stiftung neue verantwortung

Impulse

NEW AMERICA FOUNDATION
OPEN TECHNOLOGY INSTITUTE

25/13

September 2013

Law and Policy in Internet Surveillance Programs:

United States, Great Britain and Germany[1]

Authors:

Stefan Heumann, PhD,
Deputy Program Director
sheumann@stiftung-nv.de

Ben Scott, PhD,
Program Director & Senior Advisor to the Open Technology Institute at the New America Foundation
bscott@stiftung-nv.de

Joint Publication of Program "European Digital Agenda" of stiftung neue verantwortung and the Open Technology Institute of the New America Foundation

Many Europeans are outraged about US government surveillance programs that the leaked NSA documents have documented. German and European politicians and government officials have strongly criticized the US government for disrespecting the privacy of European citizens' personal data and communications. The concerns about Internet surveillance by the NSA and other intelligence agencies are certainly warranted. And criticisms by close partners and allies will be important to push the US government to reevaluate the scope and scale of these programs and to consider meaningful reforms to improve oversight and accountability. In order to be credible spokesmen for reform, Europeans will have to follow at least the same standards that they would like to see other governments adopt. And they will have to be transparent about what these standards are and how they will be applied in practice. Germans have been among the most outspoken critics of the US government. These critics implicitly make the assumption that Germany has higher standards than the US in regard to limiting and controlling its intelligence agencies. In this paper, we test this assumption by comparing the underlying law governing signals intelligence programs aimed at non-citizen communications in the US, the UK and Germany.
We focus on three areas of analysis:

1) Legal authorization for surveillance programs;
2) Functionality and scope of the collection programs; and
3) Oversight and accountability measures that restrict and control these programs.

[1] We would like to thank Tim Maurer of the Open Technology Institute for valuable research support and Kevin Bankston of the Center of Democracy & Technology, Eric King of Privacy International, and Prof. Niko Härting for feedback and comments on previous drafts.

The discussion here is not intended as a comprehensive review of all aspects of these issues, but an accurate sketch of legal frameworks and practical operations that permits reasonable comparison. The comparison is intended to offer a baseline analysis of national surveillance policies and to identify possible areas for reform to align a new trans-Atlantic policy that balances legitimate electronic surveillance with the right to privacy.

Our findings do not support the conclusion that foreign signals intelligence programs in the US represent a fundamentally different policy choice than two of its most important European allies. It is certainly true that the NSA programs are larger in scope than those of other governments. And the US intelligence agencies have more favorable conditions for compelling cooperation from the major Internet service providers because many of them are US companies. However, there appear to be more similarities than differences between three countries when it comes to how these programs are authorized, how they function, and what oversight mechanisms exist to control them. The laws authorizing digital surveillance share a common structure, although the interpretation of how these laws are applied may diverge.

The reach of NSA's international cooperation and the scale of its programs make clear that a reform debate in Washington is necessary and appropriate. But the US policy is not sufficiently different from those of its allies that a unilateral reform will re-establish international norms at a new baseline that is responsive to citizen outrage over the Snowden revelations. This preliminary analysis suggests that the current baseline internationally is much closer to US policy than the present debate would suggest. In all three countries the intelligence agencies enjoy great discretion and independence when it comes to the collection of foreign intelligence. Legal restrictions and oversight mechanisms are only concerned with the protection of the rights of each country's own citizens. And, in most cases, these restrictions come into place mainly after the interception and collection of telecommunications traffic has already occurred. The differences in the policy structures do not necessarily reflect poorly on the US. For example, while all three countries lack robust systems for judicial review to protect citizens against undue surveillance, only the United States involves courts in the authorization of some of its programs. The German G-10 Commission, an oversight body of the national parliament, plays a similar but non-judicial role as the American FISA courts. But its mandate is broader. Great Britain has the weakest oversight mechanisms, lacking institutionalized review of surveillance programs from both the legislative and judicial branches of government. The actual work of the institutions charged with overseeing and authorizing surveillance programs is shrouded in secrecy in all three countries.

This study seeks to offer a baseline to begin an international dialogue on these questions of policy frameworks - starting with trans-Atlantic confidence building. In order to keep the scope of the paper manageable, the analysis is focused primarily on surveillance programs by intelligence agencies directed at the digital communications of non-citizens. However, in all three case studies, the rules governing surveillance at home and surveillance abroad become blurred by the nature of the technology and the methods of data acquisition and analysis. First, the

Internet is a global infrastructure. This means that the distinction between foreign and domestic Internet communications is much harder to discern. Even what we would consider as "domestic" communications between two citizens who are located inside the geographic boundaries of their home country may pass through servers around the globe and the communications data might be stored or processed abroad. Therefore even intelligence operations that are focused on communications infrastructure abroad will yield data about citizens at home. Second, the leaked documents also indicate that there is extensive cooperation between US, British, and German intelligence agencies. This provides ample opportunities for intelligence agencies to circumvent restrictions by their home governments through international cooperation and data sharing. Given the international implications of these programs, domestic reforms will make little sense, if they are not linked to reform efforts on the international level. The key question is whether the legal protections afforded to citizens may be extended to certain groups of non-citizens, and if so, whether these reforms are politically feasible and technically possible. The starting point to reach these answers begins with this analysis.

