context, since the network effects and the relative oligopoly of the major ICT market services providers make it increasingly difficult.

Finally, all companies signed up to safeguarding their users' privacy with the caveat of legal liability to provide certain data to the governments, while in certain cases (US) not being able to be completely transparent because of gag-orders, which some of them went to fight in court ("Google's Motion for Declaratory Judgment," 2013). It is an important limitation to keep in mind as we move on to the discussion of the transparency reports as a specific form of transparency policies of ICT companies.

Companies’ vision of TR as a form of accountability and the rationale for its publication

It came clear in the interviews with Microsoft, Yahoo and Facebook, that when conceptualising transparency reports, companies tend to adopt the format introduced by Google as a role model, and expect their peers to follow suit both in form and content.

1. Microsoft’s report, first launched in March 2013 and called ‘Law Enforcement Requests Report’, focuses exclusively on user data disclosure requests and is also released every six months. The respondent said that the company tried to learn as much as possible from the experience of its peers.

   Facebook at the moment of the conversation in August 2013 had only made public the data on the US ‘for very specific reasons related to PRISM story’. Apart from saying that the possibility of issuing a transparency report is ‘under active consideration’ within the company, the interviewee could not share more detail but pointed out, however: ‘it would be reasonable to expect that we’d look at other companies – how they’ve done it in formulating their transparency reports if we want to do one’[7].

   Yahoo in a public statement (Yahoo, 2013) reiterated in the interview made a one-off announcement of the requests it received in the US between December 1, 2012 and May 31, 2013 and made clear its intention to publish a transparency report on law enforcement in summer 2013. The interviewee said it would also be biannual and would look exclusively at lawful access issues statistics. The design could not be revealed during the talk.

2. All the companies see the TR practice as an instance of ‘good governance’ - as a ‘useful tool’, ‘a special effort’, encouraged by many stakeholders: user expectations, peer group, internal demand from people in the company who care about these issues and NGOs and

[7] The data are discussed as obtained from the interview where the respondent could not talk about the timing of the release. Facebook’s Global Government Requests report was issued on 27 August 2013 and its design confirms the information obtained from the interviewee.

civil society groups like GNI. Its push was especially palpable, as the emergence of the TR has generally raised the bar in accountability practices, and provided a sort of road map for developing corporate ethics for the ICT companies dealing with user data. Google's interviewee praised the efforts of the other companies and expressed confidence that 'it will become increasingly important for the governments and companies to be open about how they access the information online'. Contrary to one of the interviewees' point TR is still 'of salience to only a very small group of people', 'the audience it addresses is a very specialist one', Google remarked that the audience of the TR increases and changes with the release of new features.

3. There is still a perceived low level of user understanding of the legal environment for the services, while differences among countries' jurisdictions may be significant in terms of the variety of local regulations which can be put to use to lawfully access user data. There are more industry expectations about the allowed content and functionality of TR over time to bridge this understanding gap. Microsoft and Yahoo remarked that TR should be and will be improved over time, in particular, include more data. Google said that it is a long project involving constant learning about what other issues it can inform people on with more data; the company treats it also as a technical challenge to increase data visualisation and interactivity of the report over time.

With these goals in mind, TR allows companies to push for relevant regulation change. For Google the goals of the TR 'range from raising general awareness to being able to engage in legislative reform if that were needed'. To achieve this, the companies are lobbying the governments for more attention to the issue of citizens' privacy, and TR is seen as a useful tangible product to operationalise the multi-stakeholder debates at different levels, which 'engage NGOs, consumer representatives, governments, and pursue the discussion about where social values are' (Microsoft). For example, all four companies are currently lobbying an update to the US Electronic Communication Privacy Act dating back to 1986 (Forensicon, 2013): 'the law should keep up, the degree of data protection that people have offline should be translated online' (Google).

