A HOOVER INSTITUTION ESSAY

The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance

PETER SWIRE, JESSE WOO, AND DEVEN R. DESAI

Aegis Series Paper No. 1901

Introduction

This article addresses whether governments ever have a justified basis for treating targets of surveillance differently, in any way, based on nationality. This issue is of general importance and has become particularly important in the current legal debates about whether the United States has "adequate" protection of personal privacy under EU law. Under US surveillance law, there are often stricter privacy protections for "US persons" (US citizens and permanent residents) than for non-US persons. As we have presented this research at several conferences, almost all US experts have agreed that this approach is normatively defensible. By contrast, EU legal experts have expressed concern that the two-tier approach may constitute discrimination based on nationality, and is questionable under EU law and data privacy principles. If EU courts were to find the two-tier approach unlawful, a practical implication is that it could provide the basis for a broad ruling prohibiting transfer of personal data to the United States.[1]

This article fills a notable gap in prior writing, and shows compelling justifications for allowing nationality to matter for surveillance and protection of freedom of expression rights.[2] We also assume that any such differential treatment based on nationality is constrained. A nation cannot lawfully torture persons simply because they have a different nationality. International human rights law limits how a government can and should act toward others; one cannot treat others differently simply because of their nationality. In addition, we sharply distinguish between our discussion of the possible limited uses of nationality for surveillance purposes, on the one hand, and recent trends, on the other hand, to invoke nativism or nationalism in politics. Such trends are a far cry from the reinforcement of democratic society that this article seeks to support and foster.[3]

In this initial work in our project comparing US surveillance laws and practices to other countries', we compare the United States and Germany. We examine Germany because it is an important democracy within the European Union, known for strict privacy protection, and facing similar challenges regarding protecting rights and democracy while also protecting against national security threats. In our analysis, we define surveillance as the government's access to and gathering of data about a person (the "target"). We distinguish

between three relevant ways that surveillance rules can differ in ways related to nationality. First, US and German surveillance can be conducted for law enforcement *or* foreign intelligence purposes, and the difference matters.[4] As the European Fundamental Rights Agency has documented, a clear majority of EU member states have different rules for law enforcement and foreign intelligence surveillance.[5] Second, rules depend on the *location* where the surveillance occurs—whether the collection occurs within the country or outside of it. US and German surveillance rules differ based on the location of collection.[6] The lawfulness of this approach was upheld in September 2018 by the European Court of Human Rights in its *Big Brother Watch v. UK* decision, finding specifically "that any difference in treatment based on geographic location was justified."[7] Third, and of the greatest focus for this article, the rules vary depending on whether the *targets* of surveillance are part of the polity. For instance, US law provides stricter protections under certain laws for surveillance of US persons (citizens or permanent residents) than for non-US persons, and German law does the same for Germans.[8] That practice in Germany is subject to legal challenge, with one nongovernment organization reportedly planning litigation that argues that German surveillance law "implies discrimination against individuals without a German passport which is incompatible with the German Basic Law."[9] At this time it is not clear whether the challenge will be filed, and if filed and successful, on what grounds.[10]

Stricter protection for US persons has received considerable criticism, such as from EU officials in connection with negotiation of the EU/US Privacy Shield. Countries that apply stricter standards for surveillance of members of their own polity, such as the US and Germany, have been condemned as practicing invidious discrimination.[11] One version of the criticism, the "universalist" approach, supports a legal rule that the same surveillance standard should apply to all persons globally and argues for a universal human right to be free from unjustified surveillance. In the words of UN Special Rapporteur on the right to privacy, Joseph Cannataci, "when it comes to surveillance carried out on the Internet, privacy should not be a right that depends on the passport in your pocket."[12] Marko Milanovic has similarly stated in the surveillance context that "distinctions based on nationality alone would seem hard to justify."[13]

This article respectfully differs with that conclusion. At least where there are baseline human rights protections in how a country conducts surveillance towards all persons—in other words, where protections flow from the rule of law, such as "effective judicial review designed to ensure compliance with provisions of [the] law"[14]—applying somewhat stricter standards for surveillance based on target nationality has a number of strong justifications.[15]

Possibly the most compelling justifications are to preserve democracy, while maintaining the rule of law. There are special and significant risks to democracy and the rule of law that result from a country's surveillance of its internal political opposition and the free press. The history of Nazi Germany, the USSR, and East Germany show how the state used surveillance to identify dissent and target the press as central strategies for political

oppression. Recent expansions of surveillance power in Russia, Turkey, and Venezuela similarly illustrate aggressive actions against the press, the free Internet, and political opposition, with the consequent erosion of the rule of law.

Differing rules based on nationality also exist to protect democracy directly. As an initial point, democracies characteristically discriminate in the right to vote based on nationality—those who are part of the nation can vote, and foreigners cannot. More broadly, the United States, Germany, and other countries set limits on campaign expenditures for foreigners, compared with broader rights for those in the country to participate in the election. These campaign-related restrictions on foreigners provide a basis for law enforcement or national security surveillance of foreigners suspected of violating those laws.[16]

This article thus explains how a two-tier approach, instead of reducing fundamental rights, can serve the bedrock constitutional principles of democracy and the rule of law. Surveillance of nationals and others with a close connection to the domestic policy poses a special threat to the political opposition and free press of a country, both of which play crucial roles in limiting abuses of state power. Surveillance of persons outside the polity, by contrast, does not similarly implicate this risk to a nation's democratic institutions. Preventing a slide into authoritarianism is a compelling reason for extra-strict protections against surveillance of a nation's political opposition and free press.

A second justification for differential surveillance arises depending on the context of the surveillance—such as foreign intelligence and counterintelligence, foreign affairs, foreign adversaries, and international armed conflict—each of which can alter the analysis of what type of surveillance is proper. For example, without surveillance how can one detect an imminent invasion, enforce economic sanctions, or promote nuclear nonproliferation? This point has been made forcefully by Tim Edgar, who worked with the American Civil Liberties Union before becoming a senior official in the US intelligence community for civil liberties issues. Based on his experience, Edgar found a compelling case for having different standards for different contexts, notably between protecting domestic civil rights and democracy, contrasted with foreign intelligence.[17] As a further practical matter, even if the United States, Germany, France, or the United Kingdom chose to apply the same rules to all surveillance contexts, it seems unlikely that other countries such as Russia or China would follow suit in practice.[18]

In sum, the article addresses (1) three ways nationality can matter to surveillance; (2) reasons for stricter rules for law enforcement and domestic collection; (3) reasons for different rules based on the location of collection; (4) the universalist critique of surveillance laws based on nationality; and (5) reasons that can justify stricter surveillance rules based on nationality. These reasons have not been assessed either by the Court of Justice for the European Union nor by the European Court of Human Rights, which in 2018

addressed numerous other foreign intelligence surveillance issues in both *Big Brother Watch v. UK* and *Centrum för Rättvisa v. Sweden*.[19] This article concludes, under both the US and European legal traditions, that there are important and hitherto unarticulated reasons why nationality can be an important and justified, although constrained, part of surveillance regimes.

Three Ways Nationality Can Matter to Surveillance

In this part, we generalize the category of "US person" and "non-US person" to two categories that can apply under the law of any country: "nationals and near-nationals" ("NANNs") and "non-nationals and non-residents" ("NoNNRs"). We also examine US and German law as examples of where surveillance law can vary based on nationality considerations: (1) law enforcement versus foreign intelligence surveillance; (2) the location of surveillance; and (3) the nationality of the target of surveillance.

NANNs and NoNNRs

Part of the problem has been a lack of clarity about the way in which surveillance laws operate and who is covered by the term "national." Many countries have at least some laws that apply differently to a core group, including citizens, as contrasted with persons with no attachment to the country.

As one example, which we mention only briefly here, a country will typically have jurisdiction over its own citizens but not have the same legal power to issue binding orders on foreigners who have never established any connection with that country. These differential jurisdictional concerns arise under the recently enacted Cloud Act, which enables executive agreements between the United States and qualifying foreign governments to govern how each government can access criminal evidence from service providers. Under the Cloud Act, the United States requires stricter protections before a foreign government can access evidence about US persons than for non-US persons. For example, if an executive agreement is in place, the French government can gain streamlined access to evidence about French citizens from a US-based cloud provider, but must go through stricter procedures before accessing evidence about US persons.[20]

As a second example, consider recent concerns about disinformation campaigns by foreign actors in elections in Europe and the United States. To protect democracies and fundamental rights against foreign interference, there is a strong normative case for permitting stricter rules to detect and limit campaign-related and other expressive actions by foreign actors.

Whether for purposes of jurisdiction, free expression, or surveillance law, it is useful to establish terminology to distinguish between those who are part of the community of a nation and those who are not. Under US law, the distinction is typically between

"US persons," who are US citizens and permanent resident aliens, and "non-US persons." The same type of distinction exists under the law of other countries. We propose the acronym "NANN" to refer to nationals and near-nationals, while individuals who are not part of the polity are "NoNNRs," who are non-nationals and non-residents.

For some legal purposes, defining the precise line between NANNs and NoNNRs may be vitally important, such as determining whether an individual receives health benefits or qualifies for easier entry across the border.[21] For our purposes, we do not try to define precisely where the line is or should be between NANNs and NoNNRs. Our point is that the law recognizes two such tiers in a range of legal settings. This article discusses relevant legal rules with the two tiers relevant to surveillance, and whether and when they may be normatively appropriate.