USA

Legal Authorization

Several different statutes underlie the authorization for the system of US signals intelligence collection. The complexity of the constellation of programs and the siloed reporting on the Snowden documents often blurs the bigger picture of the overall architecture. This makes it challenging to piece together the technical functionality of each program and the corresponding laws that authorize and oversee these programs. To simplify without doing damage to the basic logic of the entire system, we can identify two major approaches to surveillance. The same framework is common to most intelligence services that conduct surveillance.

The first approach is the interception of real time information directly from the wires of telecommunications networks. This is everything from a single wire-tap to the "upstream" collection of massive amounts of Internet and telephone traffic that are redirected and stored by agency computer systems for non-real-time review. The second approach is the collection of stored information saved on the computers or servers of organizations or companies. In both cases, access is typically gained through the presentation of a legally binding instrument to a commercial firm that transmits, stores or processes data. The Foreign Intelligence Surveillance Act (FISA) and its amendments are the central elements of the statutory authority for foreign intelligence collection through electronic surveillance. These laws authorize both approaches to data collection. Section 215 of the Patriot Act is also aimed at foreign intelligence investigation. It grants authority to collect a wide variety of records from private companies, e.g. phone records. Section 215 is therefore tied to the collection of stored data.

Congress adopted FISA in 1978, drawing a line between the surveillance of foreign targets and US persons.[2] The terrorist

[2] The NSA regards US citizens, aliens with permanent residency, US corporations, and associations of US citizens or residents as US persons. http://www.nsa.gov/sigint/faqs.shtml#sigint4

attacks of September 11, 2001 led to a massive expansion of the national security apparatus. FISA amendments passed in 2001 and 2008 broadened the definition of the kinds of information that can be collected. Prior to 2008, FISA only permitted targeting "foreign powers" or "agents of foreign powers" with surveillance programs.[3] Since 2008, the NSA and other intelligence agencies are authorized to collect "foreign intelligence information" including "information with respect to a foreign power or foreign territory that relates to … the conduct of foreign affairs of the United States."[4] This definition goes far beyond counter-terrorism or national security as the main purposes of intelligence gathering. It permits the kind of mass surveillance of foreign communications exposed by the Snowden documents by broadly authorizing the acquisition of communications where at least one party is outside the US. The information that can be gathered includes the meta-data associated with phone calls and emails (e.g. numbers, call duration, email addresses) as well as the content of communications.

The bulk collection of real-time data directly from the wires requires the legal separation of the act of interception and the act of processing the data to look for targets. Mass interception and collection of Internet traffic will inevitably sweep in both foreign and domestic communications. Since targeting a US person requires a court order, the act of collection itself is not viewed as targeting. The data collected in bulk is sorted and parsed to eliminate information that may not be processed, essentially separating foreign and domestic communications. In short, the interception of all communications traffic has been broadly authorized, and the legally required minimization and restriction of use occurs only after collection.

The surveillance programs authorized by FISA also permit law enforcement to compel private companies to provide access to data that they store, transmit, and process that may be related to intelligence targets. Section 215 of the Patriot Act also allows the government to access data collected by private companies.[5] Based on Section 215 the FBI can request on behalf of the NSA that the FISA court issues an order to a US company for production of foreign intelligence information needed for an ongoing investigation. The scope of Section 215 is very broad, although again collection must distinguish between foreign and domestic communications. Data of US persons may not be collected unless the investigation relates to international terrorism or clandestine intelligence activities by foreign countries.

Scope and Conditions of Surveillance

The Snowden documents show that the US government has built massive infrastructure to support Internet surveillance. The bulk collection programs reportedly have access to the major Internet exchange points in the US, which means they can conduct surveillance on all communications that travel into and out of the country.[6] Because

[3] https://it.ojp.gov/default.aspx?area=privacy&page=1286#contentTop

[4] http://www.theatlantic.com/technology/archive/2013/06/us-government-surveillance-bad-for-silicon-valley-bad-for-democracy-around-the-world/277335/

[5] According to the business records provision of Section 215 - 50 U.S.C. § 1861(b)(2)(A)

[6] See Charlie Savage, "N.S.A. Said to Search Content of Messages to and From U.S.", "http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=all&_r=2&

some of the communications traveling over the Internet may be pertinent to foreign intelligence investigations, all of these communications may be monitored from these locations. This logic provides the justification for giving the government access to the vast majority of international telecommunications traffic transmitted through the US. Similarly, a FISA court order (made public by Snowden) based on the Patriot Act requires Verizon and reportedly AT&T and Sprint to hand over metadata of all its phone calls "on an ongoing daily basis" both within the US and between the US and abroad.[7] This data is then stored at a NSA repository. The authorization has been in place for the past seven years – renewed every three months by the FISA court. The US government has also established access to undersea fiber-optic cables for surveillance purposes – as part of a package of programs (including one called "Boundless Informant") that access huge quantities of raw data flowing over the Internet.[8]