The described above shared features shape out TR as an ICT transparency standard format of accountability. This ‘industry norm’, as highlighted by Yahoo in the interview, offers a bigger picture across various companies as well as degree of *comparability*, very useful for organisations like the GNI, which perform formal audit of the companies on their user data disclosure transparency. Besides, increasing comprehensiveness and standardisation of TR is an advantage in policy discussions. ‘It makes our life a lot easier, particularly when we have the amplified effect of the NGOs and civil society groups <…> that creates the context for the debates that we have’. (Yahoo)

The effect of the NSA surveillance leak on the approach to transparency policies and/or the transparency report in the companies which featured in the scandal

1. The NSA leak event and the public debate around provided a good testing ground for the role the transparency reports could play in further development of the public policies and defense of the right to privacy in general. All the respondents made a point of reiterating the official stances of their respective companies that none of providing direct access to users’ data to the governments.

   The interviewees stated that in the wake of the scandal, transparency reports remain a useful tool of audit despite the lack of granularity of data in the TR with the secret service requests not allowed to be published separately:

   ‘I think the data that is being disclosed is always going to be useful. And it becomes even more useful once you’ve got trends and a degree of comparability’. (Yahoo)

   Google pointed out that in the wake of the scandal its TR ‘is a wonderful way for us to get more attention on the issue because we are able to show why it’s important to be transparent’. Moreover, the interviewee made a special point that the leak made more ICT companies speed up their release of transparency reports and welcomed this development, linking this directly to the fact that ‘trust and accountability are a critical part of being an Internet business'. Other companies did not voice the same correlation but it was implicit (e.g. Facebook releasing their report shortly after publicly pledging to consider it).

2. The NSA leak offered the companies leverage to push for change in legislation regarding transparency about user data disclosure to share publicly more complete information about how they handle national security requests for customer information (Arthur, 2013)[8]:

   'The other reason to be transparent is that we can help change at the governmental level' (Yahoo)

   However, Microsoft expressed doubts if the debate will lead to actual legislative changes in a meaningful way, which is to be seen over time, and as Yahoo pointed out 'we're all here for the long term'. Still, in terms of setting a precedent, the case is illustrative of the way corporate lobby can operate. As Google remarked, there wasn't too much resistance from the authorities, indicating a level of readiness for more constructive dialogue between the public and private sector on the topic of accountability about user data.

3. The interviewees highlighted the fact that transparency should not come only from the private sector but the governments should also publish their own transparency reports on the data requests they make. Facebook cited this as one of the reasons the company has not so far released its TR:

   '… we chose for the moment not to be transparent about how much we do this in different countries, partly because transparency should lie with governments.

[8] This demand was partially satisfied: companies were allowed to publish aggregate numbers of secret FISA requests as part of their reports (Budish, 2013), and Facebook, in particular, took up this opportunity to publish its first aggregate numbers (Ullyot, 2013) shortly after the leak including both FISA and non-secret criminal requests. The deal was not accepted by Google as the one adding no clarity into the reporting data.

> Governments should be transparent about how many requests they make of different kinds of companies' (Facebook).
>
> 'The challenge now, and the thing we're trying to use all this information for, is to get the governments to do the same thing' (Yahoo)
>
> In particular, Yahoo highlighted its successful lobbying against the UK Communications Data Bill, which the company felt 'was detrimental both to the businesses of the Internet companies but more importantly the privacy interests of users' and remarked that it's easier to make those arguments 'if we are transparent about our relationship with the UK government'.

As can be seen, apart from shaping out as an ICT industry good governance standard and a 'competitive differentiator' (e.g. Microsoft's advertising campaign on privacy which ironically coincided with the leak), TR has assumed the role of a policy lever in negotiations with the governments underpinned by the association with civil society groups. As was perceived from the interviews, the NSA leak sped up its evolution as an accountability format by incentivising more companies to employ this tool in relationship with the governments. It also foregrounded the debate around privacy and surveillance and activated a public debate by asking difficult questions both the public and the private sector about what they have done and are doing to protect the citizens' rights of privacy.

