Increasing Resilience in Surveillance Societies

European responses to the Snowden revelations: A discussion paper

David Wright[1] and Reinhard Kreissl[2]

December, 2013

[1] david.wright@trilateralresearch.com
[2] reinhard.kreissl@irks.at

CONTENTS

1 NATURE OF THE ADVERSE EVENT

Beginning in early June 2013, *The Guardian*, *The New York Times* and other media have reported in unprecedented detail on the surveillance activities of the US National Security Agency (NSA) and other intelligence services, based on documents leaked by Edward Snowden, an employee of defence contractor Booz Allen Hamilton at the NSA. The leaked documents have revealed how extensively the intelligence agencies have been surveilling whole populations as well as political leaders, UN officials and businesses, such as Google, Petrobas and many others.

The leaks can be described as an adverse event for the intelligence agencies because the public now knows that the NSA has seriously infringed their privacy, ostensibly to hunt for terrorists, but the public now knows that the mass and targeted surveillance has served to give national industries an economic advantage over their competitors. The surveillance has served other purposes too. The intelligence agencies have kept an eye on dissidents and civil society organisations who might disrupt social order. The leaks have been an adverse event for political leaders such as US President Barack Obama and UK Prime Minister David Cameron because the leaks have embarrassed them and strained their relations with supposed allies, such as German Chancellor Angela Merkel, European parliamentarians, Brazilian President Dilma Rousseff, Mexican President Enrique Peña Nieto and others. The leaks have been an adverse event for Verizon, AT&T, Google, Facebook and other businesses who have given access to their networks to the NSA, the public realisation of which has undermined public confidence in these companies and the adequacy of the security of their personal data held by these companies. The leaks have also been an adverse event for the public who have been shocked and outraged that the intelligence agencies have so extensively invaded their privacy.

This chapter explores the European institutional, judicial, legal, societal, economic and media responses to the so-called Snowden revelations. While the emphasis of this paper is on the European impacts, the paper also references some non-European responses where they seem to be particularly noteworthy. It references only a selection of the many reports based on the leaked documents and only up to the end of November 2013, so it is, of course, by no means comprehensive, but enough evidence is presented here to allow us to draw some conclusions about the impacts of the Snowden revelations. While the revelations have been a shock to many, if not most people, they have had some unintended, positive impacts, which we identify. The paper concludes with some observations with regard to the failure of oversight, the privacy-security trade-off paradigm and the breakdown of open democracy. It also poses some unanswered questions and makes some recommendations on protecting privacy in a surveillance society.

On 5 June 2013, *The Guardian* published its first exclusive, revealing that the US Foreign Intelligence Surveillance Court ("the FISA court") had granted a secret order forcing Verizon, one of the largest of US telecom companies, to give the NSA access to the phone records of millions of Americans. The NSA would thus have information on all landline and mobile telephone calls in the Verizon network, both within the US and between the US and other countries. *The Guardian* said the Obama administration was collecting the communication records of millions of US citizens, regardless of whether the people were suspected of any wrongdoing.[3] Following the 11 Sept 2011 attacks, the Bush administration had greatly

[3] Associated Press, "Obama administration collecting huge number of citizens' phone records, lawmaker says", 6 June 2013. http://www.washingtonpost.com/politics/federal_government/report-government-secretly-scooping-

expanded surveillance of the US population, and the Obama administration has expanded that surveillance even more.

The NSA was collecting "metadata" not only from telecom companies, but also from Internet social networks. On 6 June 2013, *The Washington Post* reported the existence of a secret programme code-named PRISM, under which the NSA was collecting e-mails, Internet phone calls, photos, videos, file transfers and social-networking data from Google, Facebook, Apple, YouTube, Skype, Microsoft and PalTalk.[4] According to NSA watcher James Bamford, the agency runs its intercepts of millions of telephone calls and e-mails through powerful computers that screen them for particular names, telephone numbers, Internet addresses, and trigger words or phrases. Any communications containing flagged information are forwarded by the computer for further analysis.[5]

On 9 June, Edward Snowden revealed that he had leaked the documents.[6] He justified his actions by saying that he did "not want to live in a world where everything I do and say is recorded". He said that the public, not spies and secret courts, ought to decide whether the mass surveillance was right. According to *The Guardian*, "he chose to reveal himself to avoid hiding behind the secrecy he abhors".[7]

On 21 June 2013, *The Guardian* reported that the UK's Government Communications Headquarters (GCHQ) had secretly gained access to the cable networks that carry the world's phone calls and Internet traffic and had been "processing vast streams of sensitive personal information which it was sharing with the NSA without any form of public acknowledgement or debate". The GCHQ programme was codenamed TEMPORA.[8]

On 9 August 2013, President Obama said that "The people at the NSA don't have an interest in doing anything other than making sure that ... we can prevent a terrorist attack." Yet leaked documents soon showed that the NSA had also been spying on its "allies", including European Union offices, the United Nations (including UN Secretary General Ban ki-moon) and the International Atomic Energy Agency. The NSA has infiltrated the EU mission to the UN in New York and the EU embassy in Washington. The documents revealed that the NSA had secret eavesdropping posts in 80 US embassies and consulates around the world, internally referred to as the "Special Collection Service" (SCS) and jointly operated with the

---

up-phone-records-of-millions-of-verizon-customers/2013/06/05/e820deb8-ce57-11e2-8573-3baeea6a2647_story.html

[4] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[5] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

[6] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[7] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[8] MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, 21 June 2013. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

CIA.[9] On 30 October, *The Washington Post* reported that the NSA had secretly broken into the unencrypted fibre-optic cables that carry data between Google and Yahoo's data centres around the world, without the companies' knowledge.[10] In other words, the NSA has had both legal and illegal access to Google's networks. The NSA's principal tool to exploit the data links is a project called MUSCULAR, operated jointly with the GCHQ. Google and Yahoo presumably have concerns that reports that the NSA has intercepted data between their servers will erode people's trust in the companies' ability to keep their data confidential.

While the Snowden revelations created a huge media storm, they were not entirely novel. More than a decade before, news of the secret Echelon programme came to light and was the subject of an inquiry by the European Parliament.[11] The FBI had been operating a programme called Carnivore authorised by the 1994 Communications Assistance for Law Enforcement Act (CALEA) which obliged telecom operators to provide it access to their communications networks. However, what made the Snowden revelations different was the scale of the NSA's spying on ordinary citizens who had never committed any crime, nor even been suspected of having committed any crime. The furore was compounded further because the surveillance had been conducted under secret authorisation. Undoubtedly, the scale of surveillance is a function of new technologies. Had the Internet existed at the time of Echelon, the intelligence agencies may well have indulged in much greater spying in those days too. Thus, it could be argued that what has changed is capability of the techno-infrastructure of communication rather than a presumed increase in the intelligence services' desire to spy on citizens. More likely, the NSA et al. take whatever they can get and if the technology provides new opportunities, they take them.

Thus, the Verizon story was just the tip of a gigantic surveillance iceberg. While some people were aware that the NSA and other intelligence agencies were monitoring telephone calls and Internet use[12], the sheer scale of the NSA surveillance was breath-taking. It seemed that the NSA, with some help from the GCHQ, was monitoring virtually everyone's telephone calls and Internet usage.

2 INSTITUTIONAL RESPONSE

A few days after the Snowden revelations began, President Obama met President Xi Jinping of China in southern California. Obama was going to complain about Chinese cyberattacks and spying, which had attracted a fair amount of media attention in the months (and even years) before Obama's meeting, but the huge media coverage of US spying completely

[9] Poitras, Laura, Marcel Rosenbach and Holger Stark, "Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[10] Gellman, Barton, and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", *The Washington Post*, 30 October 2013. http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?hpid=z1

[11] European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), 11 July 2001. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=EN

[12] James Bamford wrote extensively about NSA surveillance in his book *The Shadow Factory*, which was published by Anchor Books in July 2009, four years before the Snowden revelations. The blurb on the back cover of the book states that "In disturbing detail, Bamford describes exactly how every American's data is being mined and what is being done with it. Any reader who thinks America's liberties are being protected by Congress will be shocked and appalled at what is revealed here."

defocussed attention on Chinese spying. The fury over the extent of NSA surveillance has distracted US efforts at applying pressure on China to rein back its cyber espionage activities. Once the NSA revelations began, Chinese cyber surveillance disappeared from the front pages of newspapers.

On 8 June 2013, US Director of National Intelligence James Clapper issued a public statement acknowledging PRISM's existence, but stressing that it was lawful and operated under the auspices of the FISA court. Just three months earlier, in March 2013, Clapper had testified under oath before the US Senate where he said the NSA did not intentionally collect "any type of data at all" on millions of Americans. That turned out to be not true. Clapper later justified his response as the "least untruthful answer" he could give.[13] Amid revelations that the NSA does indeed collect large amounts of citizens' data and metadata, he subsequently apologised, saying his previous answer was "erroneous".[14]

The head of the NSA, Army Gen. Keith Alexander, also initially denied that the United States collected telephone and e-mail records directly from European citizens, calling reports based on leaks by Edward Snowden "completely false". Subsequent leaks showed that Alexander was also misleading the public and not being truthful.[15]

This section reviews a few of the key institutional responses to the NSA revelations, notably the fury they caused in Europe when it became apparent that the NSA was not only sweeping up the communications of ordinary citizens, but also targeting European and other leaders such as the Bolivian, Brazilian and Mexican presidents, supposedly close allies.

2.1 EUROPEAN FURY

After news of the NSA's PRISM programme became public, European lawmakers threatened to abandon data sharing agreements with the United States. Members of the European Parliament (MEPs) were described as "furious" that US authorities had been accessing their e-mails and other personal data from leading Internet companies. In a heated debate in the European Parliament, lawmakers complained that for a decade they had bowed to US demands for access to European financial and travel data and said it was now time to re-examine the deals and to limit data access. "We need to step back here and say clearly: mass surveillance is not what we want," said Green Member of the European Parliament (MEP) Jan Philipp Albrecht.[16]

Other members of the European Parliament said they would redouble efforts to strengthen a proposed EU-US data protection agreement in the field of police and judicial co-operation. Hannes Swoboda, leader of the socialist group in the Parliament, told *The Financial Times*: "With all the information we've found out in recent days about how easily the US spies on people's private data I think it will be difficult for the Americans to oppose a strong data protection agreement. This issue is very critical for us in Europe … There will be growing

[13] Rusbridger, Alan, "The Snowden Leaks and the Public", *The New York Review of Books*, 21 November 2013 issue. http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/?pagination=false
[14] *The Economist*, "Sense, sensibilities and spying", 6 July 2013. http://www.economist.com/news/international/21580485-edward-snowdens-revelations-about-american-espionage-have-riled-europeans-so-has?zid=301&ah=e8eb01e57f7c9b43a3c864613973b57f
[15] Ball, James, "Separate draft memo proposes US spying on 'Five-Eyes' allies", *The Guardian*, 20 Nov 2013. http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data
[16] Davenport, Claire, "U.S. PRISM spying programme rattles EU lawmakers", Reuters, 11 June 2013. http://in.reuters.com/article/2013/06/11/usa-security-eu-idINL5N0EN1D4201306112

resistance against an agreement with the US unless there are some clear guarantees from their side that our European principles of data protection are respected."[17]

European Commission Vice President Viviane Reding also said that "Programmes such as PRISM… potentially endanger the fundamental right to privacy and to data protection of EU citizens." EU officials demanded "swift and concrete answers" from the US government about its spying programs.[18] Following revelations of GCHQ's TEMPORA surveillance programme, Ms Reding also sent a letter to UK foreign minister William Hague asking for details. She asked if TEMPORA is restricted to national security, if snooping is limited to individual cases or is in bulk, if the data is shared with third countries like the United States, and if UK and EU citizens have any legal recourse when it comes to their data.[19] Five months later, she still had not received a response.

2.2 MEMBER STATES: US MASS SURVEILLANCE IS "MONSTROUS"

The fury at European level was mirrored at the level of EU Member States too. Peter Schaar, German Federal Commissioner for Data Protection, said, "The U.S. government must provide clarity regarding these monstrous allegations of total monitoring of various telecommunications and Internet services." He added that "Statements from the US government that the monitoring was not aimed at US citizens but only against persons outside the United States do not reassure me at all."[20]

French prosecutors announced that they were conducting a preliminary investigation into whether the NSA had violated French law by secretly collecting personal data.[21] The espionage is "absolutely unacceptable", inveighed French Foreign Minister Laurent Fabius after it became known that the French embassy in Washington was also on the surveillance list.[22]

The UK's Information Commissioner's Office (ICO) said, "There are real issues about the extent to which U.S. law enforcement agencies can access personal data of UK and other European citizens. Aspects of U.S. law under which companies can be compelled to provide information to U.S. agencies potentially conflict with European data protection law, including the UK's own Data Protection Act." The ICO also said it "has raised this with its European

---

[17] Watt, Nicholas, "Prism scandal: European commission to seek privacy guarantees from US", *The Guardian*, 10 June 2013. http://www.guardian.co.uk/world/2013/jun/10/prism-european-commissions-privacy-guarantees

[18] Bracy, Jedidiah, "NSA Leaks: EU-U.S. Tensions on the Rise, Europe Reacts", *The Privacy Advisor*, International Association of Privacy Professionals (IAPP), 13 June 2013. https://www.privacyassociation.org/publications/nsa_leaks_eu_u.s._tensions_on_the_rise_europe_reacts_roundup

[19] Nielsen, Nikolaj, "EU asks for answers on UK snooping programme", EUObserver.com, 26 June 13. http://euobserver.com/justice/120656

[20] EurActiv, "US data scandal deepens EU-US divide on privacy", 10 June 2013. http://www.euractiv.com/infosociety/us-data-scandal-deepens-eu-us-di-news-528437?utm_source=EurActiv%20Newsletter&utm_campaign=47551f8aa6-newsletter_daily_update&utm_medium=email&utm_term=0_bab5f0ea4e-47551f8aa6-245739993

[21] Associated Press, "French prosecutor opens probe into NSA surveillance program", published in *The Washington Post*, 28 Aug 2013. http://www.washingtonpost.com/world/europe/french-prosecutor-opens-probe-into-nsa-surveillance-program/2013/08/28/8f63d06e-0ff2-11e3-a2b3-5e107edf9897_story.html

[22] Poitras, Laura, "Marcel Rosenbach and Holger Stark, Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

counterparts, and the issue is being considered by the European Commission, who are in discussions with the U.S. government."[23]

But, as noted above, the NSA was not the only intelligence agency conducting surveillance outside its borders. German justice minister Sabine Leutheusser-Schnarrenberger commented that if reports about TEMPORA proved to be true, it would be "a Hollywood nightmare". She sent a letter to British home secretary Theresa May and justice secretary Chris Grayling asking if media reports were true.[24]

GCHQ had tried to reassure citizens that "GCHQ takes its obligations under the law very seriously." A spokesman added, "Our work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the Interception and Intelligence Services Commissioners and the Intelligence and Security Committee."[25]

UK Foreign Secretary William Hague also insisted that UK intelligence agencies practise and uphold UK law at all times. He said there are two acts of Parliaments governing the process of obtaining permission for the security services to eavesdrop, which require a signed warrant from the Foreign or Home Secretary, and must be "necessary, proportionate and carefully targeted". They are also subject to review by an independent commissioner to ensure permission is compliant with law.[26] Hague told MPs that British spies did not "indiscriminately trawl" through their citizens' e-mails or use foreign intelligence to bypass their own legal safeguards. "It has been suggested GCHQ uses our partnership with the United States to get around UK law, obtaining information that they cannot legally obtain in the UK," Mr Hague said. "I wish to be absolutely clear that this accusation is baseless."[27]