Nationality and the US Approach to Government Surveillance

US Constitutional Law and Social Contract Theory Behind the US Approach The US legal approach to nationality and surveillance has both a constitutional and statutory dimension. The US constitution—along with other constitutions—was profoundly shaped by social contract theorists such as John Locke.[22] One of Locke's principal goals was to prevent tyranny: "*Wherever law ends, tyranny begins*."[23] To achieve that goal, he believed that a system of checks and balances was essential.[24] People who consent to the social contract will be involved in checks and balance. These people inside the community have a special role in preventing tyranny. People outside the community are not saddled with this obligation to guard against tyranny, but neither do they enjoy the community's protections and privileges.[25] In line with this logic, US courts ruling on surveillance law issues apply Fourth Amendment protections more strictly for US citizens than for individuals who are outside of the United States and who lack any citizenship or strong tie to the country.[26]

US Statutory Law on Surveillance and Nationality As a statutory matter, the distinction between US persons and non-US persons was established in law in the 1970s.[27] The Privacy Act of 1974, passed months after the Watergate-related resignation of President Richard Nixon, provided its key protection to US persons, but not to others.[28] The distinction between US persons and non-US persons for foreign intelligence surveillance was included in the 1978 passage of FISA. That law grew out of the 1972 *Keith* case, in which the US Supreme Court rejected the claim that "domestic security" was a lawful basis for surveillance without a warrant, because the concept was "so vague" that "the danger to political dissent is acute."[29] At the same time, the Court distinguished the issues of foreign intelligence surveillance.[30] Accordingly, when FISA was enacted in 1978, the new law applied specifically to foreign intelligence surveillance, when the data is collected within the United States. Stricter rules applied to surveillance of US persons than non-US persons (consistent with protection against surveillance of political opponents, such as the "enemies list" of President Nixon). The law also specifically banned surveillance against US persons when

it was based solely on First Amendment activity (protection of free speech and press).[31] But nationality is only part of the analysis about what is allowed.

How US Law Applies Nationality to Surveillance To determine the legal standards for US government surveillance, there are three questions, each of which turns on issues of what is domestic versus what is foreign: (1) law enforcement versus foreign intelligence surveillance law; (2) collection domestically versus collection done outside of the country; and (3) collection targeted at US persons versus targeted at non-US persons. Table 1 provides a summary of the applicable standards for these three legal distinctions.[32] Below we address whether these distinctions are normatively defensible, which we believe they are.

The first question is whether the surveillance is conducted *under law enforcement or foreign intelligence authorities*. As shown in the table below, law enforcement wiretaps and access to stored records take place under the Electronic Communications Privacy Act, whose sections are called the Stored Communications Act, the Wiretap Act, and the trap-and-trace provisions (collecting to/from information). These law enforcement rules are generally stricter than the rules for foreign intelligence surveillance.

Second, the *location of collection* matters. Foreign intelligence surveillance conducted within the United States generally comes within FISA, while foreign intelligence surveillance conducted outside the United States generally operates under Executive Order 12333.[33]

Third, the *nationality status* of the target matters. As the next column shows, targets who are NANNs (US persons under US law) have greater protection than NoNNRs (non-US persons under US law).

Table 1

Activity	Location	Governing Law	Target Nationality	Protection Level
Law enforcement	Domestic (or foreign)	Search warrant or Title III wiretap	NANN or NoNRR	Probable cause of a crime, with additional limits on wiretaps. Same regardless of nationality
Foreign intelligence	Domestic	FISA Title I	NANN	Probable cause that the target is an agent of a foreign power
Foreign intelligence	Domestic	FISA Section 702	NoNNR	Reasonable belief the target is within a court-approved certification
Foreign intelligence	Foreign	EO 12333	NANN	Subject to agency guidelines, qualifies as foreign intelligence information. Additional safeguards for US persons
Foreign intelligence	Foreign	EO 12333	NoNNR	Subject to agency guidelines, qualifies as foreign intelligence information. Safeguards for non-US persons set by PPD-28

As examples, two programs that have been the subject of considerable debate, Prism and Upstream, operate under Section 702 of FISA.[34] First, these programs are done for foreign intelligence purposes, rather than under law enforcement authorities. Second, Section 702 applies when collection is done within the United States, while collection abroad operates under the less strict standards of EO 12333. Third, the Section 702 programs, as well as surveillance under EO 12333, apply stricter rules for NANNs (US persons) than for NoNNRs (non-US persons).

Nationality and the German Approach to Government Surveillance

As a matter of law "all EU Member States regulate the organisation of their country's intelligence services. Almost all have established at least two different bodies for conducting civil and military intelligence."[35] This system makes for "a diverse landscape."[36] As such, European countries make distinctions similar to the three distinctions just discussed under US laws, but also unique to each respective country.[37] As an illustration, this article examines German law and summarizes the substantial German intelligence surveillance reforms passed in late 2016.[38] For the treatment of nationality, German law is strikingly similar to US law, with similar regimes in other European countries.

German law distinguishes NANNs and NoNNRs. German intelligence surveillance law "protects German citizens at home and abroad, national residents, and legal entities in Germany."[39] This definition closely tracks the definition of US persons, as US citizens (at home and abroad) and lawful permanent residents. The German law applies somewhat stricter protections for EU citizens than for other non-Germans. But Germany does not apply the same protections offered to Germans to EU citizens, thus showing another way in which it treats surveillance targets differently depending on the relationship among the country, the idea of polity, and the target.

Concerning the three categories of surveillance and nationality discussed for US law, German law distinguishes between law enforcement and intelligence surveillance, either at the German regional state (Land) level, or for foreign intelligence surveillance.[40] The prior and reformed German statutes apply to the intelligence activities of the Bundesnachrichtendienst (BND), Germany's foreign intelligence agency.

German intelligence law sets different rules depending on location. The law sets stricter rules for "foreign-domestic strategic surveillance," when either the origin or destination of a communication is in Germany. It has less strict laws for "foreign-foreign strategic surveillance," which is acquired abroad or is collected in transit through Germany. The former is similar to Section 702 of FISA, with its rules for information collected in the United States but with the target being abroad. The latter is similar to EO 12333, which has less strict rules for communications acquired abroad or in transit.

German intelligence law also sets different rules depending on target nationality.[41] As Wetzling documents, the least strict protections apply to "purely foreign strategic surveillance," which is "surveillance of communications data of foreign individuals on foreign soil."[42]

This distinction between NANNs and NoNNRs in the German surveillance oversight regime occurs under other European regimes.[43] David Cole and Federico Fabbrini write that "[d]omestic constitutional protections . . . are no longer able to secure a meaningful defense against warrantless surveillance of *non-citizens*" (emphasis in original).[44] They also note that the EU Charter and Data Protection Directive "give states broad discretion with respect to national security surveillance. And neither EU law nor the ECHR appear to constrain EU member states' surveillance of foreign nationals beyond their borders."[45] The 2018 European Court of Human Rights cases examining the surveillance rules in Sweden and the United Kingdom included major rulings permitting surveillance with certain safeguards, but have not yet addressed the issue of surveillance of foreign nationals beyond national borders.[46]

Reasons for Stricter Rules for Law Enforcement and Domestic Collection

Although we have found surprisingly little writing on point, we suggest that somewhat different rationales apply for the diverse surveillance rules in the three categories just discussed. In this part, we address the first two categories, and examine the category of target nationality in more detail below.

First, many established democracies apply different rules for law enforcement versus foreign intelligence surveillance. The Fundamental Rights Agency report on EU member states found that a clear majority had different rules for law enforcement and foreign intelligence surveillance.[47] Greater scope for foreign intelligence activities fits the reality of a dangerous world, where potentially hostile nations can send agents into a country contrary to national security. For surveillance in particular, a principal goal of law enforcement is to arrest the wrongdoer for punishment and prevention of further criminal acts. To achieve convictions, the emphasis is on amassing evidence that can be presented in open court. By contrast, surveillance of foreign powers and their agents focuses on intelligence gathering rather than incarceration. For instance, a nation may conduct ongoing surveillance on an adversary's embassy and agents, without ever wishing to reveal the existence of the surveillance, or the sources and methods, in open court.

The second distinction, based on the location of collection, appears, according to our research, not to be especially controversial. Until the recent *Big Brother Watch v. UK* decision, we had not found a clear articulation of the rationale for the distinction. We propose that the context of the surveillance—the institutional mechanisms for collection—are often different at home and abroad. At home, the government has physical sovereignty and can use coercive force. A government has huge advantages in conducting surveillance

within its territory, compared with surveillance abroad. Domestically, the government has the police force, with broad powers to interview witnesses and collect evidence of all sorts. Domestically, the government also has the judicial system, which can lawfully compel the production of evidence—uncooperative witnesses can be put in jail, and locked doors can be opened with a search warrant or similar judicial order. Historically, these police and judicial powers have meant that the government has the capability within the nation to access quite a large amount of evidence. Democracies have also placed many legal limits against abuse of these police and judicial powers.

A government's legal capacity to require surveillance is, however, much more limited outside of the country. Except under special agreement, a country's police officers lack their police powers outside of their jurisdiction. Judges often lack jurisdiction to issue search warrants or court orders where the evidence is in another country. Because the police and judges cannot compel production of evidence, the nation may seek cooperation from another country. Such cooperation, however, can encounter many obstacles. As a US court observed in connection with the search for Osama Bin Laden, "when some members of the government of the country in which the searches are sought to be conducted are perceived as hostile to the United States or sympathetic to the targets of the search, a procedure requiring notification to that government could be self-defeating."[48]

The brief discussion of this issue in *Big Brother Watch v. UK* concurs: "The Government have considerable powers and resources to investigate persons within the British Islands and do not have to resort to interception of their communications under a section 8(4) warrant. They do not, however, have the same powers to investigate persons outside of the British Islands."[49] In short, pervasive differences in context, or institutional competence, can explain different legal standards for surveillance carried out domestically (where the government has a broad range of effective tools) and abroad (where the same government has far more limited powers to conduct surveillance). These pervasive differences thus could justify the different surveillance standards described above for domestic and foreign collection, under US and German law.

The Universalist Position Supporting a Right to Privacy Regardless of Nationality

As just discussed, there has been little controversy to date about the first two categories where surveillance law applies rules differently for foreign and domestic. These two categories distinguish between (1) foreign surveillance versus domestic law enforcement and (2) collection abroad versus collection domestically. By contrast, prominent experts, especially in Europe, appear to express strong opposition to a two-tier legal approach for target nationality.

