Towards Multilateral Standards for Surveillance Reform

By Ian Brown, Morton H. Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen[1]

[1] Respectively at the Oxford Internet Institute, Open Society Foundations, Statewatch, Stiftung Neue Verantwortung, and European University Institute. This paper has been produced with the support of Open Society Foundations and the VOX-Pol Network of Excellence, funded by the European Union under the 7th Framework Programme for research, technological development and demonstration under Grant Agreement No. 312827. Some of the material in section 3 was derived from related draft papers by Ian Brown and Douwe Korff.

1 Introduction

Edward Snowden's revelations about the mass surveillance capabilities of the United States' National Security Agency (NSA) and its partners have created a unique opportunity to work towards the adoption of multilateral human rights-compliant standards for government surveillance conducted against nationals of other countries. While there is certainly much to debate about privacy concerns of citizens vis-à-vis their own security services, the core foreign policy problem is that there are no clear national standards protecting the privacy of one nation's citizens from the intelligence gathering operations of another. Moreover, to the extent that such standards can be derived from international law, there are few or no mechanisms of oversight or accountability that could give meaningful effect to such guarantees. These problems are compounded by the global nature of the Internet's infrastructure, where the distinction between foreign and domestic Internet communications is often difficult to discern.

The NSA conducts intelligence gathering operations that intercept and store enormous quantities of data from global communications networks. These bulk collection programmes are conducted either by collecting data directly from the cables and servers that carry them or by compelling commercial service providers to supply such information. These data "haystacks" are later searched for operational intelligence "needles". There is now an intense debate over how to restrict and control both the interception and the analysis of all of these communications. This paper focuses on the rules that govern the communications of private individuals who live outside a country that is collecting their data, and who do not enjoy the same privacy protections as its citizens.

While the US may be unique in terms of its sheer capacity to collect data, all states with established national security structures engage in broadly similar practices, intercepting communications in real time and compelling service providers to retain and disclose data. The general failure to recognise the privacy rights of non-nationals is by no means limited to the US or its partners in the so-called "Five Eyes" alliance (UK, Canada, Australia and New Zealand). On the contrary, few if any countries – democratic or otherwise – offer the kinds of protections for foreign nationals subject to their intelligence gathering operations that are now being demanded of the US government.

The United Nations' General Assembly has taken tentative steps in the direction of new international standards regarding the right to privacy in the context of extraterritorial and transnational surveillance programmes.[1] But it is currently inconceivable that the surveillance reforms that are necessary in the light of the Snowden revelations can be achieved through a UN Convention, an additional protocol to the International Covenant on Civil and Political Rights (ICCPR), or ushered in through the adoption of a "digital bill of rights". It is possible that in the absence of progressive reform, public outrage over the spying scandal might instead encourage moves toward "technological sovereignty" – driving a set of proposals to create protected, national information infrastructures. Some have warned that this trend could pull apart the norms and technical standards that support an open, global Internet.[2]

Notwithstanding the scale of the challenge of modernising international norms and reforming the national security laws of nation states, there will never be a better opportunity to effect change. Snowden's public disclosures have triggered major debate in democratic states about the proper balance between liberty and security. This is of course not the first time that the US government has dispensed with democratic checks-and-balances in the name of counter-terrorism. Many of the fundamental issues, however, transcend US "exceptionalism", and require an international effort that can unite civil society, business and government leaders behind an agenda for the mutual restriction of digital surveillance powers in all democratic nations. To this end, this paper attempts to map a path toward new international standards for foreign intelligence collection, in order to achieve increased transparency, control and oversight of national surveillance practices.

We begin by providing a basic comparison of the legal frameworks governing foreign surveillance law in the US and selected EU Member States. We then set out the applicable international human rights law and major reform initiatives in as far as they relate to foreign surveillance and its oversight. This exercise suggests that – while still falling short of many people's expectations – the legal framework for foreign intelligence collection in the US, as enhanced by the Presidential Policy Directive of January 2014, contains much clearer rules on the authorisation and limits on the collection, use, sharing and oversight of data relating to foreign nationals than the equivalent laws of almost all EU Member States. In the absence of clear and specific rules in other countries, ironically the US now serves as a baseline for foreign surveillance standards – although the European Convention on Human Rights, which requires the protection of the rights of all those within States parties' jurisdiction, sets a

higher general standard than the US government's interpretation of its international human rights law obligations as applying only within its own territory.[3]

Our goal is to work toward the establishment of a high ceiling rather than a low floor for human rights protection and accountability. In this vein, we attempt to identify key issues relevant to all signals intelligence reform efforts and to provide an analytical framework to guide the development of new standards and realistic options for reform.

2 Existing foreign intelligence gathering standards

The structures and powers of national security agencies vary widely, but in the US and EU Member States the surveillance of foreign nationals and the collection of communications that originate outside their territory predominantly take place under the rubric of 'signals intelligence' (SIGINT). This practice was first developed by military intelligence agencies to spy on adversaries in times of war and conflict, and is traditionally conceived of as 'espionage'. A failure to check the power and expansion of these military agencies, combined with the revolution in information and communication technologies and the 'exceptionalism' of the post-9/11 era, has massively amplified the scope and impact of SIGINT collection. We are primarily concerned with the criteria governing the authorisation of foreign surveillance operations and the oversight of such decisions. We first analyse the situation in the US, where regulation has developed since the 1970s, before assessing comparable standards in European countries, where many intelligence agencies were all but unregulated until the 1990s. We will also consider the role of the private sector – which is in the position of both legal accomplice to state surveillance and expected defender of its users' privacy – and the need for stronger commitments on data storage, transparency and policies on the handling of requests from security agencies for customer data that are necessary for any new intelligence standards to be credible and effective.

Two caveats are necessary. First, it is important to distinguish between foreign intelligence gathering and the collection of evidence in transnational investigations and prosecutions. This is because it has been suggested, quite widely, that one of the principal reasons that foreign intelligence gathering programmes have become so extensive is that the mutual legal assistance treaties (MLATs) that govern cross-border information exchange are too cumbersome to be relied on in cases where information relating to an individual in one state is urgently needed by investigators in another. This may be true up to a point (provisions for expedited requests between the EU and US, for example, were included in a 2003 framework MLAT that entered into force in 2010),[4] and there are strong arguments for establishing the principle that transnational surveillance should as far as possible take place in accordance with MLAT principles and procedures, with any "national security" exceptions properly proscribed; but revised or expedited MLAT procedures are likely to have *little or no impact* on the gathering of intelligence for national security purposes as currently practiced. Somewhat paradoxically, the

evidence suggests a "bottleneck" in MLAT requests *to* the US government by foreign law enforcement agencies, rather than the other way around.[5]

A second, related problem is that the traditional distinctions (and firewalls) between intelligence gathering for national security purposes and the collection of intelligence and evidence in the course of criminal investigations have become increasingly blurred in areas such as counter-terrorism and cyber-security. Allegations that national security arrangements in the US have been used to circumvent domestic due process requirements and to "launder" intelligence material into evidence (so-called 'parallel construction') are particularly troubling.[6] While these issues are largely beyond the scope of this paper, it is clear that any attempt to constrain the scope and breadth of foreign intelligence gathering must include controls on the use and transmission of data obtained for national security purposes.

2.1 Rules on foreign intelligence gathering in the US

SIGINT and foreign intelligence collection in the US is regulated by the Foreign Intelligence Surveillance Act (FISA), the PATRIOT Act, and various Executive Orders and Directives. Enacted after the Watergate scandals, FISA introduced various controls on the interception of telecommunications within the US targeting foreign powers or their agents but left greater leeway for targeting foreigners.[7] The collection of data on persons outside US territory was not covered by the legislation at this time. A separate Executive Order (12333) later provided explicit procedures for targeting Americans abroad, and the 2008 FISA Amendments Act (FAA) introduced the requirement of warrants for such operations.[8]

Under FAA section 702, subject to a certificate granted by the Foreign Intelligence Surveillance Court (FISC), foreigners can be targeted for a broad range of purposes as set out in the (classified) National Intelligence Priorities Framework. The precise purpose and target(s) of these orders are kept secret. FISA stipulates that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the constitution of the United States" and requires the court to determine that facts presented in support of the order are "not clearly erroneous". Section 215 of the PATRIOT Act 2001 allows security authorities to obtain any kind of "tangible" business records, including metadata, from a range of private-sector businesses. The first of the "Snowden Files" showed that s.215 was being used to collect metadata on telephone calls in bulk and s.702 to collect communications data directly from the servers of

Internet service providers. Both statutes provide for the retention of data for up to five years. Further powers to collect "non-content" related business records are available to the FBI in national security investigations in the form of "National Security Letters", which are not subject to any kind of judicial authorisation and may contain non-disclosure provisions.