But NSA's activities are not limited to accessing the data flowing over the lines of private network operators. The now famous Prism program provides NSA access specific user data compelled through court orders from nine major American Internet content and service providers. According to the Director of National Intelligence (DNI), Prism "is an internal government computer system used to facilitate statutorily authorized collection of foreign intelligence information from electronic communication service providers" dating back to 2008.[9] Prism is authorized by Section 702 of FISA. It focuses on foreign targets. In some cases, the companies have resisted cooperation. Shortly after the initial media reports, Yahoo succeeded in a court case with the FISA Court ruling to release NSA documents demonstrating Yahoo's resistance to US government requests for customer data.[10] In 2011, an undisclosed company brought a case before the FISA court, which ruled that the NSA had violated the Fourth Amendment by conducting illegal searches of private data.[11]

The constantly updated databases of monitored and stored communications are then analyzed for operational intelligence. The most powerful tool is known as XKeyscore. It is a sophisticated search interface that enables the analyst to run queries, pulling data from several collection programs. The program allows analysts to search vast databases of intercepted Internet traffic. Analysts can search by name, telephone number, IP address, keywords, browser type and language to gain access to the content of emails, online-chats, and other communications.

These programs and their legal authorizations permit the collection of global communications on an ongoing basis without regard to precisely what is collected. Obviously, this means they sweep in data that falls

[7] http://business.time.com/2013/07/03/nsa-scandal-as-tech-giants-fight-back-phone-firms-stay-mum/

[8] http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides

[9] http://www.lawfareblog.com/wp-content/uploads/2013/06/Facts-on-the-Collection-of-Intelligence-Pursuant-to-Section-702.pdf

[10] http://www.nbcnews.com/technology/court-sides-yahoo-nsa-prism-data-collection-case-6C10651458

[11] http://www.theatlantic.com/technology/archive/2013/06/us-government-surveillance-bad-for-silicon-valley-bad-for-democracy-around-the-world/277335/

outside the limited scope of foreign intelligence. Minimization procedures then narrow what data can be retained, analyzed and disseminated, once it has been collected, based on whether it was legal to collect it in the first place. For example, any communication collected off the Internet that later turns out to involve a US person must be destroyed unless the NSA director states in writing that this information constitutes foreign intelligence, contains evidence of a crime, information necessary to understand or assess a communications security vulnerability, or information pertaining to a threat of serious harm to life or property. The American Civil Liberties Union and the Electronic Frontier Foundation have filed lawsuits to try to stop many of these programs from extensive collection and targeting of domestic communications on First, Fourth, and Fifth Amendments grounds.[12]

A comprehensive overview of all known signals intelligence programs at NSA that permit the collection of telephone and Internet is beyond the scope of this paper. What the leaked documents clearly show is that US surveillance capacities are global. The NSA exploits the fact that many international communications are routed through servers located in the U.S. and serviced by US companies. US capacities are further enhanced by close cooperation with other countries. The US, Great Britain, New Zealand, Canada, and Australia have formed the "Five Eyes Alliance" to share intelligence.[13] The cooperation between the US and Great Britain seems to be particularly deep as will be discussed further below. The NSA also closely works with the German foreign intelligence service BND, but very little is still known about the exact nature and extent of intelligence sharing between the two countries.

Oversight over Intelligence Agencies and Surveillance Programs

The broad array of US signal intelligence programs carry different forms of oversight conducted by different branches of government. Most prominently, judicial oversight of the largest collection programs is exercised by the FISA court consisting of eleven Federal judges appointed by the Chief Justice of the United States. The FISA court meets in secret, only allows the government to appear before it, and provides an annual report to Congress concerning its activities. In light of the minimal number of applications being rejected by the FISA court, critics argue it is "rubber stamping" government requests.[14] However, the nature of the judicial review does not permit the FISA court to effectively oversee the implementation of surveillance programs. FISA minimization standards follow a "collection first, minimization later" model. It therefore shifts responsibility to determine FISA compliance from the FISA court to the executive.[15]

The Intelligence Committees and Judiciary Committees in the Senate and House of Representatives exercise general oversight over all intelligence collection programs and committee members are regularly briefed. Members of Congress receive detailed briefings prior to each reauthorization.

[12] http://www.dailykos.com/story/2013/07/16/1224176/-EFF-and-ACLU-Sue-NSA

[13] See, for example: http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf

[14] https://epic.org/privacy/wiretap/stats/fisa_stats.html

[15] https://www.cdt.org/files/pdfs/Analysis-Section-215-Patriot-Act.pdf

However, Members of Congress are barred from disclosing relevant information publicly and the FISA court's opinions are secret. Members of Congress have complained that they are not sufficiently informed about NSA and other intelligence agencies' activities to exercise effective oversight.[16]