We believe a significant portion of the apparent disagreement arises from how different legal systems—for this article, the United States and legal decisions of the European Court

of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU)—diverge in how privacy rights are defined. In this part, we present the legal instruments that universalists have cited in criticizing defining rights differently for NANNs and NoNNRs. We then explain why the disagreement may be less severe than initially appears.

Legal Instruments Cited in Support of Universalism

Universalists—those who believe the same privacy rights should apply regardless of nationality—draw upon a number of legal instruments to support their view. This legal tradition dates to the 1948 United Nations' Universal Declaration of Human Rights, whose Article 12 states that "no one shall be subjected to arbitrary interference with his privacy."[50] Similar language was later included in Article 17 of the 1966 International Covenant on Civil and Political Rights.[51] In a 2016 Report to the General Assembly, Professor Joseph Cannataci, the UN Special Rapporteur on the right to privacy, stated that "in terms of article 17 of the International Covenant on Civil and Political Rights, everybody enjoys a right to privacy *irrespective of nationality or citizenship*" (emphasis supplied).[52] More generally, Cannataci says states should "prepare themselves to ensure that both domestically and internationally, Privacy [*sic*] be respected as a truly universal right—and, especially when it comes to surveillance carried out on the Internet, privacy should not be a right that depends on the passport in your pocket."[53]

The European Convention on Human Rights (ECHR) adds requirements beyond these international instruments. The first paragraph of ECHR Article 8 states that "everyone has the right to respect for his private and family life." As discussed further below, paragraph 2 of Article 8 sets forth extremely relevant text applying to that right to privacy:

> "There shall be no interference by a public authority with the exercise of this right **except such as is in accordance with the law and is necessary in a democratic society in the interests of national security**, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (emphasis added).[54]

These ECHR requirements apply to forty-seven countries,[55] and cases interpreting the ECHR are under the European Court of Human Rights (ECtHR), seated in Strasbourg.

In addition, the Charter of Fundamental Rights of the European Union (Charter) applies to the twenty-eight current member states of the European Union. The Charter's privacy protections in Articles 7 and 8 must be at least as protective of fundamental rights as the ECHR. The Court of Justice of the European Union (CJEU), seated in Luxembourg, is the highest court for interpreting the Charter. Since 2009, CJEU judgments have binding effect on the member states and are similar in this respect to decisions of the US Supreme Court.

The CJEU has protected the rights to respect for private life and data protection as fundamental rights in a series of cases involving government access to personal data for law enforcement or national security purposes. A series of cases since 2014 illustrates the point. For instance, in *Digital Rights Ireland*, the CJEU struck down an entire EU law that required Internet providers across the European Union to retain records of who accessed the Internet. In 2015, the Court struck down the EU/US Safe Harbor due in part to concerns about excessive US government surveillance.[56] And it also struck down the EU agreement with Canada about passenger name records. Indeed, in the wake of *Big Brother Watch v. UK*, Théodore Christakis has noted a divergence between the ECtHR and the CJEU, with the latter applying stricter scrutiny to surveillance regimes.[57] In light of these holdings, as mentioned in the introduction, one could imagine the CJEU looking askance at a US law that discriminated on the basis of target nationality, possibly leading to a judgment that US surveillance law violates the fundamental right to privacy for that reason. It is noteworthy to highlight here that EU treaty law clearly provides that national security matters of EU member states fall outside of the scope of EU law. This may, however, be subject to change due to the outcome of a pending judgment before the CJEU.[58]

Differing and Misunderstood Views on the Operation of Rights

Despite the important legal instruments that are cited by universalists who raise concerns about a two-tier system of surveillance that varies based on target nationality, we believe there may be more room for agreement on outcomes than the quotations would suggest.[59] Notably, US and EU legal experts have different conceptions of what it means to define a privacy right.

Consider the quote by Special Rapporteur Cannataci defining "a right to privacy irrespective of nationality or citizenship." Roughly speaking, for a US lawyer, the quote means that each detail of the law must apply the same irrespective of nationality or citizenship. Under this US understanding, the language "irrespective of nationality or citizenship" would be understood as forbidding any different legal rules based on target nationality, such as different treatment in any manner for US persons as opposed to non-US persons.

By contrast, an EU lawyer would see the definition of the "right to respect for private life" as applying to the first step in a multistep process.[60] Under the jurisprudence of the ECtHR and the CJEU, the *right* is defined broadly. It is this broad definition of the right that Professor Cannataci appears to be describing, and which he states should be "irrespective of nationality or citizenship."

After this relatively broad definition of the right, the European courts next examine whether the *interference with the right* can be justified. For instance, in a 2010 case involving surveillance in the United Kingdom, the ECtHR recognized the right and then stated that any interference with the Article 8 right to privacy can only be justified

"if it is in accordance with the law, pursues one of [sic] more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim."[61] In 2018, the ECtHR cited cases finding that countries have a "margin of appreciation" in conducting national security and found that the Swedish foreign intelligence surveillance system was permissible because "it minimizes the risk of interference with privacy." Thus, under this jurisprudence, developed in the ECtHR and followed by the CJEU, the right is defined broadly, irrespective of nationality or citizenship, but then the court analyzes the interference with the right to reach some ultimate judgment about whether a regime complies with law.

Under the EU approach, deciding the legality of a two-tier system thus depends both on defining the right and assessing in detail whether the interference with the right can be justified. Before that assessment can take place, we must discuss the legitimate aims of a two-tier regime, and why it may be necessary in a democratic society to permit at least somewhat different rules for NANNs and NoNNRs.

Reasons for Stricter Rules for NANNs than NoNNRs

We next turn to reasons why a two-tier surveillance system may be justified, with stricter rules for NANNs than NoNNRs. The first set of reasons concerns national security—greater surveillance is surely needed in wartime, as well as less adverse foreign relations settings. The second set of reasons goes to the preservation of democracy and the rule of law—stricter protections help guard the domestic political opposition, freedom of speech, and participation in a country's elections.

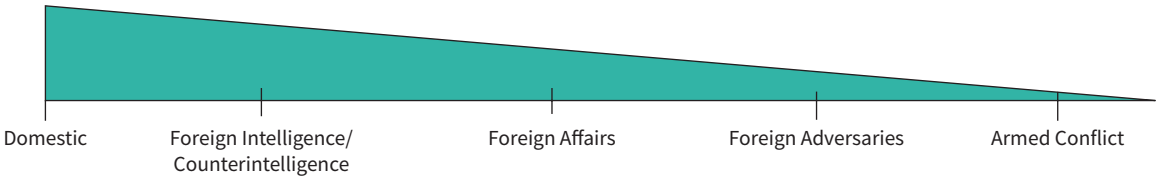
National Security Surveillance in War and Less Adverse Foreign Relations

Under US and EU law, national security is a legitimate basis for restrictions on the right to privacy. As mentioned above, the US Supreme Court in the 1972 *Keith* case provided greater scope for foreign intelligence surveillance than for domestic law enforcement. In Europe, Article 8 of the ECHR specifically states that "national security" is a legitimate aim that can justify restrictions of the right to privacy, where necessary and proportionate.

Privacy experts are often skeptical of claims of national security, however.[62] Such claims are routinely made by those supporting broader surveillance powers. Often, there is little information publicly available to assess the national security claim in a particular situation. Privacy experts thus have understandable concerns that national security will be asserted in a particular case, with no effective mechanism to distinguish legitimate from overstated claims of national security.

We believe that the context of surveillance—how it is conducted for national security and foreign affairs purposes—can help explain and justify different surveillance rules based on nationality, for the three categories discussed above: (1) domestic law enforcement versus

Figure 1. Strictness of Surveillance Rules



foreign intelligence; (2) collection domestically and abroad; and (3) different rules based on target nationality, for NANNs and NoNNRs. Instead of relying solely on the case-by-case assertion of national security, which is so difficult to assess, these categories provide the public and the courts with a way to classify more generally when national security arguments are likely to be compelling.

The proposed approach is pictured in Figure 1, which shows a continuum between a state of war (with the fewest restrictions on surveillance) and full domestic law (with the strictest protections against law enforcement surveillance). Using US law as an example, domestic investigations for law enforcement purposes are subject to the full protections of the Fourth Amendment, including probable cause warrants. The other categories, however, have fewer legal limits on surveillance.

In Figure 1, the extreme situation is international armed conflict. In this context, there is an overwhelming case for a government to undertake surveillance with fewer restrictions than apply to a domestic law enforcement action.[63] In an international armed conflict setting, it makes no sense to apply a strict universalist approach. International armed conflict justifies necessary measures to preserve the nation, and such measures may include surveillance that operates under different rules than other situations. To take a simple example, rapid surveillance and reporting may warn a unit that it is about to come under attack, and thereby save lives. Greater surveillance can be justified based on location of collection, such as in a combat zone or the territory of the hostile country. Greater surveillance can also be justified based on the nationality of the target. Even in international armed conflict, there are strong justifications for continuing to apply greater safeguards against excessive surveillance, for a country's own nationals.[64] For nationals of the hostile country, who often act on behalf of the hostile country, there is a principled basis for greater surveillance.

Figure 1 shows other categories that can lead to varying rules for surveillance:

1. *Foreign adversaries.* Although not in international armed conflict, foreign adversaries have significant disagreements and opposing geopolitical goals. Consider the situation in the Crimea when Russia sent troops there in 2014. Before the annexation, the United States and its allies had an important stake in assessing the likely Russian actions as a matter of foreign affairs. After the annexation, the United States and its allies took actions in response, including economic sanctions against Russia, which to

be effective required monitoring. As with a declared war, greater surveillance can be justified based on location of collection, notably for activities in Russia and the Crimea prior to and after the annexation. Greater surveillance can also be justified based on the nationality of the target. Suppose an American businessperson, or political leader, was traveling in the Crimea just before or after the annexation. Although there was heightened reason in general for the United States to do surveillance in this geographic area, there would be countervailing reasons to retain the usual safeguards for surveillance of this NANN. For instance, it may make sense to have a rule that the NANN retains the usual protections against surveillance, until and unless evidence indicates that the individual is acting on behalf of the foreign adversary. The same logic would apply to German surveillance of German NANNs, contrasted with German surveillance of NoNNRs with respect to Germany, in the Crimea or Russia.