More recent disclosures belie the assurances from GCHQ and the government. An investigation by *The Guardian* and Channel 4 News discovered that GCHQ and the NSA reached an agreement in 2007 that allowed the NSA to access, analyse and store the phone, Internet and e-mail records of British citizens. Sir Malcolm Rifkind, chairman of the parliamentary Intelligence and Security Committee, told *The Guardian* that he would be

---

[23] Bracy, Jedidiah, "NSA Leaks: EU-U.S. Tensions on the Rise, Europe Reacts", *The Privacy Advisor*, IAPP. International Association of Privacy Professionals, 13 June 2013.
https://www.privacyassociation.org/publications/nsa_leaks_eu_u.s._tensions_on_the_rise_europe_reacts_roundup

[24] Nielsen, Nikolaj, "EU asks for answers on UK snooping programme", EUObserver.com, 26 June 13. http://euobserver.com/justice/120656

[25] Hope, Christopher, and Tom Whitehead, "British Intelligence watchdog flies to Washington to demand answers on snooping scandal", *The Telegraph*, 7 Jun 2013.
http://www.telegraph.co.uk/technology/internet-security/10107059/British-Intelligence-watchdog-flies-to-Washington-to-demand-answers-on-snooping-scandal.html

[26] Settle, Michael, "Hague tells MPs claims of illegal spying are baseless", *The Herald* [Scotland], 11 June 2013.
http://www.heraldscotland.com/politics/political-news/hague-tells-mps-claims-of-illegal-spying-are-baseless.21306152

[27] Warrell, Helen, and James Blitz, "David Cameron rejects claims GCHQ broke law over US Prism data", *The Financial Times*, 10 June 2013.
http://www.ft.com/cms/s/0/01d745fe-d1f0-11e2-b17e-00144feab7de.html#axzz2VsHkbdAE

seeking an explanation about the secret deal that appeared to allow the NSA to "unmask" personal data about Britons not suspected of any wrongdoing.[28]

2.3 FIASCO WITH THE BOLIVIAN, BRAZILIAN AND MEXICAN PRESIDENTS

Despite the hugely embarrassing revelations, the US has made no secret of its wish to capture Snowden. Indeed, the US has engaged European countries in its efforts to that end. In early July 2013, when there was a suspicion that Snowden might be on-board the plane carrying Evo Morales, the Bolivian president, on his way back home from energy talks in Russia, his plane was forced to land in Vienna. France, Italy, Portugal and Spain were accused of withdrawing permission for the plane to pass through their airspace. However, Snowden was not on board. The Bolivian foreign minister, David Choquehuanca, said: "We don't know who invented this lie. We want to denounce to the international community this injustice with the plane of President Evo Morales." Bolivian defence minister Ruben Saavedra described forcing the plane down as a "hostile act by the United States state department which has used various European governments". Morales finally left Vienna after spending 12 hours at the airport and after Austrian officials confirmed that Snowden was not on board. Undoubtedly, Morales' flight was disrupted because he had said in a Moscow television interview that Bolivia would look favourably upon an asylum request from Snowden.[29] One can assume European complicity in refusing to let the Bolivian president's plan overfly their territory did nothing to endear Europe to Bolivia.

The US has angered other Latin American countries in addition to Bolivia. When she discovered the NSA has been monitoring her communications, Brazilian President Dilma Rousseff cancelled a planned trip to Washington in October and condemned the NSA's espionage in a blistering speech to the United Nations General Assembly. Ironically, when Rousseff took office in early 2011, one of her goals was to improve relations with Washington, which had cooled under her predecessor, the popular former labour leader Luiz Inácio Lula da Silva.[30]

Leaked documents showed that the NSA had also been systematically eavesdropping on the Mexican government for years. In September 2013, Brazilian television network TV Globo revealed that the NSA monitored then-presidential candidate Enrique Peña Nieto and others around him in the summer of 2012. Peña Nieto, now Mexico's president, summoned the US ambassador in the wake of that news, but confined his reaction to demanding an investigation into the matter.[31]

A month later, new leaks showed that the NSA had hacked into the Mexican Presidencía domain and, in particular, into former President Felipe Calderón's public e-mail account and gained deep insight into Mexican policy-making. Although the Mexican government has not

---

[28] Hopkins, Nick, and Matthew Taylor, "Watchdog demands GCHQ report on NSA's UK data storage", *The Guardian*, 21 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/21/sir-malcolm-rifkind-gchq-report-nsa-data-storage

[29] Roberts, Dan, "Bolivian president's jet rerouted amid suspicions Edward Snowden on board", The Guardian, 3 July 2013. http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna

[30] Glüsing, Jens, Laura Poitras, Marcel Rosenbach and Holger Stark, "Fresh Leak on US Spying: NSA Accessed Mexican President's Email", *Spiegel Online International*, 20 Oct 2013. http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

[31] Glüsing, Jens, Laura Poitras, Marcel Rosenbach and Holger Stark, "Fresh Leak on US Spying: NSA Accessed Mexican President's Email", *Spiegel Online International*, 20 Oct 2013. http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

reacted as publicly as the Brazilian president, the revelation surely hurt ties between the US and Mexico.

Mexico and Brazil ranked high among the nations on an April 2013 list that enumerated US surveillance priorities. That list, classified as "secret", was authorised by the White House and "presidentially approved", according to internal NSA documents. In response to an inquiry from Spiegel concerning these revelations, Mexico's Foreign Ministry replied with an e-mail condemning any form of espionage on Mexican citizens, saying such surveillance violates international law. "That is all the government has to say on the matter," stated a spokesperson for Peña Nieto.[32]

2.4 WHY WERE THE LEADERS OF ALLIED COUNTRIES TARGETED?

Predictably, the heads of the intelligence agencies initially said their actions were aimed at protecting their countries against the threat of terrorism[33], but that hasn't explained why they were targeting the leaders of Germany, Italy, Spain and other allies. *Die Zeit*, the German weekly newspaper, carried a lead article on 31 October 2013, in which the writer Heinrich Wefing claimed "The U.S. secret service has treated the chancellor as if she was an enemy herself" and that "This is exactly why 'cellphone-gate' marks a fundamental rupture" in German-US relations.

The NSA surveillance of political leaders of allied countries might have occurred simply because the NSA has the technology to do it. US Secretary of State John Kerry seems to have admitted as much when he acknowledged to a video conference on open government in London that "There is no question that the president and I and others in government have actually learned of some things that had been happening, in many ways, on an automatic pilot because the technology is there."[34]

More likely, however, the NSA surveilled allies in order to assess what the allies were thinking and planning to do in a range of different spheres, including the economic sphere.[35]

2.5 A BREAKDOWN OF TRUST

When people became aware of how massive the surveillance of virtually everyone had become, among the reactions was not only outrage and fury, but also of an "enormous loss of trust", as Elmar Brok, the chairman of the Foreign Affairs Committee at the European

---

[32] Glüsing, Jens, Laura Poitras, Marcel Rosenbach and Holger Stark, "Fresh Leak on US Spying: NSA Accessed Mexican President's Email", *Spiegel Online International*, 20 Oct 2013.
http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

[33] Roberts, Da, and Spencer Ackerman, "White House offers tentative support for plans to rein in NSA surveillance", *The Guardian*, 29 Oct 2013.
http://www.theguardian.com/world/2013/oct/29/white-house-supports-nsa-review

[34] Associated Press, "Kerry: Some NSA surveillance work reached 'too far' and will be stopped", published in *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/politics/federal_government/kerry-some-nsa-surveillance-work-reached-too-far-and-will-be-stopped/2013/11/01/37aeba76-42fd-11e3-b028-de922d7a3f47_story.html

[35] Leaked documents showed that the NSA spied on G20 leaders in Canada and London. Freeze, Colin, "Ottawa allowed U.S. to spy on G20 summit in Toronto, Snowden leak reveals", *The Globe and Mail*, 27 Nov 2013, last updated 28 Nov 2013.
http://www.theglobeandmail.com/news/politics/snowden-leak-reveals-us-spied-during-g20-summit-in-toronto/article15645575/

Parliament, put it.[36] The theme of trust was repeated by many others. For example, German federal data protection commissioner Peter Schaar was quoted as saying that "If we want to return to a relationship based on trust, it will require serious effort… Officially the Americans said that they respected German law. Now we know that was not the case."[37]

The breakdown of trust is often accompanied by embarrassment, but the embarrassment was not just in Washington. The revelations also caused embarrassment in Europe. In the summer of 2013, German Chancellor Angela Merkel defended the US, when it became known that the NSA had the whole of the German population as a target of mass surveillance. But when Merkel discovered that the US had been listening in on even her mobile calls, she rose to anger. However, she also found herself, somewhat embarrassingly, having to fend off criticism within her country that she had failed to react vigorously to the initial disclosures of extensive American eavesdropping on millions of Germans, and really became engaged only after her own personal privacy was violated.[38]

Merkel demanded that Washington reach a "no-spying" agreement with Berlin and Paris by the end of 2013, even though more than 90 per cent of Germans think that the Americans would breach a no-spying agreement anyway and continue their surveillance activities, according to a survey by public broadcaster ARD and *Die Welt*.[39]

US federal regulators have recognised that the NSA revelations have been damaging to US-Europe relations: Federal Trade Commissioner Julie Brill said (in October 2013): "There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the United States and many of our European colleagues."[40]

The intelligence committees of both the US Senate and House of Representatives have initiated hearings on the NSA practices. Bipartisan legislation calling for reform of the NSA has been introduced in both the House and Senate. President Barack Obama said his administration was conducting a complete review of intelligence activities.[41]

The European Parliament's LIBE committee on Civil Liberties, Justice and Home Affairs has been conducting its own investigation into the surveillance operations. As part of its investigation, it travelled to Washington, DC, to meet with officials from the State Department, Capitol Hill, various intelligence agencies and White House staff to discuss the

---

[36] Poitras, Laura, "Marcel Rosenbach and Holger Stark, Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[37] Landler, Mark, and David E. Sanger, "Obama May Ban Spying on Heads of Allied States", *The New York Times*, 29 Oct 2013.
http://www.nytimes.com/2013/10/30/world/europe/obama-may-ban-spying-on-heads-of-allied-states.html?_r=0

[38] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

[39] RT, "Germans lose trust in US, see NSA whistleblower Snowden as hero – poll", 8 Nov 2013.
http://rt.com/news/germany-lose-trust-us-snowden-431/

[40] Romm, Tony, and Erin Mershon, "EU to D.C.: Friends 'do not spy on each other'", Politico, 29 Oct 2013. http://www.politico.com/story/2013/10/european-union-nsa-friends-do-not-spy-on-each-other-99035.html

[41] Roberts, Da, and Spencer Ackerman, "White House offers tentative support for plans to rein in NSA surveillance", *The Guardian*, 29 Oct 2013.
http://www.theguardian.com/world/2013/oct/29/white-house-supports-nsa-review

impact that US surveillance programs have had on EU citizens. As of the end of November 2013, it is not clear what results these various hearings will achieve.

2.6 NOT ONLY THE US ENGAGED IN MASS SURVEILLANCE

European politicians have sought to play down the role their own security services have played in secret surveillance. The UK's response or, at least, that of David Cameron, to the NSA revelations has been somewhat muted, probably because GCHQ has long co-operated with the NSA, often carrying out surveillance on behalf of the United States.[42] The Snowden revelations have crossed the border between front stage and back stage politics. We can assume that most surveillance agency staff and their immediate stakeholders were aware of what was going on, but this was not a legitimate topic of public policy discourse. Bringing this "tacit" background knowledge to the foreground created a severe disturbance of policy. It is like the Mafia "Omerta" code: as long as all involved keep their secrets to themselves, the system works.

Although there has been considerable righteous indignation in Europe about the NSA surveillance, the security services in Germany, France, Spain and Sweden, and perhaps elsewhere have also been carrying out mass online surveillance and wiretapping[43] – not as extensively as the NSA and GCHQ, but mass surveillance nevertheless. According to a report in *The Guardian*, the German spy agency BND[44] had "huge technological potential and good access to the heart of the Internet".

US intelligence officials have insisted the mass monitoring in Europe was carried out by the security agencies in the countries involved and shared with the US.[45] However, US Director of National Intelligence James Clapper has acknowledged that the scale of surveillance by the NSA, with its 35,000 employees and $10.8 billion a year budget, sets it apart: "There's no question that from a capability standpoint we probably dwarf everybody on the planet, just about, with perhaps the exception of Russia and China."[46]

3 JUDICIAL AND LEGAL CONSEQUENCES

This section discusses several judicial and legal consequences of the NSA revelations, i.e., the legal secrecy underpinning US surveillance, the attempts to remove an anti-FISA provision from the proposed EU Data Protection Regulation, the botched Safe Harbor Agreement, the

---

[42] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html For a readable history of the collaboration between GCHQ and the NSA (and its antecedents), see Aldrich, Richard, *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency,* Harper Press, 2011.

[43] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden. See also *Deutsche Welle*, "Germany admits Europe's spy agencies cooperate on surveillance", 2 Nov 2013. http://www.dw.de/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903

[44] BND stands for Bundesnachrichtendienst or, in English, the Federal Intelligence Agency.

[45] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

[46] Shane, Scott, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, 2 Nov 2013. http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fworld%2Feurope%2Findex.jsonp

circumventing of laws, Brazil and Germany's resolution to the UN, a study that finds mass surveillance violates EU law and, finally, the UK government's characterisation of David Miranda as a terrorist.

3.1 LEGAL SECRECY

The US and UK governments have provided legal cover for some of the NSA and GCHQ's surveillance activities. Institutions like FISA provide a prima facie legal basis for many NSA actions, but they hollow out the idea of rule of law by doing so. Both in the US and in the UK, the legal secrecy that surrounds surveillance by the NSA and GCHQ is such that no company dares come out openly and discuss its relations with the secret services. In fact, it is illegal to do so.[47] In the US, the companies are legally required to share the data under the Foreign Intelligence Surveillance Act.[48] Nine US companies – Google, Microsoft, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL, Apple – gave the NSA access to their client data[49], but company spokespersons said they had no knowledge of a government program providing officials with access to their servers, and drew a line between giving the government wholesale access to their servers to collect user data and giving them specific data in response to individual court orders. Google, Microsoft and Twitter publish transparency reports detailing government requests for information, but these reports do not include FISA requests because they are not allowed to acknowledge them.[50] Arguably, there is an irony of legal reasoning here: the law determines that you have to provide access to your data and at the same time it contains a clause stating that you are not allowed to tell anyone that you do: so the law has a built-in rule that says you are not allowed to tell anyone that you are acting according to legal rules.

The 1978 Foreign Intelligence Surveillance Act (FISA) established the FISA court, comprising 11 judges appointed by the chief justice of the United States, as a secret part of the federal judiciary. The FISA court approves or denies government requests to listen to foreigners' calls on the ground of national security. Snowden leaked documents showing that the FISA court had instructed Verizon to hand over information about all calls on its network "on an ongoing daily basis".

Section 215 of the PATRIOT Act allows the FBI or others to apply to the FISA court for a secret order compelling companies to turn over "any tangible things", as long as they are "relevant to an authorised preliminary or full investigation to obtain foreign intelligence information not concerning a US person". Section 215 allows the FBI to obtain information from a company about their customers, ostensibly "to protect against international terrorism or clandestine intelligence activities". The company must hand over that information to the investigators under a gag order that prevents them from ever informing the customer that the company even received the order.

