EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

POLICY MEMO

SURVEILLANCE, PRIVACY, AND SECURITY: EUROPE'S CONFUSED RESPONSE TO SNOWDEN

Anthony Dworkin

SUMMARY

Europe's response to the Snowden revelations about US surveillance has failed to engage with some of the most important issues. Public and media reaction was strong but unfocused. The European Commission has been forced to work mainly through commercial regulation, with little direct influence over the security policy of the United States and member states. Despite their professed outrage, European countries have collaborated on surveillance with the US, and have little wish to curtail their own powers. Instead, they have focused on the separate issue of US spying against EU governments. Meanwhile, the aim of keeping European data within the EU now looks like a dead end.

What is needed instead is an open and far-reaching discussion about the role, limits, and oversight of surveillance in the age of big data. Security threats like the recent attacks in Paris underline the need for effective intelligence work, and the internet has transformed both communications and the scope for surveillance. The way forward lies through a reform agenda that addresses a series of fundamental questions, within the EU and with the US, including: is the widespread retention of data necessary, and by whom? How should you regulate technology companies based in the US that control global data flows? What limits should there be on governments' extra-territorial surveillance of non-citizens, and how can they be enforced?

The internet has become the front line in contemporary debates about privacy, surveillance, and security. Technological advances in global digital communications have revolutionised the way people receive and exchange information, and opened new horizons for government agencies to monitor their own citizens and foreigners. Security concerns across Europe in the wake of the attack against *Charlie Hebdo* have led to calls for greater surveillance powers, though the need for new authorities remains disputed. In a longer perspective, what is most striking is the lack of consensus and clarity about the justification and legitimate scope of large-scale surveillance – a problem that has been obvious in the European response to the revelations of Edward Snowden about the US and allied intelligence practices. Eighteen months after Snowden's documents began appearing, they continue to provide the primary reference point for consideration of mass surveillance as an intelligence tool – and Europe's response provides the best way to consider how the EU has failed to engage with many of the fundamental questions in this area.

Snowden's revelations about mass surveillance carried out by US intelligence services quickly became a dominant issue in relations between Europe and the US when they started appearing in mid-2013. A year and a half later, the after-effects of the Snowden affair continue to reverberate, but its results have not been what European citizens might have hoped for. Shaped by the policy choices and capabilities of EU member states and institutions, Europe's response has failed to engage with some of the most important

questions raised by Snowden's revelations. Instead, it has often focused on issues that have less to do with mass surveillance than with other independent European interests. Despite the public outrage and political concern that Snowden's information provoked, Europe has not yet taken the steps that would have the best chance of protecting its citizens from the sweeping collection of their personal data by both foreign and domestic security services.

The leitmotif of the European reaction to Snowden's revelations was to complain of a breakdown of trust. As successive news reports revealed the extraordinary scale of data-gathering by the US National Security Agency (NSA), European media and politicians expressed their outrage at finding that the EU's closest global ally had engaged in such behaviour. The European Commission issued a communication aimed at "rebuilding trust in EU-US data flows".[1] German Chancellor Angela Merkel warned that "actions in which the ends justify the means, in which everything that is technically possible is done, violate trust, they sow distrust".[2] After he was accorded a gala state visit in February 2014, French President François Hollande said he was satisfied that "trust has been restored".[3] US President Barack Obama was slower to declare it resolved, saying during a visit to Europe in March 2014 that "because of these revelations, we have to win back the trust, not just of governments, but more importantly of ordinary citizens, and that is not going to happen overnight."[4]

Trust is of course important between allied countries – but it is also an inherently vague concept. To frame the fallout from the Snowden affair as a matter of restoring trust between Europe and the US raises as many questions as it answers. In particular, it ignores the fact that different countries, institutions, and groups within Europe have different relationships and expectations in this area – as is also true for the US. Not least, to talk of generalised trust between the EU and the US glosses over the fact that questions of trust also arise between European governments, intelligence services, businesses, and citizens, and between the EU and its member states. In order to understand the areas on which policymakers should now focus in order to make surveillance more legitimate, we need to look back at the way different constituencies in Europe, from media to EU institutions and member state governments, have reacted since the Snowden stories first appeared and assess the limitations of the political, legal, and technical approaches they have chosen.