2. *Foreign affairs.* Foreign affairs is another realm where states have traditionally surveilled one another, even when the states are allies.[65] The Crimea before the annexation illustrates this point. At the time, Russia was part of the G8, and so had the status of an ally rather than an adversary; of course, in international affairs, there are many shades of gray between a close ally and a clear adversary. As such, especially as tensions mounted in the Crimean area, there was strong reason for the United States and its close allies to heighten surveillance based on location (the Crimean region) and target nationality (surveillance of Russians in the Crimea prior to the annexation may have had a stronger justification). Reasonable national security concerns at that point could justify greater surveillance than occurs domestically. This is not to say that surveillance targeted at allied and other countries should be unchecked—it may well be politically prudent to provide stronger protections for surveillance targeted at allies than for adversaries. President Obama's Presidential Policy Directive 28 (PPD-28), retained by President Trump, applies to signals intelligence. It institutes general privacy rules applying to non-US persons, including minimization, data security, and oversight of foreign intelligence. PPD-28 retains an exception, however, because those protections apply only "[t]o the maximum extent feasible, consistent with national security."[66] For foreign affairs, even where the PPD-28 baseline exists for protecting privacy rights regardless of target nationality, the facts may justify different surveillance safeguards based on location or target nationality.

3. *Foreign intelligence.* For surveillance that takes place within the country, as discussed above, the United States and other nations have more flexible rules for foreign intelligence surveillance than for law enforcement investigations.[67] In the United States, individual FISA warrants apply to surveillance of foreign powers and "agents of foreign powers." Surveillance under FISA takes place domestically, where the range of government investigative techniques is generally subject to stricter legal rules than for collection of information abroad. For this FISA collection, US courts have applied the Fourth Amendment to foreign intelligence investigations, but under more permissive

rules than for law enforcement actions. Since its initial passage in 1978, FISA also provides somewhat greater protections for NANNs than for NoNNRs, such as a specific provision that US persons cannot be the subject of a FISA warrant based solely on protected First Amendment activity.[68] As discussed further below, the protection of democracy and the rule of law provide strong justifications for particular care where surveillance is targeted at NANNs based on political opposition or free speech.

In sum, Figure 1 illustrates where national security interests are likely to be most compelling. In wartime and towards foreign adversaries, nations are adverse by definition, and national security is clearly at stake. The nature of foreign affairs thus can justify different surveillance rules for the three categories discussed in this article: (1) domestic law enforcement versus foreign intelligence; (2) collection domestically and abroad; and (3) different rules based on target nationality, for NANNs and NoNNRs. These different rules may exist categorically, such as where a national law creates a different surveillance rule based on one of the distinctions. In the alternative, under the proportionality analysis employed by the ECtHR and CJEU, the three categories can assist the courts in performing a case-by-case assessment of whether an interference with a privacy right is justified.

Protecting Political Freedom with Surveillance Safeguards

Perhaps the most intuitive and compelling reason for differential treatment is to preserve democracy and the rule of law, by creating strict limits on surveillance of domestic political opposition and the free press. It is no coincidence that the 1972 Watergate burglaries targeted the headquarters of the opposition political party, the Democratic National Committee. Put simply, unique threats to democracy and the rule of law occur when a government intensifies surveillance of domestic political opponents. Would-be authoritarians increase surveillance of political opponents and the free press, often without judicial oversight, as shown in recent years in countries such as Russia, Turkey, and Venezuela. Strong protections against surveillance of domestic political opponents and the free press thus support individual rights, by protecting democracy and the rule of law. Surveillance against the persons who can vote is a threat to the survival of a democracy, in a way that surveillance of others is not.

Similar concerns apply to protecting free expression, such as through the First Amendment protections of speech, press, and assembly under US law.[69] To a significant extent, individual rights enhance collective rights. For example, freedoms of assembly and association are important as individual rights that aid how individuals learn, debate, and develop political views. These individual rights also enable collective engagement and action under the rule of law. The problem, as Desai has shown, is that "pervasive surveillance chills associational freedom."[70] That is, the Fourth Amendment "is linked to collective projects of self-governance."[71] More generally, as Professor Paul Schwartz has argued, in line with

similar arguments of Privacy International, privacy enables and supports both deliberative democracy and "the individual's capacity for self-governance."[72]

In addition, recent nation-state disinformation efforts and other attempts to influence elections in Europe and the United States give a new, prominent reason to appreciate the difference between domestic and foreign actors.[73] Even before such activities came to light, countries have restricted foreign nationals' ability to participate in elections. In the United States, the prohibitions on foreign national activity relating to US elections include prohibitions on contributions and donations to federal, state, or local elections; contributions and donations to any committee or organization of any national, state, district, or local political party; and donations to presidential inaugural committees.[74] In addition, foreign nationals are barred from expenditure, independent expenditure, or disbursement "for an electioneering communication."[75] Note, however, that resident aliens, in other words US persons, are able to participate short of voting.[76]

This position is in line with the distinction between US persons and non-US persons. As the Supreme Court explained in *Johnson v. Eisentrager*,[77] "The alien, . . . has been accorded a generous and ascending scale of rights as he increases his identity with our society. Mere lawful presence in the country creates an implied assurance of safe conduct and gives him certain rights; they become more extensive and secure when he makes preliminary declaration of intention to become a citizen, and they expand to those of full citizenship upon naturalization."[78] Even while in a "probationary residence," an alien has a "right against Executive deportation except upon full and fair hearing." Furthermore, resident aliens have "important constitutional guaranties—such as the due process of law of the Fourteenth Amendment."[79] Cases involving deportation, citizenship, and First Amendment rights follow the distinction between resident aliens and others, in that these cases recognize certain rights, and US courts' jurisdiction, once an alien is on US soil, and that the rights increase as someone is closer to being a resident alien.[80]

Thus, as then District Court Judge Kavanaugh explained in addressing a challenge to limits on foreign national expenditures on US elections, although "we know from more than a century of Supreme Court case law that foreign citizens in the United States enjoy many of the same constitutional rights that US citizens do . . . But we also know from Supreme Court case law that foreign citizens may be denied certain rights and privileges that US citizens possess."[81] In the election context:

> It is fundamental to the definition of our national political community that foreign citizens do not have a constitutional right to participate in, and thus may be excluded from, activities of democratic self-government. It follows, therefore, that the United States has a compelling interest for purposes of First Amendment analysis in limiting the participation of foreign citizens in activities of American democratic self-government, and in thereby preventing foreign influence over the US political process.[82]

Other countries draw similar distinctions regarding elections. Germany restricts donations "exceeding 1,000 Euros made by a foreigner."[83] Canada's Elections Act section 331, Non-interference by Foreigners, prevents people from outside Canada from "induc[ing] electors to vote or refrain from voting or vote or refrain from voting for a particular candidate" unless those people outside Canada are citizens or permanent residents under Canadian law.[84] Israel has a similar rule requiring that only voters may contribute to elections.[85] To protect democracies and fundamental rights against foreign interference, there is a strong normative case for permitting stricter rules to detect and limit campaign-related and other expressive actions by foreign actors.[86]

In short, strong protections against surveillance of domestic political opponents, the free press, speakers, and other participants in election politics support individual rights, by protecting democracy and the rule of law.[87] Similarly, greater surveillance of foreign actors can reduce the risk that democratic elections will be undermined. This protection leads to a collective good that we emphasize: minimizing the risk that a democracy will descend into authoritarianism.[88]

The US Experience The Watergate era exemplifies the importance of having checks against tyranny. The Watergate break-in was, at its core, surveillance activity against the opposition Democratic Party. In addition, during this period, the FBI and CIA conducted domestic surveillance against the civil rights, Black Power, antiwar, and other sociopolitical movements of the time. These agencies illegally opened and read mail, tapped phones, and infiltrated groups to spy on members.[89]

As discussed above, US law addressed this activity by passing the Privacy Act of 1974 and FISA, and rejecting "domestic security" as reason to get rid of the warrant requirement, because of the "acute" danger to "political dissent."[90] NANNs received greater protections in part because they need room to be political opponents. In addition, if surveillance is based only on First Amendment activity (protection of free speech and press), it is not allowed. As stated by the 2013 NSA Review Group, on which Swire served, FISA's stricter limits on domestic surveillance express

> not only a respect for individual privacy, but also—and fundamentally—a deep concern about potential government abuse within our own political system. The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system.[91]

The Experience in Other Countries The unique risk to democracy from domestic surveillance applies far beyond the United States. Pervasive domestic surveillance is a well-known feature of authoritarian regimes, and the experience of totalitarian surveillance under the Nazi regime is an important basis for the strict privacy rules that apply today in

Europe.[92] The Gestapo cracked down on political opposition parties, investigating people suspected of belonging to the communist or social democratic parties.[93] The Nazis also pervasively controlled information and the free press, such as through the Ministry of Public Enlightenment and Propaganda.[94] Similar surveillance and oppression of political dissenters occurred under Communist regimes. The Soviet Union's KGB operated an extensive surveillance state that suppressed political dissent and imprisoned many political prisoners.[95] These are just a few of many examples throughout history, as the entire phenomenon of secret police is designed to find and silence individuals with different political views. The pattern of increased surveillance combined with suppression of the press and dissent has happened in numerous countries historically.[96]

Unfortunately, one need not look to history to find such oppressive action. Three recent examples—Russia, Turkey, and Venezuela—illustrate the risk to democracy and the rule of law that accompany these practices today. In Russia wiretaps, often targeting political opponents, have risen dramatically in recent years.[97] The government has required Internet service providers to install hardware allowing deep packet inspection, and banned virtual private networks, which previously had enabled secure access to censored content.[98] Turkey has similarly increased surveillance of, and actions against, political opposition.[99] A failed coup in 2016 resulted in broader government powers to conduct domestic surveillance.[100] By 2017, a headline read: "Turkish opposition MP jailed for 25 years as part of Erdogan's ongoing political crackdown."[101] In Venezuela, President Nicholas Maduro has relied on his intelligence services, which are governed largely though executive decree, to target and jail his political opposition with no oversight.[102]

These three countries have also restricted the free press and the ability of citizens to access information contrary to the government's views. In addition to targeted cyberattacks on journalists, the Russian government has forced closures and resignations of key editorial staff at the country's independent media outlets[103] as part of "dismantling" the independent media.[104] In Turkey, President Erdogan has been aggressive in prosecuting journalists and free press in his crackdown following the 2016 coup attempt.[105] Venezuela censors Internet and other media companies that provide independent sources of information, and filters content in response to protestors using social media and messaging apps.[106]

Accordingly, preserving democracy and the rule of law and reducing the risk of authoritarianism is a compelling reason to create very strict limits on surveillance of these domestic actors. In the language of Article 8 of the ECHR, these strict limits are "necessary in a democratic society"—their absence can undermine democracy itself. Another legitimate aim in Article 8 is "the protection of the rights and freedoms of others." Preserving the rule of law protects not only the rights and freedoms of the individuals targeted by surveillance. Such preservation also protects the rights and freedoms—democracy itself, the rule of law—of the entire population.

