Surveillance & Society

Article

International Cross-Surveillance: Global IT Surveillance Arbitrage and the Principle of Proportionality as a Counterargument

Julian Staben

Alexander von Humboldt Institute for Internet and Society, Germany.
julian.staben@hiig.de

Hannfried Leisterer

Alexander von Humboldt Institute for Internet and Society, Germany.
hannfried.leisterer@hiig.de

Abstract

In the course of the revelations about both U.S. and European national surveillance programmes, remarkable constellations have come to light. Most national programmes are focused on the surveillance of IT-based communication among foreigners and between citizens and foreigners. This fact has often been employed as a mitigating argument within the national legal and policy discourses. This paper examines some of the possible loopholes and "dents" in the law that enable intelligence agencies to engage in international IT surveillance arbitrage. Fundamental rights currently do not protect against this practice. It leads to the factual circumvention of constitutional standards by permitting wider indirect access to domestic communication through processes of information sharing.

We briefly assess possible legal answers to this phenomenon from the fields of public international law and global constitutionalism. Since international human rights law is merely territorial in focus it is incapable of constraining the above mentioned arbitrage practices. Territorial concepts of human rights protection are outdated with regards to international communication networks and ineffective for the legal regulation of state surveillance of these networks. We identify the universal legal principle of proportionality as the most promising starting point to structure and rationalise the legal debate on how to constrain international IT cross-surveillance.

I. Introduction

In his speech on the NSA reform held on 17 January 2014 U.S. President Obama said: "[...] the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders" (*The Washington Post* 2014). And as it turns out, he was right.

In fact, most states have created different sets of rules for domestic and foreign surveillance measures.[1] On the one hand, *domestic* intelligence and law enforcement agencies have to follow strict rules. Their

[1] In fact, foreign surveillance was traditionally covered by the term "espionage". Measures of espionage were resource intensive endeavours almost always targeted at government officials. By shifting the practice to groundless and bulk collection of citizens' data, the phenomenon can be more precisely described as mass-surveillance—on

Staben, Julian, and Hannfried Leisterer. 2017. International Cross-Surveillance: Global IT Surveillance Arbitrage and the Principle of Proportionality as a Counterargument. *Surveillance & Society* 15(1): 108-123. http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

surveillance abilities are limited in substance and through procedural safeguards such as court orders. This usually results in the effective prohibition of the most sweeping and invasive measures such as unwarranted blanket surveillance. On the other hand, intelligence services entrusted with the task of *foreign* surveillance enjoy considerably more leeway.

Today, our communication and everyday social interaction often happens, or is at least observable, online. In practice, this means that data is transferred through international IT infrastructures. The underlying structural phenomenon is that the internet crosses a plethora of legal spaces. The internet's immensity collides with the fact that public authorities, in this case intelligence services, are bound by different territorial constitutional and statutory legal regimes. Here, one can find legal "breaking points" or "dents" within the law: data is effectively exposed to potential monitoring by foreign states under laws for foreign surveillance which are less stringent than those for domestic monitoring. Any information collected can subsequently be used for domestic purposes or shared with other intelligence and law enforcement agencies at home and abroad.[2] This constellation can be descriptively labelled cross-surveillance.

Unfortunately, this paper cannot deliver an exhaustive analysis of surveillance laws and their application. The sheer quantity of regulation and its functional interaction plainly exceeds our resources. Additionally, the interpretation and exact application of laws by the relevant actors is widely unclear at this time; where this has come to light, the details often remain opaque or unconfirmed.

In this paper we will provide legal analysis of the laws in effect in June 2014 and present anecdotal factual evidence to outline the constellation that we have just briefly defined as international IT cross-surveillance. This will accentuate the ties between seemingly unrelated surveillance measures and shed light on the overall paradigm of global surveillance. With this, we hope to spark further research and contribute to the political and legal discourse with an approach to understand, systematise, and discuss past, on-going, and future phenomena of international IT surveillance.

We will begin by outlining possible "dents" in the legal framework of IT surveillance by identifying cases where foreigners' communication is subject to more intensive monitoring than those of citizens (section II). This includes some of the news-reported activities of cross-border data collection and consecutive pooling and sharing practices. Subsequently, we will discuss possible answers from the fields of international human rights law and global constitutionalism with the principle of proportionality as the most promising approach (section III). The paper closes with a conclusion and an outlook on normative, but non-legal starting points (section IV).

II. "Dents" in the Legal Framework: Exceptions for Foreigners

A country's law is still, first and foremost, focused on and written for its citizens.[3] In democratic countries the citizens in their entirety form the electorate to which the lawmaker is accountable. Now, many—if not all—countries' legal systems provide less protection for foreigners than for their own citizens in certain cases. In other words, a foreigner is more exposed to measures interfering with his personal sphere and enjoys less judicial protection against governmental actions than a citizen of a respective state.

---

the concept of surveillance, see David Lyon (2007: 13 et seq). This shift followed the changed scenario of increased threats by non-state actors.

[2] The reciprocal or even multilateral monitoring of foreign citizens by several states leads to a constellation that can be labelled "chiastic". The nationalities of the surveilling governments and targeted citizens are inverted: state A surveils the citizens of state B, while state B surveils the citizens of state A.

[3] That entails those individuals who form the permanent population constituent for a state recognised under international law. Citizenship is generally awarded by the conditions set out in a country's domestic laws.

We will illustrate that the law typically establishes a lower threshold for surveillance measures on three grounds: citizenship, territoriality, and factual governmental control. In many cases these categories are combined. We will examine two classic examples of exceptions for foreigners in the regulatory framework for governmental surveillance. This entails a constitutional as well as a statutory dimension.