Public and media responses: unfocused and variable outrage

The first revelations of the NSA's mass surveillance programmes, in June 2013, attracted widespread attention in European media. Beyond the extraordinary scope of the US surveillance operations, it quickly became clear that the NSA enjoyed much greater authority to examine communications from non-US citizens than from Americans. As Snowden himself put it, US citizens were in a position of the "highest privilege" compared to foreigners, including Europeans.[5] Non-Americans were liable to have their digital communications intercepted and examined with few constraints under US law. Nevertheless, outrage at the revelations in Europe, though high, was not uniform. Germany was and remains the European country where the public reaction against US surveillance was strongest. A recent poll showed that 67 percent of Germans were concerned about foreign government agencies monitoring their online activities, and a remarkable 94 percent of Germans had heard about Snowden.[6] According to another poll, conducted in November 2013, only 35 percent of Germans regarded the US as a reliable ally – less than half the level recorded in the early days of Obama's presidency.[7]

Other countries where ECFR or other research suggested significant public attention to NSA surveillance are the Netherlands, Ireland, Italy, Belgium, the UK, France, and Spain. However, opinion polls and other reports are inconsistent – and, most importantly, media attention does not necessarily equate to public outrage. In several European countries, it seems clear that a significant part of public opinion was not strongly disturbed by the revelations: this seems true, for instance, of France, Sweden, and the UK. The UK was in a unique position in any case, because from the start of Snowden's revelations it was clear that British intelligence services had worked more closely with the US than any other European service, and were essentially partners in much of the surveillance that took place.

EU institutions: a bias towards regulation

The EU institutions were at the forefront of Europe's political response. The European Parliament quickly set up an inquiry spearheaded by the British Labour MEP Claude Moraes. This produced a hard-hitting report early in 2014, condemning the "vast, systemic, blanket collection of the personal data of innocent people".[8] The Justice Commissioner Viviane Reding wrote to the US Attorney

1 "Rebuilding Trust in EU-US Data Flows", European Commission, 27 November 2013, available at http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

2 Alison Smale, "German Leader Criticises US Over Pervasive Surveillance", *New York Times*, 29 January 2014, available at http://www.nytimes.com/2014/01/30/world/europe/german-leader-criticizes-united-states-over-surveillance.html.

3 "Obama and Hollande say trust restored after NSA spying", *BBC News*, 11 February 2014, available at http://www.bbc.co.uk/news/world-us-canada-26140744.

4 Spencer Ackerman and Julian Borger, "Obama: US must 'win back the trust of ordinary citizens' over data collection", *Guardian*, 25 March 2014, available at http://www.theguardian.com/world/2014/mar/25/obama-us-nsa-data-collection-trust.

5 *Citizenfour*, dir. Laura Poitras, Praxis Films, 2014.

6 "CIGI-Ipsos Global Survey on Internet Security and Trust", Centre for International Governance Innovation and Ipsos, November 2014, available at https://www.cigionline.org/internet-survey.

7 "Spying Fallout: German Trust in United States Plummets", *Spiegel Online*, 8 November 2013, available at http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html.

8 "Draft report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", European Parliament Committee on Civil Liberties, Justice and Home Affairs, 8 January 2014, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN.

General warning that US practices could have "grave adverse consequences for the fundamental rights of EU citizens".[9] But attempts to galvanise a powerful response at the EU level rapidly encountered the stumbling block that member states were firmly determined to safeguard their own competence in the field of national security. An early indication of this was the initiative to set up an EU-US working group on surveillance and privacy: at the insistence of member states, it was split into a two-speed process, so that EU and US negotiators focused on data protection, while member states discussed security and surveillance with US officials on a separate bilateral track.

Under these circumstances, Commission officials privately concede that their ability to affect the policy of the US or EU member states on surveillance has been limited. Without any ability to determine what states do in the realm of security, the EU institutions have fallen back on an area closer to their core remit – commercial regulation. Their strategy is to work through the regulatory framework governing technology companies in an attempt to limit European exposure to US surveillance. Within the Commission, DG Justice is pushing the US to renegotiate the 2000 Safe Harbour agreement, which allows US companies to transfer data out of the EU without complying with the full criteria established by EU data protection rules, so long as they undertake to respect a specified series of principles. The Safe Harbour agreement contains an exception to the observance of these principles when national security is involved. The EU set out 13 recommendations for revising Safe Harbour in late 2013, of which two relate to the security exception (they would require greater transparency from companies and limit the scope of the exception to "strictly necessary and proportionate" use).[10] The US Federal Trade Commission has agreed to the other points, but the US government has not been willing to give ground on the security provisions.