In addition, as we argue below, democracies are unlikely to maintain surveillance rules that are similarly strict for surveillance of foreign enemies and other foreign actors. In wartime and in connection with foreign adversaries, it is hard to imagine that a nation will maintain surveillance limits as strict as those appropriate in connection with domestic political opposition. There is thus a compelling normative case for permitting stricter surveillance safeguards for NANNs than for NoNNRs, where NANNs otherwise would not receive needed protections.[107]

Conclusion

This article has set forth three important ways that nationality has been treated as relevant in surveillance law, using the United States and Germany as examples of broader patterns. Although safeguards are sometimes the same regardless of nationality, there are notable instances where safeguards are different: (1) domestic law enforcement has stricter safeguards than foreign intelligence surveillance; (2) collection of information domestically is subject to stricter legal rules than collection abroad; and (3) surveillance depends on target nationality, with NANNs subject to stricter protections than NoNNRs.

We have advanced two principal reasons why nationality can be an important reason to vary surveillance rules. First, Figure 1 showed the continuum between armed conflict, with the fewest surveillance limits, and domestic law enforcement, with the strictest limits. National security can provide a compelling reason to act differently toward foreign nations, who may be hostile, as well as individuals acting on behalf of those nations. Second, preservation of the rule of law and democracy (such as restricting foreign involvement in elections) can provide a compelling reason for extra-strict protection of domestic political opposition and the free press.

One logical response from a universalist would be to agree that strict rules should apply within a country, including to protect the political opposition and free press. The universalist may then argue that these same strict rules should apply universally, to all persons regardless of nationality. In that way, strong privacy protections would exist domestically, and persons of other nations would have the same protection of their privacy rights.

We submit that this strict universalist position is not a persuasive way to achieve the stated goal of privacy protection.[108] One reason has been offered by Tim Edgar, in discussing a proposed (but not adopted) universal agreement to ban mass surveillance practices. Edgar writes that such a treaty "would also be destabilizing. Russia, China, Iran, and other adversaries of the United States cannot be trusted to limit their intelligence capabilities."[109] The second argument against the strict universalist position is pragmatic. Assume, for sake of discussion, that a strict universalist believes it is desirable to apply precisely the same rules, regardless of target nationality. The pragmatic question is: what level of strictness

will a nation adopt over time? The strict universalist may hope that the rules will be at the protective level that applies to domestic political opposition and the free press. We submit, however, that it is far more likely that national security and foreign affairs considerations will win out over time. Supporters of foreign surveillance will gain political support when they seek to do surveillance during wartime or in the midst of a foreign affairs crisis. In considering a universalist rule prohibiting use of target nationality, we believe the result would be to adopt the watered-down standard for wartime and foreign affairs, and not the stricter domestic standard that privacy supporters would wish to have.[110]

The two-tier approach is a close match with the US legal tradition, which applies constitutional protections specifically to those within the social contract, or with other strong ties to the nation. As Professor Jamal Greene put it, a possibly unique "feature of US constitutional law is that it constitutes us, not just as a nation, but as a people as well."[111] Indeed, disapproval of the two-tier US approach under human rights law could be understood as part of a sweeping theory of international law, that rights based on a constitution— rights that are defined within the social contract—are illegal under human rights law. The US tradition, by contrast, does define some rights differently based on whether the individuals are citizens or otherwise have voluntarily linked themselves with the nation. Similarly, in the extradition context, the Court of Justice of the European Union has recognized the lawfulness of greater protections for nationals than for foreigners.[112]

In other words, there may be more room for nationality to be considered in surveillance under European law than might be apparent from some universalist statements. The broad statements about surveillance applying "irrespective of nationality" are made in the first stage of European analysis, in the definition of the fundamental right to privacy. Under Article 8 of the ECHR and other authorities, however, the analysis then proceeds to examine the "interference with the right." Nations create their surveillance regimes and are permitted a "margin of appreciation" in how they protect privacy while advancing national security and other goals recognized under Article 8.

This article elucidates a number of points that we have not seen addressed in the previous literature. These points go to why surveillance rules referring to nationality may meet legitimate aims under Article 8, such as national security and the protection of the rights and freedoms of others. Most fundamentally, we have shown why different rules based on target nationality may be vital to preserving democracy and the rule of law. The goals of protecting democracy and acting in accordance with law are explicit in Article 8, and important generally in fundamental rights jurisprudence. Put somewhat differently, the approach in this article shows how a regime that varies based on target nationality could meet the ECtHR and CJEU jurisprudence that the use of nationality in this context would be both "necessary" and "proportionate." Where this jurisprudence is satisfied, then alleged discrimination based on nationality would not be a basis for cutting off transfers of personal data from the European Union to a country such as the United States that applies

some surveillance rules differently based on nationality. We welcome further engagement with European experts on how to consider these ideas within European jurisprudence.

In conclusion, we have explored why a country **may choose** to use nationality as a consideration in the three categories related to foreign intelligence, foreign collection, and target nationality. We have explained why using nationality in this way can be both important and justifiable. Using nationality as a basis for government action also is and should be constrained. Far more than many critics have realized, domestic US law sets numerous constraints on government surveillance, including surveillance of non-US persons.[113] International law, including treaties ratified by the United States, sets additional restraints on when surveillance may discriminate based on nationality. Going forward, we hope the discussion here promotes a fuller discussion of the multiple ways that nationality has played and may play a role in crafting surveillance rules that both protect privacy and meet other legitimate goals such as national security and the protection of democracy.

ACKNOWLEDGMENTS

The first version of this research was presented in August 2017 at the Hoover Institution conference "Technology Giants, Sovereign Powers, and Surveillance." For thoughtful comments, the authors thank Joseph Canatacci, DeBrae Kennedy-Mayo, Christopher Kuner, Jack Leahey, Nóra Ni Loideain, Mario Oetheimer, Sreenidhi Srinivasan, Nico van Eijk, Peter Winn, and those who commented on earlier versions of this work at the Hoover Institution conference; the Indiana Law School Center for Applied Cybersecurity Research; Computers, Privacy and Data Protection '18; Privacy Law Scholars Conference '18—Europe; and Privacy Law Scholars Conference '18—United States.

No outside funding was provided for this article, apart from an honorarium from the Hoover Institution provided to all authors who participated in that symposium. Sources of financial support for the Georgia Tech Cross-Border Requests for Data Project are listed at http://www.iisp.gatech.edu/cross-border-data-project.

NOTES

1 Although we have not seen the argument made explicitly in print, a claim might be made that US law, such as Section 702 of the Foreign Intelligence Surveillance Act, applies different rules in a discriminatory way to US persons and non-US persons. Transfers of personal data from the European Union to the United States have already been challenged in the *Schrems 2* model contracts case in the Irish High Court, with focus on the practices of the National Security Agency as a reason not to find adequate protections when data is transferred to the United States. An alleged discrimination in surveillance based on nationality could be an additional argument, under EU law, why adequacy is lacking for transfers to the United States. For discussion of US surveillance law compared with EU practices, see *Professor Peter Swire Testimony in Irish High Court Case*, Alston & Bird (June 16, 2018, 10:06 p.m.), available at https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony.

2 For a contrasting view, see Douwe Korff et al., "Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes," at 35 (March 3, 2017) (hereinafter "Boundaries of Law") ("But most importantly, the distinction in protection between 'national persons' and 'foreigners' . . . is in fundamental breach of the principle of universality of human rights and of the prohibition of discrimination, inter alia on the basis of nationality or place of residence."), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490; see also Douwe Korff, "Expert Opinion prepared for the Committee of Inquiry of the *Bundestag* into the "5EYES" global surveillance systems revealed by Edward Snowden," sections B.2.b, B.2.c (hereinafter "Korff, 'Expert Opinion'"), available at https://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf. As we were finalizing this article for publication, we became aware of Asaf Lubin, "'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance," *Chicago Journal of International Law* 18 (2018): 502. We plan to discuss this article in future writing.

3 See, *e.g.,* Jamal Greene, "Foreword: Rights As Trumps?" *Harvard Law Review* 132 (2018): 28, 34 ("Ours is not an ethno-national or religious project but a political one, dedicated to the audacious idea that liberalism and pluralism are mutually constituted."); Peter Baker and Alissa J. Rubin, "Trump's Nationalism Rebuked at World War I Ceremony, Is Reshaping Much of Europe," *New York Times* (Nov. 11, 2018), https://www.nytimes.com/2018/11/11/us/politics/macron-trump-paris-wwi.html ("'Patriotism is the exact opposite of nationalism,' President Emmanuel Macron of France said in a speech at the Arc de Triomphe, welcoming the leaders and extolling an old system now under siege."); Jefferson Cowie, "Reclaiming Patriotism for the Left," *New York Times* (Aug. 21, 2018), https://www.nytimes.com/2018/08/21/opinion/nationalism-patriotism-liberals-.html ("The resurgence of blood-and-soil nationalism around the world seems to prove that appeals to nationhood are too racist, too tribal and too dangerous to be of value. Yet surrendering patriotism to champions of the ethno-state abdicates the fight for the soul and meaning of the American project.").