On 17 January 2014, following the completion of the President's Review Group on Intelligence and Communications Technologies (see further section 4), the US government issued Presidential Policy Directive (PPD) 28 on "Signals Intelligence Activities". It provides new protections for non-citizens living outside the US but falls short of the safeguards FISA provides to US persons at home and abroad.[9] More detailed policies and procedures relating to the use of SIGINT are required by the PPD within one year.

PPD-28 begins by noting that in the post-Snowden era, the US must take account of the costs of disclosing surveillance practices directed against non-US persons, in particular against private citizens. The US needs the cooperation of other governments on matters such as combating terrorism and supporting what the Directive refers to as "an open secure global Internet", so maintaining the trust of foreign citizens is an important consideration. The PPD thus specifies that:

> All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside. And that all persons have legitimate privacy interests in the handling of their personal information in determining why, whether, when, and how the United States conducts signals intelligence activities.

The Directive provides new limits on the purposes for which information may be collected on non-US persons abroad – counter-espionage, terrorism, cyber warfare, threats to US armed forces or transnational crimes – and rules out the collection of information for the purpose of "suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation or religion". The Directive also explicitly rules out the collection of information for the purpose of gaining a competitive advantage for US business.

Asserting that the US government must continue to collect information in bulk but recognising the threat to privacy of non-US persons, the Directive imposes new limits on the use of signals intelligence collected in bulk, in order to

"protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside". In particular, data collected in bulk will be used only for specific purposes enumerated in the Directive and not for the much broader purposes contained in FISA and other intelligence directives. ("Bulk collection" here means an entire stream, not the relatively targeted collection under s.702 of FISA etc., to which the new limits on the searching of data collected in bulk do not apply).

PPD-28 applies the same principles to the handling of personal information of all persons. It stipulates that there must be "appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides," that the term "personal interest" must have the same meaning for all persons, and that information relating to a non-US person can be retained and disseminated only if equivalent information about a US citizen could be retained or disseminated. The Directive does not mandate equal treatment, providing only that "to the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality".

A limited range of "selectors" is supposed to restrict the use of data that has been collected in bulk to searches relating to valid foreign intelligence targets and, following the new Directive, the Director of National Intelligence (DNI) maintains a list of the "permissible uses of signals intelligence collected in bulk". This list is to be "made publicly available to the maximum extent feasible, consistent with the national security". There are further rules on data minimisation, dissemination, retention, security, and access, but the five year retention period remains in place, and there is still broad scope for access and sharing through generic references to "national security and foreign policy" (though further high-level reviews are examining these issues).

The DNI reports to the National Security Council, whose Office of Intelligence Programs (OIP) is supposed to provide routine oversight of the US Intelligence community. The White House has a dedicated Foreign Intelligence Advisory Board and various executive bodies, including the Inspector General and Office of Management and Budget, also have some oversight powers. Congressional oversight began in the 1970s. While the PPD did little to enhance these mechanisms, it does suggest that in some circumstances foreign governments may be notified if their citizens were subjected to collection, retention, or dissemination of information in violation of the new procedures it contains.

Moreover, a senior official of the State Department will now serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the US.

2.2 Rules on foreign intelligence gathering in EU Member States

Whereas US law sets out the scope and criteria for which foreign intelligence operations are permitted, increasingly requires rudimentary judicial authorisation for intelligence operations, and has different layers of oversight and accountability, many of the comparative legal frameworks in European states appear to give foreign and military intelligence agencies 'carte blanche' to engage in similar conduct. Direct comparisons with the US are difficult because much less is known about practice and because the regulations that do exist often do not contain sufficient detail about the extent to which intelligence can be gathered on foreign citizens' communications that originate outside the country. For instance, in France – a country that has vast SIGINT capabilities – there is no publicly available law that spells out the precise modalities and safeguards that apply to the collection, analysis and retention of foreign intelligence by the French Directorate General for External Security (Direction Générale de la Sécurité Extérieure – DGSE).

It is also difficult to reach general conclusions about European intelligence agencies' SIGINT activities. In some of the EU's smaller Member States, foreign intelligence gathering is still the exclusive preserve of military intelligence agencies (for example the General Information and Security Service in Belgium), whereas the larger Member States tend to have dedicated foreign intelligence agencies tasked with SIGINT gathering (for example the Direction Générale de la Sécurité Extérieure (DGSE) in France, the Agenzia Informazioni e Sicurezza Esterna (AISE) in Italy, and the Bundesnachrichtendienst (BND) in Germany). These different institutional structures reflect different historical and constitutional practices. In Denmark, for instance, the Forsvarets Efterretningstjeneste (FE) is both the foreign and military intelligence service. The UK and Sweden have dedicated SIGINT agencies (the Government Communications Headquarters (GCHQ) and the Försvarets radioanstalt (FRA)), while in Spain the National Intelligence Centre (CNI) performs SIGINT activities. In the Netherlands, both the General Intelligence and Security Service (AIVD) and the military intelligence agency (MIVD) can task the National SIGINT Organisation (NSO) with the collection of foreign intelligence.

Despite these variations in structure – and their different technical capacities – laws authorising foreign intelligence gathering by European Member States are broadly similar. A comprehensive review of every European legal act that

regulates foreign intelligence collection and analysis is beyond the scope of this paper, but it can still be demonstrated that these acts share similar structures and that many countries have made similar policy choices in respect of the regulation of foreign intelligence collection.

The collection of communications data outside the territory of the state is authorised for a wide variety of purposes.[10] These purposes broadly relate to "national security" and cover external military threats, the prevention or detection of serious crimes, such as terrorism and the proliferation of weapons of mass destruction, and often include the collection of data "relevant" to a country's foreign policy or economic interests.

With the exception of Sweden, these laws do not clearly distinguish the collection of SIGINT for military purposes from other purposes. They also tend not to explicitly rule out the interception of foreign communications in bulk.[11] On the contrary, supplementary provisions often compel telecommunication service providers to cooperate with intelligence agencies in order to secure them access to foreign communications. These agencies then filter the data they have collected on the basis of "selectors", which can consist of personal data or keywords. These selectors may need to be approved in advance by the executive, usually at ministerial level, and may be subject to periodic review by the government or in some instances by an independent intelligence oversight body. In Sweden, for example, a Defence Intelligence Court was established to authorise the collection of data and the use of specific "search concepts". In Belgium, an independent intelligence oversight body has the power to prohibit interceptions that do not adhere to national law. Retention periods vary for the data that has been collected and analysed for foreign intelligence purposes.

Some countries also have safeguards aimed at minimising the amount of data held on their citizens. The Netherlands has a broad statutory provision requiring the deletion of any data that has been "wrongly processed". No country explicitly provides for minimisation procedures or remedies for non-citizens and there is a lack of detail regarding the nature, scale, purposes and oversight mechanisms of foreign intelligence gathering by European intelligence agencies. If legal frameworks are publicly available, they generally compare unfavourably with the situation in the US after the adoption of the Presidential Directive. If European governments want to see further limits to the activities of the NSA and better protections for their own citizens, it stands to reason that they need to get their own houses in order by developing,

publicising and adopting publicly available standards that govern their foreign intelligence collection.

3 State obligations under international law

Espionage is an accepted part of the laws of war,[12] but outside of this context international law has little to say about those instances where foreign intelligence gathering can be seen as a potentially lawful exercise of self-defence (in order to protect a state against the threat of armed attack, for instance) and when it constitutes an illegal interference in a country's internal affairs. This uncertainty does not prevent a country outlawing espionage in its own territory, nor does it mean that there are no human rights limitations on extraterritorial and transnational intelligence collection.