As the companies believe that transparency about the users' data requests should lie primarily with the state, they also push the governments for more transparency, since in a way the private sector has been substituting the governments in these social contract accountability efforts. As set out by the Yahoo respondent:

'It is our general view – and I think of everyone in the GNI – that it is the responsibility of states to protect their citizens and to protect human rights, to implement international human rights standards. It is our job as companies to respect human rights. And encourage governments to do so. We are in this curious position where we might have to assume that some of them [standards] protect responsibilities that governments have chosen not to follow'.

However, this self-assumed responsibility effectively places enormous power in the hands of the companies which now step in to handle some of the governmental functions as well as to decide on the lawfulness of the incoming requests. This takes us back to the initial argument around the power position of the major ICTs as data aggregators: as discussed above, this is a powerful capacity in the framework of 'social contract' with the users. The long term implications of these developments – both for the ICT industry and the legal landscape around it are yet to be seen from the efficiency of the companies' lobbying efforts for more transparency.

A COUPLE OF LAWSUITS LATER

The study carried out in summer 2013 and presented above has been useful in investigating the stance of the private sector on the transparency issues and bring out their perceived value of the TR. With the limitations of corporate bias and ethical restrictions, it is a still useful starting point for a broader research, as a true link-up with the public is apparently missing, as seen from the interviewees' comments on the narrow TR audience and the lack of internal instruments to gauge the impact on the audience. As stated by the companies, users do not seem to be abandoning the platforms or services of the companies involved almost a year after the leak. One of the respondents argued that 'the whole Snowden affair highlighted the reality of what people already knew was going on, and the event just highlighted the scale of the issue'. However, certain chilling effect is certainly present in specialist communities[9].

Nevertheless, it can be safely stated that the trend suggested in the study, which highlighted the evolution of TR as an ITC accountability standard, has been proved in the following months. As has been remarked earlier, Facebook did publish its first Global Government Requests Report on 27 August 2013, Yahoo came up with its first Transparency Report on 6 September 2013. On 7 November 2013 Apple followed suit, for the first time implementing a "warrant canary" against gag orders by stating that "Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us." Finally, in winter 2014 first telecom operators joined the effort: American Verizon, AT&T, Australian Telstra etc, which was much hailed by the Internet companies. Without going into detail about the content and comparability of these products, it can be stated that their formats and principles are very similar and continue the pattern introduced by Google.

It's hard to assess the popularity of the reports with the users. But more importantly, TR are certainly useful in assessing the growth of the political power of corporate lobby as they reflect the gradually increasing granularity in data reporting – something that the companies have been pushing for.

[9] http://www.pen.org/chilling-effects

First step was made in March 2013 even before the revelations: the US government allowed publishing aggregate numbers of FBI's National Security Letters, special type of request for metadata which normally imposes a gag order on the receiver.

Shortly following the leak in early June the US authorities granted the permission to the Internet companies to disclose the amount of the secret national security requests they get (FISA requests) but only if combined with the rest of the criminal, non-secret, requests. Facebook, Yahoo, Microsoft and Apple jumped at the offer while Google argued that this would not add much sense to the final dataset. Later it was joined by the rest of the companies in the strong push for more meaningful data disclosure to the users, and coupled with a lawsuit which Google and Microsoft filed against NSA for its spying activities, it was finally, yet partially, satisfied only in January 2014. The data on secret requests can't be itemised beyond the band of thousands of requests from the FISA court, besides they can only be disclosed with a 6-month delay.

Most recently, on 1 May the White House published its Big Data review, which features a long lobbied for recommendation that Congress should amend ECPA [the Electronic Communications Privacy Act] "to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world" and advance the Consumer Privacy Bill of Rights because "consumers deserve clear, understandable, reasonable standards for how their personal information is used in the big data era".