1. USA: The 4th Amendment, the NSA, and FISA

Under U.S. law, the fourth constitutional amendment, which requires a judicial warrant and probable cause for "searches and seizures", may theoretically offer protection against the surveillance of foreigners by governmental authorities, such as the NSA. This follows primarily from the open wording of the fourth amendment, which explicitly protects "the people".[4] The Supreme Court has held some constitutional protections applicable to foreigners on U.S. territory.[5] Some protections have also been applied to U.S. citizens abroad.[6] For the fourth amendment, however, lower courts generally assume an exception to the guarantee when it comes to the surveillance of non-U.S.-citizens abroad.[7] For the case of a traditional physical search of a foreign residence of a non-U.S.-citizen this stance was embraced by the Supreme Court.[8] Nevertheless, it is to be noted that the Supreme Court has not determined this matter for cases of abroad surveillance of foreigners conclusively.[9] In any case, a possible assessment by the lawmaker and the Supreme Court would most likely be highly dependent on the concepts of citizenship and territorial whereabouts of the subject.[10] These factors are closely related to the notion of jurisdiction in the U.S. legal tradition.[11] In short, fourth amendment protection in foreign IT surveillance cases remains unclear, but the jurisprudence of U.S. courts points towards a non-existent or at least lowered constitutional protection in these cases.

Especially readers with a civil law background should also note that the fourth amendment is traditionally construed merely as a criminal procedural right and not as a general right to personality. Its enforcement is practically ensured by the so-called *exclusionary rule*, which classifies illegally obtained material as inadmissible in proceedings before courts and similar bodies or authorities.[12] Thus, fourth amendment cases in higher courts are often based on reviews of verdicts based on questionable evidence. Cases with this exact scope are exceptional, since foreigners in the US are rarely subject to traditional criminal procedures resulting from searches and seizures on foreign territories. So, it is to be assumed that lawsuits

[4] See David Cole (2003: 367, 370). A narrower understanding of the phrase "the people" can be found in *United States v. Verdugo-Urquidez,* 494 U.S. 259, 264-273 (1990).

[5] Cf. For the fifth and the fourteenth amendments *Mathews v. Diaz,* 426 U.S. 67, 77 (1976); Elizabeth A. Corradino (1989: 617-8).

[6] "When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land." *Reid v. Covert*, 354 U.S. 1, 6 (1957). Differently, *In re Terrorist Bombings of U.S. Embassies in East Africa (Fourth Amendment Challenges),* 552 F.3d 157 (2d Cir.2008) a court held only the reasonableness requirement and not the warrant requirement of the fourth amendment applicable.

[7] Cf. *United States v. Truong,* 629 F.2d 908 (4th Cir. 1980). The United States Foreign Intelligence Surveillance Court of Review (FISCR), which reviews denials of applications for surveillance by the United States Foreign Intelligence Surveillance Court (FISC), operates under the same assumption, *In re Directives*, 551 F.3d 1004 (2008). Although this is highly disputed, see Steve Vladeck (2012).

[8] See *United States v. Verdugo-Urquidez,* 494 U.S. 259 (1990).

[9] Cf. the remarks in *United States v. U.S. District Court*, 407 U.S. 297 (1972): 308-309 (note 8), 322.

[10] These factors can be summarised under the arguably vague concept of a "substantial" or "significant connection with the U.S.", *United States v. Verdugo-Urquidez,* 494 U.S. 259, 260, 265, 271 (1990).

[11] Jurisdiction is commonly understood as the power of a court to hear and decide a case. In cases with governmental actors this power was and still is traditionally linked to the territory of a respective state.

[12] *Weeks v. United States*, 232 U.S. 383 (1914); *Mapp v. Ohio*, 367 U.S. 643 (1961).

filed by foreigners are unlikely to be admissible due to procedural limitations, such as the requirement of standing.[13]

It is also notable that the assumption of a *foreign intelligence exception* to the fourth amendment is the basis for the design of the well-known *Federal Intelligence Surveillance Act* (FISA) and the conduct of U.S. intelligence services when it comes to foreign citizens.[14]

Following the advice of the Church Committee, which had been formed in response to the Watergate Affair, FISA was enacted in 1978 and has been amended several times since.[15] Its original aim was to allow for more judicial and congressional control over intelligence activities. Naturally, today's FISA and its Amendments Act (FISAA) still rely on definitions of nationality and residence[16]: *Foreign powers* as defined by 50 U.S.C. §1801(a) and *agents of a foreign power* as defined by 50 U.S.C. §1801(b) are the main targets of surveillance, while there are certain safeguards for *United States persons* as defined by 50 U.S.C. §1801(i). In short, the term *United States persons* applies foremost to United States citizens, but also to foreigners who have been lawfully granted permanent residence as well as associations formed by these persons. Under FISA, electronic surveillance *without* a court order is possible under 50 U.S.C. §1802, provided that it is unlikely to capture communication to which a United States person is a party. On the other hand, when electronic surveillance is conducted *with* a court order, certain *Minimization procedures* (50 U.S.C. §1801(h)) need to be in place in respect to the aforementioned United States persons.[17] Interestingly, the FISAA has numerous provisions that provide certain safeguards solely for United States persons.[18] Additionally, this act follows a concept of protection differentiating by the whereabouts of a person.[19]

This insight into the doctrine of the constitution's fourth amendment and a small part of U.S. foreign intelligence laws supports two main propositions: first, that the degree of legal protection which a person enjoys depends largely on his/her country of citizenship and residence. Second, that the possibility of challenging certain surveillance activities or the laws underpinning them in court successfully is low due to both a lack of merit (foreign intelligence exception) and procedural reasons (lack of standing).

2. Germany: Art. 1 (3) and Art. 10 GG, the BND, and the G 10 Act

According to the wording of the German constitution, all public authorities must respect fundamental rights, Art. 1 (3) *Grundgesetz* (GG, Basic Law). On closer examination, however, this creates an obligation merely in principle. The specific scope of this obligation is anything but clearly determined when it comes to the individual case. This issue is traditionally further distinguished under German law: First, the constitutional right's territorial scope (*ratione loci*) is to be clarified. This pertains to the question whether certain rights apply at all outside the German territory. If the respective right is applicable, then, second, the substantial scope (*ratione materiae*) of the right must be ascertained.

---

[13] U.S. organisations have also sometimes failed to establish standing *ACLU v. NSA* 493 F.3d 644 (6th Cir. 2007).

[14] Comparable to the presumed German re-interpretation of surveillance laws that will be mentioned below (see the accompanying text to *infra* note 37), the broadening of the provisions and their interpretation gradually encompassing the communication of domestic citizens forms an interesting parallel. Cf. Louis Fisher and David Gray Adler, *American Constitutional Law*, 7th ed. (2007: 738 et seq.).

[15] USA Patriot Act 2001, Protect America Act 2007, and FISA Amendments Act 2008.