But the lack of clarity around the authorisation and scope of foreign intelligence practices stands in stark contrast to the array of international human rights standards that should apply to laws and policies in this area. The surveillance of Internet activities and the electronic communications of individuals (and of the patterns of their interactions), affects a range of human rights protected by international (global and regional) human rights treaties. This directly impacts on the right to privacy (or "private life") and correspondence, but also clearly affects other rights, including freedom of expression, freedom of information, and freedom of association.

The main global and regional human rights treaties[13] all stipulate that rights can only be restricted or interfered with on the basis of "law"; and that such restrictions or interferences must serve a "legitimate aim" and must be "necessary" to achieve that aim. Secret rules – or secret guidelines on or interpretations of the rules – that an affected person cannot know, are not "law".[14] Neither are rules that give the authorities excessive discretion or that fail to protect against arbitrary exercise of the powers in question. The scope and manner of exercise of any discretion granted must therefore be indicated (in the law itself, or in binding, published guidelines) with "reasonable clarity" so that, again, individuals can reasonably foresee how the law will be applied in practice.[15]

It is one of the hallmarks, and one of the greatest achievements, of modern, post-WWII international human rights law that human rights must be accorded to "everyone". This approach was confirmed by, and under, the binding international human rights treaties adopted to implement the Universal

Declaration of Human Rights, including both the UN ICCPR and the European Convention on Human Rights (ECHR).[16] While positive human rights obligations on states (to ensure, to protect, or to legislate) may not apply outside a country's own territory, the negative obligation not to violate (i.e. the more modest obligation to respect) human rights applies everywhere and with respect to everyone. As former UN Human Rights Committee member and Special Rapporteur Martin Scheinin has observed:

> The question about surveillance abroad is not whether it *per se* is prohibited under the ICCPR. Obviously, it is not. The pertinent question is whether such specific *forms of surveillance that would constitute a human rights violation if performed at home* will be immune from review under the ICCPR if performed by the same state in relation to the same individuals but outside the national territory.[17]

3.1 The basic principles applied to surveillance

A joint declaration on surveillance programmes by the UN and the Inter-American special rapporteurs on freedom of expression, which draws on the case law of the UN's Human Rights Committee and the Inter-American Commission and Court of Human Rights, says:[18]

> [...] states must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged.
>
> Given the importance of the exercise of these rights for a democratic system, the law must authorize access to communications and personal information only under the most exceptional circumstances defined by legislation. When national security is invoked as a reason for the surveillance of correspondence and personal information, the law must clearly specify the criteria to be used for determining the cases in which such surveillance is legitimate. Its application shall be authorized only in the event of a clear risk to protected interests and when the damage that may result would be greater than society's general interest in maintaining the right to privacy and the free circulation of ideas and

> information. The collection of this information shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society.

As the UN and Inter-American rapporteurs make clear (as did the European Court of Human Rights on numerous occasions), there is an interference with fundamental rights as soon as communication data is intercepted and collected, not just at the moment data is extracted from a bulk interception database and used in respect of the relevant person (as some governments have suggested). As such, individuals must be protected against their data being "hoovered" up for the purpose of analysis and data mining. This was explicitly stressed in terms of the ECHR by Judge Zupančič of the European Court of Human Rights at the hearing into mass surveillance of the European Parliament's civil liberties committee (LIBE).[19] It has also been stressed in recent reports from the High Commissioner for Human Rights,[20] and the Special Rapporteur on Counter-Terrorism and Human Rights, who noted:[21]

> By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality analysis. It permits intrusion on private communications without independent (or any) prior authorization based on suspicion directed at a particular individual or organization. Ex ante scrutiny is therefore possible only at the highest level of generality.

3.2 The applicability of international human rights treaty obligations to extra-territorial acts of states that are parties to these treaties[22]

States must ensure (or secure) the rights guaranteed by international human rights treaties without distinction or discrimination to "everyone within their territory or jurisdiction" or simply "within their jurisdiction" or "subject to their jurisdiction" (ICCPR, Art. 2(1); ECHR, Art. 1; IACHR, Art. 1(1)).[23] This has consistently been the position of the Human Rights Committee, as expressed in its views in the cases of Lopez Burgos v. Uruguay and Celiberti de Casariego v. Uruguay,[24] and as summed up in its General Comment on "the Nature of the General Legal Obligation Imposed on States Parties to the Covenant".[25]

If a state intercepts, extracts copies of, and analyses communications made by individuals and organisations outside its borders, that "produces effects" on those concerned, even if they are "foreigners" and not physically on the territory of the state concerned. It is therefore difficult to maintain that if a

state explicitly legislates to authorise such surveillance, it is not exercising its "jurisdiction" in that respect: bringing something within its law is perhaps the most conspicuous way to exercise a country's jurisdiction. It can be argued that in international legal terms, the country would be exercising both "legislative" and "enforcement jurisdiction" (executive powers to enforce the law, including by investigating a crime) over the data.

This would be the case even if the exercise of that jurisdiction violated the sovereignty of another state, for example by concerning data physically located in another country. The fact that the act was contrary to international law does not mean that the state perpetrating the act was not bound by its human rights obligations. However, certain states, most notably the US and Israel, do not accept any extraterritorial effect of their international human rights treaty obligations, in particular in relation to the ICCPR. In its 2006 Concluding Observations on the US report under the ICCPR, the Human Rights Committee[26] urged the US to review this approach. The Special Rapporteur on counter-terrorism and human rights concluded: "States are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction."[27]

3.3 Transnational data collection and state sovereignty

Quite separate from the duty of states to comply with their international human rights obligations when acting extraterritorially, there is the question of when transnational collection of data by one state from servers or routers or other devices in another state, as part of a general surveillance programme by the first state, is compatible with general public international law and in particular with the principles of respect for other states' sovereignty and non-interference in the internal affairs of another state. We are talking here of data being actively "pulled" from a server in the latter country by – or at the behest of – an agency of the first country.[28]

For instance, we know from the Snowden revelations that corporations established in the US, controlled from the US, or even just active in the US, can be ordered by the US authorities to produce such data from servers they own or operate in other countries; and can be ordered by the US authorities to not inform either the authorities in the countries from which they pull the data, or the entities whose data they are handing over, or indeed the data subjects, of such compulsory data disclosures.

Leaving the broader, more complex issues aside,[29] we should note that:[30] "The governing principle is that a state cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter". More specifically, as the International Law Commission has stated:[31] "With regard to the jurisdiction to enforce, a state may not enforce its criminal law, that is, *investigate* crimes or arrest suspects, in the territory of another state without that other state's consent" (emphasis added).

As noted above, rather than consenting to extraterritorial investigations by foreign agents on the territory of other states, in international law enforcement cooperation the established norm is to provide mutual legal assistance through Mutual Legal Assistance Treaties. The transnational collection of data by law enforcement agencies is highly contentious even when possible under domestic law, as demonstrated by proposals to supplement the Cybercrime Convention with a protocol clarifying that transnational access to data, and the "pulling" of data from other countries, without the consent of such other countries, is contrary to public international law.[32]

Similarly, the post-WWII treaties between Western states on international cooperation in relation to national security also start from the premise that – outside of times of war – spying by one nation on the activities of citizens of another nation is, in principle, a violation of the sovereignty of the latter nation. That the states in question felt the need for treaties in this regard suggests that they believe that without such treaties transnational surveillance (outside of times of war) is unlawful under public international law. The Western Allies equally felt obliged to enter into formal (treaty) agreements on intelligence with the Federal Republic of Germany at the end of the WWII occupation period.[33]

Crucially, it is not enough to argue that just because many states in practice collect data held in other countries in the absence of a treaty (either in a law enforcement or a national security operations context) that the requirement of consent from the target country has somehow gone away, or even that transnational access to data without such consent from the target country is now allowed under customary international law.[34] The creation of new customary law requires not just wide state practice (and it is even doubtful whether the practice really is that widespread) but also, crucially, *opinio iuris*: acceptance by states that the practice takes place under a legal rule.

The strong protests against transnational surveillance, as expressed both by individual states in Europe, South America and elsewhere, and by major intergovernmental bodies and fora such as the UN General Assembly, the Council of Europe, and the European Parliament and Commission suggest that transnational collection of data from a country without that country's consent, for either law enforcement or national security purposes, is not formally tolerated under customary international law outside a situation of armed conflict.