---

[47] Rusbridger, op. cit.

[48] Cain Miller, Claire, "Tech Companies Concede to Surveillance Program", *The New York Times*, 7 June 2013. http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html

[49] Greenwald, Glenn, and Ewen MacAskill, "NSA taps in to systems of Google, Facebook, Apple and others, secret files reveal", *The Guardian*, 7 June 2013. http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data?CMP=EMCNEWEML6619I2

[50] Cain Miller, Claire, "Tech Companies Concede to Surveillance Program", *The New York Times*, 7 June 2013. http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html

The Economist sarcastically commented that authorities seem to believe that obtaining records of every telephone call made in America is either relevant to an investigation or an essential bulwark against international terrorism.[51]

As for PRISM, on paper, the protections against privacy abuse seem robust. Supposedly, the government does not unilaterally obtain information from company servers, nor does it target anyone for information-gathering without "an appropriate, and documented foreign-intelligence purpose to the acquisition". Also supposedly, it does not intentionally target any American citizen. The process is monitored by a FISA court, by Congress (through twice-yearly reports) and by independent inspectors-general. The information is subject to "minimisation procedures", designed to protect Americans unconnected to an investigation whose information is accidentally gathered.[52] However, the Snowden revelations have shown these suppositions to be wholly without merit.

FISA orders do not give the government the right to listen to the content of calls. For that, law-enforcement agents need a separate warrant which requires suspicion of particular individuals and proof that "normal investigative procedures have been tried and failed". Instead, the NSA has collected metadata, the records of who people call, when, for how long, and so on.[53] However, computerised analysis of metadata can now provide a detailed portrait of who people know, where they go and their daily routines,[54] which is almost good or perhaps even better than intercepting the content of communications.[55]

When it became known that the NSA sweeps us some 5 billion records every day about the location data for hundreds of millions of mobile phones worldwide, an NSA spokesperson said the collection of the global mobile phone location data is legally authorised under Executive Order 12333, which governs all US espionage. That means congressional committees and relevant inspectors general can oversee the programme, but the secret court established under the Foreign Intelligence Surveillance Act (FISA) would not.[56]

3.2 THE TOOTHLESS FISA COURT

The reality is that the FISA seems to give virtually free reign to the NSA and FBI. Between 18 May 1979 and the end of 2004, the FISA court granted 18,742 NSA and FBI applications;

---

[51] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will
[52] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will
[53] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will
[54] *The Economist*, "Surveillance: Look who's listening", 15 June 2013.
http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will
[55] For a good, brief description of how much metadata can reveal about a person, see Lithwick, Dahlia, and Steve Vladeck, "Taking the "Meh" out of Metadata", *Slate*, 22 Nov 2013.
http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html
[56] Associated Press, "NSA defends global mobile phone tracking as legal", published in *Gulf News*, 7 Dec 2013.
http://gulfnews.com/news/world/usa/nsa-defends-global-mobile-phone-tracking-as-legal-1.1264432

it turned down only four outright.[57] In 2012, the government made 1,856 applications for electronic surveillance to FISA, and none was denied.[58] Thus, the government met formal legal requirements but the legal requirements were essentially a smokescreen to allow the NSA to do as it wished.

Despite the apparent weakness of the FISA court, President Bush secretly decided in 2001 that the NSA would no longer be bound by the FISA. Until then, before the NSA could place the name of an American on its watch list, it had to go before a FISA-court judge and show that it had probable cause to believe an individual was somehow connected to terrorism in order to get a warrant. Under Bush's new procedures, warrants do not always have to be obtained, and the critical decision about whether to put an American on a watch list is left to the vague and subjective "reasonable belief" of an NSA supervisor.[59]

The FISA Amendments Act of 2008 allows the US government to obtain an order from a national security court to conduct surveillance of foreigners abroad without individualised warrants even if the interception takes place on American soil.[60] Congress authorised the PRISM program and maintained that it minimises the collection and retention of information "incidentally acquired" about Americans and permanent residents. Several of the Internet companies said they did not allow the government open-ended access to their servers but complied only with specific lawful requests for information.

The law, which Congress reauthorised in late 2012, is controversial in part because Americans' e-mails and phone calls can be swept into a database without an individualised court order when they communicate with people overseas. While newspapers claimed the leaked documents showed that the NSA obtained direct access to the companies' servers, several of the companies, including Google, Facebook, Microsoft and Apple, denied that the government could do so. Instead, the companies said they had negotiated with the government technical means to provide specific data in response to court orders.[61] However, in October 2013, more leaked documents showed that the NSA was directly tapping into the companies' servers without the companies' knowledge.

The US government can rely on still other legislation to conduct secret surveillance. As mentioned above, the 1994 Communications Assistance for Law Enforcement Act (CALEA) required telephone companies to provide the government with secret access to their networks. The FCC has now extended the act to cover "any type of broadband Internet access service" and the new Internet phone services and ordered company officials never to discuss any aspect of the program.[62]

---

[57] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

[58] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[59] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

[60] Savage, Charlie, Edward Wyatt and Peter Baker, "U.S. Says It Gathers Online Data Abroad", *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?hp&_r=1&

[61] Savage, Charlie, Edward Wyatt and Peter Baker, "U.S. Says It Gathers Online Data Abroad", *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?hp&_r=1&

[62] Bamford, James, "Big Brother Is Listening", *The Atlantic*, 1 Apr 2006. http://www.theatlantic.com/magazine/archive/2006/04/big-brother-is-listening/304711/?single_page=true

3.3 WATERING DOWN THE PROPOSED DATA PROTECTION REGULATION

On 29 November 2011, someone leaked a draft of the proposed EU Data Protection Regulation, which contained a provision (Article 42.1) as follows:

> No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.

In point of fact, this provision meant that Europe would not recognise an order from the FISA court requiring a company to turn over European data to the US government, at least not without some kind of formal agreement with the EU. Article 42.1 would have eviscerated the FISA's power, at least as far as Europeans are concerned, by nullifying "any US request for technology and telecoms companies to hand over data on EU citizens".[63]

But between 29 November 2011 when a draft of the proposed Regulation was leaked and 25 January 2012, when the proposed Regulation was officially released, the US was successful in lobbying against the so-called "anti-FISA" clause and getting it removed.

The NSA revelations have occurred at a time when the European Parliament continues its consideration of the proposed Regulation. Until the Snowden revelations, US lobbyists, including those representing Google, Facebook, Microsoft, Amazon and Yahoo, had been successful in watering down various provisions of the proposed Regulation and in getting Europe to abandon Article 42.1, a measure that would have shielded Europeans from requests by American authorities to share online data gathered by some of the biggest American Internet companies. However, the Snowden revelations made parliamentarians realise that the proposed Regulation needed, if anything, to be stronger. European Commission Vice President Viviane Reding, among others, seized on the NSA revelations as justification for more stringent European data protection rules.

Hence, when the proposed Regulation emerged from the European Parliament's LIBE committee in October 2013, the above clause had been restored, word for word. It would forbid US companies from complying with US government requests for Europeans' personal data unless expressly approved by EU authorities. Since American companies can't agree to rules that would require them to ignore lawful US requests for information, the provision could effectively undermine US-EU data transfers.[64]

Restoration of the provision was a serious reversal for Washington. Furthermore, American technology companies worry that fines for breaking those rules and others could run as high as 5 per cent of a company's global annual revenue or €100 million, whichever is higher,[65] a provision that emerged from the LIBE committee in October 2013, which is somewhat stronger than the 2% figure mentioned in the January 2012 draft of the Regulation.

---

[63] Meyer, David, "U.S. secretly watered down Europe's proposed privacy rules, report claims", GigaOm, 13 June 2013. http://gigaom.com/2013/06/13/u-s-secretly-watered-down-europes-proposed-privacy-rules-report-claims/

[64] Mershon, Erin, "U.S. to EU: Don't scapegoat Safe Harbor over NSA", *Politico*, 7 Nov 2013. http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html?hp=l11

[65] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

3.4 SAFE HARBOR AGREEMENT IN DANGER OF SINKING

The Snowden revelations have put the proposed Safe Harbor agreement in trouble – again. The Safe Harbor agreement between the US and EU came into operation in 2000 after the EU determined that US standards were "inadequate" in meeting the data protection principles of the EU's Data Protection Directive of 1995. The agreement allows US companies that want to handle or store European citizens' data to self-certify annually with the Department of Commerce that they will abide by the standards. The FTC is tasked with enforcing breaches of that agreement. European regulators became more vocal in their criticism of the framework following the first Snowden revelations, pointing out that Safe Harbor specifically provides for exemptions "to the extent necessary to meet national security, public interest or law-enforcement requirements". However, such exemptions are a kind of Trojan horse which allow questionable activity not always in the public interest, even though security agencies say it is. Who is going to challenge them if such activities are not subject to public scrutiny or effective oversight?

Some EU officials, alarmed by reports of the NSA's access to Internet companies, say Safe Harbor gives US companies a way to evade the EU's more stringent privacy regime.[66] European Parliament member Jan Philipp Albrecht told US officials in October 2013 that the agreement allows U.S companies to "circumvent" democratically established law. Albrecht said Europe "shouldn't allow our standards to be undermined by certain loopholes", which he said the Safe Harbor agreement facilitates.[67]

German federal data protection commissioner Peter Schaar called the Safe Harbor agreement a "fiction," given how much technology and the flow of information have changed in the past decade and how many new regulations Washington has drawn up since the treaty was signed. "Consequently, I do not think it is right that we continue to facilitate the transfer of data into the USA," Schaar said. The agreements "must be renegotiated, and must include reasonable protections against eavesdropping by state and secret services."[68]

In addition to their critique of Safe Harbor's lack of stringency, European regulators and others have attacked the agreement on the grounds that it is poorly enforced. EU officials released two reports critical of the program's enforcement in 2002 and 2004. Australian consulting firm Galexia reported hundreds of Safe Harbor violations in a 2008 report that criticised both the EU and the US for not taking enforcement more seriously. Indeed, the FTC did not bring its first enforcement under Safe Harbor rules until 2009, and its batch of seven enforcement actions that year targeted companies for falsely advertising their Safe Harbor certification, not for any failures to protect Europeans' data. Since then, the FTC has brought three Safe Harbor enforcement actions against Facebook, Google and MySpace.[69] Other testimony to the LIBE committee contends that "The Safe Harbor does not (and cannot) cover major categories of data that appear to be the subject of surveillance, including financial

[66] Mershon, Erin, "U.S. to EU: Don't scapegoat Safe Harbor over NSA", *Politico*, 7 Nov 2013. http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html?hp=l11

[67] Romm, Tony, and Erin Mershon, "EU to D.C.: Friends 'do not spy on each other'", *Politico*, 29 Oct 2013. http://www.politico.com/story/2013/10/european-union-nsa-friends-do-not-spy-on-each-other-99035.html

[68] Landler, Mark, and David E. Sanger, "Obama May Ban Spying on Heads of Allied States", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/obama-may-ban-spying-on-heads-of-allied-states.html?_r=0

[69] Mershon, Erin, "U.S. to EU: Don't scapegoat Safe Harbor over NSA", *Politico*, 7 Nov 2013. http://www.politico.com/story/2013/11/us-european-union-safe-harbor-nsa-99495.html?hp=l11

records, travel records, and significant portions of voice and data traffic carried by US telecommunications providers."[70]

In late November 2013, the European Commission released a Communication which was critical of the Safe Harbor Agreement, but did not completely sink it.[71] The Communication concludes that

> Due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed:
> a) transparency of privacy policies of Safe Harbour members,
> b) effective application of Privacy Principles by companies in the US, and
> c) effectiveness of the enforcement.
> Furthermore, the large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data in transferred to the US.

The Commission makes 13 recommendations for improving the agreement. It says U.S. authorities have until the summer of 2014 to implement the recommendations, at which point Commission will review the agreement and the actions taken by, inter alia, the FTC.

3.5 CIRCUMVENTING LAWS

Some of the documents leaked by Snowden reveal how the intelligence agencies have attempted to circumvent or simply ignore laws that would limit the extent of their surveillance. According to a report in *The Guardian*, GCHQ was helping European partners to circumvent national laws.[72] "The files [leaked by Snowden] also make clear that GCHQ played a leading role in advising its European counterparts how to work around national laws intended to restrict the surveillance power of intelligence agencies."[73]

The Guardian claimed that it had obtained documents that show that GCHQ has had access to the PRISM system since at least June 2010. As a result, GCHQ might have been able to circumvent UK restrictions on accessing people's communications by obtaining the information from the NSA instead.[74] David Cameron has rejected allegation that GCHQ acted illegally by receiving information from the US.[75]

---

[70] Connolly, Chris (Galexia), EU/US Safe Harbour – Effectiveness of the Framework in relation to National Security Surveillance, Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) Inquiry on "Electronic mass surveillance of EUY citizens", Strasbourg, 7 Oct 2013, pp. 2, 6. http://www.europarl.europa.eu/committees/en/libe/events.html#menuzone

[71] European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847, Brussels, 27 Nov 2013. http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

[72] Deutsche Welle, "Germany admits Europe's spy agencies cooperate on surveillance", 2 Nov 2013. http://www.dw.de/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903

[73] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

[74] Hope, Christopher, and Tom Whitehead, "British Intelligence watchdog flies to Washington to demand answers on snooping scandal", *The Telegraph*, 7 June 2013. http://www.telegraph.co.uk/technology/internet-security/10107059/British-Intelligence-watchdog-flies-to-Washington-to-demand-answers-on-snooping-scandal.html

[75] Warrell, Helen, and James Blitz, "David Cameron rejects claims GCHQ broke law over US Prism data", *The Financial Times*, 10 June 2013. http://www.ft.com/cms/s/0/01d745fe-d1f0-11e2-b17e-00144feab7de.html#axzz2VsHkbdAE

Some intelligence agencies have not had to circumvent national legislation because they have already been given a free hand. Such is the case in Sweden which passed a law in 2008 allowing its intelligence agency to monitor cross-border e-mail and phone communications without a court order.[76]

3.6 UNLAWFUL ACCESS TO SWIFT?

The Dutch and Belgian data protection authorities are leading an investigation into whether the SWIFT payment network is safe, following media reports that the NSA has or has had unlawful access to SWIFT data concerning international bank transfers. In October 2013, SWIFT said it had conducted an audit that showed that nothing wrong had happened. The European Parliament, however, demanded a halt to bank-data transfers to US counter-terrorism investigators because of possible data protection violations. The Article 29 Data Protection Working Party agreed that Belgium and the Netherlands should lead the investigation because SWIFT is based in Belgium and has an important data processing centre in the Netherlands.[77]

3.7 BRAZIL AND GERMAN RESOLUTION TO UN

Brazil and Germany formally presented a resolution on "The right to privacy in the digital age" to the UN General Assembly on 1 November 2013 urging all countries to extend internationally guaranteed rights to privacy to the Internet and other electronic communications.[78]

The draft resolution

> 1. Reaffirms the rights contained in the International Covenant on Civil and Political Rights, in particular the right to privacy and not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, and the right to enjoy protection of the law against such interference or attacks, in accordance with article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights;

It calls upon States

> 4 (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law
>
> 4 (d) To establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data;

It also

> 5. Requests the United Nations High Commissioner for Human Rights to submit an interim report on the protection of the right to privacy in the context of domestic and extraterritorial surveillance of communications, their interception and collection of personal data, including

[76] Borger, Julian, "GCHQ and European spy agencies worked together on mass surveillance", *The Guardian*, 1 Nov 2013. http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

[77] Bodoni, Stephanie, "Global Data Network Probed by EU Regulators Over NSA Reports", *Bloomberg News*, 13 Nov 2013. http://www.bloomberg.com/news/2013-11-13/global-data-network-probed-by-eu-regulators-over-nsa-reports.html

[78] A copy of the resolution can be found at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45

> massive surveillance, interception and collection of personal data, to the General Assembly at its sixty-ninth session.