4 We acknowledge that some people think of surveillance as only intelligence activity, but we use the broader view because questions of possibly differential treatment based on nationality necessarily raise issues about law enforcement surveillance. Cf. Korff et al., "Boundaries of Law," *supra* note 2, at 58 ("The German Constitution, the 'Basic Law' (*Grundgesetz*), grants strong protection to the right to privacy and confidentiality of communications and data protection. Quite different legal regimes apply, however, for surveillance by law enforcement as opposed to intelligence services.").

5 A 2015 report by the Fundamental Rights Agency found that 23 of 28 EU member states separate intelligence services from law enforcement agencies, and a 2017 follow-up report found that "[t]he majority of intelligence services in the EU Member States have their own structure, organisation, and accountability, independent of the police and other law enforcement authorities." European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume I: Member States' Legal Frameworks*, 27 (2015) (hereinafter *Volume I: Member States' Legal Frameworks*); European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume II: Field Perspective and Legal Update*, 28 (2017) (hereinafter *Volume II: Field Perspective and Legal Update*).

6 See *Volume II: Field Perspective and Legal Update*, *supra* note 5, at 43–44, 46 (describing Germany's "enhanced safeguards for domestic surveillance" and the differences in German law for foreign surveillance including a "citizenship criterion" under "Section 6 (4) of the BNDG prohibit[ing] the BND from collecting and processing data on German citizens outside Germany" and the lack of application of German constitutional protection to foreign intelligence telecommunication surveillance); *accord* Thorsten Wetzling, "Stiftung Neue Verantwortung/Policy Brief—Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls," at 12–15 (June 2017) (summarizing 2016 changes to German intelligence laws and the distinction between allowed practices depending on where surveillance takes

place) at https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

7 *Big Brother Watch v. United Kingdom,* European Court of Human Rights (Sept. 13, 2018), No. 58170/13 et al., ¶ 518, available at http://hudoc.echr.coe.int/eng?i=001-186048.

8 Current German surveillance law makes distinctions among German citizens, public institutions of EU bodies and member states, EU citizens, and the rest of the world. In addition, the collection of non-Germans' data on non-German "soil" is unregulated. See Wetzling, *supra* note 6, at 14, 23.

9 Nora Markand, "GFF and Amnesty are Challenging Strategic Mass Surveillance," *Gesellschaft für Freiheitsrechte* (Nov. 6, 2016), available at https://freiheitsrechte.org/g10.

10 *Id*.; *accord* Wetzling, *supra* note 6, at 19 ("Whereas the German Constitutional Court has not equivocally positioned itself on the territorial reach of Art. 10 Basic Law question in the past, it will soon have to take a stance. Litigation is currently being prepared by the Society for Civil Rights [Gesellschaft für Freiheitsrechte, GFF] that will require a definite position by the court.").

11 See, e.g., Markand, *supra* note 9.

12 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, U.N. Doc. A/HRC/34/60, paragraph 44 (2017), available at https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

13 Marko Milanovic, "Human Rights Treaties and Surveillance: Privacy in the Digital Age," *Harvard International Law Journal* 56, no. 81 (2015): 99.

14 Korff et al., "Boundaries of Law," *supra* note 2, at 23. To be clear, a main critique of Korff et al., as well as Wetzling's argument against current German surveillance law, is that German surveillance law lacks sufficient judicial oversight, transparency, reporting, and other rule of law related structures. See *id.* at 21–26, 29 (arguing German laws governing law enforcement are examples of good rule of law structures and comparing those standards with German and other countries' intelligence gathering laws as lacking similar structures; see also Wetzling, *supra* note 6, at 24–25 (listing rule of law "deficits" in German intelligence law reforms and concluding, "Legal clarity and the rule of law were not the key objectives of this reform.").

15 There has been a surprising lack of discussion to date assessing why it is normatively appropriate to have different legal standards based on the nationality of the target. As we were completing an intermediate draft of this article, we discovered a draft article by Eric Manpearl that addresses some of the same topics. Eric Manpearl, "The Privacy Rights of Non-US Persons in Signals Intelligence," available at https://ssrn.com/abstract=3066161. Manpearl makes arguments consistent with the general thesis of this article, that it can be normatively appropriate to have different legal rules applying to citizens and non-citizens. Our article provides a considerably more comprehensive normative justification of differential treatment based on target nationality. We also have different views on a number of issues addressed in the Manpearl article, including its conclusion that the United States should rescind the privacy protections for non-US persons contained in Presidential Privacy Directive 28.

16 Our thanks to Nóra Ni Loideain for suggesting the possible relevance to this project of campaign-related rules based on nationality.

17 Tim Edgar, *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA* (Washington, DC: Brookings Institution, 2017), 169–70. For an analysis of reasons why international law has permitted or supported the use of espionage, see generally Ashley Deeks, "An International Legal Framework for Surveillance," *Virginia Journal of International Law* 55 (2015): 291.

18 Edgar, *supra* note 17, at 170.

19 *Centrum för Rättvisa v. Sweden,* European Court of Human Rights (June 13, 2018), No. 35252/08, available at https://hudoc.echr.coe.int/eng?i=001-183863.

20 We expect to explore these sorts of jurisdiction-related issues in our ongoing work about the Cloud Act, Mutual Legal Assistance Treaties, and cross-border data flows. "Cross-Border Requests for Data Project," Georgia Tech Institute for Information Security & Privacy (June 29, 2018, 10:00 p.m.), available at http://www.iisp.gatech.edu/cross-border-data-project. Swire is also research director for the recently created Cross-Border Data Forum, https://www.crossborderdataforum.org.

21 We are aware of and are concerned about recent actions or proposals in the United States to use nationality to limit access in areas such as education, welfare, and travel. The focus of this article, however, is on justifications that may apply to surveillance activities, and the specific issues of national and international security that go with such surveillance.

22 Manpearl similarly documents the belief of the Framers in social contract theory. Manpearl, *supra* note 15, at 11–14 (quoting Alexander Hamilton that "the origin of all civil government, justly established, must be a voluntary compact.").

23 John Locke, *Two Treatises of Government and a Letter Concerning Toleration*, (I. Shapiro, ed.), (Binghamton, New York: Vail-Ballou Press, 2003), 189.

24 *Id.* at 194 ("And therefore, when the legislative is broken or dissolved, dissolution and death follows."); *id.* at 196 ("[the prince] alone is in a condition to make great advances toward such changes, under pretence of lawful authority, and has it in his hands to terrify or suppress opposers, as factious, seditious, and enemies to the government.").

25 *Id.* at 141–42 ("The only way whereby any one divests himself of his natural liberty, and puts on the bonds of civil society, is by agreeing with other men to join and unite into a community, for their comfortable, safe, and peaceable living one amongst another, in a secure enjoyment of their properties, and a greater security against any that are not of it.").

26 In the wake of cases such as *United States v. Verdugo-Urquidez*, 494 US 259 (1990), there can be disagreements about precisely where the line exists between those who receive Fourth Amendment protections and those who do not, but the law is clear that individuals lacking a strong connection with the United States are outside of the line: "At the time of the search, [the defendant] was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico. Under these circumstances, the Fourth Amendment has no application." *United States v. Verdugo-Urquidez*, 494 US 259, 274–75 (1990).

27 Congress created the distinction in large part as a reaction to intelligence abuses such as the FBI's COINTELPRO, which had surveilled civil rights groups and leaders including Martin Luther King, Jr. See S. Rep. No. 94-755, Book III at 10–12 (1976); see also S.J. Comm. on Gov't Operations, Legis. History of The Privacy Act of 1974 S.3418 (Public Law 93-579), at 794 (Sept. 1976) (94th Cong. Rec. [1974]) (statement of Edmund Muskie) (". . . the "cointelpro" program—the FBI's secret surveillance and disruption of organizations which the FBI considered to be a threat.").

28 "[T]he term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence." The Privacy Act of 1974 S.3418, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as 5 USC. § 552a (a)2). Privacy Act protections were extended for citizens of qualifying countries, including EU member states, in the Judicial Redress Act of 2016. *Professor Peter Swire Testimony in Irish High Court Case, supra* note 1, at 7-4 to 7-5.

29 U.S. v. U.S. Dist. Court for Eastern Dist. of Mich., Southern Division, 407 U.S. 297, 314 (1972).

30 "[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* at 308.

31 Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1783 (1978).

32 The details of each legal standard are provided in Appendix A, "The Legal Standards for Government Access to Communications," in The President's Review Group on Intelligence and Communications Technology, "Liberty and Security in a Changing World," 263–71 (Dec. 12, 2013) (presenting diagrams and text explaining legal standards under various authorities) (hereinafter "The President's Review Group").

33 See Laura K. Donohue, "Section 702 and the Collection of International Telephone and Internet Content," *Harvard Journal of Law and Public Policy* 38 (2015): 117, 144–45.

34 See The President's Review Group, *supra* note 32, at 263–71 (presenting diagrams and text explaining legal standards under various authorities).

35 *Volume II: Field Perspective and Legal Update*, *supra* note 5, at 27.

36 *Id.*

37 See generally *id.* at 40–48 (surveying details of and differences in EU member countries regarding domestic and foreign intelligence laws and practices).

38 As we are not German legal experts, we are grateful for and rely on the detailed accounts, in English, by Dr. Thorsten Wetzling of Stiftung Neue Verantwortung. Dr. Wetzling is a project director on surveillance and democratic governance, at the think tank Stiftung Neue Verantwortung (SNV). See https://www.stiftung-nv.de/en/person/dr-thorsten-wetzling. SNV focuses on digital technologies, politics, and society. See https://www.stiftung-nv.de/en/about-us.