[16] This purely "person-focused" approach is often criticised as it does not match the practical ways and needs of online surveillance anymore—see Kerr (2008).

[17] Cf. 50 U.S.C. §1804(a)(4); §1805(a)(3), (c)(2)(A), (c)(3)(C), (d)(3), (e)(2).

[18] The provisions can be found in Sec. 702-704 FISAA. Cf. especially Sec. 702(b)(3); (k)(3)(A)(iv); 703(c)(7); (d)(4); 704(a)(2) FISAA. Note that Sec. 2.3 of Executive Order 12333 considerably widens the possibilities for warrantless incidental surveillance of U.S. persons as long as the information is collected in the context of a "foreign intelligence investigation".

[19] Sec. 703(a)(2); (c)(1)(B); (g) FISAA.

The extent to which the *Bundesnachrichtendienst* (BND, the federal intelligence service)—mostly responsible for foreign intelligence—is bound to respect fundamental rights, has not been conclusively decided by the German *Bundesverfassungsgericht* (BVerfG, Federal Constitutional Court). Nevertheless, certain indicators can be found in a decision concerning the powers of the BND for surveilling communications abroad as permitted by the G 10 Act.[20,21] In this decision the court held that the protection of confidentiality of correspondence, post, and telecommunications as guaranteed by Art. 10 GG is not limited to national territory. It is indeed applicable, if the foreign communication in question has a sufficient nexus or connection to German authorities. This is at least the case when the collection or analysis of data takes place domestically.[22]

Interestingly, the court emphasised that the German constitution's coordinative power is not limited to the domestic organisation of the German state. The German constitution further defines the state's relationship with the international community. The BVerfG even outlined features of this "responsive legal pluralism" when it stated: "[The constitution] is based on the need for delineation and coordination with other states and jurisdictions".[23] From this, the court deduces two general criteria for determining the application of fundamental rights abroad[24]: First, the extent to which German authorities are accountable and responsible[25] must be taken into account. Second, constitutional law must be reconciled with public international law.[26] The court also added that with respect to applicability "modifications and differentiations are admissible or necessary".[27] However, it is to be noted that these remarks are merely an obiter dictum of the decision.

Meanwhile, the BVerfG has similarly held in previous decisions that it may establish a reduced standard of constitutional protection in constellation with an international nexus. Accordingly, modifications in comparison to domestic cases are possible prospects—especially with regard to the legal systems of other countries, intergovernmental relations, or the specific conditions of international markets.[28] The criteria for this decreased standard result partly from the respective rights themselves and partly from the facts and circumstances of each individual case: First, the fundamental right must be interpreted in the light of its precise protective function (*Schutzrichtung*). Another important factor is whether the fundamental right is guaranteed internationally. The court has provided a positive answer to this question for the confidentiality of telecommunications.[29] The more characteristics of a general human right a fundamental right has (and

---

[20] *Gesetz zur Beschränkung des Brief-, Post und Fernmeldegeheimnisses* (G 10-Gesetz, Act for the Limitation of Privacy of Correspondence, Post, and Telecommunication). The Act allows for warrantless automated wiretaps of domestic and international communications by states' and federal intelligence services (such as the BND) for purposes of protecting freedom and the democratic order, preventing terrorism, and illegal trade of drugs and weapons. The BVerfG held the G 10 Act constitutional, as long as it is interpreted in a certain manner.

[21] Decision of the Federal Constitutional Court (hereinafter: BVerfGE) 100, 313. In its wording, Art. 10 GG does not distinguish in terms of *ratione personae*, but protects both Germans and foreigners.

[22] BVerfGE 100, 313 (313, Headnote no. 2; 363-364). This certainly does not provide a conclusive answer to the question if Art. 10 GG applies in cases where the BND eavesdrops on communication between foreigners in foreign territories and already analyses the data abroad. Additionally, the test of a sufficient nexus or connection as applied by the court in this case has only limited value due to the global and interconnected nature of contemporary communication. It will need judicial refinement in future decisions to prevent arbitrary results.

[23] BVerfGE 100, 313 (362).

[24] BVerfGE 100, 313 (362 et seq.).

[25] "Verantwortlichkeit und Verantwortung", BVerfGE 100, 313 (363).
What may seem like a circular argument in this translation, is instead sound reasoning as the terms are to be understood rather *factually* and not *normatively*.

[26] This can be seen as a general expression of the *Völkerrechtsfreundlichkeit* of the German constitution.

[27] BVerfGE 100, 313 (363).

[28] BVerfGE 92, 26 (42).

[29] BVerfGE 100, 313 (363).

is less a peculiarity of the national legal system), the more likely is its application in cross-border situations. Additionally, it may prove to be important, whether the individual involved is affected intentionally or merely *de facto*. Finally, the necessary effort to ensure an adequate degree of protection shall be taken into account. Not surprisingly, according to the BVerfG this issue can only be solved satisfactorily on a case-by-case approach.[30]

This allows the conclusion that German fundamental rights provide *prima facie* protection outside the federal territory when actions can be sufficiently attributed to German authorities (as actors—independent from their location).[31] Yet, this principal extraterritorial application does not imply a fixed extent to which the substantive protection of Art. 10 GG is granted.

Additionally, Art. 10 GG can also be invoked when it comes to the steps of gathering, exploiting, and analysing of telecommunication data.[32] This may apply even though the data in question has originally been collected and then subsequently been shared by a foreign intelligence service. This practice marks an important step in the emerging pattern of cross-surveillance as outlined above. Recently, the BVerfG ascertained that constitutional requirements for the collection, storage, and processing of data must not be undermined through a practice by which an authority, that is subject to less stringent requirements, provides or furnishes access to data to another authority, which is in contrast subject to stricter requirements.[33] There are, hence, reasons to believe that arranged exchanges of data circumventing German domestic law could in principal be deemed unconstitutional by the BVerfG.