3.4 The European Convention on Human Rights

Despite the relatively weak standards on foreign intelligence collection by EU Member States, the European Convention on Human Rights to which those states are parties sets relatively high standards in terms of the compliance of all surveillance regimes with the rule of law. Douwe Korff has identified the following minimum standards, which should apply to all surveillance practices by Council of Europe Member States:

- Surveillance powers must be set out in statute law, rather than in subsidiary rules, orders or manuals. The rules must moreover be in a form that is open to public scrutiny and knowledge. Secret, unpublished rules in this context are fundamentally contrary to the Rule of Law; surveillance on such a basis would ipso facto violate the Convention.

- The offences and activities in relation to which surveillance may be ordered should be spelled out in a clear and precise manner;

- The law should clearly indicate which categories of people may be subjected to surveillance;

- There must be strict limits on the duration of any ordered surveillance;

- There must be strict procedures to be followed for ordering the examination, use and storage of the data obtained through surveillance;

- There must be strong safeguards against abuse of surveillance powers, including strict purpose/use-limitations (e.g., preventing the too-easy disclosure of intelligence data for criminal law purposes) and strict limitations and rules on when data can be disclosed by national security agencies to law enforcement agencies, etc.;

- There must be strict rules on the destruction/erasure of surveillance data to prevent surveillance from remaining hidden after the fact.

- Persons who have been subjected to surveillance should be informed of this as soon as this is possible without endangering national security or criminal investigations, so that they can exercise their right to an effective remedy at least ex post facto; and

- The bodies charged with supervising the use of surveillance powers should be independent and responsible to, and be appointed by, Parliament rather than the Executive.[35]

4 Proposals for surveillance reform

For all the shock and outrage generated by the Snowden disclosures, many of the current questions around extra-territorial surveillance capabilities, national sovereignty, human rights protection and the need for international agreements limiting the interception of communications had already been raised by the European Parliament's 2001 report on "the existence of a global system for the interception of private and commercial communications (ECHELON interception system)".[36] More proposals for surveillance reform have been tabled since the Snowden disclosures, the four most prominent of which we draw on to help frame the discussion that follows.

First are the 13 "necessary and proportionate" principles, elaborated prior to the Snowden revelations, which seek to codify and apply the human rights obligations described above to all forms of communications surveillance.[37] Second are the five principles for surveillance reform endorsed by eight of the US's best known technology companies in December 2013, urging governments across the world to enact measures to put them into practice.[38] Third are the 46 recommendations of President Obama's Review Group on Intelligence and Communications Technologies.[39] Fourth is the report of the European Parliament Civil Liberties (LIBE) Committee special enquiry into the Snowden revelations.[40] A summary of the different sets of principles as far as they relate to state surveillance of nationals of other countries is provided in Table 1.

The four sets of principles/proposals include some broadly similar provisions, such as an end to the limitless, "bulk collection" documented by Edward Snowden's documents in respect of the NSA; enhanced disclosure of the legal authorities underpinning orders that compel companies to provide data about their customers; increased transparency around the number and nature of such orders; and better oversight of the agencies conducting communications surveillance. However, the proposals differ markedly in their approach, scope and substance, particularly with regard to forms of judicial control, the rights of subjects of foreign surveillance, and obligations vis-à-vis data use and minimisation. In particular, the "necessary and proportionate" principles make no distinction between surveillance by police or intelligence agencies, or between investigative and preventative measures, and are designed to apply "regardless of the purpose for the surveillance – law enforcement, national security or any other regulatory purpose".[41] They also make no distinction between the rights of nationals and non-nationals subject to surveillance by a

particular government, and advocate both notification of the data subject that surveillance has taken place and full access to a judicial process enabling them to challenge the warrant or order against them.

At the other end of the spectrum, the "company principles" make no mention whatsoever of individual rights and assume instead that, given adequate opportunity, communications service providers and data controllers will always advocate in their customers' best interests and challenge those surveillance requests they deem to be overbroad or illegitimate. Somewhere between these two stools sit President Obama's review panel's proposals to extend the 1974 Privacy Act to non-US persons – which the PPD went some way to meeting – and to introduce a "Public Interest Advocate" into FISC proceedings.

Despite the understandable outrage directed at the NSA and White House policymakers, it is worth repeating that this and other standards proposed by the Review Group (and even the much weaker version adopted by the President in the PPD) would again mean that US law has by far the most specific and transparent statement of principles, procedures and oversight for foreign intelligence collection. Any international attempt to raise these standards to a higher level will have to recognise the US as the new benchmark, and point toward tighter controls in other states.

Table 1: Summary of reform proposals

Issue	Necessary and Proportionate	Company principles	Obama Review Group	European Parliament
Mandatory retention of metadata	*a priori* data retention or collection should never be required of service providers[42]	limitations on governments' ability to compel service providers to disclose user data that balances need for data in limited circumstances with users' privacy interests[43]	US government should introduce a system in which metadata is held by private providers or by a private third party; access to such data should be permitted only with an order from FISC[44]	Report refers to opinion of Advocate-General Cruz Villalón on Directive 2006/24/EC concluding that data retention as a whole is incompatible with Article 52(1) of the Charter of Fundamental Rights of the European Union[45]
Bulk collection	prohibited; see minimisation, below	prohibited [46]	end to collection and storage of *all* mass, undigested, non-public personal information; any programme involving collection or storage of such data must be narrowly tailored to serve an important government interest;[47] agencies should examine feasibility of creating software allowing targeted information acquisition[48]	calls on the US authorities and the EU Member States, where this is not yet the case, to prohibit blanket mass surveillance activities;[49] points to world's leading technology companies' call for sweeping changes to national surveillance laws, including an international ban on bulk collection of data[50]

Data mining	not addressed	not addressed	Civil Liberties Impact Assessments to ensure that any big data and data-mining programmes are statistically reliable, cost-effective and protective of privacy[51]	not addressed
Judicial control	an independent, impartial, and competent authority capable of establishing that other available less invasive investigative techniques have been considered[52]	reviewing courts should be independent and include an adversarial process[53]	duly enacted laws or properly authorised executive orders;[54] create position of Public Interest Advocate to represent privacy and civil liberties interests before FISC[55]	respect the principles of legality, necessity, proportionality, due process and transparency, in line with the standards of the European Convention on Human Rights as regards data protection, privacy, and the presumption of innocence;[56] strict limits on duration and scope of any surveillance ordered unless its continuation is duly justified by the authorising/oversight authority[57]
Disclosure of legal authorities	see notification, below	disclosure of important rulings in a timely manner so that the courts are accountable to the public[58]	detailed information about legal authorities requiring third parties to hand over personal data to be made available on a regular basis (with strong presumption of transparency for unclassified programmes);[59] non-disclosure orders may only be issued subject to	convinced that secret laws and courts violate the rule of law[62]

			judicial finding of reasonable grounds[60] and last for no longer than 180 days without judicial re-approval[61]	
Rights of subjects of foreign surveillance	access to a fair and public hearing within reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life[63]	not addressed	USG should apply 1974 Privacy Act to both US persons and non-US persons[64] and explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens with a small number of closely allied governments[65]	calls on the US to revise legislation without delay so as to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens, to put rights of EU citizens on an equal footing with rights of US citizens, and to sign the Optional Protocol allowing for complaints by individuals under the ICCPR[66]
Notification of data subjects	individuals should be notified of decisions authorising communications surveillance with enough time and information to enable them to appeal unless notification would seriously jeopardise the purpose for which the surveillance is authorised[67]	not addressed	not envisaged	respect the principle of user notification[68]
Data minimisation	data accessed must be confined to what is reasonably relevant and any	not addressed	extend provisions on data minimisation for US citizens in S.215 of Patriot Act to	not addressed except as general principle for governance of the Internet[71]

	excess information collected must be promptly destroyed or returned to the impacted individual[69]		National Security Letters; PPD-28 effectively extends provisions to all subjects of signals intelligence[70]	
Onward transmission/purpose limitation	surveillance data can only be accessed by the specified authority and used for purpose for which authorisation was given[72]	not addressed	no dissemination of information about non-US persons unless the information is relevant to protecting the national security of the US or its allies[73]	not addressed
Transparency	governments to publish periodic reports and other information relevant to communications surveillance[74]	companies to publish the number and nature of government demands for user information; governments should also promptly disclose this data publicly[75]	recipients of orders may publicly disclose on a periodic basis general information about the number of such orders, the number complied with, general categories of information and number of users affected unless government makes compelling demonstration that disclosures endanger national security;[76] government should publicly disclose on a regular basis general data about such orders[77]	only refers to transparency in general terms; calls for EU proposal on standardised general terms and conditions for online and telecommunications services[78]
Oversight	independent mechanisms that ensure transparency	strong checks and balances[80]	Director of National Intelligence should establish	should be based on both democratic legitimacy (strong

	and accountability and have the authority to access all potentially relevant information about state actions, including, where appropriate, access to secret or classified information, to evaluate whether the state has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers[79]		a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers. To this end, the Director of National Intelligence should prepare an annual report on this issue to the National Security Advisor, to be shared with the Congressional intelligence committees[81]	legal framework, ex ante authorisation and ex post verification) and adequate technical capability and expertise – the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;[82] should include power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments[83]

5 A roadmap for multilateral standards

We have shown that there is a vast gulf between national SIGINT practices and international human rights law, significant variations among the national legal frameworks governing such surveillance (which range from inadequate to wildly inadequate), and numerous unmet demands for surveillance reform. The global political and economic pressure generated by the Snowden revelations provides us with an opportunity to modernise standards across the democratic world in a manner that respects privacy and accounts directly for the way that information technology is transforming social and material life, and with it the capacity for surveillance.

This opportunity will be missed, however, unless attempts are made to establish a genuine multi-stakeholder process that seeks to bridge the gaps between the views of different interest groups and the silos in which they continue to work. More research, new ideas and much discussion is required, but it is clear already that the lacuna in human rights protection caused by foreign intelligence gathering and exchange can only be addressed through a transnational process anchored in common goals and shared objectives. To kick-start this process we suggest focusing specifically on three simple yet unanswered questions, initially as far as they relate to SIGINT collection and the privacy rights (or lack thereof) of foreign nationals/non-citizens:

i. What laws and procedures authorising surveillance should be put in place?
ii. What rules should govern the operational practice?
iii. What methods of oversight and accountability should apply to these laws and practices?

These questions reflect the existing structure of surveillance policy and practice in most countries and can be answered by considering what intelligence agencies should be allowed to do, how they should be allowed to do it, and how their actions should be scrutinised and held in compliance with fundamental rights and democratic responsibilities.

5.1 Laws and procedures for authorising surveillance

Any discussion of when surveillance may be authorised in a rule of law framework begins with an assessment of its impact on individual, civil and

political rights. In open and democratic societies any infringement upon these rights can only be justified on the basis of the greater societal need. Historically we have become accustomed to a high bar: that is, judicial authorisation based on probable cause and due process demonstrating that the interception of communications is necessary and proportionate to the nature of the offense or conduct being investigated. As we have shown, the interception of foreign communications by intelligence agencies in the Internet age has a much lower threshold. Three fundamental issues must be addressed in order to establish a clear procedure for seeking authorisation: the justification, scope and scale of communications surveillance for SIGINT purposes.

The first issue is the specific national security purposes for which surveillance may be justified. The US's Presidential Policy Directive of January 2014 offers a point of departure insofar as it moves beyond the mere 'relevance' to national security or foreign policy standard which has long provided a catch-all justification. But there is still a big gap to the bright lines of international human rights law, which makes clear that any interference in the right to privacy on such grounds must be legitimate, proportionate, narrowly proscribed and necessary in a democratic society.

The second issue is the standard of privacy protection that applies extraterritorially to the communications of persons subject to foreign intelligence collection. Most states appear to routinely ignore the privacy rights of persons affected by SIGINT collection, and current law and practice relies overwhelmingly on distinctions that technology has rendered more difficult if not impossible to draw, between internal and external communications, citizens and non-citizens, content and traffic etc., all of which have the effect of imposing a lower standard of protection for communications data relating to foreign nationals. It is clear that international law places an obligation on states to recognise the right to privacy and security of communications of foreign surveillance targets, but a fierce debate now rages among international jurists as to the precise nature of those obligations and the best way of demarcating them within the international legal order. However, even if some clarity is provided by the United Nations Human Rights Council, it will still be left to Member States to meet these commitments through domestic law and policy. How can this be achieved and what standards will apply?

In Europe, much of the debate about how to protect European citizens from the foreign intelligence gathering operations of the US has come to rest on EU

data protection law, which requires foreign companies and third states processing data that originates in the European Union to apply an adequate standard of protection for that data. The US is now unusual in explicitly offering any kind of guarantee to respect the privacy of foreign persons subject to its foreign intelligence gathering operations, but these protections are to an explicitly lower standard than those afforded to US persons. This issue has long hampered EU-US cooperation in the area of counter-terrorism, and following Snowden's revelations now represents the greatest impasse between the US, which has steadfastly refused to amend its privacy framework, and many in the EU who demand equal treatment and the possibility for European citizens to seek redress for violations of privacy. In leveraging data protection in this way, the EU is essentially advocating for foreign nationals to be able to complain to privacy commissioners or surveillance courts, where these exist, about foreign intelligence operations that affect them. Although EU data protection law provides for a reciprocal complaints mechanism, many intelligence agencies in Europe are effectively beyond the scope of national data protection authorities, and it is doubtful that all EU Member States provide redress where foreign or military intelligence is concerned (though the Investigatory Powers Tribunal in the UK has considered complaints from non-nationals against GCHQ's bulk collection programmes).[84]

An alternative to a top-down standard is for cooperating states to limit SIGINT collection within agreed geographical areas in favour of a commitment to MLATs based on due process and a greater degree of protection for one another's citizens. But even in the European Union, where mutual recognition and cooperation between different jurisdictions is most developed, the larger powers clearly retain a strong preference for unilateral intelligence gathering capabilities. which undermines precisely the trust needed for states to commit to greater police and judicial cooperation in sensitive areas like counter-terrorism. Like the proposed "no-spy" agreements, such cooperation mechanisms raise the prospect of two or even three-tier protection systems, where a state's own citizens enjoy the highest level of protection, the citizens of friendly states enjoy reciprocal guarantees, and persons located in the rest of the world remain largely unprotected. In this scenario, the broader goal of a rights-based international standard for protecting the privacy of foreign nationals remains elusive.

The third issue is the amount of surveillance that is allowed. In the absence of meaningful standards, the authorisation for SIGINT operations in many nations appears to be almost automatic, allowing the interception, storage and

subsequent analysis of that data as long as it is "relevant" to the national interest. This is where the largest disjunct between international human rights norms and the existing regulation of surveillance powers is located: SIGINT agencies have essentially been allowed to decide for themselves how much data they need in order to fulfil their mandates, and they have become accustomed to collecting this data.

This practice, and the discourse around it, is typically framed in terms of looking for "needles" in data "haystacks"; a narrative which views bulk interception and data storage as an *a priori* legitimate tool in effective intelligence operations and not an infringement of individuals rights *per se*. It is further assumed by the intelligence community that the infringement of the data subject's rights takes place only at the point at which their data is retrieved from the "haystack" on the basis of a search term, keyword or other selector. At this point the justification for privacy violations is reduced to a matter of SIGINT operating procedures.

As shown above, this position cannot be reconciled with international human rights law, and most stakeholders agree that the bulk collection programmes revealed by Snowden are unacceptable. The UN Special Rapporteur on Counter-Terrorism and Human Rights went as far as to call them "indiscriminately corrosive of online privacy and imping[ing] on the very essence of the right guaranteed by article 17. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law."[85]

If we start from this principle, the challenge then is to think through the contours of legitimate intelligence gathering in today's increasingly data-driven world. Any discussion about the authorisation of SIGINT operations and access to communications systems overlaps with debates about private sector mandates for 'data retention', i.e. the imposition of obligations on service providers to retain metadata for law enforcement and security purposes. The NSA review panel proposed an end to the bulk metadata collection by the NSA, but suggested instead that service providers should keep data for 30 months, with access controlled by the surveillance courts. The EU has moved in the other direction. Its Court of Justice determined the EC "Data Retention" Directive, and the principle of keeping data for 6-24 months, on the basis that it might later prove useful to police and security agencies, to be an unacceptable intrusion into a fundamental right, which is compounded by a lack of safeguards.[86]

The need for some standards in this area is underscored by the tension that arises when one country has retention and access policies that violate the laws of another. Such standards must therefore address both the powers of national security agencies and the specific role of private sector actors mandated by law to participate in SIGINT operations, including the appropriate legal procedure for responding to intelligence requests.[87]

5.2 Rules governing intelligence practice

The second key element of privacy-conscious intelligence reform is enforceable standards that restrict authorised surveillance operations to their intended purpose and that guard against abuse. This includes rules on the minimisation of data collected during a legitimate operation, limits on what the data can be collected or used for, provisions for the deletion of data not relevant to an investigation, and provisions for retaining data. This set of criteria should also address conduct that should be prohibited or more tightly controlled such as the undermining of encryption protocols, the use of "zero-day attacks" and the sharing of data internationally where this would have the effect of circumventing domestic privacy safeguards.