Other mechanisms for accountability do exist, and they are attached to specific authorizing legislation. For example, the oversight regime regarding section 215 of the Patriot Act includes all three branches and consists of (1) a semi-annual report to Congress, (2) a meeting at least once every 90 days between the executive agencies Department of Justice, Office of the DNI, and the NSA, and (3) a report filed with the FISA court every 30 days. Foreign surveillance is subject to less oversight from the executive, judicial, and legislative branches of the US government. The regime includes (1) annual reviews from the NSA Inspector General, (2) a semi-annual reports to the FISA court and Congress on the program's implementation, (3) semi-annual reports to the FISA court and Congress on compliance by Attorney General and DNI, and (4) a quarterly report to the FISA court on compliance. Within the executive, the NSA must report to the Department of Justice and the office of the DNI any incidents of non-compliance with FISA such as intentional targeting or persons believed outside the US being in the US. Finally, there is a new and untested oversight body – the Privacy and Civil Liberties Oversight Board (PLCOB). It is now engaging in a review of the NSA's surveillance activities.[17]

Great Britain

Legal Authorization

The Intelligence Services Act (ISA) 1994 and the Regulation of Investigatory Powers Act (RIPA) 2000 provide the legal framework for the Government Communication Headquarters (GCHQ), Britain's intelligence agency responsible for signals intelligence and information assurance. ISA authorizes the work of the intelligence services for the purposes of national security, foreign policy, economic interests, and the prevention or detection of serious crimes. GCHQ is under the authority of the Secretary of State. The director of GCHQ is supposed to ensure that "no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions." GCHQ and other intelligence agencies such as the Security Service (MI5) and the Secret Intelligence Service (MI6) must apply for a warrant issued by the Secretary of State to conduct telecommunications surveillance. The Secretary of State determines whether the requested surveillance activity falls within the statutory function of the intelligence agencies.

RIPA regulates a wide range of surveillance activities by law enforcement and intelligence agencies. RIPA mandates cooperation and the provision of interception capacities from telecommunication operators for authorized surveillance programs.[18] Surveillance warrants issued by the Secretary of State have to be proportionate and necessary for the defined purposes of the intelligence agencies as stated above. Warrants must be kept secret and be renewed every six months. A warrant can either target a single

[16] http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access
[17] http://www.pclob.gov/newsroom
[18] http://www.liberty-human-rights.org.uk/materials/introduction-to-ripa-august-2010.pdf

person or a set of premises. For example, an office could be targeted as a premise, putting all communications to and from that location under surveillance. The language on "safeguards" is broad, leaving much room for interpretation by the intelligence agencies. RIPA requires the minimization of the number of people given access to data, the extent to which it is disclosed, and the number of copies made. No specification of targeted individuals or premises is needed for requests for the surveillance of foreign communications.[19]

According to the documents made public by Snowden, RIPA serves as legal basis for the taps that have been placed on fibre-optic cables. GCHQ refers to paragraph 4 of section 8 of RIPA to request warrants related to the interception of communications external to the UK.[20] They allow the agency to intercept external communications where, for instance, one of the people being targeted is outside Britain. In most RIPA cases, a minister has to be told the name of an individual or company being targeted before a warrant is granted. But section 8 permits GCHQ to perform more sweeping and indiscriminate trawls of external data, if a minister issues a "certificate" along with the warrant. According to the documents, the current certificate authorizes GCHQ to search for material under a number of themes, including: intelligence on the political intentions of foreign governments; military postures of foreign countries; terrorism, international drug trafficking and fraud. Reportedly there are "10 basic certificates, including a "global" one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus."[21]

19 http://ohrh.law.ox.ac.uk/?p=2056
20 http://ohrh.law.ox.ac.uk/?p=2056 and http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

Scope and Conditions of Surveillance

The structure and functionality of the UK's surveillance programs appear to be similar to the US and nearly as broad in scope. Due to the UK's geographical position, a large number of undersea fiber-optic cables that carry Internet traffic land in the UK before they cross the Atlantic Ocean. The *Guardian* reported that by the summer of 2001, GCHQ had attached probes to more than 200 of these cables to filter and store data for intelligence purposes.[22] This program is codenamed Tempora and part of two projects entitled "Mastering the Internet" and "Global Telecoms Exploitation" that reflect GCHQ's sweeping ambitions for Internet surveillance. As a member of the Five Eyes intelligence community, an alliance between the United States, Canada, Great Britain, New Zealand and Australia, Great Britain closely collaborates with the NSA for the purpose of intelligence collection and sharing. The *Guardian* cites leaked documents stating that "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures."[23] Currently, 300 analysts from GCHQ and 250 from NSA are directly assigned to examine the collected material. Full access was provided to NSA in fall 2011. A key question (which we have not yet been able to answer with our research) is how domestic communications that are inadvertently captured along with the foreign communi-

21 http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world?INTCMP%3DSRCH
22 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
23 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

cations are treated by the British intelligence agencies.