39 Thorsten Wetzling, "New Rules for SIGINT Collection in Germany: A Look at the Recent Reform," *Lawfare* (June 23, 2017), available at https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

40 See *Volume II: Field Perspective and Legal Update*, *supra* note 5, at 28.

41 This practice is under legal challenge. *See supra* note 9.

42 See Wetzling, *supra* note 6, at 14 n. 20.

43 Manpearl, *supra* note 15. For discussion of French practices, see Danny O'Brien, "France's Government Aims to Give Itself—and the NSA—Carte Blanche to Spy on the World," Electronic Frontier Foundation (Sept. 30, 2015) available at https://www.eff.org/deeplinks/2015/09/frances-government-aims-give-itself-and-nsa-carte-blanche-spy-world; *accord* Marko Milanovic, "Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?" EJIL: *Talk!* Blog of the *European Journal of International Law* (Nov. 25, 2013), available at https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/.

44 David Cole and Federico Fabbrini, iCourts—The Danish National Research Foundation's Centre of Excellence for International Courts, "Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders," 5 (2015), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657514.

45 *Id.* at 10.

46 See *Big Brother Watch v. United Kingdom,* European Court of Human Rights, *supra* note 7, at ¶ 518. For discussion of the issue of nationality in the case, see Marko Milanovic, *ECtHR Judgment in Big Brother Watch v. UK,* EJIL:*Talk!* Blog of the *European Journal of International Law* (Sept. 17, 2018), available at https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk.

47 See *supra* note 5.

48 *United States v. Bin Laden,* 126 F. Supp. 2d 264, 274 (S.D.N.Y. 2000), aff'd sub nom. *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157 (2d Cir. 2008).

49 See *Big Brother Watch v. United Kingdom,* European Court of Human Rights, *supra* note 7, at ¶ 518.

50 UN General Assembly, "Universal Declaration of Human Rights," 217 A (III), art. 12 (Paris, 1948), http://www.un-documents.net/a3r217a.htm.

51 International Covenant on Civil and Political Rights, Article 17 (adopted 1966), http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx. The United States has signed the ICCPR, but has consistently taken the view that its provisions do not govern persons outside of US jurisdiction. For instance, in a 1995 statement, the US government stated this position: "The Covenant was not regarded as having extraterritorial application. . . . Article 2 of the Covenant expressly stated that each State party undertook to respect and ensure the rights recognized 'to all individuals within its territory and subject to its jurisdiction'. That dual requirement restricted the scope of the Covenant to persons under United States jurisdiction and within United States territory." Statement of Conrad Harper, Human Rights Committee, Summary of Record of the 1405th Meeting (Mar. 31, 1995), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FSR.1405&Lang=en.

52 Special Rapporteur, "Right to Privacy," delivered to the General Assembly, U.N. Doc A/71/368 at 21 (Aug. 30, 2016), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/71/368. In his 2017 annual report to the Human Rights Council, Professor Cannataci similarly wrote that the global Internet requires a privacy regime that "cannot discriminate between people of different nations, origins, races, sex, age, abilities, confessions, etc. There needs to be a core of rights and values which is consistently respected, protected and promoted throughout the international community." Report of the Special Rapporteur on the right to privacy, *supra* note 12, at paragraph 21.

53 See Report of the Special Rapporteur on the right to privacy, *supra* note 12, at paragraph 44.

54 European Convention on Human Rights, Article 8 (adopted 1950), http://www.echr.coe.int/Documents/Convention_ENG.pdf.

55 "The Council of Europe," Austrian Embassy, Washington, DC (Jan. 14, 2015), https://web.archive.org/web/20150114005241, http://www.austria.org/foreign-policy/europe/the-council-of-europe.

56 Nóra Ni Loideain, "The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law," *Journal of Internet Law* 19, no. 8 (Feb. 21, 2016): 7, 7–8, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2734698.

57 Théodore Christakis, "A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment," *European Law Blog* (Sept. 20, 2018), available at http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment.

58 Christopher Kuner, Christopher Millard, Nóra Ni Loideain, Fred H. Cate, Orla Lynskey, and Dan Jerker B. Svantesson, "An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security" *International Data Privacy Law* 8, no. 1 (2018): 1, 1–3, available at https://academic.oup.com/idpl/article/8/1/1/4980995.

59 EU legal scholar Christopher Kuner has similarly concluded, on the topic of surveillance and nationality, that "the legal situations in the EU and the US are more similar than they might seem." Christopher Kuner, "Foreign Nationals and Data Protection Law: A Transatlantic Analysis," in *Data Protection Anno 2014: How to Restore Trust?* (2014): 213, 220.

60 *See Volume II: Field Perspective and Legal Update*, *supra* note 5, at 33 (setting out "stages of control by ECtHR in the context of surveillance" as a multistep flowchart where Step 1 asks, "Is the case admissible?/"Is there an interference with the right to private life?"; Step 2, "Is surveillance in accordance with the law?"; Step 3, "Does the surveillance follow a legitimate aim?"; and Step 4 "Is the measure necessary in a democratic society?").

61 *Kennedy v. the United Kingdom* - 26839/05 [2010] ECHR 682 (18 May 2010), http://www.bailii.org/eu/cases/ECHR/2010/682.html. See also Nóra Ni Loideain, "A Bridge too Far? The Investigatory Powers Act 2016 and Human Rights Law" in *Law, Policy and the Internet*, 2nd ed. (L. Edwards, ed.), (London: Hart, 2018), ch. 6.

62 See, e.g., Jack M. Balkin, "The Constitution in the National Surveillance State," *Minnesota Law Review* 93, no. 1 (2008).

63 *Cf.* Korff, "Expert Opinion," *supra* note 2, at 55 ("one can basically accept that in situations in which an 'enemy' can be lawfully shot at and killed (subject to the laws of armed conflict and international humanitarian law), listening in to the enemy's communications or hacking into his computer systems may well also be lawful (subject to those same constraints)").

64 A principled justification for continued safeguards, as discussed below, is to limit the surveillance of citizens in order to preserve democracy and reduce the risk of descending into an authoritarian regime.

65 Peter Baker and Jodi Rudoren, "Jonathan Pollard, American Who Spied for Israel, Released After 30 Years," *New York Times* (Nov. 20, 2015), https://www.nytimes.com/2015/11/21/world/jonathan-pollard-released.html; "I Spy, You Spy," *Economist* (June 27, 2015), available at https://www.economist.com/news/europe/21656108-wikileaks-releases-evidence-american-spying-french-say-they-are-shocked-espionage-revealed; Tony Todd, "Paris Also Snoops on US, Says French Former Spy Boss," *France 24* (Oct. 26, 2013) available at http://www.france24.com/en/20131024-nsa-france-spying-squarcini-dcri-hollande-ayrault-merkel-usa-obama.

66 Press Release, Office of the Press Secretary, Presidential Policy Directive PPD-28, Signals Intelligence Activities (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

67 Peter Swire, "The System of Foreign Intelligence Surveillance Law," *George Washington Law Review* 72 (2004): 1306.

68 *Supra* note 31.

69 See, e.g., Tabatha Abu El-Haj, "Friends, Associates, and Associations: Theoretically and Empirically Grounding the Freedom of Association," *Arizona Law Review* 56, no. 53 (2014): 92; Ashutosh Bhagwat, "Associational Speech," *Yale Law Journal* 120 (2011): 978; John Inazu, "The Forgotten Freedom of Assembly," *Tulane Law Review* 84 (2010): 565; "Freedom's Associations," *Washington Law Review* 77 (2002): 639. On the way surveillance and new technologies affect freedoms of speech and association, see, e.g., Peter Swire, "Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment," *North Carolina Law Review* 90 (2012): 1371.

70 See Deven R. Desai, "Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding," *Notre Dame Law Review* 90 (2014): 579, 619–25 (2014) (explaining how unchecked domestic surveillance in the past and present threatens the ability for political opposition within the rule of law).

71 David Gray, *The Fourth Amendment in an Age of Surveillance* (Cambridge: Cambridge University Press, 2017), 152; see also David Gray at 148–55, 165, 169, 171.

72 Paul Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52 (1999): 1609, 1613.

73 For example, the UK's National Cyber Security Centre (NCSC) has recently released a report on "a campaign by the GRU, the Russian military intelligence service, of indiscriminate and reckless cyber attacks targeting political institutions, businesses, media and sport." See "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed" (Oct. 4, 2018), https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed. Sweden reportedly prepared for potential meddling in its election in the summer of 2018. See Erik Brattberg and Tim Maurer, "How Sweden

Is Preparing for Russia to Hack Its Election" (May 31, 2018) (piece commissioned by BBC as an expert report), https://www.bbc.com/news/world-44070469.

74 See 52 U.S.C. § 30121.

75 See 52 U.S.C. § 30121.

76 See, e.g., "Foreign Nationals," FEC Outreach (June 23, 2017) ("The Act does not prohibit individuals with permanent resident status (commonly referred to as "green card holders") from making contributions or donations in connection with federal, state or local elections, as they are not considered foreign nationals."), https://www.fec.gov/updates/foreign-nationals.

77 339 U.S. 763 (1950).

78 339 U.S. at 770.

79 339 U.S. at 770–71.

80 See *Bridges v. Wixon,* 326 U.S. 135, 161 (1945) (Murray, J. concurring) ("But once an alien lawfully enters and resides in this country he becomes invested with the rights guaranteed by the Constitution to all people within our borders. Such rights include those protected by the First and the Fifth Amendments and by the due process clause of the Fourteenth Amendment. **None of these provisions acknowledges any distinction between citizens and resident aliens.**") (emphasis added); *Kwong Hai Chew v. Colding,* 344 U.S. 590, 596 n. 5 (1953).

81 *Bluman v. Fed. Elec. Com'n.,* 800 F. Supp. 2d. 281, 286-87 (D.D.C. 2001), aff'd 132 S. Ct. 1087 (2012) (citations omitted).