With respect to minimisation, broadly comparable standards for operational data protection in the police sector do exist in most democratic countries, and part of the challenge is to effectively extend and apply those standards to the largely unregulated realm of foreign intelligence gathering. The basic provisions in the PPD provide a point of departure for this exercise. More complex is the "big data" dimension of the SIGINT framework and the issue of how analytical tools capable of profiling entire personal networks can be regulated or minimised. In this context we should take seriously, as did President Obama's Review Group, the possibility that technology could ultimately minimise infringements of privacy by performing certain techniques in 'real-time', thus reducing much of the need for bulk interception and storage.

With respect to conduct that should be prohibited, the Snowden documents revealed many of the operational practices of US and UK intelligence agencies, but comparable information for other countries is not available. Nevertheless, a case-by-case assessment of the legitimacy of the actions that have been revealed can be used to inform standards internationally. More general concerns about the purpose of surveillance – economic espionage and 'political policing' for example – can also be addressed. The US's Presidential Policy Directive appears to provide a straightforward prohibition on economic

espionage but does so only by ruling out the collection of information for the purpose of gaining a competitive advantage for US business, thus allowing the ongoing surveillance of economic actors for national security purposes.

There is a geopolitical dimension to these issues as well, as evidenced in debates over the existence and extension of “no-spy” agreements, raising the prospect of groups of countries agreeing to limitations with respect to one another’s territories and/or citizens. The European Parliament goes so far as to suggest that the EU principle of “sincere cooperation” requires that Member States refrain from conducting intelligence activities in other Member States' territories. Obama’s Review Group proposed a set of criteria for negotiating special arrangements covering these issues with third states.

5.3 Methods of oversight and accountability

The third element of communications surveillance reform is the methods of oversight and accountability that should apply to these laws and practices. Even if detailed new laws restricting the authorisation of surveillance operations and strict operational procedures for their conduct were to be put in place, the age old question of ‘who watches the watchers’ requires substantial thought and novel application. Despite comprising the majority of the work undertaken by intelligence agencies, SIGINT is subject in many countries to minimal oversight. This is due to the reasons outlined above, as well as to the outdated notion that SIGINT does not affect citizens or domestic communications. So what role should the executive, judicial, and legislative branches of government play with respect to the operations and activities of SIGINT agencies?

There is growing acknowledgement that existing models of oversight and accountability have failed completely to ensure that surveillance is both properly authorised and legitimately practiced, but there is no consensus on what constitutes best practice in terms of SIGINT collection. This is hardly surprising given the difficulty of applying these precepts to organisations that are shrouded in secrecy and fiercely resistant to change.

Two issues in particular must be addressed. First is the role of the judiciary – both in authorising intelligence collection and, as noted above, reviewing the legality of specific operations and programmes. In the US, the Review Group proposed the introduction of an adversarial counsel into the FISA court, or some other form of ombudsman to guard the public interest. Many European states do not even have clear legal processes in which such offices could

participate.

Second is the capacity for legislative review and democratic oversight within a classified environment. This issue is intimately related to the resources available for oversight, the technical competence of the reviewers, the avoidance of regulatory capture (of the overseer by the overseen), and the intractable difficulty of imposing any mechanism for international oversight of national intelligence agency cooperation.

The Civil Liberties (LIBE) Committee in the European Parliament has called for "minimum European standards or guidelines on the (*ex-ante* and *ex-post*) oversight of intelligence services… including the issue of oversight bodies being considered as a third party under the 'third party rule', or the principle of 'originator control', on the oversight and accountability of intelligence from foreign countries". This is the principle that prevents intelligence agencies disclosing the source or content of information received through bilateral cooperation. It undermines in practice the potential for oversight, because it prevents any review whatsoever of international exchanges of intelligence data.

The LIBE report calls on EU Member States to establish the power for oversight bodies to conduct on-site visits of intelligence agencies, interrogate senior officials and ensure strict independence of inspectors from their respective governments. For such functions to be credible in the eyes of the public, standards for transparency and reporting requirements, including the methods used to correct instances of non-compliance (whether malicious or otherwise), must also be developed.

Because the vast majority of data relevant to foreign intelligence collection is gathered, stored, processed and transmitted by private companies, frameworks for oversight and accountability must be broadened to encompass these entities, who find themselves effectively sandwiched between their legal obligations to provide data to national security agencies on one side and their users' reasonable and legitimate expectations with regard to their right to privacy on the other. This situation is particularly acute for US companies, whose data represents a highly disproportionate share of the world's Internet traffic.[88] Their role is further compromised because even when they provide networks and services that are entirely outside the US, they remain subject to US law.[89]

Transparency is an essential part of any oversight system and provides a good foundation for public accountability more broadly.[90] In the past few years,

some Internet service providers have begun publishing comparative international information about government and law enforcement agency demands for their users' data.[91] Since the Snowden revelations, more companies have begun producing transparency reports, and those already doing so have petitioned the US government to let them publish information about their hitherto secret dealings with the NSA. The US government is now cooperating with the private sector to permit some level of transparency with aggregate figures.

The key question is whether the current model of aggregated transparency reporting can provide sufficient detail to allow the public to ascertain the true extent of surveillance practices and the extent to which the private sector is pushing back against undue or overbroad requests. Whether companies are resisting (and failing in secret) or whether they are not, what policy changes would incentivise legal departments to push back on dubious requests for customer or traffic data?

A final, related issue is the steps that data controllers should take to protect data from unauthorised access. It is widely accepted that a failure on the part of key service providers to fully encrypt communications flowing between their data centres has enabled intelligence services to intercept personal information on an unacceptable scale. Some companies have already implemented new standards or announced their intention to do so in future. The Obama Review Group and European Parliament reports are both firmly behind mandatory minimum levels of security, including encryption on both commercial services and communications networks. In terms of policy choices were strong encryption to become widespread, practice in this area inevitably begs the question whether, and if so under what circumstances, companies should be legally compelled to hand over encryption keys.

6 Next steps

Governments on both sides of the Atlantic have strong political and economic interests in repairing the damage caused by the Snowden revelations to the development of a rights-based Internet that is valued as a trustworthy information system. Yet despite the severity of the consequences, current political responses have focused either on consolidating power over information networks at the national level (technological sovereignty) or finding a way to manage public alarm while allowing intelligence agencies to continue to operate as before. Many governments will adopt both of these approaches and deepen the problem. Without better answers, we risk diminishing the value of the Internet as a public good, the sanctity of civil and human rights in a digital world, and the commercial imperative of trustworthy online markets.

The European Parliament's report notwithstanding, the loudest response from the EU has been economic rather than political. Among the most common reactions is a threat to extract penalties from US companies doing business in Europe who do not comply with EU data protection rules, a position that will continue to affect negotiations on the Transatlantic Trade and Investment Partnership, the EU Data Protection Regulation, the US's status as a "safe harbour" and the existing EU-US agreements on the exchange of Passenger Name Records (of airline travellers), and SWIFT data (on international financial transactions). While these agreements are rightly being leveraged to advocate higher privacy standards, they cannot solve the fundamental problems engendered by a lack of trust in foreign intelligence gathering capabilities and unilateral decisions about what is and is not acceptable.