Although General Assembly resolutions are not legally binding, they do reflect world opinion and carry moral and political weight.[79] The 4(d) provision above is especially interesting in view of one of the conclusions we draw in this paper, i.e., the failure of existing oversight mechanisms.

Meanwhile, in advance of adoption of the resolution, the Frankfurter Allgemeine Sonntagszeitung (FAS) reported on 2 November 2013 that Germany and the US had struck an agreement not to spy on each other following discussions between a delegation of officials from Merkel's office and German intelligence officials and officials at the White House.[80]

In late November 2013, the UN General Assembly's human rights committee unanimously adopted the resolution. The United States did not oppose it, but lobbied successfully to water it down somewhat by dropping a key provision stating that the domestic and international interception and collection of communications and personal data, "in particular massive surveillance", may constitute a human rights violation.[81]

3.8 STUDY FINDS MASS SURVEILLANCE VIOLATES EU LAW

While the intelligence agencies and political leaders have said that the surveillance conducted was within the law, the media, academics and advocacy organisations have disputed those claims. A study presented by Sergio Carrera of the Centre for European Policy Studies (CEPS) and Francesco Ragazi of Leiden University shows that mass Internet surveillance by US and UK intelligence agencies violates EU law. The authors presented their findings to the European Parliament's LIBE Committee on Civil Liberties, Justice and Home Affairs.[82]

Carrera and Ragazi are not alone. Others also believe that, with few exceptions, NSA spying on the EU and the UN "not only contravenes the diplomatic code, but also international agreements. The Convention on the Privileges and Immunities of the United Nations of 1946, as well as the Vienna Convention on Diplomatic Relations of 1961, long ago established that no espionage methods are to be used. What's more, the US and the UN signed an agreement in 1947 that rules out all undercover operations."[83]

---

[79] The Associated Press, "Internet privacy resolution presented to United Nations", published in the *Portland Press Herald*, 8 Nov 2013. http://www.pressherald.com/news/nationworld/Internet_privacy_resolution_presented_to_United_Nations_.html

[80] *Deutsche Welle*, "Germany admits Europe's spy agencies cooperate on surveillance", 2 Nov 2013. http://www.dw.de/germany-admits-europes-spy-agencies-cooperate-on-surveillance/a-17200903

[81] Spielmann, Peter James, "UN advances Internet privacy resolution", Associated Press, published in *The Miama Herald*, 26 Nov 2013. http://www.miamiherald.com/2013/11/26/3780690/un-advances-internet-privacy-rights.html

[82] Ashford, Warwick, "NSA and GCHQ mass surveillance violates EU law, study finds", *ComputerWeekly.com*, 8 Nov 2013. http://www.computerweekly.com/news/2240208711/NSA-and-GCHQ-mass-surveillance-violates-EU-law-study-finds. The full study, by Bigo, Didier, Sergio Carrera, Nicholas Hernanz, et al., *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, October 2013, can be found here: http://www.europarl.europa.eu/committees/en/studies.html

[83] Poitras, Laura, "Marcel Rosenbach and Holger Stark, Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

Months before the Carrera and Ragazi presentation, in fact, within days of the first revelations, the Council of Europe alerted its 47 member states to the risks of digital tracking and other surveillance technologies for human rights, the rule of law and democracy, and recalled the need to ensure their legitimate use. In a Declaration issued to governments, the Committee of Ministers said that legislation allowing for overly broad surveillance of citizens can challenge their privacy and have a chilling effect on their freedom of expression and the freedom of the media. The Committee said that tracking and surveillance measures by law enforcement authorities should comply with the Council of Europe's human rights standards set out in the European Convention on Human Rights. Such measures should also strictly respect the limits, requirements and safeguards set out in the Data Protection Convention 108. The Declaration drew attention to the criminal law implications of unlawful surveillance and tracking and to the relevance of the Budapest Convention on Cybercrime.[84]

3.9 IS DAVID MIRANDA REALLY A TERRORIST?

On 18 August 2013, David Miranda, the partner of Glenn Greenwald, the journalist who has written many of the stories based on the leaked NSA documents, was detained at Heathrow for nine hours as he was flying from Berlin to Rio. He was in possession of some of the NSA documents leaked by Snowden. Police detained him on the excuse that possession of the documents could be a crime under the Terrorism Act 2000, which prohibits possessing information that might be useful to terrorists and specifically "eliciting, publishing or communicating" information about members of the armed forces, intelligence agencies and police which terrorists could use. The police were also considering charging Miranda with crimes under section one of the Official Secrets Act 1911 which deals with communication of material to an enemy and "various offences" under the Official Secrets Act 1989.[85]

During his trip to Berlin, Miranda met Laura Poitras, the US film-maker who had been working with Glenn Greenwald and *The Guardian*. Officials confiscated Miranda's mobile phone, laptop, camera, memory sticks, DVDs and games consoles. After his release and return to Rio, Miranda filed a legal action against the British government, seeking the return of materials seized from him by British authorities and a judicial review of the legality of his detention. At a London court hearing for Miranda's lawsuit in early November, Scotland Yard – in consultation with the MI5 – claimed that Miranda was indeed involved in "terrorism" when he tried to carry documents through the London airport.[86]

[84] Council of Europe, "Council of Europe alerts governments on risks of digital tracking and surveillance", Press release, DC 081(2013), Strasbourg, 12 June 2013. http://hub.coe.int/web/coe-portal/press/pressreleases

[85] Booth, Robert, "UK took three weeks to act over data at New York Times, says Guardian", *The Guardian*, 30 Aug 2013. http://www.theguardian.com/world/2013/aug/30/david-miranda-police-powers-data

[86] Hosenball, Mark, "UK: Snowden reporter's partner involved in 'espionage' and 'terrorism'", Reuters, 1 Nov 2013. http://www.reuters.com/article/2013/11/01/us-uk-nsa-idUSBRE9A013O20131101

4 SOCIETAL RESPONSE

4.1 GORE: BLANKET SURVEILLANCE IS OBSCENELY OUTRAGEOUS

The societal response can be judged by, inter alia, comments from members of the public in response to news stories and public opinion surveys.

Here is an example of a comment:

> How is spying on the leaders of allied nations useful in fighting terrorism? How did it save lives? So the leaders of France, Germany, Italy, Spain, etc should all thank us for our intrusive, abrasive, and illegal acts, is that right? Have the leaders of the American government gone completely mad?[87]

This comment has been echoed by other stakeholders. Former Vice President Al Gore tweeted that privacy is essential in the digital era: "Is it just me, or is secret blanket surveillance obscenely outrageous?"[88]

Anthony Romero of the American Civil Liberties Union denounced the surveillance as an infringement of fundamental individual liberties. "A pox on all the three houses of government," Mr. Romero said. "On Congress, for legislating such powers, on the FISA court for being such a paper tiger and rubber stamp, and on the Obama administration for not being true to its values."[89]

Democratic Senator Ron Wyden of Oregon said he hoped the disclosure would "force a real debate" about whether such "sweeping, dragnet surveillance" should be permitted — or is even effective. The UK's Lord Ashdown has said that surveillance should only be conducted against specific targets when there was evidence against them and that dragnet surveillance was unacceptable.[90]

Moreover, Lord Ashdown has said it was time for a high-level inquiry to address fundamental questions about privacy in the 21st century, and railed against "lazy politicians" who frighten people into thinking "al-Qaida is about to jump out from behind every bush and therefore it is legitimate to forget about civil liberties…Well it isn't."

Various other public figures have commented on the surveillance revelations. For example, World Wide Web creator Sir Tim Berners-Lee has warned that the democratic nature of the Internet is threatened by a "growing tide of surveillance and censorship".[91]

---

[87] From crygdyllyn, 29 Oct 2013:http://www.politico.com/gallery/2013/10/nsa-spying-15-great-quotes/001396-019790.html

[88] Associated Press, "Obama administration collecting huge number of citizens' phone records, lawmaker says", 6 June 2013. http://www.washingtonpost.com/politics/federal_government/report-government-secretly-scooping-up-phone-records-of-millions-of-verizon-customers/2013/06/05/e820deb8-ce57-11e2-8573-3baeea6a2647_story.html

[89] Savage, Charlie, Edward Wyatt and Peter Baker, "U.S. Says It Gathers Online Data Abroad", *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?hp&_r=1&

[90] Nick Hopkins and Matthew Taylor, "Surveillance technology out of control, says Lord Ashdown", *The Guardian*, 18 Nov 2013. http://www.theguardian.com/world/2013/nov/18/surveillance-technology-out-of-control-ashdown

[91] BBC News, "Tim Berners-Lee says 'surveillance threatens web'", 22 Nov 2013. http://www.bbc.co.uk/news/technology-25033577

4.2 PUBLIC OPINION SURVEYS

There have been various surveys of the public's views of the massive surveillance since the NSA revelations began, especially in the US.

A Pew Research Center survey taken there a few days after the leaks found that a majority of respondents (56%) believed that monitoring their phone calls was an "acceptable" way to investigate terrorism, though a substantial minority (41%) disagreed. On the question of e-mail monitoring, the split went the other way: 52% said it was unacceptable while 45% approved. Interestingly, 62% said it was more important for the federal government to investigate possible terrorist threats, even if that intrudes on personal privacy. Just 34% said it was more important for the government not to intrude on personal privacy, even if that limits its ability to investigate possible terrorist threats.[92]

In a mid-July Washington Post-ABC News survey, nearly half (49 per cent) said they thought that the NSA's surveillance program intruded on their personal privacy rights. And 74 per cent said it infringed on some Americans' privacy, if not their own. Nevertheless, when asked to balance security worries against privacy concerns, Americans continued to opt for security. In that same Washington Post-ABC News poll, 57 per cent felt that it was important for the federal government to investigate terrorist threats, even if it intrudes on personal privacy. Just 39 per cent said that the government should not intrude on personal privacy, even if it limits the ability to investigate possible terrorist threats. [93]

A Pew Research poll in July 2013 found that a majority of Americans – 56% – said that federal courts fail to provide adequate limits on the telephone and Internet data the government is collecting as part of its anti-terrorism efforts. An even larger percentage (70%) believed that the government has been using this data for purposes other than investigating terrorism. And despite the insistence by the president and other senior officials that only "metadata", such as phone numbers and e-mail addresses, were being collected, 63% thought the government was also gathering information about the content of communications – with 27% believing the government has listened to or read their phone calls and e-mails.[94]

In another poll in July, Annalect, a US data analytics company, found that the percentage of Internet users worried about their online privacy jumped 19 per cent, from 48 per cent in June (when the NSA revelation stories first appeared in *The Guardian* and *The Washington Post*) to 57 per cent in July. When consumers were asked about their response to the NSA's collection of online information, nearly one-third (31 per cent) said they were now taking action to protect their online privacy, such as changing their browser settings, deleting or opting out of mobile tracking, disabling cookies and editing social media profiles.[95]

A majority of Americans oppose the NSA's collection of data on telephone and Internet usage, according to a poll conducted by the Associated Press-NORC Center for Public Affairs

---

[92] Pew Research Center, "Public Says Investigate Terrorism, Even If It Intrudes on Privacy", 10 June 2013. http://www.people-press.org/files/legacy-pdf/06-10-13%20PRC%20WP%20Surveillance%20Release.pdf

[93] Stokes, Bruce, "Trading Privacy for Security", *Foreign Policy*, 4 Nov 2013. http://www.foreignpolicy.com/articles/2013/11/04/trading_privacy_for_security?wp_login_redirect=0

[94] Pew Research Center for the People & the Press, "Few See Adequate Limits on NSA Surveillance Program", 26 July 2013. http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/

[95] Bachman, Katy, "Study: NSA Scandal Is Still Setting Off Privacy Alarm Bells Among Consumers", *AdWeek*, 13 Aug 2013. http://www.adweek.com/news/technology/study-nsa-scandal-still-setting-privacy-alarm-bells-among-consumers-151835

Research in August 2013, following more than two months of disclosures about the NSA's mass surveillance programs. The poll showed that a majority of Americans believed the US government was doing a poor job of protecting privacy rights, that 71 per cent did not want officials eavesdropping on US phone calls without court warrants while 62 per cent opposed collection of the contents of Americans' e-mails without warrants.[96]

Another survey, the results of which were published by the Pew Research Center in November 2013, found that 56 per cent of Americans thought it was unacceptable for the United States to monitor the phone calls of the leaders of allied nations, including German Chancellor Angela Merkel.[97]

An October 2013 survey of American, Canadian and British adults by Angus Reid Global indicated that people distrust their national leaders to be good guardians of the information gathered or to restrict its use to national security purposes. When asked whether they trusted their national government to be "a good guardian of citizens' personal information", 60 per cent of Americans and 64 per cent of Britons and Canadians said they had "not that much trust" or "no trust at all". In each country polled, at least 75 per cent of respondents described the issue of government surveillance of the public's Internet communications as "very" or "quite" important to them (US: 77%, Canada: 78% UK: 82%). Asked to assume their national government is routinely conducting electronic surveillance of the general public, 60% of Americans and Canadians described this as "unacceptable", while Britons were more split, (52% unacceptable versus 48% acceptable). Only one in five respondents believe information gathered by governments will be used for "strictly national security/anti-terrorism efforts" (US: 21%, UK: 19%, Canada: 18%).