The cooperation between NSA and GCHQ seems to go much deeper than the Tempora program. According to reports by the *Guardian* the NSA has paid GCHQ £100 Million for surveillance programs.[24] Apparently British intelligence officials used low data protection standards and a forgiving regulatory regime as "selling points" for NSA officials. NSA funding seems to be an important source of income for GCHQ and provides US intelligence officials not only access to British programs but also puts them in a position to shape them. More recent reports reveal that NSA and GCHQ also work together to compromise widely used encryption standards for Internet communications.[25]

GCHQ also has programs that compel cooperation from UK based Internet companies that offer network access, content and services. The German newspaper *Sueddeutsche Zeitung* reported that GCHQ closely works with telecommunication service providers British Telecom, Verizon, Vodafone, Global Crossing, Level 3, Viatel and Interroute not only to gain access to their communication networks but also to develop surveillance programs and software.[26]

Oversight over Intelligence Agencies and Surveillance Programs

According to ISA, the director of GHCQ has to prepare an annual report for the Prime Minister and the Secretary of State. In addition, the Interception of Communications Commissioner (ICC) ensures that government agencies act in accordance with their legal responsibilities as stated in RIPA when intercepting communications.[27] The Commissioner also reviews the role of the Home Office Secretary of State in issuing interception warrants. However, the ICC appears to review only a small portion of warrants and only after the Secretary of State has already issued them.[28] If she finds wrongdoing, the ICC has to report to the PM, but there is no obligation to make the finding public. Thus the authorization and the review process are entirely contained within the executive branch.

The Investigatory Powers Tribunal, composed of nine senior members of the legal profession, hears complaints from individuals who allege that they have been subject to illegal surveillance.[29] However, the Tribunal cannot initiate its own investigations. People outside of the intelligence agencies hardly ever learn about misconduct so that they can file a complaint. In addition, strict standards of secrecy apply to the work of the Tribunal to protect information whose non-disclosure is considered to serve public or national interests.

The Intelligence and Security Committee of Parliament (ISC) exercises statutory oversight of the UK intelligence community, including the expenditure, administration and policies of the intelligence agencies.[30]

[24] http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden
[25] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[26] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791
[27] http://www.iocco-uk.info/
[28] http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf, p. 50
[29] http://ipt-uk.com/default.asp
[30] http://www.legislation.gov.uk/ukpga/1994/13/section/10

The ISC publishes an annual report. The most recent report for 2012/2013 focuses on the performance, effectiveness, and budget of the intelligence agencies. It does not examine intelligence activities with regard to their implications for civil liberties, privacy or data protection. On July 17, the ISC published a statement on GCHQ's alleged interception of communications under the US Prism program.[31] After receiving "detailed evidence from GCHQ," the committee concluded that allegations of unlawful conduct by the GCHQ were unfounded. However, the ISC also announced an examination of the "complex interaction between the Intelligence Services Act, the Human Rights Act and the RIPA" as well as the "policies and procedures that underpin them." This review appears to be ongoing.

It does not appear that the British surveillance programs require judicial review. The RIPA powers generally do not require court approval and may be used for a wide range of purposes. While the position of the Commissioner is filled with a former high court judge, critics of the current surveillance regime believe that court authorizations would provide the most meaningful improvement of the current system.[32] Overall, the oversight of the UK surveillance program is quite limited. There seems to be very limited legislative and no judicial review. Little is known about the specific minimization procedures that GCHQ may use to restrict access or delete information from the raw traffic databases that was inappropriately collected. Privacy International has announced that it is considering challenging the legality of the Tempora program and the cooperation between GCHQ and Internet Service Providers in court.[33]

Germany

Legal Authorization

The German foreign intelligence service BND operates based on a law passed by the German parliament in 1990.[34] §1, Section 2 of the BND law authorizes the BND to gather foreign intelligence relevant to German foreign policy and national security interests. The law requires a strict separation of the intelligence service from police and law enforcement functions. §2, Section 4 mandates the BND to use the method of intelligence gathering with the least disruptive impact on the targeted person. There also has to be a balance between negative consequences of the surveillance and the intended benefit. As this language above indicates, the law is written so broadly that it offers very little concrete guidance regarding the legal limits of surveillance programs. The law also authorizes the BND to request data from telecommunications providers for the purposes stated in §1, Section 2.

While the BND has a broad mandate to collect foreign intelligence information that serves German foreign policy and national security interests, any activities that interfere with Article 10 of the Constitution (protection of the privacy of correspondence, posts, and telecommunications) are subject to the G-10 Law and to the approval of the G-

[31] http://isc.independent.gov.uk/news-archive/17july2013
[32] http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf
[33] http://www.theguardian.com/uk-news/2013/aug/08/privacy-international-challenges-bt-vodafone-gchq
[34] http://www.gesetze-im-internet.de/bndg/BJNR029790990.html

10 Commission (discussed below). It applies to all German intelligence agencies including BND, the Military Intelligence Agency, and the Federal and State Offices for the Protection of the Constitution. The G-10 Law defines more narrowly the purposes for the authorization of surveillance programs of international telecommunications. It lists among others the threat of an imminent military attack against Germany, threat of international terrorist attacks related to Germany, or international proliferation of military equipment as legitimate purposes for surveillance. But the mandate is still broadly defined. It also includes drug trafficking, international money laundering, and trafficking of persons.