The European Commission has threatened to suspend the operation of Safe Harbour if the US doesn't agree to its requests. However, most observers believe that this is an empty threat, and that the Commission would not ultimately revoke an agreement used by over 3,000 US companies for their European operations (however much it would boost the fortunes of European technology companies). The Commission has also tried to use the Snowden affair to give impetus to its pre-existing drive for a new EU-wide data protection regulation, which may be agreed in 2015. Reding said that the regulation would be an answer to Snowden's "wake-up call".[11] An earlier draft of the regulation contained a provision that would have forbidden companies from complying with any legal requirement to disclose personal data to third countries, thus setting up a conflict for US technology companies between their obligations under EU and US law. This provision was dropped before Snowden's revelations, but the European Parliament is attempting to reintroduce it, and Germany has supported the move. It remains unlikely, however, that the full Council will endorse such a measure.

Both these measures, if enacted, would certainly cause problems for US technology companies, forcing them to comply with EU data protection rules in full and face a conflict of legal regimes. But these changes would be likely to have at best a limited impact in constraining US mass surveillance. The handover of information by technology companies is only one part of the panoply of US surveillance techniques. More significantly, assuming that the goal is not to force US technology companies out of Europe altogether, the Commission's strategy relies on using these companies as an indirect way of driving policy change in the US. But the big US technology companies are already pushing for reform of US surveillance practices with little success. Apple, Facebook, Google, Microsoft, and others launched a campaign in late 2013 urging the US to set a global standard in making surveillance "clearly restricted by law, proportionate to the risks, transparent and subject to independent oversight". They played a prominent role in campaigning for the Senate to support the USA Freedom Act, which would have implemented several of the reforms suggested by Obama early in 2014. Nevertheless, the measure failed in the Senate in November 2014, as Republicans put concerns about national security and terrorism above any libertarian leanings.

EU states: an exercise in misdirection

Many EU member states were strongly critical of the US surveillance practices that Snowden revealed, but their public statements often seemed driven above all by concern not to fall behind the reaction of their citizens. One concrete step in which some EU member states were involved was to push for a resolution on digital privacy in the UN General Assembly. The resolution, sponsored by Germany in association with Brazil, was adopted by consensus in November 2013, and led to a tough report from the UN High Commissioner for Human Rights, Navi Pillay, in July 2014. Pillay argued that surveillance was only permitted when it was necessary and proportionate to specific security risks, and called for greater oversight by independent monitoring institutions.[12] Beyond noting the report, however, the General Assembly was not able to agree on any steps to encourage the implementation of tougher standards.

While European countries were often publicly outspoken on the principle of privacy rights, they remained much less forthcoming on the questions of what they had known about surveillance within their territory and what relationship their own intelligence services had with the NSA. The

9 Viviane Reding, Letter to US Attorney General Eric Holder, 10 June 2013, available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/p6_ltr_holder_/p6_ltr_Holder_en.pdf.

10 "Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", European Commission, 27 November 2013, available at http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

11 Kelly Fiveash, "EU ministers respond sleepily to Viv Reding's 'Snowden wake-up call' on data protection", *The Register*, 9 June 2014, available at http://www.theregister.co.uk/2014/06/09/viv_reding_justice_council_of_ministers_data_protection/.