The NSA revelations seem to have had a salutary effect on the public's paying more attention to their privacy. A Harris poll released 13 November 2013 showed that four out of five people have changed the privacy settings of their social media accounts, and most have made changes in the previous six months.[98]

Interestingly, public opinion in the UK does not seem to be so opposed to what the intelligence agencies have been doing. According to a YouGov poll in September 2013, only 19% of the public think that the British security services should cut back their surveillance powers – and they tend to believe recent leaks about them are a bad thing. While there has also been widespread distress over the content of the leaks, YouGov found little public support for scaling back the surveillance state. Only 19% of British adults say the British security services have too many powers. The largest group, 42%, say the current balance is about right, and 22% say they do not have enough powers.[99]

4.3 SNOWDEN: HERO OR TRAITOR?

[96] Associated Press, "Poll: American public's concerns rise over surveillance programs and privacy erosion", 10 Sept 2013. http://www.foxnews.com/us/2013/09/10/poll-american-public-concerns-rise-over-surveillance-programs-and-privacy/

[97] Pew Research Center, "Most Say Monitoring Allied Leaders' Calls Is Unacceptable", 4 Nov 2013. http://www.people-press.org/2013/11/04/most-say-monitoring-allied-leaders-calls-is-unacceptable/

[98] Acohido, Byron, "Snowden effect: young people now care about privacy", *USA Today*, 13 Nov 2013. http://www.usatoday.com/story/cybertruth/2013/11/13/snowden-effect-young-people-now-care-about-privacy/3517919/

[99] Dahlgreen, Will, "Little appetite for scaling back surveillance", YouGov, 13 Oct 2013. http://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/

Former US Vice President Dick Cheney has called Snowden a "traitor" for leaking NSA documents.[100] While Cheney and other US government officials have said Snowden should be captured and punished, others regard Snowden as a hero. Edward Snowden has been likened to Daniel Ellsberg, the man who in 1971 leaked the Pentagon Papers to *The New York Times*, which revealed that the US government had been less than truthful with the public about the conduct of the Vietnam war. The Pentagon Papers came as a shock to the public, and to lawmakers. Ellsberg, like Snowden, was initially accused of espionage and conspiracy, though those charges were ultimately dropped. Today, he is mostly seen as a hero of open government and free speech[101] and as having brought the Vietnam war to an end sooner than might otherwise have been the case. Writing in *The Washington Post*, Ellsberg defended Snowden's fleeing the US, and said he hoped "Snowden's revelations will spark a movement to rescue our democracy, but he could not be part of that movement had he stayed here".[102]

According to the above-mentioned Angus Reid Global online poll, 51 per cent of Americans viewed Snowden as a hero, and 49 per cent as a traitor.[103] However, in Canada, 67% and in the UK, 60% of respondents say Snowden should be commended for his actions. In a separate survey conducted by public broadcaster ARD and *Die Welt*, 60 per cent of Germans regard Snowden as a hero. Meanwhile, Germans' trust in the US has plummeted from 76 per cent when Obama made his first official visit to Berlin in November 2009 to only 35 per cent four years later, in November 2013.[104]

The Council of Europe issued a press release saying "'Whistleblowers' who disclose state wrongdoing in the public interest should be protected from retaliation, provided they acted in good faith and followed procedures, a committee of the Parliamentary Assembly of the Council of Europe (PACE) said in a draft resolution" in June. While the press release didn't mention Snowden by name, the message was clear enough.[105] As it turns out, a pro-Snowden petition on the White House website garnered more than 100,000 supporters within three weeks of the initial leaks.[106]

One of the first to call Snowden a hero was film-maker Oliver Stone who hailed Snowden as a hero for exposing the NSA's mass surveillance programme. "It's a disgrace that Obama is more concerned with hunting down Snowden than reforming these George Bush-style eavesdropping techniques," the Oscar-winning director told audiences at an international film festival in the Czech Republic in early July 2013.[107]

---

[100] Rhodan, Maya, "Dick Cheney Calls Snowden a 'Traitor,' Defends NSA", *Time*, 28 Oct. 2013. http://swampland.time.com/2013/10/28/dick-cheney-calls-snowden-a-traitor-defends-nsa/

[101] *The Globe and Mail*, "Is Edward Snowden a hero?", Globe editorial, 8 Nov 2013. http://www.theglobeandmail.com/globe-debate/editorials/is-edward-snowden-a-hero/article15354202/

[102] Ellsberg, Daniel, "Snowden made the right call when he fled the U.S.", *The Washington Post*, 7 July 2013. http://articles.washingtonpost.com/2013-07-07/opinions/40427629_1_daniel-ellsberg-pentagon-papers-snowden-s

[103] Raphael, Daniel, "Why Edward Snowden Is a Hero", *Huffington Post*, 7 Nov 2013. http://www.huffingtonpost.com/daniel-raphael/why-edward-snowden-is-a-h_b_4227605.html

[104] RT, "Germans lose trust in US, see NSA whistleblower Snowden as hero – poll", 8 Nov 2013. http://rt.com/news/germany-lose-trust-us-snowden-431/

[105] Council of Europe, "PACE committee calls for protection of 'whistleblowers' who reveal state wrongdoing", Press release, AP117(2013), Strasbourg, 24 June 2013. http://hub.coe.int/web/coe-portal/press/pressreleases

[106] Nelson, Steven, "White House Says It Will Respond to 'Pardon Edward Snowden' Petition", *U.S. News & World Report*, 25 Nov 2013. http://www.usnews.com/news/articles/2013/11/25/white-house-says-it-will-respond-to-pardon-edward-snowden-petition

[107] Brooks, Xan, "Oliver Stone defends Edward Snowden over NSA revelations", *The Guardian*, 5 July 2013. http://www.guardian.co.uk/film/2013/jul/05/oliver-stone-edward-snowden-nsa

Another public figure of note to describe Snowden as a hero is James Wales, founder of Wikipedia. Wales said of Snowden that "he has never leaked anything that would put any particular agents at risk and so forth. He has exposed what I believe to be, very likely to be judged, criminal wrongdoing, lying to Congress and certainly a shock and an affront, in America, an affront to the 4th amendment. I think that history will judge him very favourably."[108]

In an editorial, Canada's national newspaper, *The Globe and Mail*, argued that Snowden has performed a service to the public. The editorial noted, "There's is no perfect balance that can ever be struck between privacy and national security. In a post-9/11 world, the arguments of national security were often treated as irresistible, and impossible to counter. Mr. Snowden's revelations have altered the debate, and for the better."[109]

Venezuelan President Nicolás Maduro similarly said Snowden should be given a "humanitarian medal" for revealing details of NSA surveillance programmes on US and foreign citizens. "He did not kill anyone and did not plant a bomb…. What he did was tell a great truth in an effort to prevent wars. He deserves protection under international and humanitarian law."[110]

Stephen Walt, a professor of international affairs at Harvard University, writing in *The Financial Times*, made similar comments. "Mr Snowden's motives were laudable: he believed fellow citizens should know their government was conducting a secret surveillance programme enormous in scope, poorly supervised and possibly unconstitutional. He was right." Walt argued that Snowden deserves a presidential pardon. "Gerald Ford pardoned Richard Nixon, George HW Bush pardoned the officials who conducted the illegal Iran-Contra affair, and Mr Obama has already pardoned several convicted embezzlers and drug dealers. Surely Mr Snowden is as deserving of mercy as these miscreants."[111]

4.4 APPLYING PRESSURE ON COUNTRIES, SNOWDEN AND JOURNALISTS

After Ecuador withdrew its offer of asylum to Snowden, a US state department spokeswoman denied the US had bullied other potential host countries. She said that the US has simply impressed upon possible host countries the seriousness of the crimes with which Snowden has been charged.[112]

Some politicians favour prosecuting the newspapers publishing the reports based on the documents leaked by Snowden. In the UK, Tory MP Julian Smith said the newspaper had broken the law and should be prosecuted. The backbencher reportedly made a complaint about *The Guardian* to the police, and criticised the newspaper for writing stories "with no

---

[108] Al Jazeera, "Wikipedia founder calls Edward Snowden a hero", 25 Nov 2013. http://www.aljazeera.com/pressoffice/2013/11/wikipedia-founder-calls-edward-snowden-hero-20131125142412647981.html

[109] *The Globe and Mail*, "Is Edward Snowden a hero?", Globe editorial, 8 Nov 2013. http://www.theglobeandmail.com/globe-debate/editorials/is-edward-snowden-a-hero/article15354202/

[110] Roberts, Dan, "Bolivian president's jet rerouted amid suspicions Edward Snowden on board", *The Guardian*, 3 July 2013. http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna

[111] Walt, Stephen, "Snowden deserves an immediate presidential pardon", *The Financial Times*, 8 July 2013. http://www.ft.com/cms/s/0/0ccf2d14-e7c1-11e2-babb-00144feabdc0.html#axzz2YiI70RAU

[112] Roberts, Dan, "Bolivian president's jet rerouted amid suspicions Edward Snowden on board", *The Guardian*, 3 July 2013. http://www.theguardian.com/world/2013/jul/03/edward-snowden-bolivia-plane-vienna

consultation with government". Home Office minister James Brokenshire said that *The Guardian*'s publication of the Snowden leaks had damaged national security.[113]

Some of the journalists who have brought the NSA documents leaked by Snowden to light have been isolated or harried by the US and UK governments. Sarah Harrison, the British journalist and WikiLeaks staffer who had been working with Snowden since his arrival in Moscow, eventually left Russia (in November 2013) and joined other activists in Berlin. Her lawyers reportedly advised her that it was "not safe to return home" to the UK. Harrison joined other journalists and activists who were involved in the publication of Snowden's files and are now living in the German capital "in effective exile", including Laura Poitras and Jacob Applebaum.[114]

5 ECONOMIC RESPONSE

Many people think the NSA surveillance practices have not only been aimed at intercepting communications by terrorists, but also aimed at helping US industry. US Director of National Intelligence James Clapper has said the US does not use its foreign intelligence capabilities "to steal the trade secrets of foreign companies on behalf of . . . US companies to enhance their international competitiveness or increase their bottom line." But leaked documents showing that the NSA spied on Brazilian oil company Petrobras and gained access to data held by US cloud providers including Google and Yahoo indicate otherwise.[115] The fact that the US Trade Representative asked the NSA to collect data on organisations also suggests the NSA's surveillance capabilities were used in order to further US trade policies.[116] Other leaked documents purportedly show that the NSA and GCHQ both spied on OPEC.[117] And former US Vice President has said that the US intelligence capability "is enormously important to the United States, to our conduct of foreign policy, to the defense matters, to *economic matters*"[118] [Italics added.] – which further suggests that the NSA's surveillance activities are not only directed towards countering terrorism, but giving the US and American companies economic leverage as well as insight into the negotiating strategies of other countries and companies.

---

[113] Mason, Rowena, "Edward Snowden NSA files: Guardian should be prosecuted, says Tory MP", *The Guardian*, 22 Oct 2013. http://www.theguardian.com/politics/2013/oct/22/edward-snowden-guardian-should-be-prosecuted-tory-mp

[114] Oltermann, Philip, "Sarah Harrison joins other Edward Snowden files 'exiles' in Berlin", *The Guardian*, 6 Nov 2013. http://www.theguardian.com/world/2013/nov/06/sarah-harrison-edward-snowden-berlin

[115] Bryant, Chris, "NSA revelations boost corporate paranoia about state surveillance", *The Financial Times*, 31 Oct 2013. http://www.ft.com/intl/cms/s/0/ec02a8ca-422b-11e3-bb85-00144feabdc0.html

[116] Shane, Scott, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, 2 Nov 2013. http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fworld%2Feurope%2Findex.jsonp The same story says the NSA's "official mission list includes using its surveillance powers to achieve… 'economic advantage' over Japan and Brazil, among other countries".

[117] Spiegel Online International, "Oil Espionage: How the NSA and GCHQ Spied on OPEC", 11 Nov 2013. http://www.spiegel.de/international/world/how-the-nsa-and-gchq-spied-on-opec-a-932777.html

[118] Rhodan, Maya, "Dick Cheney Calls Snowden a 'Traitor,' Defends NSA", *Time*, 28 Oct. 2013. http://swampland.time.com/2013/10/28/dick-cheney-calls-snowden-a-traitor-defends-nsa/

5.1 NSA REVELATIONS THREATENED EU-US TRADE AGREEMENT

There were concerns that the surveillance revelations would complicate negotiations on a wide-ranging free trade agreement between Europe and the United States.[119] Some politicians said the free trade negotiations should be put on hold. European Commission Vice-President Viviane Reding stated, "We cannot negotiate on a large trans-Atlantic market if there is the slightest suspicion that our partners are spying on the offices of our chief negotiator."[120]

Nevertheless, the trade talks on the so-called Transatlantic Trade and Investment Partnership (TTIP) resumed in early November 2013. Some have estimated that a deal could bring annual benefits of €119 billion for the 28 EU Member States. Personal data protection still remains a potential stumbling block. An EU official close to the trade talks conceded "there may be issues of trust", but stressed that Europe would not compromise its personal data protection standards even as it must discuss the wider issue of information transfer.[121]

5.2 STORMS IN THE CLOUD

The European Parliament commissioned a report in 2012 that revealed that the EU was failing to protect its citizens from US surveillance. The October 2012 report warned the European Parliament that the FISA law had granted American spies "heavy-calibre mass-surveillance firepower" and recommended that cloud-storage providers should be required to warn European users of the risks.[122]

The Information Technology and Innovation Foundation, a nonpartisan research and advocacy group funded in part by the technology industry published a report in August 2013 estimating that US data cloud providers could lose $21.5 billion to $35 billion in business over the next three years as a result of the revelations.[123] Some US companies have said they have already lost business, while UK rivals have said that UK and European businesses are increasingly wary of trusting their data to American organisations, which might have to turn it over secretly to the NSA.[124]

A survey by the US-based Cloud Security Alliance found that of those outside the US, 10% had cancelled a project with a US-based cloud computing provider, and 56% would be "less

---

[119] Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

[120] Poitras, Laura, Marcel Rosenbach and Holger Stark, "Codename 'Apalachee': How America Spies on Europe and the UN", *Der Spiegel Online*, 26 Aug 2013. http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[121] AFP, "EU, US return to trade talks under spy scandal cloud", published in *The Nation*, 12 Nov 2013. http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/international/12-Nov-2013/eu-us-return-to-trade-talks-under-spy-scandal-cloud

[122] *The Economist*, "Surveillance: Look who's listening", 15 June 2013. http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

[123] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[124] Arthur, Charles, "Fears over NSA surveillance revelations endanger US cloud computing industry", *The Guardian*, 8 Aug 2013. http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing

likely" to use a US-based cloud computing service.[125] European officials have also talked about the need to have stronger cloud computing capabilities in Europe to provide stronger privacy protections for citizens.[126]

NSA surveillance has already caused considerable political damage in the case of Brazil, seriously undermining the trust between Rousseff and Obama. Brazil now plans to introduce a law that will force companies such as Google and Facebook to store their data inside Brazil's borders, rather than on servers in the US, making these international companies subject to Brazilian data privacy laws. The Brazilian government is also developing a new encryption system to protect its own data against hacking.[127]

5.3 EUROPEAN CLOUDS

Some German companies have seen the Snowden revelations as a marketing opportunity – by offering German customers services that keep German e-mail and Internet traffic within German borders. The companies claim they can improve the security of German communications where they are subject to stricter privacy regulations than the US.[128] The German initiative somewhat mimics that of Brazil whose president, Dilma Rousseff, was also allegedly monitored by the NSA.[129]

European Union leaders have advocated that their 28 nations develop "cloud" data storage that is independent from the United States.[130] Out-Law.com notes that businesses should evaluate their data storage and outsourcing contracts in light of the recent NSA disclosures. "The news could have major implications for outsourcing," the report states, "and will have been unsettling reading for many companies which use cloud services."[131]

Such talk may be one reason why some US industry representatives have reacted angrily to the Snowden revelations. Google Executive Chairman Eric Schmidt, for example, said it was "outrageous", if reports were correct, that the NSA intercepted the company's data centers, especially without authorisation.[132]

---

[125] Arthur, Charles, "Fears over NSA surveillance revelations endanger US cloud computing industry", *The Guardian*, 8 Aug 2013. http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing

[126] Dyer, Geoff, and Richard Waters, "Spying revelations will speed fragmentation of internet, say experts", *The Financial Times*, 31 Oct 2013.
http://www.ft.com/cms/s/0/e028f49c-4257-11e3-9d3c-00144feabdc0.html#axzz2jMUcr8o3

[127] Glüsing, Jens, Laura Poitras, Marcel Rosenbach and Holger Stark, "Fresh Leak on US Spying: NSA Accessed Mexican President's Email", *Spiegel Online International*, 20 Oct 2013.
http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

[128] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[129] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[130] Birnbaum, Michael, "Germany looks at keeping its Internet, e-mail traffic inside its borders", *The Washington Post*, 1 Nov 2013. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html

[131] Bracy, Jedidiah, "NSA Leaks: EU-U.S. Tensions on the Rise, Europe Reacts", *The Privacy Advisor*, IAPP. International Association of Privacy Professionals, 13 June 2013.
https://www.privacyassociation.org/publications/nsa_leaks_eu_u.s._tensions_on_the_rise_europe_reacts_roundup

[132] Kan, Deborah, "Google Chairman Lambastes NSA Actions as 'Outrageous'", *The Wall Street Journal*, 4 Nov. 2013. http://online.wsj.com/news/articles/SB10001424052702304391204579177104151435042

5.4 BETTER ENCRYPTION VS TARGETED ADVERTS

Standards organisations and many companies are reviewing their encryption practices to see how they can make their communications more secure. Google, Yahoo, Twitter and others are doing likewise, but the snag for such companies is that when communications are encrypted and more secure, it makes it more difficult to monitor users' e-mails and to inflict adverts on them.[133]

The Internet Engineering Task Force (IETF) have asked the architects of Tor, networking software designed to make Web browsing private, to consider turning the technology into an Internet standard. The IETF is already working to encrypt more of the data that flows between the individual's computer and the websites she visits.[134]

Tor is the predominant example of onion routing, which is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes called onion routers. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents the intermediary nodes from knowing the origin, destination, and contents of the message.