There is a dispute among legal scholars, whether Article 10 of the Constitution also protects the communications between foreigners abroad and the G-10 Law thus also applies to them.[35] Berthold Huber, a judge and a member of the G-10 Commission, wrote in recent law journal article that the government treats foreign communications abroad as not covered by Article 10 of the Constitution and thus not subject to the G-10 Law and oversight by the G-10 Commission.[36] Niko Härting claims that the BND is only subject to data protection laws, if the agency operates in Germany.[37] Those are not the only controversial issues. Härting also argues that the current legal regime does not allow the BND to collect metadata.[38]

According to the BND law, the BND is authorized to collect, store, change, and analyze personally identifiable information in accordance with its mission. The creation of new databases with personally identifiable information has to be approved by the Chancellery. The data protection provisions of the Office for the Protection of the Constitution apply. Data that is no longer needed for specified purposes or was obtained by unauthorized methods has to be deleted. The data protection provisions of the G-10 law are stricter. §5 prohibits the capture of data concerning the core of personal privacy. §6 obligates the intelligence services to evaluate (once information is obtained, afterwards at least every six months) regularly whether captured data is needed for authorized purposes. If this is not the case, the data has to be immediately deleted. The deletion of the data has to be documented. The law also puts strict limitations on how and under what conditions data obtained under the G-10 law can be shared with other government agencies or foreign intelligence services. The structure of the intelligence collection system is similar to the UK and the US. The law permits broad collection of information consistent with foreign intelligence needs

[35]http://www.golem.de/news/datenueberwachung-die-bnd-auslandsaufklaerung-im-rechtsfreien-raum-1309-101324.html

[36] Dr. Berthold Huber, „Die Strategische Rasterfahndung des Bundesnachrichtendiestes – Eingriffsbefugnisse und Regelungsdefizite“ Neue Juristische Wochenschrift, 2013, Heft 35, page 2576 See also point 9 in the Chancellory's response to parliamentary inquiry by the Left Party. A link to the document can be found here: http://www.cr-online.de/blog/2012/05/24/bundesregierung-bestatigt-bnd-prufte-2010-die-nachrichtendienstliche-relevanz-von-37-mio-mails/ Georg Mascolo makes this argument here: http://www.faz.net/aktuell/feuilleton/debatten/internationale-datenaffaere-die-aussenwelt-der-innenwelt-12243822.html

[37] http://www.cr-online.de/blog/2013/07/26/nsa-und-bnd-rechtsgrundlagen-gemeinsamkeiten-unterschiede/

[38]http://www.cr-online.de/blog/2013/08/06/warum-die-erhebung-von-metadaten-durch-den-bnd-verfassungswidrig-ist/

and interests. The restrictions and minimization – while perhaps stronger in Germany – are only applied after initial monitoring has occurred.

Scope and Conditions of Surveillance

Very little is known about specific German foreign intelligence service (BND) surveillance programs. According to reports in the media the BND routinely monitors international telecommunications on Germany's largest Internet exchange point DE-CIX in Frankfurt.[39] The authority for this network surveillance is based on sections in the G-10 Law (§5 and §10, Section 4). They state that general surveillance of international telecommunications can be conducted for authorized, broadly defined purposes, but only using up to 20% of the "telecommunication transmission capacity." It is unclear what exactly is meant by "telecommunications transmission capacity" and how this standard limits surveillance programs of the BND. A definition based on capacity grants a much broader reach for the BND into Internet data than the commonly reported figure of 20% of traffic.

Every year the parliamentary control committee issues a brief, general report on surveillance activities. The report for the year 2010 received a lot of attention in the media because it stated that automatic searches with more than 15,000 keywords identified over 37 million telecommunications, mostly Emails, for further examination.[40] In the end, 213 of these telecommunications were deemed relevant for investigation and stored. The report provides further evidence that the BND filters Internet traffic on a large scale.[41] The BND claims that the very high number of captured telecommunications was the result of an unusual amount of spam Email. For 2011 the report lists just less than 3 million captured telecommunications.[42] Since the number of keywords dropped only slightly, the most likely explanation for the substantial decrease of captured telecommunication is the improvement of automated filtering functions.[43] The Left Party used a parliamentary information request to learn more about the BND surveillance of telecommunications. The response from the Chancellery confirmed that the BND performs automatic searches of Internet communications. The report contains very little information regarding the scope of the programs and minimization procedures. This information remains classified since according to the BND it could reveal methods and capacities of the BND and thus undermine the ability of the German government to protect the country. However, it is stated that after the automatic filtering process several layers of evaluation and assessment by analysts are supposed to ensure that only data relevant to the mission of the BND is stored for further analysis. All other data is supposed to be deleted.