What looks like a steady progress of the corporate lobby, is taking baby-steps towards more transparency in user data handling by the state agencies. Aggregate numbers might not be very informative but as more companies start publishing their statistics on user data requests, it becomes easier to compare datasets and have a better picture of the data mining strategies across platforms. It's hard to expect full openness about these activities for obvious security reasons but the increased demand for more transparency will keep this balance very flexible. And it's arguably reasonable to expect the ICTs to push for more as it would win them trust points with the users given the increased awareness of risks to privacy. The recent successful audit by the

GNI of Google, Microsoft and Yahoo has proclaimed their compliance with the human rights principles which strengthens their reputation.

On the other hand, the hacking capacities of the security agencies across the world should not be discounted in this context. The mere ability of tapping into the systems at the code level for data interception might seem to be rendering the whole transparency reporting exercise meaningless, since those inquiries would never appear on any dataset. However, its very existence apparently allows the US government in particular to make concessions in public reporting of its activities, declassifying bigger amounts of data. It's yet to be seen how far this race for transparency, offset by more surveillance techniques, goes, but it would be naïve to expect special services across the world to scale down the latter significantly. The pockets of geopolitical instability will always give enough ground to keep them running, it might be hoped that at least these techniques could be eventually refined technologically to curb the dragnet surveillance.

Notably, we are discussing here the legislative advances in the US due to corporate lobby, as most mentioned companies are headquartered in the US or have most operations there. In the UK, where GCHQ, the UK NSA counterpart, and other security services also faced public interrogation and gave evidence before Parliament's intelligence and security committee, basically defending their own surveillance practices, no tangible response has been made by the Parliament in almost a year's time since the leak.

It was pointed out by the interviewees that while the UK government has a lot to handle in the pre-electoral period, it gives scope for a multi-stakeholder approach, whereby a solution could be worked out by a wide coalition of civil society, different politicians from different parties and industry, academia to strike a balance between transparency, privacy and investigative tools for law enforcement. 'Ideally you want somebody to come up with a package of some extra capability with greater transparency by government. I think a package like that formulated by a civil society group could carry weight and get cross-party support as well as from the industry' (Facebook).

However, so far key lobbying in the UK comes from the civil society sector advocating for the protection of citizens' privacy against excessive data collection and profiling, which culminated in a joint lawsuit against GCHQ in ECHR by campaign groups Big Brother Watch, the Open Rights Group, English PEN and the German internet activist Constanze Kurz. Regardless of the outcome of this case, its filing is sure to keep the topic on the agenda for a long while. The only policy-maker call for a more articulate investigation of the GCHQ practices under RIPA legislation, a review of the legislative framework, which allowed for cooperation with NSA in cables interception, and notably more granularity in the UK data requests reporting for companies was made by LibDem leader Nick Clegg in March 2014.

In the long run, the validation of the ICT public policies, and TR in particular, is predicated on keeping up the public debate around surveillance and privacy by engaging as many stakerholders as possible. Now that the issue of user privacy is no longer niche and can hardly be played down back to this niche, the only feasible strategy is to keep the public aware of the efforts undertaken to inform them on all the caveats of using online services. And high expectations are placed with international human rights organisations like the Council of Europe, and civil society groups to help steer the debate about privacy and data protection laws and represent the citizens' interests by asking the questions which the general public do not necessarily grasp.

Therefore, privacy in the context of compliance with state authorities' requests seems to be effectively an area where the companies involved welcome new legislation equally binding both the private sector and the governments to be more transparent. This *quasi-self-regulation* indicates a significant rise in the ICTs power boosted by an event which paradoxically had all chances to undermine user trust in their services marred by privacy failure. TR evolved as one of the tools which 'upgraded' the 'social contract' between the private sector and its customers. Moreover, it offered ICTs the bargaining ground with the states as intermediaries and holders of user data.

CONCLUSION

This paper has looked at the major ICT companies' transparency policies development and the shaping of transparency report (law enforcement report), with special attention to the NSA surveillance scandal as setting the scene for a broader debate on the issues of privacy as well as putting a spotlight on the private sector transparency in handling users' data.