5.5 LAVABIT REFUSES TO BE "COMPLICIT IN CRIMES AGAINST THE AMERICAN PEOPLE"

Not all US companies bowed to the demands of the US surveillance. Ladar Levison, the founder of Lavabit, the secure e-mail service used by Edward Snowden, shut down his service rather than be "complicit in crimes against the American people", as he put it. He shut down the service rather than comply with a court order to co-operate with the US government in surveillance of his customers. In shutting down his service, Levinson said he "would strongly recommend against anyone trusting their private data to a company with physical ties to the United States". Silent Circle, another provider of secure online services, announced that it too would shut down its own encrypted e-mail service, Silent Mail, rather than support government surveillance of its customers.[135]

5.6 OTHER ECONOMIC IMPACTS: BELGACOM HAS TO CLEAN ITS COMPUTERS OF NSA SPYWARE

The NSA's surveillance activities have generated a variety of economic impacts and responses, not least of which is the cost for some organisations to clean their computers of NSA-installed malware, aimed at spying on high-interest individuals. A leaked document in November 2013 shows that the agency installed malware on some 50,000 computer networks, one of which was Belgacom, the Belgian telecom company.[136]

---

[133] *The Economist*, "Internet security: Besieged", 9 Nov 2013. http://www.economist.com/news/science-and-technology/21589383-stung-revelations-ubiquitous-surveillance-and-compromised-software

[134] Talbot, David, "Group Thinks Anonymity Should Be Baked Into the Internet Itself", *MIT Technology Review*, 26 Nov 2013. http://www.technologyreview.com/news/521856/group-thinks-anonymity-should-be-baked-into-the-internet-itself/

[135] Ackerman, Spencer, "Lavabit email service abruptly shut down citing government interference", *The Guardian*, 9 Aug 2013. http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden

[136] Manning, Craig, "Report: NSA installed malware on 50,000 computer networks worldwide", *National Monitor*, 24 Nov 2013.

6 MEDIA RESPONSE

6.1 NOT A ONE-DAY WONDER

The phrase "one-day wonder" refers to an event that gets splashed across the front pages of newspapers, but the story only gets visibility for a day. The Snowden revelations about the extent of the NSA's surveillance have managed to hold the media's attention for months since *The Guardian* broke the first story in early June 2013. That story made the front pages in various countries around the world, and the media have continued to give the Snowden revelations front-page treatment virtually every day since the first leaks appeared. Initially the revelations appeared in *The Guardian*, *The New York Times* and *The Washington Post*, but since the early days of June, many newspapers have had "exclusives".

The Snowden revelations are arguably different from other leaks in the sense that the media have given them far more attention. The so-called "one-day wonder" does not apply to the revelations. Some newspapers say that Snowden passed on some 58,000 documents – and perhaps even more[137] -- to the media, notably Glenn Greenwald of *The Guardian* and free-lancer Laura Poitras. Hence, the revelations are expected to continue some time to come.

One could also argue that Snowden revelations have made headlines for such a long time because of a smart media strategy by *The Guardian* and others. They let out only bits and pieces and as soon as the media interest seems to be waning, they produce new stories, so that keeps the topic on the public agenda.

Austrian critic Karl Kraus has said a scandal begins when the police put an end to it, i.e., many people in the trade knew about the extent of surveillance, about the more or less secret co-operation of different security services worldwide, about the exchange of intelligence – but that was kept secret! Now such knowledge has become public, and that changes the rules of the game, since "secret service" has turned into a kind of "public service".

6.2 POLITICAL PRESSURE ON THE MEDIA

One member of the US Congress has already likened what journalists Laura Poitras and Glenn Greenwald have done to a form of treason, and they are well aware of the Obama administration's unprecedented pursuit of not just leakers but of journalists who receive the leaks.[138] Especially the US and UK governments have put pressure on *The Guardian* and *The New York Times* to stop publishing stories based on the leaked documents. They have said the media have threatened efforts to curtail terrorism.

---

http://natmonitor.com/2013/11/24/report-nsa-installed-malware-on-50000-computer-networks-worldwide/

[137] NSA director general Keith Alexander has been quoted as saying that "Snowden has shared somewhere between 50 and 200,000 documents with reporters". Mathew, Jerin, "Edward Snowden Leaked up to 200,000 NSA Top Secret Documents", *International Business Times*, 15 Nov 2013.
http://www.ibtimes.co.uk/articles/522484/20131115/edward-snowden-nsa-scandal-keith-alexander.htm?utm_source=dlvr.it&utm_medium=gplus

[138] Maass, Peter, "How Laura Poitras Helped Snowden Spill His Secrets", *The New York Times*, 13 Aug 2013.
http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=1&_r=0

Lord Carlile of Berriew, a leading QC and former terrorism watchdog in the UK, has described publication of stolen secrets by *The Guardian* as a "criminal act" and that it was wrong to paint the newspaper's journalists as "virtuous whistleblowers".[139]

UK cabinet secretary Sir Jeremy Heywood told *The Guardian* to destroy the NSA files in its possession, apparently on instruction from prime minister David Cameron, as the files represented a threat to national security. *The Guardian* agreed to destroy two hard drives in the presence of two security experts from GCHQ after the government threatened to take legal action. *Guardian* editor Alan Rusbridger told officials that *The Guardian* would continue to report from the leaked documents because it had back-up copies in the US and in Brazil.[140]

David Cameron has said he would take stronger action against *The Guardian* and other newspapers to stop them from publishing stories about GCHQ surveillance.[141] *The Guardian*, he said, was refusing to behave with "social responsibility", despite repeated warnings that the revelations are damaging to national security.[142]

In early December 2013, *Guardian* editor Alan Rusbridger was summoned to give evidence at a parliamentary inquiry by the House of Commons Home Affairs Select Committee, where some MPs accused him of helping terrorists by making top secret information public and sharing it with other news organisations. One MP said Rusbridger had committed an offence under Section 58A of the Terrorism Act which says it is a crime to publish or communicate any information about members of the armed forces or intelligence services. At the same parliamentary inquiry, London Metropolitan Police Assistant Commissioner Cressida Dick told MPs the police were examining whether *Guardian* newspaper staff as well as David Miranda, partner of Glen Greenwald, should be investigated for terrorism offences over their handling of data leaked by Edward Snowden.[143]

The New York Times carried a trenchant editorial in support of *The Guardian* and decrying the challenge by the Cameron government to a free British press. *The Times* said in part:

> Unlike the United States, Britain has no constitutional guarantee of press freedom.
> Parliamentary committees and the police are now exploiting that lack of protection to harass, intimidate and possibly prosecute The Guardian… the public has a clear interest in learning about and debating the N.S.A.'s out-of-control spying on private communications. That interest is shared by the British public as well.

The Times attacks British parliamentarians for not asking tough questions of the British intelligence agencies and, instead, for going after *The Guardian*.

---

[139] Barrett, David, "Publishing Edward Snowden security secrets a 'criminal' act, says former terrorism watchdog", *The Telegraph*, 24 Oct 2013. http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10401711/Publishing-Edward-Snowden-security-secrets-a-criminal-act-says-former-terrorism-watchdog.html

[140] Watt, Nicholas, "Guardian told to destroy NSA files for national security, says Clegg", *The Guardian*, 21 Aug 2013. http://www.theguardian.com/uk-news/2013/aug/21/nsa-nick-clegg-guardian-leaked-files

[141] BBC News, "Cameron threatens to act against newspapers publishing security leaks", 28 Oct 2013. http://www.bbc.co.uk/news/uk-politics-24710826

[142] Shipman, Tim, "Prime Minister threatens Guardian with legal action over 'damaging' spy leaks", *Daily Mail*, 29 Oct 2013. http://www.dailymail.co.uk/news/article-2478692/Prime-Minister-threatens-Guardian-legal-action-damaging-spy-leaks.html

[143] James, William, and Michael Holden, "British news staff may face terrorism charges over Snowden leaks", Reuters, 3 Dec 2013. http://uk.reuters.com/article/2013/12/03/uk-britain-snowden-guardian-idUKBRE9B20TI20131203

> Alan Rusbridger, the newspaper's editor, has been summoned to appear before a parliamentary committee next month to testify about The Guardian's internal editorial decision-making regarding the Snowden information. Members of Parliament have also demanded information on the newspaper's decision to make some of the leaked information available to other journalists, including those at The Times. That should be none of Parliament's business. Meanwhile, Scotland Yard detectives are pursuing a criminal investigation into The Guardian's actions surrounding the Snowden leaks.
>
> These alarming developments threaten the ability of British journalists to do their jobs effectively… The global debate now taking place about intelligence agencies collecting information on the phone calls, emails and Internet use of private citizens owes much to The Guardian's intrepid journalism. In a free society, the price for printing uncomfortable truths should not be parliamentary and criminal inquisition.

It is, principally, the media who stand between the Orwellian surveillance practices of government and big industry on the one hand and the public on the other. Governments, such as the UK's Cameron government, play a dangerous game with democracy by attacking the media's reportage of their abuses against the people.

Meanwhile, *The Guardian* cited remarks by Frank La Rue, the UN special rapporteur on freedom of expression, who said he was alarmed at the political reaction to the Snowden revelations. "I have been absolutely shocked about the way the Guardian has been treated, from the idea of prosecution to the fact that some members of parliament even called it treason," said La Rue. "I think that is unacceptable in a democratic society."[144]

6.3 THE MEDIA REMAIN DEFIANT

In an editorial soon after the initial Snowden revelations, *The New York Times* commented in an editorial that

> the Obama administration issued the same platitude it has offered every time President Obama has been caught overreaching in the use of his powers: Terrorists are a real menace and you should just trust us to deal with them because we have internal mechanisms (that we are not going to tell you about) to make sure we do not violate your rights. Those reassurances have never been persuasive….[145]

Certainly such reassurances have not persuaded newspapers such as *The Guardian* which has continued to publish stories based on the revelations. Glenn Greenwald and his colleagues have remained defiant. "Exclusives" based on the leaked documents have now appeared in many newspapers, not only in the UK and US, but also in other countries, notably Germany, France, Spain, Brazil and elsewhere.

6.4 THE MEDIA HAVE BEEN RAISING PUBLIC AWARENESS

Laura Poitras, one of the first three journalists to interview Snowden, commented about the NSA revelations: "Do I think the surveillance state is out of control? Yes, I do. This is scary, and people should be scared. A shadow and secret government has grown and grown, all in

---

[144] Matthew Taylor, Nick Hopkins and Phil Maynard, "UK's reputation is damaged by reaction to Edward Snowden, says UN official", *The Guardian*, 15 Nov 2013.
http://www.theguardian.com/world/2013/nov/15/uk-reputation-edward-snowden-un

[145] The Editorial Board, "President Obama's Dragnet", Editorial, *The New York Times*, 6 June 2013.
http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=all&_r=

the name of national security and without the oversight or national debate that one would think a democracy would have."[146]

The media have played an enormous role in raising citizen awareness of the surveillance revelations and its consequences. The reportage has had a strongly ripple effect throughout society as civil society activists have mobilised against dragnet surveillance and other public figures have lent their support for reining back the extent to which the NSA and others are able conduct their activities with little effective oversight and massive budgets.

7 POSITIVE IMPACTS OF THE REVELATIONS

The Snowden revelations have immeasurably helped to raise society's awareness of the pervasiveness of surveillance by the NSA and, to a lesser extent, GCHQ and other intelligence agencies. The revelations may also have increased public attention on the ubiquity of surveillance more generally, including that by the large corporations.

The revelations have placed surveillance high on the political agenda. The issue of accountability is now being discussed. Until the revelations began, it appeared that there was minimal or no accountability of the NSA and GCHQ to their elected officials.

Awareness of the extent of surveillance by the NSA and GCHQ has led to resistance, i.e., some politicians, such as Angela Merkel, have called for the NSA to stop monitoring her mobile phone calls. Brazilian president Dilma Rousseff showed her anger at NSA monitoring her communications by cancelling a meeting with Obama and by promoting legislation to force global Internet companies to store data obtained from Brazilian users inside the country.[147] Some of the companies subject to surveillance intrusions have increased their security to make it more difficult for governments to surveil their networks.[148]

The revelation that the NSA has been monitoring not only the communications of ordinary citizens but also the political leaders of 35 ally countries has led to greater solidarity between the political leaders and citizens. Angela Merkel did not say much when the NSA's monitoring of Germans was made public, but she was much more forthright when she learned that the NSA had been monitoring her calls since 2002. At first, when the revelations began, Merkel defended German co-operation with the NSA. "The work of intelligence agencies in democratic states was always vital to the safety of citizens and will remain so in the future," Ms. Merkel was quoted as saying in an interview published in the newspaper *Die Zei*t. "For me, there is absolutely no comparison between the Stasi in East Germany and the work of intelligence services in democratic states," she added, calling the programs "two totally different things." In the *Die Zeit* interview, Ms. Merkel reminded Germans of the important

[146] Maass, Peter, "How Laura Poitras Helped Snowden Spill His Secrets", *The New York Times*, 13 Aug 2013. http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=1&_r=0

[147] Israel, Esteban, and Anthony Boadle, "Brazil to insist on local Internet data storage after U.S. spying", Reuters, 28 Oct 2013. http://www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028

[148] Smith, Chris, "Twitter adds another layer of security to keep out the government snoops", *Tech Radar*, 23 Nov 2013. http://www.techradar.com/news/internet/twitter-adds-another-layer-of-security-to-keep-out-the-government-snoops-1202147

role the United States has played in the country's postwar history.[149] A couple of months later, when she discovered her mobile calls were being intercepted, she was not quite so relaxed about it.

While the media attention has been on the extent of the NSA's surveillance, the media have not focussed so much on the extent of surveillance by companies such as Google, Facebook, Amazon, Yahoo and other large multinats. However, if a whistleblower were to leak how extensive surveillance by these companies has been, there might be similar outrage.

8 CONCLUSIONS

8.1 FAILURE OF OVERSIGHT

Stephen Walt, Harvard professor of international affairs, has stated that "Once a secret surveillance system exists, it is only a matter of time before someone abuses it for selfish ends."[150] Hence, there is an apparent need for oversight of such systems. However, as the NSA revelations have continued, it has become obvious that the intelligence agencies in the US and UK (and perhaps elsewhere) have lacked proper oversight. *The New York Times* has commented that "Despite the agency's embrace of corporate jargon on goal-setting and evaluation, it operates without public oversight in an arena in which achievements are hard to measure."[151]

In late October 2013, Congressional Democrats and Republicans introduced a bill that would curb some of the NSA's practices. Representative John Conyers Jr., Democrat of Michigan, a sponsor of the bill, said at the time that "Our intelligence community has operated without proper congressional oversight or regard for Americans' privacy and civil liberties."[152] The issue of oversight of the intelligence agencies is now firmly on the public agenda.