12 "The right to privacy in the digital age", Office of the UN High Commissioner for Human Rights, 30 June 2014, available at http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

reason was not hard to fathom: it rapidly became clear that co-operation between the NSA and European intelligence services had often been close, and that several EU member states had significant surveillance programmes of their own. As two knowledgeable analysts put it, the "muted and often contradictory reactions of many governments to the disclosure of National Security Agency programmes indicates the scope of probable cooperation between allied intelligence services".[13]

In one of his more striking phrases, Snowden himself claimed that there had been a "European bazaar" in data collection, whereby European intelligence services evaded legal restrictions (where they existed) by collecting data on other countries and swapping information where necessary.[14] Britain's GCHQ was in a category of its own, but intelligence services in France, Germany, Italy, Sweden, Spain, and the Netherlands were also among those revealed to have collaborated with the NSA. Norway took the unusual step of refuting reports that the NSA had recorded data on millions of phone calls out of Norway, revealing that it had carried out the surveillance itself to support counter-terrorism at home and abroad.[15] In line with the philosophy of its former director Keith Alexander, who reportedly asked, "Why can't we collect all the signals, all the time?", the NSA operated on a scale that might have taken EU governments by surprise, but many of its practices were similar to Europeans' and technology and data were often shared.

Moreover, some European countries have expanded the scope of their own surveillance powers during the period since Snowden's revelations began to emerge. In late 2013, France passed a new law to consolidate the ability of intelligence services to monitor digital communications without judicial oversight. After the European Court of Justice struck down the EU Data Retention Directive in the spring of 2014, the UK enacted emergency legislation to require communications companies to keep phone and internet data for 12 months so that security services could access it. Investigative reports have highlighted the fact that even Germany has limited restrictions on surveillance conducted on people outside its territory. The German BND intelligence agency has the advantage of oversight of the Frankfurt internet exchange, the world's largest routing centre for international internet traffic.[16] The recent growth in concern about terrorist threats in Europe, linked to the rise of the Islamic State in Syria and Iraq and confirmed by the attack against *Charlie Hebdo*, has given added weight to the case for effective surveillance – though it does not obviate the need to conduct such surveillance within a legitimate and democratic framework. Since the Paris attackers were already well known to French intelligence, it is hard to see how greater surveillance powers could have helped prevent them.

The second wave of national response: pushing back against spying

There was, however, a second dimension to the reaction of EU member states, focusing not on mass surveillance but more traditional spying directed against European governments. This raised rather different questions than mass surveillance, but public reaction and media reporting often failed to distinguish between the two. Snowden's documents revealed that the US had tapped the phones of 35 world leaders and targeted embassies or offices of countries including France, Italy, Greece, and the EU. Most notoriously, of course, it was alleged in the autumn of 2013 that the NSA had tapped the phone of German Chancellor Angela Merkel. Alongside these revelations, there was a growing belief, especially in Germany, that the US might be spying on German companies for commercial reasons, though no evidence to support these concerns has emerged and Obama expressly prohibited commercial espionage at the beginning of 2014.[17] One concrete result of these concerns was that the governing Christian Democrats and Social Democrats in Germany agreed to establish a special committee in the Bundestag to investigate NSA surveillance.

Concern about this more conventional form of espionage triggered a new wave of European action, led by Germany, which aimed to eliminate US spying on allied countries and their governments. The model for this initiative was the "Five Eyes" intelligence partnership between the US, the UK, Canada, Australia, and New Zealand. This partnership is based on a series of agreements that began in 1946, and involves the widespread sharing of signals intelligence and joint operations centres. The Five Eyes agreements are often said to include a commitment not to spy on partner countries, but according to some analysts this is a myth.[18] Instead, there is only a general understanding that citizens will not be directly targeted, which can be overridden when national interests require.

After the news about Merkel's mobile phone emerged, Germany launched a push for the US to give it a "no-spy agreement" of its own. Obama had already promised that the Chancellor's phone was no longer being monitored, but efforts to conclude a wider intelligence-sharing agreement broke down. According to news reports, the US was willing to step up its intelligence co-operation with Germany, but unwilling to make a commitment that its agents would always observe German law (which would effectively prevent all espionage, and set a precedent beyond that in place with any other country).[19] Tensions between the US

13 Georg Mascolo and Ben Scott, "Lessons from the Summer of Snowden – the Hard Road Back to Trust", New America Foundation/Open Technology Institute/Wilson Center, October 2013, p. 2, available at http://www.newamerica.net/sites/newamerica.net/files/policydocs/NAF-OTI-WC-SummerOfSnowdenPaper.pdf.

14 Andrew Byrne, "Snowden: US spy agencies pressed EU states to ease privacy laws", *Financial Times*, 7 March 2014, available at http://www.ft.com/cms/s/0/9f45bcb2-a616-11e3-8a2a-00144feab7de.html#axzz3NyJdKv66.