German intelligence services have strong historic ties with US intelligence agencies based on close cooperation during the Cold War.[44] It is well known that the NSA and

[39] http://www.phoenix.de/content//713040
[40] http://www.cr-online.de/blog/2012/02/28/massive-eingriffe-in-grundrechte-bnd-filtert-systematisch-e-mails/
[41] Link to the report: http://dipbt.bundestag.de/dip21/btd/17/086/1708639.pdf
[42] http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf
[43] http://www.cr-online.de/blog/2013/04/04/der-bnd-liest-mit-knapp-3-mio-mails-wurden-2011-kontrolliert/
[44] http://www.sueddeutsche.de/politik/historiker-foschepoth-ueber-us-ueberwachung-die-nsa-darf-in-deutschland-alles-machen-1.1717216

other American intelligence agencies have facilities and staff on US military bases in Germany. After 9/11 cooperation between German and U.S. intelligence agencies was further expanded. Documents leaked by Snowden give some insights into the nature of this close cooperation. US officials claim that the director of BND lobbied the German government for a legal interpretation of data protection standards that would facilitate data sharing with US intelligence agencies.[45] The *Spiegel* reports that the BND sends huge amounts of metadata to the NSA on a regular basis.[46] The BND claims that the data stems from foreign communications and is stripped of any data concerning communications of German citizens. The documents also revealed that the BND is using NSA's "Xkeyscore" system which is supposed to give analysts access to all telecommunications of a target.

Oversight over Intelligence Agencies and Surveillance Programs

The parliamentary control commission exercises legislative oversight over the intelligence agencies. The Chancellery is obligated to regularly (at least once every six months) inform this committee about the activities of the intelligence services. The commission can request documents and data and conduct hearings with members of the intelligence services. The parliamentary control committee's deliberations are kept secret. However, it can request public deliberations with a two-thirds majority. The parliamentary control committee issues an annual report with the total number of information requests and breakdowns according to each intelligence service and the type of information requested.

The parliamentary control committee also appoints the four standing and the four deputy members of the G-10 Commission which serves as a permanent control body for intelligence activities. The Commisssion reviews and authorizes all requests for surveillance activities subject to the G-10 law.[47] The chair of the G-10 Commission needs to have the qualifications to serve as a judge. It meets at least once a month and can schedule on-site "control visits" at German intelligence facilities. The G-10 Commission does not only authorize surveillance programs, but also controls how these programs are implemented regarding the collection, storage, and analysis of personal data. The intelligence agencies have to justify their surveillance requests and specify their scope and targets. The G-10 Commission also receives complaints by citizens and investigates potential abuses. Placed under the authority of the German parliament, the German oversight mechanism belongs to the legislative branch and does not include judicial review.

Other oversight procedures flow through the executive institutions. The BND has to report its activities to the German Chancellery. The Chancellery, the Ministry of Interior (to which the office for the protection of the Constitution reports), and the Ministry of Defense (to which the military intelligence service reports) have to inform the parliamentary control commission about the activities of German intelligence agencies at least every six months. According to the G-10 law the BND needs the

[45] http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html

[46] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

[47] http://www.bundestag.de/bundestag/gremien/g10/

approval of the Chancellery to share information collected under this law with foreign intelligence agencies of other countries.

Citizens who believe that they have been under surveillance can request from the BND information collected about them.[48] The request needs to explain why the citizen believes that he has been under surveillance and indicate a special interest in the disclosure of this information. The BND can reject the request, if disclosure would threaten its mission, sources, or public safety or if there are compelling reasons of a third party to keep the information secret.

German data protection officers have publicly criticized the German government for its refusal to investigate the scope of surveillance of German citizens by German and foreign intelligence agencies and called for a reform of oversight mechanisms in order to put German surveillance programs under greater scrutiny.[49] They also would like to see their authority to examine data protection procedures for data collected under the G-10 law expanded.

Findings

Although we do not have all of the relevant facts for each case to accomplish a clear "apples to apples" comparison, this analysis demonstrates that all three countries studied share a similar approach to the collection of signals intelligence from telecommunications networks. If this hypothesis is correct, subsequent disclosures about surveillance programs are likely to fill in the details of operations within this common framework. For now, we can assert the following conclusions:

Legal Authorization: In each country, the laws authorizing the programs targeting foreign communications are broadly worded and permit wide discretion to intelligence agencies to pursue their missions. There are much stricter standards for domestic surveillance versus foreign surveillance. However, each country intercepts data that is a mixture of foreign and domestic communications. Because of the difficulties of parsing domestic from foreign data in real-time filtering on the Internet, the minimization procedures (i.e. the restrictions on access and utilization of collected data) are often applied after the initial interception and collection occurs. This means that the act of interception or monitoring is permitted irrespective of the origin or content of the communication. It is the targeting or search of the resulting databases and the operational dissemination of that data which is subject to legal restriction and oversight. The logic of these minimization practices as a form of meaningful oversight is circular. The collecting agencies intercept all communications on the network because a tiny fraction will have relevance to foreign intelligence matters. If some of the communications are later discovered to be restricted (i.e. originating from a citizen), they are deleted - but only if they do not contain information relevant to foreign intelligence. In other words, all communications swept up from the Internet that have relevance to foreign intelligence are kept and disseminated regardless of what legal regime technically governs their collection.