In the UK, at the first public hearing of the parliamentary Intelligence and Security Committee (ISC), GCHQ director Iain Lobban, head of MI5 Andrew Parker, and head of MI6 John Sawers all said the current oversight system is working well and there was no pressing need to update technology-neutral laws as the principles of necessity and proportionality within the law were sufficient to guide the actions of the intelligence agencies.

Not everyone shares their views. If anything, the Snowden revelations have made abundantly clear the failure of oversight. Gus Hosein, executive director at Privacy International, told the LIBE committee of the European Parliament that the UK parliamentary committees that are supposed to keep intelligence services in check have become nothing more than "cheerleaders" for those intelligence agencies. He said there had been no discussion of the NSA's PRISM surveillance programme or GCHQ's TEMPORA fibre-optic tapping

---

[149] Eddy, Melissa, "Merkel Appears to Weather Anger Among German Voters Over N.S.A. Spying", *The New York Times*, 11 July 2013. http://www.nytimes.com/2013/07/12/world/europe/merkel-seems-to-weather-german-anger-over-nsa-spying.html?_r=0

[150] Walt, Stephen, "Snowden deserves an immediate presidential pardon", *The Financial Times*, 8 July 2013. http://www.ft.com/cms/s/0/0ccf2d14-e7c1-11e2-babb-00144feabdc0.html#axzz2YiI70RAU

[151] Shane, Scott, "No Morsel Too Minuscule for All-Consuming N.S.A.", *The New York Times*, 2 Nov 2013. http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?src=un&feedurl=http%3A%2F%2Fjson8.nytimes.com%2Fpages%2Fworld%2Feurope%2Findex.jsonp

[152] Landler, Mark, and Michael S. Schmidt, "Spying Known At Top Levels, Officials Say", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/officials-say-white-house-knew-of-spying.html

programmes by the UK Parliament's Intelligence and Security Committee prior to Snowden's whistleblowing.[153]

The Financial Times and *The Guardian* both found the UK's Intelligence and Security Committee wanting; the members failed to provide the spymasters with a tough grilling.[154] Sources subsequently told *The Sunday Times* that the heads of MI5, MI6 and GCHQ agreed to appear before the ISC on the condition that they were told the questions beforehand – which led one MP to comment: "'Evidently the whole thing was a total pantomime."[155]

A Conservative MP in the UK has suggested parliamentary oversight of surveillance could be improved if the Intelligence and Security Committee were chaired by a member of the opposition to ensure its independence and be freely elected by MPs.[156] Transparency – in making such hearings public, as occurred when the spymasters appeared before the ISC – should also help improve oversight, but on this occasion, the transparency was a charade. Not feeding or agreeing questions beforehand with those appearing before the committee would have been a wiser course of action. Subjecting the spymasters to interrogation by the media might have led to tougher questions. Even so, the spymasters felt sufficiently powerful that they could, and did, refuse to answer questions on the grounds of national security. However, if spymasters refuse to answer such questions, at least in camera, then it becomes another indication of the breakdown of democracy.

8.2 THE BANE OF THE PRIVACY–SECURITY TRADE-OFF PARADIGM

The NSA revelations have shown just how endemic and widespread is the paradigm of a "balance" or "trade-off" between security and privacy. For example, when the Spanish government summoned the American ambassador to address allegation that the NSA had been surveilling the Spanish population, the ambassador told reporters afterwards that "Ultimately, the United States needs to balance the important role that these programs play in protecting our national security and protecting the security of our allies with legitimate privacy concerns." Ironically, Spanish secretary of state Iñigo Méndez de Vigo, in a separate statement, referred to the same paradigm when he said there was a need to maintain "a necessary balance" between security and privacy.[157]

The Obama White House uses this paradigm, as when a spokesman said: "The president welcomes a discussion of the trade-offs between security and civil liberties." Use of this paradigm has appeared in public opinion surveys. The Angus Reid Global survey, mentioned

---

[153] Ashford, Warwick, "NSA and GCHQ mass surveillance violates EU law, study finds", ComputerWeekly.com, 8 Nov 2013. http://www.computerweekly.com/news/2240208711/NSA-and-GCHQ-mass-surveillance-violates-EU-law-study-finds

[154] Blitz, James, "Parliamentary panel fails to serve up a good grilling", *The Financial Times*, 7 Nov 2013. http://www.ft.com/cms/s/0/fb09950a-47d9-11e3-b1c4-00144feabdc0.html#axzz2jztTy1by; Weaver, Matthew, "Key questions the chief spooks were asked, and those they did not hear", *The Guardian*, 8 Nov 2013. http://www.theguardian.com/world/2013/nov/08/nsa-leaks-parliamentary-questions-analysis

[155] *Daily Mail*, "So much for the interrogation: Spy chiefs knew what questions were going to be asked BEFORE parliamentary committee", 17 Nov 2017. http://www.dailymail.co.uk/news/article-2508779/Spy-chiefs-fed-questions-advance-parliamentary-committee-hearing.html

[156] Quinn, Ben, "Tory MP adds to calls for improved oversight of UK intelligence services", *The Guardian*, 5 Nov 2013. http://www.theguardian.com/world/2013/nov/05/tory-mp-intelligence-services

[157] Minder, Raphael, "Spain Summons American Ambassador on New Reports of N.S.A. Spying", *The New York Times*, 28 Oct 2013. http://www.nytimes.com/2013/10/29/world/europe/spain-calls-in-us-ambassador-in-spying-scandal.html?_r=0

above, found public support for the argument that security and anti-terrorism efforts include trade-offs against civil liberties and personal information privacy. In its survey of Canada, the US and the UK, the pollsters found that 60 per cent of UK respondents took this view, compared with 54% of Americans. Canadian public opinion was almost evenly split on the issue (49% vs 51%).[158]

The media also use the balance metaphor.[159] In spite of the fact that various officials, politicians, the media and others have referred to the need for a proper balance between privacy and security, the metaphor is a red herring, conceptually flawed and downright dangerous for civil liberties. If privacy is being traded off against national security, individual privacy will always lose out to collective security, even though privacy is a cornerstone of democracy. Many experts and academics have discredited the trade-off paradigm.[160] It is possible to have both privacy and security, without reducing one or the other. A better paradigm is risk management, i.e., to identify risks to privacy and security, either separately or together, and, preferably in consultation with stakeholders, to identify ways of overcoming those risks with no or minimal negative impacts on privacy and/or security.

Although even senior industry people seem to think in terms of the trade-off paradigm, Google Executive Chairman Eric Schmidt said the right balance of security and privacy starts with finding the appropriate level of oversight. "There clearly are cases where evil people exist, but you don't have to violate the privacy of every single citizen of America to find them."[161] The balance paradigm may be wrong, but the oversight is surely right. Ironically, many regulators struggle to provide adequate oversight of Google itself. The surveillance in which Google is engaged is arguably just as damaging to privacy as that of the NSA.

Jo Glanville, the chief executive officer of English PEN, has said that keeping the country safe does not entitle the government or the intelligence services to act without regard to our human rights. Glanville, importantly and correctly, made the point that "They are not mutually exclusive. It is possible to conduct targeted surveillance with effective oversight while according respect to all our rights."[162]

8.3 UNANSWERED QUESTIONS

The Snowden revelations have raised a host of issues for Europe as well as other countries. Among these issues are the following:

To what extent are European countries able to protect their citizens from unauthorised surveillance by the US?

---

[158] Angus Reid Global, "More Canadians & Britons view Edward Snowden as 'hero' than 'traitor', Americans split", 30 Oct 2013. http://www.angusreidglobal.com/polls/48837/more-canadians-britons-view-edward-snowden-as-hero-than-traitor-americans-split/

[159] "The disclosures of the National Security Agency's activities by a former contractor for it, Edward J. Snowden, have set off a fierce debate on both sides of the Atlantic about the proper balance between privacy and economic, security and other interests." Higgins, Andrew, and James Kanter, "As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home", *The New York Times*, 29 Oct 2013. http://www.nytimes.com/2013/10/30/world/europe/as-it-denounces-us-spying-europe-delays-privacy-protection-at-home.html

[160] See, for example, Zedner, Lucia, *Security*, Routledge, Abingdon [UK], 2009, pp. 134-137.

[161] Kan, Deborah, "Google Chairman Lambastes NSA Actions as 'Outrageous'", *The Wall Street Journal*, 4 Nov. 2013. http://online.wsj.com/news/articles/SB10001424052702304391204579177104151435042

[162] Quinn, Ben, "Tory MP adds to calls for improved oversight of UK intelligence services", *The Guardian*, 5 Nov 2013. http://www.theguardian.com/world/2013/nov/05/tory-mp-intelligence-services

To what extent is the US threatening European economic interests by US surveillance of European trade negotiations and strategy?

Is the US gaining an unfair advantage over European companies by its surveillance?

Is European press freedom threatened by comments from David Cameron to stop *The Guardian* and other newspapers from continuing to publish leaked information?

Are political leaders simply embarrassed by the revelations and, to cover their embarrassment, are making comments that the revelations are damaging national security?

Are intelligence agencies sufficiently accountable to elected representatives?

Should secret laws be permitted in an open democracy?

Could the NSA influence the outcome of elections in Europe (or elsewhere) by leaking damaging information about a candidate?[163]

What do we have to fear as ordinary citizens? As we know, there is the problem of information overload: the needle in the haystack will not be found easily and the less so, the bigger the haystack. With regard to personal data and privacy, we do not know what algorithms are applied to the data scooped up by the NSA, and whether we will be swept up as part of the dragnet. Certainly, that is the rational basis of public concerns about the extensive NSA surveillance. But what are the chances of that happening for otherwise ordinary citizens? We don't know. Nor do we know how metadata are analysed, and what it takes to end up on the screens of the secret services.

The main drivers for the whole surveillance process are heavily economic in nature: industry wants to sell their equipment and services, and big corporations want to protect their (online) assets from espionage. This economic rationale is reinforced by administrative logic and political strategies, i.e., the intelligence agencies want to increase their powers and the political actors want to make sure they have taken any necessary precautions to protect their homelands from terrorists.

8.4 THE BREAKDOWN OF OPEN DEMOCRACY

If the leaked documents were a revelation to the American and European peoples, they were also a revelation for some of their political leaders. According to the Liberal Democrat former cabinet minister Chris Huhne, neither the cabinet nor the National Security Council was informed about the PRISM and TEMPORA programs. "The cabinet was told nothing about…their extraordinary capability to vacuum up and store personal emails, voice contact, social networking activity and even internet searches," he wrote in *The Guardian*.[164]

[163] A recent example of an attempt by an intelligence agency to influence a democratic election is recounted here: Sang-Hun, Choe, "Prosecutors Detail Attempt to Sway South Korean Election", *The New York Times*, 21 Nov 2013. http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?_r=0. "Prosecutors have indicted several top intelligence officials, including Won Sei-hoon, the former director of the spy agency [the National Intelligence Service of South Korea], on charges of ordering an online smear campaign against opposition candidates in violation of election law."

[164] Rusbridger, Alan, "The Snowden Leaks and the Public", *The New York Review of Books*, issue of 21 Nov 2013. http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/?pagination=false

Similarly, reports suggest that Obama did not know that the NSA was intercepting Angela Merkel's mobile phone.[165]

The Snowden revelations have led to a breakdown in trust, as various European leaders have said, between Europe and the US. Trust is easy to break, but hard to repair. But the issue of trust is not only between Merkel and Obama, and other political leaders, but also between citizens and their leaders. In the UK, citizens have to trust a government committee whose members are themselves not trusted to know about the most significant surveillance programs of all.[166]

The New York Times has commented that "To casually permit this surveillance — with the American public having no idea that the executive branch is now exercising this power — fundamentally shifts power between the individual and the state, and it repudiates constitutional principles governing search, seizure and privacy."[167]

The NSA revelations call into question the nature of our democracies. It puts a whole new spin on the open nature of democracy, i.e., the openness of our democracy has made it easy for the NSA to exploit. The safeguards against abuse have been inadequate. Can a government of the people for the people exist when powerful minorities completely overwhelm democratic values? According to Guardian editor Alan Rusbridger:

> The security apparatus is today able in many democracies to exert a measure of power over the other limbs of the state that approaches autonomy: procuring legislation which prioritises its own interests over individual rights, dominating executive decision-making, locking its antagonists out of judicial processes and operating almost free of public scrutiny.[168]

The Observer, the sister newspaper to the Guardian has seen the dangers to democracy. The newspaper carried an item in which the following comment was made:

> The "mess" that the NSA (and our own dear GCHQ) has landed us in is a symptom of a major failure of our political systems. All democracies are impaled on the horns of the same dilemma: they need openness, because the consent of the governed requires that people know what is being done in their name; but sometimes openness undermines the efficacy of the secret (and perhaps necessary) things that are done in their name. The choice is then between sacrificing accountability or sacrificing secrecy… We urgently need something better and if we don't get it then we could be, as one spook put it, "a keystroke away from totalitarianism".[169]

A Conservative backbench MP, David Davis, has expressed strong support for the role played by Snowden and argued that "The only protection for us all in this sort of area is actually whistleblowers. It's the only thing that makes these sorts of organisations behave properly."[170]

---

[165] *The Economist*, "Cloaks off", 2 Nov 2013. http://www.economist.com/news/international/21588890-foreign-alarm-about-american-spying-mounting-sound-and-fury-do-not-always-match-0

[166] Rusbridger, op. cit.

[167] The Editorial Board, "President Obama's Dragnet", Editorial, *The New York Times*, 6 June 2013. http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=all&_r=

[168] Rusbridger, op. cit.

[169] Naughton, John, "Why the NSA has landed us all in another nice mess", *The Observer*, 1 Dec 2013. . http://www.theguardian.com/world/2013/dec/01/nsa-edward-snowden-survelliance-internet

[170] Quinn, Ben, "Tory MP adds to calls for improved oversight of UK intelligence services", *The Guardian*, 5 Nov 2013. http://www.theguardian.com/world/2013/nov/05/tory-mp-intelligence-services

It seems appropriate to conclude this section with a statement from Edward Snowden, one that he made (in writing) to the European Parliament's LIBE committee:

> The surveillance of whole populations, rather than individuals, threatens to be the greatest human rights challenge of our time…. A culture of secrecy has denied our societies the opportunity to determine the appropriate balance between the human right of privacy and the governmental interest in investigation. These are not decisions that should be made for a people, but only by the people after full, informed, and fearless debate. Yet public debate is not possible without public knowledge, and in my country, the cost for one in my position of returning public knowledge to public hands has been persecution and exile. If we are to enjoy such debates in the future, we cannot rely upon individual sacrifice. We must create better channels for people of conscience to inform not only trusted agents of government, but independent representatives of the public outside of government.[171]

8.5 RESILIENCE IN A SURVEILLANCE SOCIETY

The Snowden revelations have not been a uniform horror for privacy. While the extent of surveillance in society is far greater than most people might have managed, the revelations have served to demonstrate resilience and resistance too.