Even the European governments most critical of the US have been unwilling to reveal the nature of their own intelligence gathering practices, or commit themselves to the specific, rights-based standards that they demand of Washington. None have stepped forward with a clear proposal for bringing communications surveillance under the rule of law and protecting privacy across borders. Nor have any national movements emerged of political and economic stakeholders united around a pragmatic call for reform. Silicon Valley has been quick to call for government reform but is less sanguine on the digital rights aspect of that agenda. Civil society needs to show how the principles for necessary and proportionate communications surveillance can be applied in practice to legitimate national security operations.

It is logical that this kind of coalition building should begin in Germany. It is the most influential country in the European Union, and the outrage over the Snowden revelations presents the best opportunity for initiating a reform effort and championing a common standard among European states. The German government has been among the most outspoken in its demands for restrictions on the NSA, particularly in the wake of revelations that the German Chancellor was a personal target of surveillance. Germany is also a recognised leader in commercial data protection and German technology companies have been quick to develop "made in Germany" cybersecurity products.

The government in Berlin has launched a parliamentary investigation, and the political energy that has animated the public debate over the Snowden affair continues unabated, refreshed by every new revelation published in the *Guardian* or *Der Spiegel*. For the majority in Germany, the NSA is a serial violator of human and civil rights, and these excesses fit into the narrative of American overreach in the name of counterterrorism that includes torture, Guantanamo Bay, and unrestricted drone assassinations. If organised around a policy agenda, these politics could fuel a German-led coalition within the EU that is strong enough to change minds in Washington. Germany has a unique combination of political power in Europe, commercial interest in strengthening its digital economy, and international integrity on issues of data privacy and human rights. The circumstances are ripe for leadership to step forward in Germany and link up with parallel movements in Europe and beyond to present a strong and credible alternative to Washington leaders locked in a post-9/11 security mindset. If Germany were to show leadership on domestic reform, it could provide a model for the EU, and in turn the basis for a transatlantic agreement and an international norm.

The EU and US already have a particularly close relationship in the areas of economic and security cooperation, and since 9/11 have reached a dozen agreements on police cooperation, surveillance, mutual legal assistance and data protection. Ultimately, the two sides will have to resolve the issues raised in this paper if existing EU-US cooperation is to be maintained or deepened. One potential framework for the approach to the US is the "New Transatlantic Agenda" (NTA) between the US and EU, stemming from the 1990 "Transatlantic Declaration". With sufficient political will this framework could provide a starting point for the adoption of multilateral agreements limiting communications surveillance and ultimately serve as a model for the rest of the world. In the short term, these issues could be taken up by a core group of EU Member States, resulting in some kind of 'minilateral' agreement that can

gradually be extended to other countries. It is hoped that this paper can serve as a basis for deliberation, the formation of a policy agenda, and a rallying point for a multi-stakeholder reform coalition.

[1] *The right to privacy in the digital age*, UN General Assembly Third Committee, 19 November 2014, A/C.3/69/L.26/Rev.1, available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1

[2] Tim Maurer, Robert Morgus and Isabel Skierka Mirko Hohmann, *Technological Sovereignty: Missing the Point?* Transatlantic Dialogues on security and freedom in the digital age, November 2014

[3] UN Human Rights Committee, *Concluding observations on the fourth report of the United States of America*, 23 April 2014, CCPR/C/USA/CO/4, para. 4: "The Committee regrets that the State party continues to maintain the position that the Covenant does not apply with respect to individuals under its jurisdiction, but outside its territory"

[4] *Agreement on mutual legal assistance between the European Union and the United States of America*, Official Journal of the European Communities L 181/34, 19 July 2003, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:22003A0719%2802%29:EN:HTML.

[5] According to the NSA Review Group report, "Requests [to the US government] appear to average approximately 10 months to fulfill, with some requests taking considerably longer", see p.227, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[6] See for example 'IRS manual detailed DEA's use of hidden intel evidence', *Reuters*, 7 August 2013, available at: http://www.reuters.com/article/2013/08/07/us-dea-irs-idUSBRE9761AZ20130807.

[7] FISA contained critical distinctions between standards for collection of US persons and others by providing for two definitions of "agent of a foreign power": one for "any person other than a United States person", and the other for "any person". Furthermore, non-US persons may be subject to data gathering if it "relates" to the ability of the US to protect itself from enumerated threats, whereas for US citizens the standard is "necessary" to protect the US. Similarly, information about a foreign power relating simply to defence or foreign affairs may be collected from a non-US person but only from a US person if "necessary".

[8] See also the analysis in Caspar Bowden, *The US surveillance programmes and their impact on EU citizens' rights*, European Parliament, PE 474.405, September 2013.

[9] *Presidential Policy Directive PPD-28* on "Signals Intelligence Activities" adopted January 17, 2014, available at: http://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf.

[10] See for instance, Sweden, which allows foreign intelligence collection for "actions and aims of foreign powers of material interest for Swedish foreign-, security- and defence policy" (Sweden Government Bill 2008/09:2201 as quoted in Mark Klamberg, 'FRA and the European Convention on Human Rights – A paradigm shift in Swedish electronic surveillance law', *Nordic Yearbook of Law and Information technology*, Fagforlaget: Bergen, 2010, p.119). In Germany such operations are permitted with respect to "events abroad, that are of relevance for the foreign and security policy of the Federal Republic of Germany" (BND-Gesetz vom 20. Dezember 1990, amended in 2013, §2(1)4). The G-10 law also lists more detailed national security purposes for interception methods that interfere with the right to private life (Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), §5). The Netherlands allows collection about unspecified "subjects" regarding "other countries" (Wet op de inlichtingen- en veiligheidsdiensten (WIV) 2002, article 6.2.d). In the UK a permitted purpose is "safeguarding the economic well-being of the United Kingdom, in circumstances appearing to the Secretary of State to be relevant to the interests of national security" (Regulation of Investigatory Powers Act (RIPA), s5(3)(c)). Italy's AISE is responsible for those intelligence activities that are performed outside the national territory in order to "protect Italy's political, military, economic, scientific, and industrial interests" (Law No. 124 of 3 August 2007 Published in the Official Journal no. 187 of 13 August 2007, section 6(2)). Belgium's military intelligence agency can collect intelligence relating to the "scientific and economic interests" of those sectors that are related to defence issues, "or any other interest" of the country. Article 11.1 W.I&V.

[11] UK, RIPA s8(4): an interception warrant to intercept external communications need not name one person as the interception subject, or a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place. Netherlands, WIV, article 27(1) allows for the "non-targeted receiving and storing of non-cable-based telecommunications". In Sweden, Communication Service Providers are obliged to transfer "all cable communication crossing Swedish borders" (Klamberg, ibid. p.118). Belgium's military intelligence can 'search' every form of communication that is transmitted abroad (Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (W.I&V), 4 Feb. 2010, art. 38).

[12] The International Committee of the Red Cross defines espionage as the "gathering or attempting to gather information in territory controlled by an adverse party through an act undertaken on false pretences or deliberately in a clandestine manner". This definition makes no distinction between 'extraterritorial' signals intelligence collection, in which both the communication and the interception of that communication take place on the territory of another state, and 'transnational' signals intelligence collection, in which the communication (but not the interception) takes place on the territory of another state. See Jean Marie Henckaerts, Louise Doswald-Beck (eds), *Customary International Humanitarian Law. Volume I: Rules*. Cambridge, Cambridge University Press, 2005, 391.

[13] The International Covenant on Civil and Political Rights (ICCPR), the Inter-American Convention on Human Rights (IACHR), the European Convention on Human Rights (ECHR), and the African Charter of Human and Peoples' Rights (ACH&PR).

[14] At the European Court of Human Rights, see Siver v. the UK, 1983 and Petra v. Romania, 1998. From the Human Rights Committee, see General Comment No. 34, CCPR/C/GC/34, 12 September 2011, paras. 24 – 26.

[15] Petra v. Romania, paras. 37-38. In Malone v. the UK, the Court used the expression "sufficient clarity": para. 68. See also *The right to privacy in the digital age* - Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30 June 2014, para. 20

[16] Note that the ECHR, too, is expressly inspired by the Universal Declaration of Human Rights: see the first two preambular considerations.

[17] Written testimony by Prof. Martin Scheinin for the Privacy and Civil Liberties Oversight Board's hearing on Wednesday, March 19th in Washington, D.C, relating to the surveillance programme conducted under Section 702 of the FISA Amendments Act.