Similar to U.S. intelligence laws, the respective German statutes show exceptions when it comes to foreigners. § 5 (2) G 10 Act does not allow the use of keywords in telecommunication surveillance which could lead to a targeted surveillance of certain telecommunication terminals or interfere with the "innermost core of a person's private life".[34] According to § 5 (2) sentence 3 G 10 Act, however, the BND is not confined to this when it is factually precluded that German citizens are intentionally affected. In general, the *Bundesnachrichtendienstgesetz* (BNDG, Federal Intelligence Agency Act) in conjunction with the G 10 Act allows for much wider and encompassing surveillance measures than, for example, the *Bundesverfassungsschutzgesetz* (BVerfSchG, Federal Office for the Protection of the Constitution Act—which establishes the German domestic intelligence service and its capabilities) in conjunction with the G 10 Act.[35] For surveillance measures based on § 5 of the G 10 Act, which are conducted by the BND, § 10 (4) sets a peculiar limit in volume: not more than 20 per cent of the maximum telecommunication transmission capacity of a certain path may be used.

[30] In doctrinal debates this approach has been criticised for being sweeping and ambiguous. For further references, see Martin Kment (2010). For a more general insight, see Heike Krieger (2008); Bertold Huber (2013: 2572); see also the legal analysis of Wolfgang Hoffmann-Riem for the hearing of the parliamentary investigation committee of the German parliament on the NSA revelations from May 22, 2014, accessed June 18, 2016, http://www.bundestag.de/blob/280846/04f34c512c86876b06f7c162e673f2db/mat_a_sv-2-1neu--pdf-data.pdf.

[31] Cf. Florian Becker (2013: § 240, margin no. 14-16).

[32] BVerfGE 125, 260 (310).

[33] BVerfG, *Neue Juristische Wochenschrift* (2013): 1503. The underlying constellation of the case was, however, a merely domestic one.

[34] "Kernbereich der privaten Lebensgestaltung".

[35] Recent comments in legal literature, therefore, argue that this provision is unconstitutional, cf. Bertold Huber (2014: § 5 G 10-Gesetz, margin no. 44); Fredrik Roggan (2012: G 10 § 5, margin no. 22).

3. Reported Measures of Global Cross-Surveillance

The possibilities for legal cross-surveillance outlined above become even more crucial as a phenomenon once actual surveillance practices are taken into account. According to the manifold revelations of the last years the pooling and sharing of vast amounts of data gathered through surveillance is daily business for intelligence agencies.

As reported by *DER SPIEGEL*, the German *Bundesnachrichtendienst* (BND, Federal Intelligence Service) supplies the U.S. *National Security Agency* (NSA) with large amounts of data collected from facilities located on German territory (Hubert et al. 2013).[36] Similarly, according to *The Guardian*, the British *Government Communications Headquarters* (GCHQ) had access to the infamous *PRISM* programme run by the NSA (Hopkins 2013). Overall, GCHQ seems to orchestrate and facilitate North Atlantic surveillance and data sharing activities (Borger 2013). However, these are just a few cases of the various practices which have been exposed in the last few years and which could be labelled "cross-surveillance".

Details as to where exactly the targeting, gathering, analysing, and sharing of data is carried out and by which intelligence service have only partly come to light. However, the precise structure of data collection and transfer of data can (theoretically) be tailored to the relevant legal framework in order to facilitate the most sweeping and intrusive surveillance. The transfer of selected cases and data sets is one possible practice, as is the pooling of large amounts of unprocessed data and organ swapping.[37]

In addition, some intelligence services such as the German BND have reportedly resorted to a broad re-interpretation of the term "foreign communication" (Bergmann and Weller 2013; Fischer 2013; Stadler 2013). This interpretation could not only serve to include large amounts of the foreign internet traffic routed through Germany, but also potentially entails connections from German users to German servers where these are routed abroad before they return.

The extent to which lower standards for the surveillance of foreigners are exploited *intentionally* by intelligence services still remains unclear.[38] However, the technical feasibility and thus the likeliness of the circumvention of national laws through concerted international surveillance practices has undoubtedly increased greatly. This sufficiently underpins the practical relevance of the previous legal analysis, even if a deliberate collusion of said services is not necessarily implied.

Due to the internet's decentralised infrastructure, the almost unpredictable routing of connections, and the mostly unencrypted transfer of data, the majority of users could be subject to eavesdropping by the intelligence services of states of which they are not citizens. In short: everyone is a foreigner when it comes to international IT surveillance.

---

[36] Further details on the cooperation between NSA and BND under the operation name "Eikonal" were published by Süddeutsche Zeitung and other news outlets a few months later (see Mascolo et al. 2014). See also a more recent German parliamentary minor interpellation addressing the data sharing practice between INTERPOL, Europol, the *Bundeskriminalamt* (BKA, Federal Criminal Police Office) and the US military, BT-Drs. 18/1411, May 14, 2014. Accessed June 18, 2016: http://dipbt.bundestag.de/dip21/btd/18/014/1801411.pdf.

[37] For references see the sources in the paragraph above.

[38] This is disputed for the NSA by spokesperson Vanee Vines: "As we've said before, the National Security Agency does not ask its foreign partners to undertake any intelligence activity that the US government would be legally prohibited from undertaking itself" (Ackerman and Ball 2014).

III. Answers from International Law and Global Constitutionalism

The analysis conducted above shows certain tensions between the presumed original intent of the lawmaker, the law, and its application in IT surveillance practices. Notably, the laws and higher court jurisdiction have hardly kept track with the rapid development of factual possibilities of surveillance and adhere to at least partially obsolete categories of territoriality and citizenship. The additionally resulting "dents" when it comes to foreigners are admittedly often perceived to follow a country's (self) interest, but become problematic at the latest when own citizens are under surveillance of foreign powers. National laws and constitutions mostly allow exceptions for foreigners. Additionally, the foreigner's prospects for successful proceedings before national courts are limited. Hence, the nation state is most likely not the appropriate place to seek immediate relief (Beck 2016). We are therefore making a selective attempt to look for solutions to this problem in international human rights law as part of public international law and global constitutionalism.

1. International Human Rights Law

Global safeguards for human rights are in recent decades increasingly enshrined in public international law. Given the situation of cross-surveillance and national legal loopholes, one could look for an underlying legal safety net in international law. As there are no international legal treaties specifically dealing with the subject of cross-border mass-surveillance or spying (Radsan 2007) the international human rights documents are the sources of possible legal protection. We therefore undertake a brief look at these potential safeguards in the field of public international law that lie beyond the field of soft law[39] and mere customary international law[40] without providing a conclusive legal opinion on the matter.