If one were to ask how can resilience be operationalised, one could consider at least two different paradigms. Nominally, one paradigm for resilience in a surveillance society might be like that of a command centre that takes various measures to stimulate societal resilience and/or resistance to the increasing prevalence and pervasiveness of surveillance in society. Another paradigm might be that resilience is like a mesh network: it builds across society, with no central point. In other words resilience becomes viral and out of the hands of any central authority.

The Snowden revelations, however, present an interesting exercise in mapping resilience in a surveillance society. In this case, one person, Edward Snowden, a whistleblower of heroic proportions (in more senses than one) has leaked thousands of documents showing what the NSA has been doing in mass and targeted surveillance. He leaked the documents to two journalists, Glenn Greenwald and Laura Poitras, and those journalists broke the story in *The Guardian* which then created a media sensation as other newspapers, especially including *The New York Times* and *The Washington Post*, picked up the story and started to publish some exclusives based on leaked documents. While *The Guardian* has continued to publish exclusives, many other newspapers and media outlets in various other countries – Germany, Spain, the Netherlands, Australia, Brazil, Indonesia, etc., have been publishing "exclusives" too. Snowden claims not to have kept any documents on his laptops or memory sticks when he flew from Hong Kong to exile in Moscow. Thus, the media have been passing leaked documents among themselves. So in terms of news flow, we see a phenomenon of one (Snowden) to two (Greenwald and Poitras) to many.

In terms of the societal response to these stories, there have been many. The public in general and many politicians (those spied upon especially) have expressed outrage. Their awareness of surveillance has certainly been ratcheted up a lot. While people may be "coping" with a new awareness of how extensive surveillance is, there has been a lot of resistance too.

---

[171] Snowden, Edward, Statement to the LIBE Inquiry meeting of 30 September 2013. http://www.europarl.europa.eu/committees/en/libe/events.html?id=hearings

In efforts to counter mass and targeted surveillance, many people, political leaders, industries are other stakeholders are taking a range of political and technological measures to increase their privacy. Some of these efforts are co-ordinated, many are not.

Citizens are taking steps to protect their privacy. They are adopting technologies and services to protect their privacy. So are companies such as Google, Yahoo, Twitter and others, by encrypting links between their servers. It is difficult to say how successful these efforts will be in countering the depredations of the intelligence agencies, but at least efforts are being made. Other businesses are protesting surveillance and secret orders to reveal who are using their services: Lavabit has taken the extraordinary measure of shutting down its business altogether.

Brazil, Germany and others are considering efforts to keep traffic within their countries or at least forcing foreign-based businesses wanting to provide services in their countries to meet their standards and requirements. Brazil and Germany have also co-sponsored a resolution at the UN to roll back surveillance.

The European Parliament has reinstated Art. 41.1 in the proposed Data Protection Regulation. MEPs and data protection authorities are renewing their scrutiny of the Safe Harbor agreement. The European Parliament (the LIBE committee) has been holding hearings to which various experts have been providing their views.

The public are expressing their views in many unco-ordinated ways – e.g., in their comments to news stories, in their petition to the White House to pardon Snowden, in placing adverts on buses in Washington about Snowden and so on.

The public is also expressing its lack of trust in politicians and other institutions in opinion polls. Obama, especially, will have to do a lot to re-establish trust in his government.

There is a ground swell of public opinion questioning how extensive surveillance needs to be. The issue is now high on the public agenda and politicians will need to develop a policy on what is acceptable, and try to convince voters that they can be trusted to take public opinion into account. One can expect better oversight of the intelligence agencies in the weeks, months and perhaps years to come.

In resilience terms, people and organisations are both "coping" and taking anticipatory measures. They assume that this high level of surveillance will continue, hence they are "anticipatory" – they are taking technical measures (e.g., to encrypt communications) to protect their communications as well as social measures (such as those mentioned above) that anticipate continued surveillance but also, at the same time, are acts of resistance.

Thus, as a paradigm of resilience in a surveillance society, we have witnessed a mixture of both resilience (as coping and as anticipatory) and resistance, in short a blending of the two above-mentioned paradigms. Above all, the Snowden revelations show us that resilience builds from communications, whether one-to-many or many-to-many.

The next section of this paper outlines a set of recommendations that can further strengthen resilience and resistance to the extent of surveillance in society today.

8.6 PROTECTING PRIVACY IN A SURVEILLANCE SOCIETY – A WAY FORWARD

The default setting in political, corporate and societal thinking is that there should be no mass surveillance unless any particular system can be justified, starting with a privacy impact assessment, review by a regulatory authority and parliamentary oversight committee.

Governments and companies should be obliged, thereby, to undertake a privacy impact assessment, which should include stakeholder engagement, publication of the PIA report and independent, third-party review.

Existing mass surveillance systems that have not heretofore been subject to a privacy impact assessment should be reviewed and terminated where there is no good justification for such systems.

Parliamentary or congressional oversight committees should be, as recommended above, led by a member of the opposition.

Transparency is essential if governments (and corporate leaders) are to rebuild trust. There should be no secret laws.

Politicians, such as Angela Merkel, are right to feel aggrieved about the extent to which they have been subject to surveillance by the NSA or other intelligence agencies. But the public is entitled equally to feel aggrieved. While politicians of allies should not be subject to surveillance, neither should the public.

Mass surveillance operations, supposedly to catch terrorists or criminals, that endanger the privacy of citizens should be terminated. While terrorism is intolerable, the rape of privacy in a democracy is also intolerable. Intelligence agencies need to find more targeted alternatives to apprehending terrorists.

To protect privacy in a surveillance society, society needs to impose controls on surveillance, specifically, political leaders and regulators must introduce legislation that places controls on, especially, mass surveillance systems, whether they are governmental systems or private systems created by the Google, Facebook, Amazon and their like.

Governments, especially, should conduct regular opinion surveys to have an unbiased reading of what the public thinks about the extent of surveillance in society.

Parliaments should have independent annual reports on the state of privacy and surveillance, which should include recommendations on how citizens, groups and society can better protect privacy.

8.7 IN THE FINAL ANALYSIS

What we have presented so far is the emergence of a debate over the legitimacy of surveillance in contemporary societies, triggered by the revelation of a single individual and distributed through media channels.

Looking at the recent events and discussions in the wake of the Snowden revelations from a perspective of social and political theory a number of issues emerge that point beyond the

immediate debate over the questionable practices of the intelligence-industrial complex. The events can be put in a larger context of social and cultural patterns of social integration, governance and control. Taking this wider perspective can help to better understand how to adequately react to the problems made visible by an individual whistleblower and the subsequent investigations by media and surveillance activists.

One of the important questions raised by this affair is whether a society as a whole in the medium of public discourse can develop a balanced and reasonable understanding of threats and dangers and how these should be addressed.

From ancient times, cultures have developed ideas about their powerful enemies. The inner social working of groups was threatened by the wrath of gods, by external demons, by hostile neighbours, brute force of nature, pandemics or other forces of evil. What all these evil forces had in common was their intangibility. Present day societies display a similar ecology of fear. They develop popular images of imminent threats to social order, life and limb of the citizens. A whole pandemonium of threats can be brought into the foreground to justify an array of remedial actions. From a sociological perspective, these threats work as mechanisms to mark and maintain the boundary of a social group or society. They introduce the distinction between "Us" and "Them". In the age of globalised, multi-cultural, multi-ethnic, trans-national, media-driven societies, it becomes difficult to sustain such boundary maintenance mechanisms. While in the recent past, during the so-called bipolar world order, such a boundary could be drawn by pointing to communism as the dominant threat to the "Free West", today we see a shift from the East-West to the North-South divide. The dominant threat is construed no longer along ideological lines but along religious and cultural lines. Jihadists and Islamic fundamentalists, operating from the global South, have replaced communist agitators and infiltrators.

Taking this analytical perspective, a number of politically salient topics can be interpreted as means to maintain the boundary of the social group at different scales. Public concern about climate change, global warming and pollution re-creates "Nature" as the "Other" to society. Threats are emanating from beyond the social sphere jeopardising the very survival of mankind. Beyond these global threats are suitable enemies to be found at national and local levels performing the task of defining the line between Us and Them: criminals, welfare mothers, drug addicts and many others can be activated as popular images to demonstrate who the good guys are and where the realm of evil begins against which the law-abiding citizens have to be protected.

These threats have a number of features in common: they are made visible and tangible by the media; they require massive surveillance to be kept under control and some sort of remedial action curtailing the freedom of citizens seems necessary to combat these threats. Take the ozone hole as an example: as a hybrid object comprised of scientific observation, political discourse and massive media coverage, it emerges in society carrying with it the warning to change consumption and production patterns of industrial economies. It is coming from outside, threatening society and requiring urgent action. The same could be said about criminals, drug users and of course Jihadists and Islamic fundamentalists. They emerge as objects of public concern and policy, coming from outside the realm of our life world, threatening social order and are made visible as objects of fear primarily through media coverage. To understand the logic of this ecology of fear, fuelled by different types of public enemies, one has to understand the dynamics and working of public media discourse. The media compete for a share of voice and public attention is limited. Public policy is tied into

this process of generating arousal and concern, rallying for support for remedial action. In order to establish an object or group as an imminent and massive threat to society many different actors and stakeholders have to cooperate: media, policy actors, social movements, and other groups and organisations have to pool their resources in order to create the momentum for a successful campaign establishing a sustainable idea of an enemy in public consciousness.

What makes the Snowden revelations stand out in this game of media-amplified construction of public enemies is the reversal of the logic. Instead of focussing on the threats posed by an external enemy, the remedial actions to combat the presumed threat were scandalised. This has created the rare situation of a balance of means among proponents and critics of the political game of fear. What Snowden and all the others making the information he collected public did was to turn the logic of the media against a security-political-industrial complex distributing images of an imminent threat using the very same mechanisms. Applying the notion of boundary maintenance, this for the first time created a situation where a substantial portion of the general public started to entertain the idea that the cure might be worse than the disease. Instead of strengthening social cohesion by focussing on the external enemy, people were irritated as to whether they could rely on some of their entrenched beliefs about the working of the state. This seemed to trigger a hitherto unknown activity of what could be called practices of self-defence against actions of state authorities targeting the private sphere of the citizens.

While at first glance the massive surveillance of citizens can be seen as a serious attack on public discourse and democratic procedures, the controversial debate about these practices has also fuelled a new debate about adequate protection against an intrusive state, spying indiscriminately on its population. Probably with hindsight the Snowden revelations will appear historically as one of the single most important irritations of the general public's trust in the legitimate exercise of state power. By the same token, the public may start to question the threat assessments flagged on a regular basis by the security-industrial-political complex. How threatening are the threats? How successful are the means to counter them? This type of questioning, hitherto entertained primarily among a small group of experts and critics of present-day surveillance practices, now is entering the front pages and talk shows. National intelligence services in several European countries have come under pressure to defend their practices and the present proof of successful actions in combatting crime and terrorism. The evidence presented so far seems not very convincing.

At the same time, public attention has turned to a couple of other problems regarding the idea of privacy, democratic self-governance and rule of law. As the events have clearly demonstrated, legal safeguards as such are not a guarantee against mass surveillance. The intelligence community was acting within the realm of law (at least, to some extent), albeit the legal regulations were problematic from a political and democratic perspective. Laws were tailored to the demands of the intelligence community or had a built-in backdoor allowing for the expansion of surveillance under the pretext of security threats. These threats are difficult to substantiate. One of the main argumentative frames applied in the controversy about the limits of surveillance draws on the metaphor of balancing freedom (or liberty or privacy) and security. Citizens are asked to trade some of their freedoms in exchange for increased security. More surveillance is supposed to produce a more secure society and the intrusion upon their privacy is what the citizens have to trade in for this. A closer look at this metaphor reveals its shortcomings. The balancing model operates with three actors or groups: the general public or the citizens, the state or the intelligence and law enforcement agencies and a

third group that could be termed the target group, e.g., the undetected perpetrators who are supposed to be detected to prevent future damage. The target group, according to this logic is hiding somewhere among the members of the general public and hence the public has to be targeted by mass surveillance to identify the members of the target group. The measures are justified with the damage to society caused by attacks from the target group. A simple thought experiment helps to demonstrate the built-in biases of this approach. When replacing the target group terrorists with the target group financial institutions, while leaving the overall logic of the argument as it was, the bias becomes becomes obvious. It could easily be demonstrated that not all of the individuals working for the financial sector are following a criminal path. Nonetheless, the fact of being a member of this sub-culture entails the risk of becoming radicalised and engaging in illicit behaviour (like selling securities to clients while at the same time placing a bet against them). This can create massive damage and so it would be perfectly rational, following the reasoning of the balancing metaphor, to trade in some of the freedoms enjoyed by the financial institutions for more security of society as a whole.
Also there are international networks involved in these illicit transactions, a hedge fund as an organisation can display a structure similar to a Jihadist group – activists spread across the globe cooperating and communicating among each other transferring funds without being exposed to full scrutiny of state institutions or even working actively to prevent such scrutiny.
What this little exercise of hypothetically replacing one target group with another demonstrates is the moral and political dimension of surveillance practices. Sacrificing civil liberties for a cause can be justified, depending on the cause and the domain. While the basic idea of imposing controls and curtailing certain freedoms for certain groups in a liberal society may be justified, the mass surveillance of whole populations is not acceptable. This line of reasoning raises issues of a moral economy and reflexively points to a process of democratic deliberation, addressing the question: what should we as a society do to prevent substantial damage to the polity? What do we conceive as such damage and last not least: what are we willing to trade in to protect us from future damage.

Taking the perceived threat of a terrorist attack out of the narrow frame of a group of determined criminals targeting “our” societies can create a broader and more comprehensive understanding of the underlying problems. It can also foster a more complex understanding of the different trade-offs and balances involved in the debate about security. Introducing a third element into the equation of security vs. liberty and/or privacy demonstrates this quite clearly. This third element could be called “convenience”. The use of electronic communication media makes many activities of daily life more convenient or “user-friendly”, while at the same time producing the data on which the intelligence community operates: mobile phones, social media, online shopping, credit cards; browsing the Internet creates the infamous data doubles of citizens that can be monitored by the intelligence services to identify suspicious behaviour, find evidence for future deviance or detect potential perpetrators.

Establishing a more responsible use of this convenient infrastructure would entail a change in established modes of action – from encryption to changes in consumption patterns. But convenience in this context can also be spelled in a different way. The life style of modern consumer society rests on a severe imbalance at the global level between the rich North and the impoverished south. This imbalance creates an unequal distribution of resources and produces economic, social, cultural and ecological problems of a global scale. Increasing wealth in northern countries produces poverty in the global south and poverty breeds radicalisation. Awareness of the social and economic dynamic fuelling processes of political radicalisation seems to be growing in the wake of the debate about mass surveillance. The threat assessments produced to justify the surveillance of global communication streams, of

migration and mobility focussing on those geographical areas from which the perceived threat of terrorist attacks is supposed to originate begs the question as to whether Western open democratic societies should pay the price of such highly intrusive mass surveillance and a politics of exclusion, creating, for example, a “Fortress Europe” to protect against an enemy who could turn out to be a rebel with a cause. Looking at the strategic objective of the terrorists, one could argue that they seem to have succeeded by creating a deep paranoia simply by launching a few unpredictable attacks and keeping up the fear of new strikes in the near future.

In terms of resilience what we see here is a kind of collateral enlightenment and broadening of the public debate about surveillance, the state and some fundamental assumptions about contemporary societies. A society under the influence of illegal practices of surveillance enters into a sobering process of looking at itself and begins to question its own institutional and legal set-up against the fundamental values of democracy, accountability and openness.