15 Karsten Friis, "Snowden: impact in Norway", Norwegian Institute of International Affairs, February 2014, available at http://www.nupi.no/content/download/495223/1647131/file/NUPI%20Policy%20Brief%202-14-%20Friis.pdf.

16 Chris Bryant, "Welcome to Frankfurt, the plumbing capital of the world wide web", *Financial Times*, 17 April 2014, available at http://www.ft.com/cms/s/0/b93e8888-bf25-11e3-8683-00144feabdc0.html#axzz3NyJdKv66.

17 David E. Sanger and Alison Smale, "US-Germany Intelligence Partnership Falters Over Spying", *New York Times*, 16 December 2013, available at http://www.nytimes.com/2013/12/17/world/europe/us-germany-intelligence-partnership-falters-over-spying.html?pagewanted=all.

18 "Eyes Wide Open", Privacy International, November 2013, pp. 15–19.

19 David E. Sanger, "US and Germany Fail to Reach a Deal on Spying", *New York Times*,

and Germany escalated further after two US agents were uncovered within the German security services in July 2014, and Germany expelled the CIA station chief in Berlin. In an attempt to repair the harm caused by this episode, the US let it be known that it had ordered a suspension in spying against allied governments. There have also been reports that the US offered Germany new "guiding principles" for intelligence co-operation.[20]

The false promise of technological sovereignty

Germany and other EU member states also tried to push back against NSA surveillance through a series of proposals to keep European data in European hands, an objective known as "technological sovereignty". Germany and France announced their intention to look into the possibility of a "Europe-only internet". "One could build up a communication network inside Europe", Merkel announced in February 2014.[21] According to different variants of this idea, companies handling the personal data of European citizens could be required to store the data on servers within the EU, or to route all communications between Europeans within the Schengen Area. Not surprisingly, some European technology and cloud-storage firms were keen advocates of such an approach. But the avenue of technological sovereignty looks increasingly like an ineffective way to deal with concerns about surveillance, and officials admit that many initiatives in this area are being quietly dropped.

Keeping data flows within European borders would be technologically demanding and seems to conflict with the open nature of the internet. Storing EU data on European servers might be possible in some cases – indeed some US cloud companies such as Amazon are now offering servers based in Europe – but, if required for all personal data, the spread of such "data localisation" would cause problems for smaller internet companies that are trying to compete internationally, including European ones. It would also put the EU in the company of undemocratic regimes that use domestic data storage requirements to increase their control over the digital communications of their citizens. Most importantly, such measures would do little to enhance the security of European data. Local routing might make it harder for the NSA to obtain access, but it would not make it impossible, and might correspondingly make it easier for European intelligence services to collect it. Local data storage would not solve the problem that US companies such as Facebook and Google are in any case bound by US law covering the data they possess, no matter where it is located.[22]

Germany also launched its own attempt to exclude US technology companies from government procurement contracts, by introducing a "no-spy requirement" obliging bidders for security-sensitive contracts to certify that they are not under any obligation to disclose information to a foreign government. The German government dropped a contract with Verizon in mid-2014. But the idea of expanding this approach has met resistance. Critics denounce it as a form of protectionism that will not necessarily solve the problem of surveillance. Meanwhile, some large German multinationals are opposed to the idea of requiring "Made in Germany" solutions because the domestic industry is not sufficiently advanced to supply replacements for US-made digital goods and services, and it could require high switching costs for public bodies and contractors.[23]

In Germany, surveillance remains the subject of political controversy, and pressure for the government to address the subject remains high. The continuing inquiry of the NSA committee in the Bundestag will ensure that the topic remains in the public eye. But across the rest of the EU, the political impetus for decisive action on surveillance has dropped. While EU-level commercial regulation may yet be used to impose new burdens on US technology firms, at the moment it remains at the level of threat rather than action. In addition, it remains a clumsy tool to reduce the overall level of surveillance against EU citizens. The European Parliament remains vocal on the issue, but it can do little apart from threatening to block any eventual free-trade agreement that emerges from the TTIP negotiations. One of the more lasting effects of the Snowden crisis is likely to be acute scrutiny of the data protection implications of any possible trade deal.