The reported surveillance programmes may violate the International Covenant on Civil and Political Rights (ICCPR). Practically all states involved in foreign mass surveillance have ratified the covenant and its Art. 17 (1) protects against any arbitrary or unlawful interference with privacy, home, or correspondence.[41] Clearly, international IT surveillance measures do interfere with some if not all of the mentioned domains. However, Art. 2 (1) ICCPR mentions that with regard to the applicability of the rights every state (only) "undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant". While the word *"and"* suggests that both criteria territoriality and jurisdiction have to be established in order to apply, a state's factual control or rather a sufficient relationship between the state and the individual is in practice deemed to be sufficient by the Human Rights Committee.[42] If the processing and analysis of data collected through surveillance is sufficient to satisfy the requirements of the test, has yet remained unresolved. Additionally, governments can still try to show that their surveillance is neither arbitrary nor unlawful and therefore does not breach Art. 17 (1) of the Covenant. An additional impassibility for evening out the diagnosed "dents" are the non-judicial politically inhibited ways of enforcement of the ICCPR. The Covenant, for instance, still heavily relies on reports compiled by the Covenant's parties themselves (Art. 40 ICCPR).

Similar in substance, the European Convention on Human Rights (ECHR) recognises a right to private life, home, and correspondence in Art. 8. The protective scope of this right closely resembles Art. 17 ICCPR, so that its applicability *ratione materiae* can be assumed. The European Court of Human Rights (ECtHR) has laid out more detailed prerequisites based upon Art 8 (2) ECHR for the lawfulness of surveillance matters. Yet again, Art. 1 ECHR states that the parties of the Convention "shall secure to

[39] Cf., for instance, General Assembly Plenary of the United Nations, *GA/11475*. Accessed June 18, 2016: http://www.un.org/press/en/2013/ga11475.doc.htm.

[40] A brief assessment of possible violations can be found at Anne Peters' *Blog of the European Journal of International Law* (2013a).

[41] Cf. also the almost identical Art. 12 of the Universal Declaration of Human Rights.

[42] *Sergio Euben Lopez Burgos v. Uruguay*, Communication No. R.12/52, para. 12.

everyone within their jurisdiction the rights and freedoms" that are subsequently defined in the document. The ECtHR developed a test of "*effective control*"[43] to determine jurisdiction. If the *virtual control* over data through means of surveillance is able to satisfy this test, remains judicially unresolved (Peters 2013b).

As demonstrated, possible international legal answers to emerging international cross-surveillance and surveillance arbitrage encounter recurring constraints. Apparently, international human rights documents were implicitly designed to address the relationship between citizens and *their own* state and not foreign authorities. This is especially the case when it comes to the question of jurisdiction as well as territorial and personal applicability of rights. These legal uncertainties and perhaps practical loopholes are mainly results of legal sources and jurisprudence developed in the pre-internet era. A higher likeliness of protection in substance through international human rights documents may presumably be attributed to their supranational and encompassing character and scope in comparison with national sources of law. This possible advantage may, however, be effectively rendered void by general insufficiencies in their enforcement.

2. Global Constitutionalism and the "Principle of Proportionality" as a Counterargument

The idea of constitutionalisation refers to the growing demand for and to the increasing legalisation of international relations. Both the past and the present call for a response to what is emanating from sovereign states. In short, sovereign states must submit to universally recognised rules, which bind and tame states even against their will. Global constitutionalism is not only about studying legal documents; beyond that, it can be understood as "an academic and political agenda that identifies and advocates for the application of constitutionalist principles in the international legal sphere in order to improve the effectiveness and the fairness of the international legal order" (Peters 2009). If this concept is embraced by national constitutional courts, it brings the chance to patch some of the dents in national surveillance laws that were outlined above. As a universal concept it provides the theoretical foundation for universal and collective reciprocal protection under surveillance laws.

The principle of proportionality is widely understood to be one of the most important general principles of law and may constitute a structural element of global constitutionalism. The principle of proportionality has recently witnessed a dramatic spread.[44] Some even believe this principle to be inherent to the rule of law and human rights,[45] although it remains disputed when it comes to details and its grounds of validity (Reimer 2013). It is continuously applied in EU law[46] and by the ECtHR (Rivers 2006). The BVerfG was one of the first to begin to operationalise and establish this principle.[47] Numerous international constitutional theorists have meanwhile been introducing the principle to the international constitutionalism discourse.[48] At this point, we are convinced that the principle's potential to structure and rationalise the discourse is sufficient to bestow consideration upon it for the purpose of this paper.

The principle of proportionality, of course, is only one test among others in the set of criteria for determining the lawfulness of an interference with fundamental rights. Some other criteria which may be

[43] ECtHR, *Loizidou v. Turkey (Preliminary Objections)*, No. 15318/89, 23 Mar 1995, §§ 62-63.

[44] David M. Beatty (2004: 162): "a universal criterion of constitutionality"; Alec Stone Sweet and Jud Mathes (2008: 160). Many important aspects remain, however, disputed. For an example of the controversy, cf. Stavros Tsakyrakis (2009: 468); Madhav Khosla (2010: 298); Matthias Klatt and Moritz Meister (2012: 687); Kai Möller (2012: 709).

[45] Cf. Art. 8 (2) ECHR which anticipates testing standards for determining the lawfulness and proportionality of government's interferences with the right to respect for family and private life.

[46] Cf. Art. 5 (1) 2, (4) TEU and Art. 52 (1) 2 CFREU; furthermore, see Takis Tridimas' *The General Principles of EU Law* (2006: 135 et seq.).

[47] BVerfGE 7, 377.

[48] Cf. in particular, Robert Alexy (2002); David Beatty (2004: 162); Matthias Kumm (2010: 141).

generalised were, for example, reiterated by the ECtHR in a landmark case,[49] in which the court examined the lawfulness of the extension of powers of the BND with regard to the recording of telecommunication in the course of so-called "strategic monitoring" as well as the use of personal data obtained and its transmission to other authorities. The court held that the expression "in accordance with the law"[50] required, first, that the impugned measure should have some basis in domestic law and, moreover, that it also referred to the quality of the law in question, i.e. that the law is accessible and the consequences for the person concerned foreseeable, and compatible with the rule of law.[51] Among all the criteria and tests to determine the lawfulness of state actions, the principle of proportionality demands special attention as it encompasses all actions by any branch of government, i.e. the law itself and the respective surveillance activities based upon it.