The theoretical research into corporate transparency practices and the concepts underlying the emergence of transparency reports were tested through semi-structured interviews with relevant representatives of the four companies (Google, Microsoft, Yahoo and Facebook) which signed up to the values of privacy through self-regulation in the framework of the GNI organisation. This membership in its own right is seen as an incentive to come up with some form of open accountability on sharing these data with the authorities in respect of the right for privacy. On the other hand the mentioned event helped to highlight the current transparency policies and prove the following:

- Transparency is conceptualised by the interviewees predominantly in terms of user trust, best practices and good governance, and respect of right of privacy;
- Transparency report is increasingly treated by the companies as an industry standard of accountability on handling data requests from the governments: as they decide on disclosing this information, the format of preference tends to be designed along the lines of the ones previously issued by other companies.
- The NSA surveillance leak helped activate the lobbying potential of transparency policies and transparency reports in particular by offering the companies leverage in public negotiations with the authorities about the amount of information that can be disclosed to the public, relevant legislative change, while at the same time pushing for more transparency on the state side. All these help boost a favourable image of the companies also empowering them in the regulatory field.

This study attempted a brief investigation of public policies development that is taking place at the major Internet corporate players (Google, Microsoft, Yahoo and Facebook) in the intensified public debate around privacy which has been triggered by the NSA leak story. While it does not seek to be comprehensive or strictly representative, it might give a launch pad for further research into transparency policies as well as, and perhaps increasingly more important, consumer vision of them in relation to their own perception of privacy and security of their data; finally, the media representation of the event itself as well as its interpretation by the stakeholders would give a better understanding of the public sphere context for further development of these debates which seem to be here to stay.

Bibliography

Akrivopoulou, C., Garipidis, N., Colburn, B. C., Nolin, J., Giannakaki, M., Bülow, W., . . . Daly, A. (2012). *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies*: Information Science Reference.

Arsenault, A., & Castells, M. (2008). Switching Power: Rupert Murdoch and the Global Business of Media Politics A Sociological Analysis. *International Sociology, 23*(4), 488-513.

Arthur, C. (2013). US tech companies appeal to Obama over secret demands for user data. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2013/jul/18/tech-companies-appeal-barack-obama-surveillance

Bennett, A., & George, L. (2005). *Case studies and theory development in the social sciences* Cambridge, Mass.: MIT Press.

Bennett, C. C. J., & Raab, C. D. (2003). *The governance of privacy: Policy instruments in global perspective*: Ashgate Publishing.

Bennett, C. J. (2010). International Privacy Standards: can Accountability be Adequate? *Privacy Laws and Business International, 106*, 21-23.

Bentham, J., & Bowring, J. (1843). The works of Jeremy Bentham (Vol. 7): W. Tait.

Berger, A. A. (1998). *Media research techniques*: Sage.

Berry, J. M. (2002). Validity and reliability issues in elite interviewing. *PS-WASHINGTON-, 35*(4), 679-682.

Birnhack, M. D., & Elkin, N. (2008). The Invisible Handshake: The Reemergence of the State in the Digital Environment. *Tel Aviv University Legal Working Paper Series*, 54.

Boyatzis, R. (1998). *Thematic analysis : coding as a process for transforming qualitative information* Thusand Oaks, CA Sage Publications.

Brin, D. (1999). *The transparent society: Will technology force us to choose between privacy and freedom?* : Basic Books.

Brown, I., & Marsden, C. T. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*: The MIT Press.

Budish, R. (2013). Tech firms should be allowed to publish more data on US surveillance. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2013/jul/18/tech-firms-letter-nsa-surveillance-transparency

Campbell, J. E., & Carlson, M. (2002). Panopticon. com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586-606.

Carey, P. (2009). *Data protection: a practical guide to UK and EU law*: Oxford University Press, Inc.

Council of Europe Convention on Cybercrime (2001).

Dann, G. E., & Haddow, N. (2008). Just doing business or doing just business: Google, Microsoft, Yahoo! and the business of censoring China's Internet. *Journal of Business Ethics, 79*(3), 219-234.

Dexter, L. A. (1970). *Elite and specialized interviewing*. Evanston: Northwestern University Press.