Other avenues: courts and encryption

Aside from the political initiatives (or lack of them) coming from European countries, two other avenues for further progress remain. One is the courts. A case alleging that mass surveillance by GCHQ violates European citizens' privacy rights is pending before the European Court of Human Rights, which has in the past shown a willingness to weigh in on security questions. A ruling that the European Convention on Human Rights sets tougher limits on government surveillance would require not only the UK but many other member states to revise the frameworks under which their intelligence services operate. As a recent report issued by the Human Rights Commissioner of the Council of Europe argued, basic principles of human rights demand that there be clear legal rules that allow individuals to foresee how intelligence powers may be used, and effective supervisory systems to ensure those rules are followed.[24] There is good reason to believe that these standards are not being met, especially in connection with surveillance against non-citizens.

1 May 2014, available at http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying.html.

20 David Ignatius, "The US and Germany are rebuilding a spy partnership", *Washington Post*, 22 July 2014, available at http://www.washingtonpost.com/opinions/david-ignatius-the-us-and-germany-are-rebuilding-a-spy-partnership/2014/07/22/bobdc7e0-11e2-11e4-8936-26932bcfd6ed_story.html.

21 "Data protection: Angela Merkel proposes Europe network", *BBC News*, 15 February 2014, available at http://www.bbc.co.uk/news/world-europe-26210053.

22 For a detailed and helpful analysis of these possible measures, see Mirko Hohmann, Tim Maurer, Robert Morgus, and Isabel Skierka, "Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013", Global Public Policy Institute and New America's Open Technology Institute, 24 November 2014, available at http://www.gppi.net/publications/global-internet-politics/article/technological-sovereignty-missing-the-point/.

23 Author interview with Ben Scott, 28 November 2014.

24 "The rule of law on the internet and in the wider digital world", Council of Europe Commissioner for Human Rights, December 2014, pp. 109–110, available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2654047&SecMode=1&DocId=2216804&Usage=2.

Meanwhile, the Court of Justice of the EU is hearing a case challenging the Safe Harbour regime, arising out of a complaint against Facebook made by an Austrian campaigner in Ireland. The campaign claims that the Safe Harbour framework is incompatible with the Charter of Fundamental Rights and is asking the Court to overturn it. The Court's ruling that struck down the EU's Data Retention Directive in April 2014, on the grounds that its sweeping and untargeted scope violated the Charter of Fundamental Rights, suggests it may look critically at the Safe Harbour regime as well.

The second avenue is technology. Faced with a threat to their businesses from consumer fears of surveillance, several technology companies are working to improve the security of information stored with them via more effective encryption. Google chairman Eric Schmidt claimed recently that the company had introduced new encryption techniques that "no one believes the NSA can break during our lifetime".[25] Apple has announced that data stored on iPhones and other devices would be encrypted by default. In effect, counter-surveillance measures have become a field of commercial competition. These initiatives have aroused fierce complaints from British and US intelligence services.[26]

The way forward: an open and realistic debate

Through marketplace competition and official resistance, the debate over fundamental questions of privacy and security that governments have largely avoided since Snowden's revelations is being partially forced into the open. That debate, however, should be happening more fully and at a higher level. It is striking that European countries have not yet begun to articulate what a coherent and principled set of standards for balancing security and privacy rights might look like in the age of global digital communications. While the US is the market leader in mass surveillance, new standards to govern this area must be based on more than a simple critique of US practices. Unless European countries attempt to develop such principles and show a commitment to abide by them, it is hard to believe that their complaints about US practices will have any constructive impact.

A transatlantic dialogue is needed not only on guiding principles for intelligence collaboration, but more generally on the appropriate limits of surveillance in the age of big data. The internet and other technological developments have revolutionised the possibilities for collecting data about individuals, and much of the internet's commercial model relies on individuals trading this information to companies in exchange for their own convenience. Old models of regulation have failed to keep up with the scale and global nature of modern communications, and intelligence agencies have developed procedures that do not enjoy democratic consent. To find an effective way to reconcile privacy rights, security, and democratic legitimacy, Europe needs to engage in an open and realistic debate, internally and with the US, involving civil society and business as well as government officials.