[18] *Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression*, issued by the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013, paras. 8 and 9, available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

[19] *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - 7th Hearing*, Video recording of the hearing, 14 October 2013, available at: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE.

[20] *The right to privacy in the digital age* (o.c. note 15), para. 20.

[21] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397, 23 September 2014, para. 12.

[22] This sub-section draws on sub-section 3.4 of the recently-published Council of Europe Commissioner on Human Rights' issue paper by Douwe Korff, *The rule of law on the Internet and in the wider digital world,* CommDH/IssuePaper(2014)1 08 December 2014. For a more in-depth academic analysis and more extensive references to the case-law of the Human Rights Committee and other sources, see Martin Scheinin and Mathias Vermeulen, 'Unilateral Exceptions to International Law: Systematic legal Analysis and Critique of Doctrines that seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism', section 3.7, *Denial of Extraterritorial Effect of Human Rights (Treaties)*, available at:
http://projects.essex.ac.uk/ehrr/V8N1/Scheinin_Vermeulen.pdf.

[23] The ACH&PR instead stipulates that "*The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Chapter and shall undertake to adopt legislative or other measures to give effect to them*." (Art. 1).

[24] Case nos. 52/1979 and 56/1979, both of 29 July 1981, at §§ 12.3 and 10.3, respectively. See also the Committee's Concluding Observations on the reports by Israel in 1998 and 2003, mentioned in Scheinin and Vermeulen, o.c. note 22, p. 37, footnote 80.

[25] *General Comment No. 31*, CCPR/C/GC/21, 29 March 2004, para 10.

[26] HRC 2006 Concluding Observations CCPR/C/USA/CO/3, para. 10, available at:
http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/CCPR.C.USA.CO.3.En?Opendocument.

[27] Para. 43, Promotion and protection of human rights and fundamental freedoms while countering terrorism

[28] We are not discussing other scenarios here, such as access by a state national security or law enforcement agency to data held on the territory of the state in question, but when the data is owned by a foreign company or by a foreign public body (e.g., by a company or public body using a cloud service in the country where the data are accessed); or access by a state agency to data flowing through cables running through the territory of the state (even if the data relates to communications between entities that are both, or all, outside the state); or interception of radio or Wi-Fi communications data in one state by interception stations or satellites operated by another state. These scenarios too raise serious questions, also as concerns the different levels of control exercised by different countries over the global Internet and e-communications infrastructure.

[29] For a detailed discussion, see the 2006 Report of the International Law Commission (58th session), *Annex E – Extraterritorial Jurisdiction*, at p. 516ff, available at: http://legal.un.org/ilc/reports/2006/2006report.htm.

[30] Ian Brownlie, *Principles of Public International Law*, 6th ed., 2006, at p. 306. The classic expression of the principle can be found in the award of the sole arbitrator in the *Palmas Island* case, Max Huber: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. The development of the national organization of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations." *Island of Palmas Case* (*Netherlands/United States of America*), Award of 4 April 1928, UNRIAA, vol. II (1928), pp. 829-871, at p. 838, available at: http://legal.un.org/riaa/cases/vol_II/829-871.pdf. See also the *Lotus judgment* of the Permanent Court of International Justice (the forerunner of the International Court of Justice), 7 September 1927, pp. 18-19, available at: http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

[31] 2006 Report of the International Law Commission, *Annex E* (o. c. note 29), para. 22, on p. 526.

[32] At the *Octopus Conference on Cooperation against Cybercrime* (Strasbourg, 4-6 December 2013), it was agreed to explore drafting a new protocol to either the Cybercrime Convention or the Council of Europe Data Protection Convention (or an entirely new, separate treaty) to address this issue. This indicates that transnational access to data, and the "pulling" of data from other countries, without the consent of such other countries, is seen as clearly contrary to public international law; and that Art. 32(b) of the Cybercrime Convention, by itself, does not express such consent. The conference proceedings are available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2013/Octopus2013_en.asp.

[33] See Joseph Foschepoth, *Überwachtes Deutschland*, 3rd ed., 2013, chapter 2. The (German) text of the "Memorandum of Understanding" between the Western allies and the young FRG (full title in English: "Agreements affecting the Intelligence Situation in Germany after the Termination of the Occupation", 11.5.1955, ref. NACP, RG 84) can be found on pp. 291-292. It was only declassified in the last few years.

[34] This was argued by some representatives at the aforementioned *Octopus Cybercrime Conference* in Strasbourg (see note 32).

[35] See further Korff, D. (2013), *Note on European and International Law on Transnational Surveillance prepared for the Civil Liberties Committee of the European Parliament*, 23 August 2013, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf.

[36] *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, European Parliament Temporary Committee on the ECHELON Interception System, 11 July 2001, available at: http://cryptome.org/echelon-ep-fin.htm#13.

[37] *International Principles on the Application of Human Rights to Communications Surveillance*, 10 July 2013, available at: https://en.necessaryandproportionate.org/TEXT [hereafter "Necessary and Proportionate principles"].

[38] *Global Government Surveillance Reform: The Principles*, 9 December 2013, available at: https://www.reformgovernmentsurveillance.com [hereafter "Company Principles"].

[39] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, o.c. note 5 [hereafter "Obama Review Group"].

[40] *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, 21.2.2014 [hereafter "European Parliament report"].

[41] Preamble, Necessary and Proportionate Principles.

[42] "Integrity of communications systems", Necessary and Proportionate Principles.

[43] Para. 1, Company principles.

[44] Recommendation 5, Obama Review Group.

[45] Preamble, European Parliament report.

[46] Para. 1, Company principles.

[47] Recommendation 4, Obama Review Group.

[48] Recommendation 20, Obama Review Group.

[49] Para. 21, European Parliament report.

[50] Para. 17, European Parliament report.

[51] Recommendations 35 and 36, Obama Review Group.

[52] "Proportionality" and "Competent judicial authority", Necessary and Proportionate Principles.

[53] Para. 2, Company principles.

[54] Recommendation 13, Obama Review Group.

[55] Recommendation 28, Obama Review Group.

[56] Para. 22, European Parliament report.

[57] Para. 77, European Parliament report.

[58] Para. 2, Company principles.

[59] Recommendation 7, Obama Review Group.

[60] That disclosure would significantly threaten the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest.

[61] Recommendation 8, Obama Review Group.

[62] Para. 14, European Parliament report.
[63] "Due process", Necessary and Proportionate Principles.
[64] Recommendation 14, Obama Review Group.
[65] Recommendation 21, Obama Review Group.
[66] Para. 30, European Parliament report.
[67] "User notification" principle: such authorisation must granted by the authority authorising the surveillance and the individual affected should be notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed, Necessary and Proportionate Principles.
[68] Para. 22, European Parliament report.
[69] "Proportionality" and "Competent judicial authority", Necessary and Proportionate Principles.
[70] Recommendation 3, Obama Review Group; see also section 4(a)(i) of *Presidential Policy Directive PPD-28* o.c. note 9.
[71] Para. 106, European Parliament report.
[72] "Proportionality" and "Competent judicial authority", Necessary and Proportionate Principles.
[73] Recommendation 13(4), Obama Review Group.
[74] "Public oversight", Necessary and Proportionate Principles.
[75] Para. 2, Company principles.
[76] Recommendation 9, Obama Review Group.
[77] Recommendation 10, Obama Review Group.
[78] Para. 62, European Parliament report.
[79] "Public oversight", Necessary and Proportionate Principles.
[80] Para. 2, Company principles.
[81] Recommendation 18, Obama Review Group.
[82] Para 74, European Parliament report.
[83] Para. 79, European Parliament report.
[84] Complainants include Liberty, Privacy International, Bytes For All (Pakistan), the American Civil Liberties Union, Amnesty International, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union and the Irish Council for Civil Liberties. See *Liberty (The National Council of Civil Liberties) v The Government Communications Headquarters & Ors* [2014] UKIPTrib 13_77-H (05 December 2014).
[85] Para. 59, Promotion and protection of human rights and fundamental freedoms while countering terrorism, note 21.
[86] Joined cases *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Ors* C-293/12 and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others,* C 594/12.
[87] See further Ian Brown and Douwe Korff, *Digital Freedoms in International Law*, Global Network Initiative, June 2012, available at: https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf
[88] *Ibid*.