Proportionality is defined as a "test to determine whether an interference with a *prima facie* right is justified".[52] It hence serves as a "doctrinal tool" to resolve a conflict between the right and a competing right or interest. Initial starting points for deducing and establishing the aforementioned *prima facie* rights can be found in Art. 12 IDHR, Art. 17 ICCPR, Art. 8 ECHR, Art. 7 CFREU, Art. 10 GG, and in the fourth amendment of the U.S. constitution. For the purpose of this paper we assume the as-if-applicability of such rights protecting privacy and correspondence in order to operationalise the proportionality test.

In accordance with this principle of proportionality, *first*, an act of a governmental power (that can also be a law or a court decision) interfering with a right must pursue a legitimate goal. *Second*, the act must be a suitable means of achieving the goal (or rather: at least it must not be obviously unsuitable). *Third*, the act must be necessary insofar as there is no less intrusive but equally effective alternative. *Finally*, the act must not impose a disproportionate burden on the right-holder (proportionality in the strict sense). At this last stage the conflicting interests are conciliated.

a. Legitimate Aim

The governmental act at issue must be objectively justifiable, which means that a mere subjective personal intent is irrelevant. The question is whether the interest(s) pursued justifying the interference satisfy a low standard of reasonability. Without providing a theory of legitimacy, there are goals to be excluded as impermissible, e.g. moralistic and paternalistic aims which find no credible legal foundation do not count as legitimate.

Purposes like safeguarding national security, public safety, the economic well-being of a country, and the prevention of crime will hardly ever be *per se* illegitimate in most surveillance cases. The ECtHR, to take the above-mentioned case as an example, took the view that the protection of national security and the prevention of crime were legitimate aims.[53] Nevertheless, the aim in question has to be examined in every single case. Surveillance measures applied in manners that discriminate merely on the basis of (political) opinion or that are obviously aimed at discrediting political adversaries on personal grounds, would be incompatible in democratic societies.

b. Suitability

The principle of suitability demands that there must be a (presumable) causal relationship between the interference and the realisation of the legitimate aim. The means interfering with fundamental rights must be suitable to achieve the aim at least to a small extent. Thus, all those governmental actions are eliminated which do not or cannot contribute to reaching an alleged aim.

[49] ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, June 29, 2006.
[50] In the relevant case within the meaning of Article 8 (2) ECHR.
[51] ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, June 29, 2006, § 84.
[52] Kai Möller (2012: 710 et seq., emphasis in the original), *supra* note 44 with reference to Alexy (2002: 66).
[53] ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, June 29, 2006, § 104.

It can be assumed that the conducted surveillance, at least as reported, is not *per se* unconducive to its aim. It has been brought forward that international surveillance measures and the subsequent sharing of data has led to arrests and prevented certain crimes or terrorist attacks (Calmes 2013), although this remains disputed (Bergen et al. 2014). However, in order to thoroughly assess the suitability of the interferences, every single measure of data collection, storage, and analysis must be examined with regards to its potential to foster the purposes of national security and public safety. Under the current state of affairs too many facts remain in the dark to conduct a thorough assessment of suitability.

c. Necessity

The principle of necessity holds that there must be no other means more lenient but still equally effective in achieving the legitimate aim. Both the legislative power and the executive branch have to choose alternative, less restrictive means if available. It is sometimes problematic that hypothetically milder alternatives can be found which are to a certain extent disadvantageous. The government enjoys a prerogative here, especially when there are two means equally restrictive of fundamental rights. This does, however, not imply that the judiciary is deprived of assessing the necessity of the interference.[54] This remains a legal question that is to be reviewed in its entirety.

In the context at hand, the precise scale of surveillance can be problematic. A large-scale or blanket surveillance requires a special effort for justification, if justifiable at all. And while—yet again—a solid factual base for assessing current measures and their possible alternatives is missing, a generalised approach along the lines of "more information means more national security" would be impermissible.

d. Balancing (Proportionality in a Strict Sense)

At this last stage of the proportionality assessment, which is most frequently subject to (legal) debate, the identified conflicting interests and values have to be balanced. There are at least two notions of balancing, the first of which can be called *interest balancing* and the second *balancing as reasoning*.[55] Convincing and consistent considerations require a logical structure as it has been developed and presented in an exemplary manner by Robert Alexy (2002).

In practice, balancing means that an interference can be justified if the burden placed on the affected person(s) is not disproportionate in relation to the legitimate aim(s) pursued. The more serious the interference with the right is, the more demanding are the requirements for its "successful" justification. More precisely, the more serious the interference with the right is, the higher are the requirements for the importance of the purpose pursued.[56] The stage of balancing is the appropriate place to ultimately solve or release the legal tension[57] between security and freedom.

In the *Weber* case outlined above, the ECtHR also established a set of criteria for proportionality in the context of surveillance and interference of communication which can again be useful for balancing.[58] To begin with, the considerations have to depend on all circumstances of the case, such as the nature, scope, and duration of the possible surveillance measures, the grounds required for ordering them, the authorities competent to authorise, carry out, and supervise them, and remedies for possible breaches provided by national law. Interestingly, the court stressed that, in view of the risk that a system of secret surveillance

[54] Cf. ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, § 105-107.
[55] Kai Möller (2012), *Proportionality: Challenging the critics*: 715, *supra* note 44.
[56] There are, of course, absolute limits. As Möller (2012: *supra* note 44) states, balancing is not only about a rational cost-benefit analysis, but also a "balancing of all relevant considerations". Thus, taking the famous exemplary *transplant case*, killing one person in order to save five other persons would be impermissible.
[57] Be it in the variant "security versus liberty" or "security through liberty".
[58] ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, June 29, 2006, § 105 et seq.

for the protection of national security may undermine or even destroy democracy under the pretence of defending it, it is absolutely compulsory that there are adequate and effective guarantees against abuse of powers and arbitrariness in place. Having defined its standard of review, the court continued with examining whether the interferences in question were proportionate and conducted an overall assessment.