It is possible to sketch out some of the areas that a credible reform agenda could start by considering. Although these questions have not yet received systematic political attention, they have been the focus of several reports as well as research by independent experts and scholars, and their work could provide an initial basis for discussion.[27] Such an agenda would have to revisit the traditional questions of reconciling human rights and national security, providing democratic legitimacy for intelligence practices, and ensuring effective oversight and accountability, assessing them in the new context of the online world. It would also have to consider the new questions raised by the global nature of digital communications, in particular the question of what restrictions there should be on the collection of information about non-citizens, and how to regulate companies with global operations that have access to the data of many millions of people.

A reform programme might not immediately lead to binding international agreements, but it could develop a set of principles that could be embodied in national legislation and government policy. These should focus above all on the issue of mass surveillance, as opposed to more traditional espionage, and in particular on the vexed question of standards governing the collection of data and communications of non-citizens overseas. A central dilemma would be to find a model for the different obligations relating to commercial data gathering and retention, and access by intelligence services. Another central issue would be to deal with the blurring of domestic and foreign regulation that springs from the global reach of technology companies – and in particular to find a way of ensuring that the legal obligations placed by the US on companies based there are compatible with the sovereign authority of the countries where they operate.

As Snowden's documents showed, the US stands alone in its combination of technology and resources, the sheer scale of its surveillance, its domination of the global technology sector, and its effort to apply its own laws extra-territorially without acknowledging any corresponding human rights obligations. But the US is far from alone in its failure to engage with the fundamental questions raised by the opportunities for communication and surveillance that modern technology has created. The issues involved are hugely important for Europe's security, its economic future, its values, and the rights of its citizens. It is hard to see any meaningful progress taking place in resolving the complex problems of this field unless the EU tackles them in a far more serious, searching, and self-critical way than it has done up to now.

25 "Google claims it installed unbreakable encryption after NSA spying", *CBC News*, 23 October 2014, available at http://www.cbc.ca/news/business/google-claims-it-installed-unbreakable-encryption-after-nsa-spying-1.2810773.

26 Robert Hannigan, "The web is a terrorist's command-and-control network of choice", *Financial Times*, 3 November 2014, available at http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3NyJdKv66.

27 See, in particular, Ian Brown, Morton Halperin, Ben Hayes, Ben Scott, and Mathias Vermeulen, "Towards Multilateral Standards for Surveillance Reform", Oxford Internet Institute, January 2015, available at voxpol.eu/wp-content/uploads/2015/01/HERE.pdf, on which I have drawn in the recommendations that follow.

About the author

Anthony Dworkin is a senior policy fellow at ECFR and leads the organisation's work on human rights, democracy and justice. He has worked extensively on counter-terrorism and human rights and is the author of the ECFR publications *Beyond the 'War on Terror': Towards a New Translatlantic Framework for Counter-terrorism* (2009) and *Drones and Targeted Killing: Defining a European Position* (2013). He has also written papers on international justice, EU human rights strategy, and political developments in North Africa since 2011.

Acknowledgements

This paper was made possible by a grant from the Fritt Ord Foundation. It draws on research conducted for ECFR's European Foreign Policy Scorecard in 2013 and 2014. I benefited greatly from the expert advice of Ian Brown, Jens-Henrik Jeppesen and Ben Scott, and of ECFR Council members Andrew Puddephatt and Marietje Schaake. An early draft was presented to a public meeting organised by Fritt Ord in Oslo in April 2014, and I would like to thank Erik Rudeng, Karsten Friis, and Jon Wessel-Aas for their comments there. Within ECFR I am grateful to Rachel Tausendfreund for editing the memo.

ABOUT ECFR

The **European Council on Foreign Relations** (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy.

ECFR has developed a strategy with three distinctive elements that define its activities:

- **A pan-European Council.** ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Martti Ahtisaari and Mabel van Oranje.

- **A physical presence in the main EU member states.** ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.

- **A distinctive research and policy development process.** ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to advance its objectives through innovative projects with a pan-European focus. ECFR's activities include primary research, publication of policy reports, private meetings and public debates, 'friends of ECFR' gatherings in EU capitals and outreach to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions.

www.ecfr.eu

ISBN: 978-1-910118-23-8

Published by the European Council on Foreign Relations (ECFR), 35 Old Queen Street, London, SW1H 9JA, United Kingdom

london@ecfr.eu

Design by David Carroll & Co davidcarrollandco.com