Donaldson, T. (1982). *Corporations and morality*: Cambridge Univ Press.

Dunfee, T. W. (2009). Business ethics and extant social contracts. *Business Ethics Quarterly*, *1*(1), 23-51.

Forensicon. (2013). ECPA Amendment Could Require Warrants to Obtain Email. Retrieved from Forensicon website: http://www.forensicon.com/forensics-blotter/ecpa-amendments-warrants-to-obtain-email/

Fort, T. L. (2001). Ethics and governance: Business as mediating institution. *OUP Catalogue*.

Foucault, M. (1979). Discipline and Punish: The Birth of the Prison. New York: Vintage.

Fromholz, J. M. (2000). European Union Data Privacy Directive, The. *Berk. Tech. LJ, 15*, 461.

Gandy Jr, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries*: Westview Press, Inc.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. Oxford; New York: Oxford University Press

Google's Motion for Declaratory Judgment. (2013). *The Washington Post*. Retrieved from http://apps.washingtonpost.com/g/page/business/googles-motion-for-declaratory-judgment/238/

Google. Transparency Report. Retrieved from http://www.google.com/transparencyreport/

Goold, B. J., & Neyland, D. (2013). *New Directions in Surveillance Privacy*: Willan.

Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link

Guagnin, D., Hempel, L., Ilten, C., Kroener, I., & Neyland, D. (2012). *Managing privacy through accountability*: Palgrave Macmillan.

Gunningham, N., & Rees, J. (1997). Industry self-regulation: an institutional perspective. *Law & Policy, 19*(4), 363-414.

Hakim, C. (2000). *Research Design: Succesful Designs for Social Economics Research*: Routledge.

Hölmstrom, B. (1979). Moral hazard and observability. *The Bell Journal of Economics*, 74-91.

Hood, C., & Heald, D. (2006). *Transparency: the key to better governance?* Oxford; New York Oxford University Press for The British Academy.

Locke, J. (1947). *Social contract: essays by Locke, Hume and Rousseau*: Oxford University Press.

Lyon, D. (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*: Routledge.

MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for Internet freedom. *Politique étrangère, 50*, 2.

Mansell, R. (2007). *Handbook of Information and Communication Technologies*: Oxford Handbooks Online.

Microsoft. Law Enforcement Requests Report. Retrieved from http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev., 79*, 119.

Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights (2003).

Raab, C. (2006). Privacy Protection and ICT: Issues, Instruments and Concepts: Oxford: Oxford University Press.

Recommendation of the Committee of Ministers to member States on the protection of human rights with regard to search engines (2012).

Richards, D. (1996). Elite interviewing: approaches and pitfalls. *Politics, 16*(3), 199-204.

Ruebhausen, O. M., & Brim, O. G. (1965). Privacy and behavioral research. *Columbia Law Review, 65*(7), 1184-1211.

Silverstone, R., & Haddon, L. (1996). Design and the domestication of ICTs: technical change and everyday life. *Communicating by Design: The Politics of Information and Communication Technologies*, 44-74.

Sinclair, D. (1997). Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy, 19*(4), 529-559.

Tansey, O. (2007). Process tracing and elite interviewing: a case for non-probability sampling. *PS: Political Science & Politics, 40*(04), 765-772.

Twitter. Transparency Report. Retrieved from https://transparency.twitter.com

Ullyot, T. (2013). Facebook Releases Data, Including All National Security Requests. Retrieved from http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests

van den Hoven, J. (2008). Information technology, privacy, and the protection of personal data. *Information technology and moral philosophy*, 301-322.

Who Has Your Back? (2013). Retrieved from https://www.eff.org/who-has-your-back-2013

Yahoo. (2013). Our Commitment to Our Users' Privacy. Retrieved from http://yahoo.tumblr.com/post/53243441454/our-commitment-to-our-users-privacy

Yin, R. K. (1994). Case study research: design and methods. 1994. *Thousand Oaks, CA*.