In our broader case it cannot be neglected that intelligence services directed towards foreign powers have a particular need for secrecy and security, namely, for their own institution but also for their sources of information since activities carried out for the benefit of foreign intelligence are often criminalised under respective foreign criminal codes. In the context of global surveillance in a chiastic constellation, the role of internet intermediaries, i.e. those mostly private entities that provide and host content and platforms, and provide internet infrastructure, shall be briefly taken into account in order to paint a full picture. The intermediaries traditionally handled the users' communication data, such as phone connections and post. Now, while in cases of domestic surveillance for purposes of intelligence or law enforcement the respective existing intermediaries can simply be instructed and compelled by their own governments,[59] any attempt of a foreign government to compel an intermediary located in another country to help with surveillance seems comparably futile. Hence, laws for foreign surveillance traditionally allow for greater secrecy and less governmental control, as the intelligence measures could otherwise hardly be successful.

The underlying practical constellation of traditional foreign *espionage* has however changed in two ways. First, today we rely more heavily on intermediaries for every step that we take online to communicate and to shape our personality and, more importantly, these intermediaries can and do follow every single one of these steps. Second, these intermediaries are often foreign to us,[60] so their respective government can easily resort to means that were formerly confined to cases of domestic surveillance, such as instructions directed towards an intermediary.

The remaining differences to classic cases of domestic surveillance are that the targeted person is presumably not a citizen[61] of the surveilling country and—more importantly—not subject to *more than informational* power (i.e. factual control) exercised by the government.[62] The latter distinguishing factor is at least practically repealed once the information has been shared with a citizen's country of residence following the chiastic structures outlined above.

The process of balancing cannot be aspired to the fullest extent possible here, but we hope to provide ideas for lines of argument for this endeavour. The distinctions between domestic and foreign surveillance are surely fading. Due to the developments outlined above and the intrinsic secrecy of intelligence surveillance the governmental control of intelligence services' actions is of rising importance. More adequate and efficient parliamentary, judicial and executive control and verification mechanisms may need to be installed. Mechanisms to rebalance the scale can be sought in: well-resourced independent judicial oversight exercised with institutional and financial independence, a more adversarial procedure with an attorney entrusted with the rights of the objects of surveillance, additional in-depth democratic (parliamentary) control, and time-dependent notification and report rules among other possibilities.

---

[59] Cf. for example, Sec. 215 of the PATRIOT Act.

[60] The aforementioned steps often leave marks with several intermediaries and are therefore a potential object of surveillance to more than one government.

[61] Possibly following contractual constitutional theories there have been attempts to justify differing surveillance requirements based on the status of citizenship. Non-resident foreigners were missing any obligations or a duty of allegiance towards a state, Elizabeth Corradino (1989: 630-633). If this notion of statehood and citizenship is still true and appropriate and—more importantly—if it can still account for the distinction between several types of surveillance, has to remain unresolved here.

[62] The risk of following tangible consequences for persons has sometimes been used as an argument for the severity of a previous mere informational interference, cf. BVerfGE 118, 168 (186, 197).

IV. Conclusions and Outlook

In this paper we have looked for "dents" in the regulatory framework of surveillance, which constitute possible legal loopholes for intelligence services. A peek into the international practices in this field, that have been reported in the last few years, has confirmed that cross-surveillance is a grave possibility, with the risk of overarching international IT surveillance arbitrage on the rise.

From a *constitutional* perspective, the surveillance of foreign communication becomes the litmus test for the question of jurisdiction, especially if framed as a procedural problem. This substantively corresponds with questions for applicability of fundamental rights on grounds of territoriality (or: *ratione loci*), citizenship (or: *ratione personae*), and factual governmental control. Notably, the constitutional and international legal grounds for this issue have been built in the era predating IT mass surveillance.

As discussed, a presumably insufficient level of protection can be detected in U.S. and German law for cases with foreign elements. Generally, exceptions are established on the grounds of foreign citizenship, extra-territoriality, or lack of factual governmental control. These criteria have, however, lost their power to distinguish in practice between types of surveillance along the lines of "*domestic v. foreign*". This may even highlight the partial failure of categories of space or territoriality and national identity as means of distinction when it comes to online regulation.[63]

Additionally, there are at present hardly any satisfactory standards in international law suitable to grant relief for the specific chiastic constellation at hand. The principle of proportionality, as a potential structural element of global constitutionalism, proves to be a promising starting point to formalise lines of legal reasoning. Thus, we hold the hope for better-structured and rational arguments in cases within the surveillance context leading to more balanced and just results.

With this contribution to the overall discourse of international surveillance we hope to have (re)located the role of law in the debate. At the same time, our paper illustrated how national law has become weak as a guiding force when it comes to the transnational online realm. An increased cooperation between law and other means of governance, but also institutions such as national courts, seems inevitable.

Philosophy, or more precisely ethics, could also be an appropriate field in which the legitimacy of certain surveillance practices can be assessed. Any answers found there may contribute to the debate on how to overcome national short-termed self-interests and reach a consensus on questions of reciprocity.[64] The golden rule as it has found its expression in *Immanuel Kant's Categorical Imperative*,[65] serves as our last point and hopefully someone else's starting point: *Surveil* only according to that maxim whereby you can at the same time will that it should become a universal law without contradiction.

References

Ackerman, Spencer, and James Ball. 2014. Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ. *The Guardian*, February 27. Accessed June 18, 2016: http://gu.com/p/3n57z.

Alexy, Robert. 2002. *A Theory of Constitutional Rights.* (First published in German 1986.) Oxford: Oxford University Press.

Beatty, David M. 2004. *The Ultimate Rule of Law.* Oxford: Oxford University Press.

Beck, Ulrich. 2016. *The Digital Freedom Risk: Too Fragile An Acknowledgment.* Accessed June 18, 2016: http://www.opendemocracy.net/printpdf/75073.

[63] *Nota bene*: The underlying constellation can therefore also be framed as a (legal) problem of direct or indirect discrimination on grounds of nationality, or arbitrary unequal treatment.

[64] These answers may later curdle and become yet again law.

[65] His late essay *Perpetual Peace: A Philosophical Sketch* (Zum ewigen Frieden. Ein philosophischer Entwurf, 1795), offers another promising starting point.

Becker, Florian. 2013. Grenzüberschreitende Reichweite deutscher Grundrechte. In: *Handbuch des Staatsrechts*, 3rd ed. Heidelberg: C.F. Müller.

Bergen, Peter, David Sterman, Emily Schneider and Bailey Cahall. 2014. Do NSA's Bulk Surveillance Programs Stop Terrorists? *New America Foundation*, January 13. Accessed June 18, 2016, https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/.

Bergmann, Christian and Markus Weller. 2013. Unklare Regelungen bei der Überwachung von Auslandskommunikation". *Mdr Fakt*, November 12. Accessed June 18, 2016: http://www.mdr.de/fakt/bnd114-download.pdf.

Borger, Julian. 2013. GCHQ and European Spy Agencies Worked Together on Mass Surveillance. *The Guardian*, November 1. Accessed June 18, 2016: http://gu.com/p/3k3h8/stw.

Calmes, Jackie. 2013. Obama Says Surveillance Helped in Case in Germany. *New York Times*, June 19. Accessed June 18, 2016: http://nyti.ms/13SVPYj.

Cole, David. 2003. Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens? 25 *Thomas Jefferson Law Review* 25: 367-388.

Corradino, Elizabeth A. 1989. The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far? *Fordham Law Review* 57: 617-618.

Fischer, Sebastian. 2013.Neue Späh-Enthüllungen: Europäische Geheimdienste sollen kooperiert haben. *Spiegel Online*, November 1. Accessed June 18, 2016: http://spon.de/ad4sl.

Fisher, Louis, and David Gray Adler. 2007. *American Constitutional Law*, 7th ed. Durham, NC: Carolina Academic Press.

Hopkins, Nick. 2013. UK Gathering Secret Intelligence via Covert NSA Operation. *The Guardian*, June 7. Accessed June 18, 2016: http://gu.com/p/3gdh6.

Huber, Bertold. 2013. Die strategische Rasterfahndung des Bundesnachrichtendienstes—Eingriffsbefugnisse und Regelungsdefizite . *Neue Juristische Wochenschrift* 66(35): 2572-2577.

Huber, Bertold. 2014. *Sicherheitsrecht des Bundes.* München: C.H. Beck.

Hubert Gude, Laura Poitras, and Marcel Rosenbach. 2013. Mass Data: Transfers from Germany Aid US Surveillance. *Spiegel Online*, August 5. Accessed June 18, 2016: http://spon.de/adZ9l.

Kant, Immanuel. 1917. "Perpetual Peace—A Philosophical Sketch". (First published in German 1795.) London: George Allen and Unwin.

Kerr, Orin S. 2008. Updating the Foreign Intelligence Surveillance Act. *University of Chicago Law Review 75:* 225-243.

Khosla, Madhav. 2010. "Proportionality: An assault on human rights?: A reply." *International Journal of Constitutional Law* 8(2): 298-306.

Klatt, Matthias, and Moritz Meister. 2010. "Proportionality—a benefit to human rights? Remarks on the I·CON controversy". *International Journal of Constitutional Law* 10(3): 687-708.

Kment, Martin. 2010. *Grenzüberschreitendes Verwaltungshandeln.* Tübingen: Mohr Siebeck.

Kumm, Matthias. 2010. The Idea of Socratic Contestation and the Right to Justification: The Point of Rights-Based Proportionality Review. *Law & Ethics of Human Rights* 4(2): 142-175.

Krieger, Heike. 2008. Die Reichweite der Grundrechtsbindung bei nachrichtendienstlichem Handeln. *Berliner Online Beiträge zum Völker- und Verfassungsrecht.* Accessed June 18, 2016: http://www.jura.fu-berlin.de/fachbereich/einrichtungen/oeffentliches-recht/lehrende/kriegerh/dokumente/berliner_online_beitraege_krieger08_01.pdf.

Lyon, David. 2007. *Surveillance Studies: An Overview*. Polity: Cambridge University Press.

Mascolo, Georg, Hans Leyendecker, and John Goetz. 2014. Codewort Eikonal—der Albtraum der Bundesregierung. *Süddeutsche.de*, October 4. Accessed June 18, 2016: http://sz.de/1.2157432.

Möller, Kai. 2012. "Proportionality: Challenging the critics". *International Journal of Constitutional Law* 10(3): 709-731.

Peters, Anne. 2009. The Merits of Global Constitutionalism. *Indiana Journal Global Legal Studies* 16: 397-411.

Peters, Anne. 2013a. Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon (Part I). November 1, 2013, *Blog of the European Journal of International Law.* Accessed June 18, 2016: http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/.

Peters, Anne. 2013b. Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon (Part II). November 4, 2013, *Blog of the European Journal of International Law.* Accessed June 18, 2016: http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/.

Radsan, John. 2007. The Unresolved Equation of Espionage and International Law. *Michigan Journal of International Law* 28(597): xx.

Reimer, Philipp. 2013. "'… UND MACHET ZU JÜNGERN ALLE VÖLKER'? Von "universellen Verfassungsprinzipien" und der Weltmission der Prinzipientheorie der Grundrechte". *Der Staat* 52 (1): 27-57.

Rivers, Julian. 2006. Proportionality and Variable Intensity of Review. *Cambridge Law Journal* 65(1): 174-207.

Roggan, Fredrik. 2012. *G-10-Gesetz.* Baden-Baden: Nomos.

Stadler, Thomas. 2013. Was überwacht der BND. *Internet-Law, Onlinerecht und Bürgerrechte 2.0,* November 13. Accessed June 18, 2016: http://www.internet-law.de/2013/11/was-ueberwacht-de?r-bnd.html.

Stone Sweet, Alec, and Jud Mathes. 2008. Proportionality, Balancing and Global Constitutionalism. *Columbia Journal of Transnational Law* 47: 73-165.

Tridimas, Takis. 2006. *The General Principles of EU Law*. Oxford: Oxford European Community Law Library.

Tsakyrakis, Stavros. 2009. "Proportionality: An assault on human rights?" *International Journal of Constitutional Law* 7(3): 468-493.

Vladeck, Steve.2012. More on Clapper and the Foreign Intelligence Surveillance Exception. *Lawfare*, May 23. Accessed June 18, 2016: http://www.lawfareblog.com/2012/05/more-on-clapper/.

Washington Post, The. 2014. Transcript of president Obama's January 17 speech on NSA reforms, January 17, 2014. Accessed June 18, 2016: http://www.wapo.st/1mgJ3wk.