[48] http://www.bfdi.bund.de/cln_029/nn_531474/DE/Themen/InnereSicherheit/Nachrichtendienste/Artikel/Bundesnachrichtendienst.html__nnn=true

[49] http://www.spiegel.de/netzwelt/netzpolitik/nsa-affaere-datenschuetzer-fordern-aufklaerung-von-der-bundesregierung-a-920592.html

Scope and Conditions: Each government seeks to intercept large amounts of data traveling over telephone or Internet networks - either utilizing their own capabilities or in cooperation with one another. And each nation's intelligence services appear to use similar tools for finding, analyzing, and operationalizing information that pertains to their intelligence goals. Available evidence indicates that intelligence services of allies such as Britain and Germany are eager to cooperate with the US in order to get access to its powerful surveillance capacities. The relationship between Britain and the US is particularly close. As member of the Five Eyes intelligence community Britain enjoys privileged access to US intelligence operations and closely cooperates with US intelligence agencies. In addition, GHCQ receives direct financial support from the NSA. The German foreign intelligence service BND also has strong ties to the NSA dating back to Cold War era partnerships that have been updated for global counter-terrorism efforts. The exact nature and extent of these partnerships remains unknown. However, it is clear that the opportunity exists through such cooperation to rely on other intelligence agencies to monitor domestic communications that would be legally impermissible for national intelligence agencies to process.

Oversight: Review and accountability for these surveillance programs are limited in all cases. Each government has direct executive oversight and reporting requirements. The British system is the most lenient as neither courts nor the legislative branch are significantly involved. The US is the only case that requires some degree of court supervision - though it rarely contests intelligence requests. Germany is the only case in which the oversight body not only authorizes programs but holds responsibility for their implementation and holds investigative powers. The FISA court and the G-10 Commission, even though they are located in different branches of the government, actually operate on quite similar terms. Their main responsibility is to weigh government requests for surveillance to protect national security against the constitutional rights of each country's citizens. But in none of the countries studied does any form of oversight appear to have created a significant barrier to the expansion of these programs. And in all cases, the proceedings of the oversight bodies are almost entirely secret and the results of any internal conflicts over policy or implementation remain unknown.

Conclusion

Edward Snowden pulled back the curtain on massive Internet surveillance programs run by Western intelligence agencies. Media, government officials, civil society, and businesses around the globe are struggling to assess the implications and prepare for the consequences. This is a huge challenge with high stakes.

The global Internet relies upon a relatively fragile system of cooperative technocratic governance and a mutual commitment among nations to maintain an open market for ideas and commerce despite the risks to privacy and security that are tied to open communications. It is a system that depends on trust. The Snowden revelations have dealt a powerful blow to that trust. If trust declines too sharply, markets and information flow on the Internet will be disrupted. National governments will pursue a self-interested course and balkanize this global resource into a system of national networks guarded and restricted by national

interests. Few desire this outcome; and yet even fewer have presented concrete ideas for how to prevent it. Ironically for both intelligence agencies (whose programs have battered public trust in the Internet) and Edward Snowden (who professes to protect the free and open Internet), the most likely result of this debate is that the goals of both will be undermined.

As a matter of public policy, the capabilities of surveillance technology in many countries have extended far beyond what the underlying laws could anticipate and contain in current legal frameworks. To address this problem requires national debates about updating laws to re-set the balance between security and liberty in accordance with national values. But because the Internet is a global system, the policies of one nation impact the people in others. And so the prospect of rebooting trust in the policies that govern the Internet will require an international process to set standards for expected behavior, to draw red lines around illegitimate conduct, and to align national policies to international standards. The solution will require much more than reform in Washington, and we need to identify a starting point for international engagement. This paper makes a contribution to that work

| About the program *European Digital Agenda*

The Program European Digital Agenda combines the expertise of thought-leaders and experience of practitioners in technology business, law and politics to deliver innovative ideas and expert analysis to digital policy debates. The program brings together stakeholders from government, business, academia, and civil society to discuss the challenges of digitalization, to develop policies to realize its potential, and to engage with government from concept to implementation. This work seeks to raise public awareness about the importance of technology policy issues, elevate digital solutions as political priorities, and provide neutral forums for cross-sectoral debate, discussion, and coalition building.

| About the *Open Technology Institute*

New America's Open Technology Institute formulates policy and regulatory reforms to support open architectures and open source innovations and facilitates the development and implementation of open technologies and communications networks. OTI promotes affordable, universal, and ubiquitous communications networks through partnerships with communities, researchers, industry, and public interest groups and is committed to maximizing the potentials of innovative open technologies by studying their social and economic impacts – particularly for poor, rural, and other underserved constituencies. OTI provides in-depth, objective research, analysis, and findings for policy decision-makers and the general public.

| About stiftung neue verantwortung

Stiftung neue verantwortung is an independent, non-profit, and non-partisan German think tank located in Berlin. It promotes interdisciplinary and intersectoral thinking about the most important societal and political challenges of our time. Through its Fellow- and Associate-Programs the think tank brings together young experts and thought leaders from politics and administration, business, academia, and civil society to develop creative ideas and solutions and introduce these into public discourse through a variety of publications and events.

Impressum

stiftung neue verantwortung e.V.
Stefan Heumann, Deputy Program Director
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T. +49 30 81 45 03 78 80
F. +49 30 81 45 03 78 97
www.stiftung-nv.de
sheumann@stiftung-nv.de