82 *Id.* at 288.

83 See Political Parties Act, Section 25(2).3.c (official translation as of March 15, 2009), available at https://www.bundestag.de/blob/189734/2f4532b00e4071444a62f360416cac77/politicalparties-data.pdf.

84 See Canada Elections Act, S.C. 2000, c. 9, § 331.

85 See Knesset Election Law (Consolidated Version), 5729-1969, 23 LSI 110 (5729-1968/69), as amended; *accord* "Party Financing and Elections Financing In Israel, Background Material Prepared at the Request of the Secretary General of the Knesset, Mr. Arie Hahn, for Dr. Thomas Grant, for the Amicus Curiae Brief Submitted to the Supreme Court of the United States Concerning the Mc. Connell v. FEC Case," 6 (July 21, 2003), at https://www.knesset.gov.il/mmm/data/pdf/me00636.pdf.

86 Our thanks to Nóra Ni Loideain for suggesting the possible relevance to this project of campaign-related rules based on nationality.

87 A wide range of writers and experts have recognized the special risks to democracy and freedom that come from surveillance of domestic political opponents and the free press. See, e.g., Privacy International, "Privacy as a Political Right" (2012), available at https://www.privacyinternational.org/report/705/privacy-political-right; Steven Walt, "10 Ways to Tell if Your President Is a Dictator," *Foreign Policy* (Nov. 23, 2016), available at http://foreignpolicy.com/2016/11/23/ten-ways-to-tell-if-your-president-is-a-dictator; Naomi Wolf, *The End of America: Letter of Warning to a Young Patriot* (White River Junction, VT: Chelsea Green Publishing, 2007), 85 ; Sheena Chestnut Greitens, *Dictators and Their Secret Police: Coercive Institutions and State Violence* (Cambridge: Cambridge University Press, 2016), 43–44.

88 See, e.g., Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), 23–26 (distinguishing between authoritarian and democratic models of privacy); Lewis Mumford, "Authoritarian and Democratic Technics," *Technology and Culture* 5, no. 1 (1964): 1–8; (noting a long historical dialectic between "authoritarian" and "democratic" modes of technological development).

89 Peter Swire, "The System of Foreign Intelligence Surveillance Law," *George Washington Law Review* 72 (2004): 1306, 1315–20.

90 U.S. v. U.S. Dist. Court for Eastern Dist. of Mich., Southern Division, 407 U.S. 297, 314 (1972).

91 See The President's Review Group, *supra* note 32, at 154.

92 Hannah Bloch-Wehba, "Confronting Totalitarianism at Home: The Roots of European Privacy Protections," *Brooklyn Journal of International Law* 40, no. 3 (2015): 749.

93 See Robert Gellately, *The Gestapo and German Society: Enforcing Racial Policy, 1933–1945* (Oxford: Oxford University Press,1992).

94 United States Holocaust Memorial Museum, Ministry of Propaganda and Public Enlightenment, https://www.ushmm.org/wlc/en/article.php?ModuleId=10008224 (last visited Dec. 30, 2017).

95 See Amir Weiner and Aigi Rahi-Tamm, "Getting to Know You: The Soviet Surveillance System, 1939–57," *Kritika: Explorations in Russian and Eurasian History* 13 (2012): 5; Amnesty International, *Prisoners of Conscience in the USSR: Their Treatment and Conditions* (1975).

96 For more examples of authoritarian measures of surveillance, see Phil Howard, *Pax Technica* (New Haven, CT: Yale University Press, 2015).

97 Aaron Tilton, "Over 1 Million Russians Could Be Surveillance Targets by Year's End," *Deutsche Welle* (Oct. 21, 2016) http://www.dw.com/en/over-1-million-russians-could-be-surveillance-targets-by-years-end/a-36113272; Nathalie Maréchal, "Are You Upset About Russia Interfering With Elections?" *Slate* (Mar. 20, 2017), http://www.slate.com/articles/technology/future_tense/2017/03/russia_s_election_interfering_can_t_be_separated_from_its_domestic_surveillance.html; see also ECtHR 4 December 2015 [GC], *Roman Zakharov v. Russia,* ECLI:CE:ECHR:2015:1204JUD004714306 (finding flaws in Russian surveillance regime).

98 Jon Fingas, "Russian Censorship Law Bans Proxies and VPNs," *Engadget* (July 30, 2017), https://www.engadget.com/2017/07/30/russian-censorship-law-bans-proxies-and-vpns.

99 Pen Int'l, "Surveillance, Secrecy and Self-Censorship: New Digital Freedom Challenges in Turkey," ch. 3, available at https://pen-international.org/app/uploads/Surveillance-Secrecy-and-Self-Censorship-New-Digital-Freedom-Challenges-in-Turkey.pdf.

100 Erin Cunningham and Hugh Naylor, "Turkish Authorities Granted Emergency Powers Amid 'Cleansing' After Failed Coup," *Washington Post* (July 21, 2016), https://www.washingtonpost.com/world/state-of-emergency-begins-in-turkey-with-new-arrests-of-judges-generals/2016/07/21/604afada-4eb2-11e6-bf27-405106836f96_story.html?utm_term=.f38486f70b02.

101 Agence France-Presse, "Turkish opposition MP jailed for 25 years as part of Erdogan's ongoing political crackdown," *Telegraph* (June 14, 2017), http://www.telegraph.co.uk/news/2017/06/14/turkish-opposition-mp-jailed-25-years-latest-political-crackdown.

102 Privacy International, "The Right to Privacy in Venezuela (Bolivarian Republic of)" (2016), 7, available at https://privacyinternational.org/sites/default/files/2017-12/venezuela_upr2016.pdf; Kieren McCarthy, "Venezuela Increases Internet Censorship and Surveillance in Crisis," *The Register* (May 25, 2017), https://www.theregister.co.uk/2017/05/25/venezuela_increases_censorship_surveillance.

103 Roman Dobrokhotov, "Under Surveillance in Russia," *Al Jazeera* (Nov. 8, 2016), http://www.aljazeera.com/indepth/opinion/2016/11/surveillance-russia-161107133103258.html.

104 Konstantin Benyumov, "How Russia's Independent Media Was Dismantled Piece by Piece," *Guardian* (May 25, 2016), https://www.theguardian.com/world/2016/may/25/how-russia-independent-media-was-dismantled-piece-by-piece.

105 Elena Becatoros, "Turkey's Erdogan Says 'Journalists Commit Crimes Too,'" *Christian Science Monitor* (July 12, 2017), https://www.csmonitor.com/World/Middle-East/2017/0712/Turkey-s-Erdogan-says-journalists-commit-crimes-too; Pen Int'l, "Surveillance, Secrecy and Self-Censorship: New Digital Freedom Challenges in Turkey" (2014), https://pen-international.org/app/uploads/Surveillance-Secrecy-and-Self-Censorship-New-Digital-Freedom-Challenges-in-Turkey.pdf.

106 *Supra* note 102.

107 Although not the focus of the current article, recent news stories have shown the ongoing relevance of strict safeguards for surveillance of the political opposition. Some critics of the Obama administration have expressed concern that surveillance may have improperly "unmasked" persons who worked with the Trump campaign. We have seen no evidence of improper action. Nonetheless, the criticisms themselves show the vital importance of maintaining a credible system to protect against politically motivated surveillance. Going forward, it is worth considering additional transparency and safeguards in the United States to assure the public that such improper surveillance does not take place.

108 Asaf Lubin has reached a similar conclusion, that "in fighting this absolutist battle for universality, human rights defenders are losing the far bigger war over ensuring privacy protections for foreigners in the global surveillance context." Lubin, *supra* note 2, at 509.

109 Edgar, *supra* note 17, at 170. For an analysis of reasons why international law has permitted or supported the use of espionage, see generally Deeks, *supra* note 17.

110 The discussion here is consistent with the approach of Presidential Privacy Directive 28, which applies intelligence safeguards equally, "regardless of nationality," but only "to the maximum extent feasible" in light of considerations such as national security. Press Release, Office of the Press Secretary, Presidential Policy Directive PPD-28, Signals Intelligence Activities (Jan. 17, 2014), available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

111 Greene, *supra* note 3, at 34.

112 *Pisciotti v. Bundesrepublic Deutschland,* EU:C:2018:222 (Apr. 10, 2018), http://curia.europa.eu/juris/document/document.jsf?docid=200883&doclang=en; PETRUHHIN, C-182-15, EU:C:2016:630 (Sept. 6, 2016), http://curia.europa.eu/juris/document/document.jsf?text=&docid=183097&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=593013.

113 Swire has published sworn testimony of more than 300 pages explaining the US system of surveillance law, with comparisons to EU law. *See Professor Peter Swire Testimony in Irish High Court Case, supra* note 1.

The preferred citation for this publication is Peter Swire, Jesse Woo, and Deven R. Desai, *The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance,* Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1901 (January 10, 2019), available at https://www.lawfareblog.com /important-justifiable-and-constrained-role-nationality-foreign-intelligence-surveillance.

About the Authors

PETER SWIRE

Peter Swire is the Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business. He is Senior Counsel with Alston & Bird, LLP. Swire served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Under President Clinton, Swire was Chief Counselor for Privacy in the Office of Management and Budget.

JESSE WOO

Jesse Woo is a 2018–19 Fulbright Fellow and Visiting Researcher at the University of Kyoto, Graduate School of Law, in Kyoto Japan. His research focuses on cross-border data and international privacy regimes, mutual legal assistance, and the foreign policy implications of AI. He was previously a research faculty member at the Georgia Tech Scheller College of Business.

DEVEN R. DESAI

Deven R. Desai is an associate professor of Law and Ethics at Georgia Tech Scheller College of Business. He was the first Academic Research Counsel at Google, Inc., and a Visiting Fellow at Princeton University's Center for Information Technology Policy. His scholarship examines how technology affects privacy law and society's interest in the free flow of information and development.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION