An International Right to Privacy? Be Careful What You Wish For

Stephen J. Schulhofer

NYU School of Law, stephen.schulhofer@nyu.edu

Follow this and additional works at: http://lsr.nellco.org/nyu_plltwp

Part of the Communications Law Commons, Comparative and Foreign Law Commons, Computer Law Commons, Constitutional Law Commons, Criminal Procedure Commons, Fourth Amendment Commons, Human Rights Law Commons, International Law Commons, Internet Law Commons, National Security Commons, Science and Technology Commons, and the Transnational Law Commons

Recommended Citation

http://lsr.nellco.org/nyu_plltwp/508

This Article is brought to you for free and open access by the New York University School of Law at NELLCO Legal Scholarship Repository. It has been accepted for inclusion in New York University Public Law and Legal Theory Working Papers by an authorized administrator of NELLCO Legal Scholarship Repository. For more information, please contact tracythompson@nellco.org.
An International Right to Privacy? Be Careful What You Wish For

Stephen J. Schulhofer*
New York University

Abstract:

The digital era upends many traditional privacy safeguards. Nations now have unprecedented capacity to spy on global communication, and yet they typically acknowledge no legal restrictions on their right to surveil non-citizens outside their borders. People now have little protection against spying by foreign countries, and the realities of incidental collection and inter-governmental cooperation can put their private communications in the hands of their own governments as well.

Privacy advocates recognize the need to plug this loophole, and there is growing support for doing so by a multilateral agreement that would establish internationally applicable safeguards. The present paper concludes that such an agreement, far from strengthening global privacy protection, would almost certainly weaken it. Even among Western democracies, the search for transnational common ground and the institutional priorities of the negotiators would be inimical to a privacy-protective accord. Paradoxically, privacy will be better served by embracing “American exceptionalism” and leaving all nations free to go their own way. The paper discusses the political and economic dynamics that render needed reforms more likely through U.S. domestic law than through international agreements, and the reasons for optimism that such reforms would benefit not only Americans but also the world at large.

Everywhere in the world, twentieth-century safeguards for privacy vis-à-vis the government were radically incomplete. But individuals nonetheless had many practical ways to shield private information. Moreover, government surveillance faced further obstacles because it was for the most part territorially confined, with substantial legal and operational barriers to surveillance outside a nation’s own borders.

The Snowden revelations vividly document how the digital revolution has upended this structure. At the operational level, changes are dramatic. Now, personal information typically is not, and often cannot be, stored entirely at home or even within the physical control of the person*

*I am grateful for helpful discussions with Grainné de Burca and Chris Sprigman.
it affects. Government access to such records and ability to extract revealing personal details from them are exponentially simplified. The conversion of information to digital form also subverted legal safeguards, because data now moves over arbitrary paths; its jurisdictional location in transit and in storage is often unpredictable or unknown.

Although these developments largely work to the advantage of State surveillance capabilities, jurisdictional uncertainty also can inhibit state spying because ambiguity about governing law harms commercial interests, chills inter-governmental cooperation and casts doubt on the admissibility of evidence in court. Law enforcement thus has its own needs for clarification, at the same time that citizens need new means of refuge from state scrutiny.

An emerging consensus holds that the answer to these problems lies in a comprehensive international agreement requiring signatory states to adhere to uniform, privacy-sensitive standards for internet surveillance, with no discrimination between their own nationals and those of other countries.1 That approach is powerfully attractive, both morally and practically; as a substantive matter, it is surely right to frame the issues within the perspective of universal human rights. Yet as a procedural and institutional matter, the turn to an international agreement will sideline the courts, disempower legislative bodies and privacy advocates, defuse commercial pressure for strong privacy safeguards, and create a dynamic controlled almost exclusively by the executive and its national security establishment.

I do not want the fox to design this henhouse. The present paper explains why that would happen in a multilateral process and why its consequences for worldwide privacy are not

---

1 See, e.g., Ian Brown, Morton H. Halperin, et al., Towards Multilateral Standards for Surveillance Reform (forthcoming 2015); David Cole & Federico Fabbrini, Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders, in CONSTITUTIONALISM ACROSS BORDER IN THE STRUGGLE AGAINST TERRORISM (forthcoming 2015); Jennifer Daskal, XXX.
attractive. I argue that in this unique context, national sovereignty and American exceptionalism should continue to frame the search for solutions.

Part I describes privacy protection in the pre-digital world and explains how the digital era has eroded many customary safeguards. Part II summarizes recent proposals for restoring a more privacy-protective environment by means of agreements at the international level. The remainder of the paper argues that these thoughtful proposals are nonetheless unlikely to accomplish their objective.

Although my ultimate concern is for privacy and democracy worldwide, Part III opens the analysis parochially, by arguing that a multilateral approach would be bad for Americans. An international framework would leave U.S. persons less secure than at present for two reasons: in national security matters, any plausible, internationally acceptable agreement will be far less protective than current American law, and American courts would then hold that Fourth Amendment safeguards must give way to internationally agreed standards, even when such standards are more permissive than what American constitutional law would otherwise require.

Part IV moves the discussion to more universal terrain. It argues that international agreements of the kind proposed would be bad for privacy and democracy in the rest of the world as well, because American exceptionalism in digital technology and American commitments to national security oversight can, if left to their own devices, exert a stronger upward pull on global norms than can the terms of any foreseeable international agreement.

I take no pride in speaking well of American exceptionalism. The concept has a well-deserved reputation for moral insensitivity and catastrophic consequences in other contexts. In the setting of the global privacy dilemma, however, the normally powerful attractions of international cooperation and universal conceptions of human rights pose unique problems; the
effort to find international common ground in this area should not be encouraged but instead strenuously opposed.

I. Spheres of Privacy - Before and After the Digital Transformation

In the pre-digital era, safeguards for privacy vis-à-vis the government were at best incomplete. This was true throughout the world. Nonetheless, individuals everywhere who cherished their privacy or sought to shelter parts of their lives from government spying had recourse to many mechanisms of self-protection. Physical facts on the ground typically afforded a refuge, often a better one than the legal rights conferred by statutes and constitutions. Records could be hidden in drawers or under floor boards; walls were opaque. With or without justification or prior judicial approval, any search of a home or office was constrained by material prerequisites -- the personnel and resources necessary to execute it. And insofar as legal rights mattered, an individual traveling from one part of the world to another knew what jurisdiction he was in, and could determine to what extent those legal rights varied as a result.

Governments that sought information outside their own borders typically needed the cooperation of the jurisdiction in which the information was located, cooperation that for many countries was formalized by a Mutual Legal Assistance Treaty (MLAT). Intelligence agencies readily shared information with their counterparts in other nations, but for law enforcement purposes, a government had only limited ability to rely on cooperating foreign police, because the admissibility of shared information in court could depend on compliance with the formal legal arrangements governing assistance on gathering evidence.
No one would think to extoll that world as a privacy paradise. But a person’s pre-digital vulnerability to government surveillance was subject to some degree of oversight, and individuals had at least some opportunities for self-protection.

The information age radically alters this equation. Digital files concerning a person’s health, finances, travel, and consumption are not – and rarely can be – stored entirely within the physical home. Correspondence and other communication records are even more certain to be found elsewhere – in “the cloud.” Although that cloud has a geographic location, ISP users typically do not know where that would be, and in any event they usually have little direct ability to shield their stored records from outside scrutiny.

At the same time, government access to such records has become exponentially faster and cheaper. Dispensing with the team of armed agents needed to execute a search warrant (and even dispensing with the inconvenience of a grand jury subpoena), a government spy can bring those records to his desk with little more than the tap of a finger, and without even alerting the target of the search that the intrusion has occurred.

Surveillance of movement and activity outside the home likewise has become much simpler and cheaper. CCTV cameras enable a single agent to monitor dozens of locations simultaneously and to preserve a permanent record of what happened where and when.² Locational tracking technology permits similar surveillance even when a citizen seeking privacy attempts to obscure his face and identity.

Compounding these enhanced surveillance capabilities, the conversion of information to digital form permits almost limitless, cheap, permanent storage of these sorts of data. Digital

---

² See, e.g., United States v. Jones, 132 S. Ct. 945, 963-64 (2012) (Alito, J., concurring) (“Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case -- constant monitoring of the location of a vehicle for four weeks -- would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. . . . Devices like [GPS tracking], however, make long-term monitoring relatively easy and cheap.”)
data, in turn, lend themselves to relatively inexpensive opportunities to extract links and patterns revelatory of intimate personal actions and associations, matters otherwise invisible even to teams of investigators with unlimited access to the corresponding information in physical form. As David Cole and Federico Fabbrini observe, data mining even enables government to learn one’s inner desires, because it affords access to what one reads and the topics one looks for on the internet. For law enforcement and the intelligence community, digital transmission and storage of information create “force multipliers” that dwarf those associated with high-tech weaponry on the conventional battlefield.

These developments also destabilize legal safeguards. Because data now moves over capricious routes to its destination and because its place of private-sector storage may not even be known, the protections of domestic law and jurisdictional principle erode. Now information often can be accessed from locations that bear little relationship to the nationality of the persons affected or the physical site of pertinent data. Police and intelligence agents can therefore search in another country without ever setting foot in it and (arguably) without meeting the privacy safeguards or legal-assistance procedures of the other country. And since the US, the EU and many other nations do not extend their privacy protections to foreign nationals abroad, the two sets of privacy safeguards – those of the searching country and those of the nation where the search occurs – both may fall by the wayside.

---

3 Cole & Fabbrini, supra note 1, at [MS 12].
4 When a server is located in country Y (and particularly when it is controlled by a company headquartered in country X), a search of the server by country X arguably is not rendered illegal by X’s failure to comply with other-country privacy law and MLAT procedures. In any event, as a practical matter, such non-compliant searches, whether technically legal or not, can be readily executed on a routine basis, with little to no opportunity for oversight under whatever legal regime is nominally in force in country Y. The de facto insulation from legal constraint or oversight is of course doubly certain when country X has no intention to use the resulting information as evidence in court. By contrast, in the pre-digital world, on-the-ground physical gathering of intelligence and law enforcement information was typically difficult and legally constrained in the absence of other-county cooperation.
The Snowden revelations document the consequences. Although NSA’s vast metadata collection program is illegal under U.S. law, its warrantless spying on EU citizens who are in Europe, which includes interception of both metadata and content, appears to be perfectly lawful as a matter of U.S. domestic law, and conversely EU Member States can legally spy on Americans who are in the U.S. That loophole is compounded by two further factors – mutual assistance and incidental collection. Each nation can acquire information on its own citizens through cooperation with foreign intelligence services. Each nation can also acquire information (including content) on its citizens directly, by targeting suspects of unknown nationality (who turn out to be its own citizens) and foreign nationals who communicate with its citizens. From all these directions, the sheltered spaces for private life face unprecedented threats, to the obvious advantage of governments keen to spy.

But law enforcement and the intelligence community face new challenges as well. Global communication multiplies the capacity of extremist groups to recruit and support people prepared to commit acts of violence; new weapons enable isolated individuals to cause great harm; new vulnerabilities result from the cyber-dependent character of contemporary commercial and military infrastructure. Even the legal loopholes that result from jurisdictional ambiguity are a mixed blessing for law enforcement, because uncertainty about governing law can chill private-sector cooperation, impede the rapid acquisition and sharing of time-sensitive intelligence, and cast doubt on the ability to use acquired information in court. Jurisdictional complexity presents other concerns for government as well, because it stands to disrupt the seamless fluidity of the global internet and puts the commercial interests of ISPs in jeopardy.

---

7 TBS.
Law enforcement thus has valid needs to gain a legal imprimatur for its newly powerful surveillance modalities. But at the same time citizens have an urgent need for new ways to preserve zones of private life sheltered from government intrusion. Effective limitations on surveillance power and effective forms of oversight are more essential than ever.

II. Emerging Proposals for Reform

A developing consensus holds that the solution to these problems lies in a comprehensive multilateral agreement requiring signatory nations to adhere to mutually shared principles or uniform standards for internet surveillance. Cole and Fabbrini envision a transatlantic charter, in which the United States and EU member nations would accept common privacy safeguards for counter-terrorism investigations and commit themselves to apply the same standards to their own and each other’s nationals.8 Ian Brown, Morton Halperin and their collaborators propose an even more ambitious framework.9 In their conception, the anticipated international agreement would unite a broader cohort of cooperating states (possibly including nondemocratic states). It would aim to establish for foreign intelligence gathering “a high ceiling rather than a low floor for human rights protection”10 and would include tough threshold requirements for interception and access to stored data, “minimization” to insure that acquired data is used only for its intended purpose, and robust mechanisms for oversight and accountability.11

A clear, internationally applicable framework of this sort would be powerfully attractive. It would permit rapid implementation and assured legitimacy for justified intelligence-gathering while plugging the legal black holes that currently are ripe for exploitation and abuse. A

8 Cole & Fabbrini, supra note 1.
10 Id., at [MS] pp. 3-4.
11 See, id. at [MS] 25-32.
“privacy-conscious” international framework,12 which I shall here refer to as PCIF, would reflect and strengthen international human-rights norms. At the same time, it would meet the commercial needs of ISPs whose business now, inevitably, transcends national borders. And it would preserve the social, political and economic benefits that people the world over have reaped from the unobstructed global internet. Supporters of the PCIF approach include a number of knowledgeable scholars and advocates with a long track-record of good judgment and demonstrated commitment to civil liberties.13 Nonetheless, the present paper sounds some notes of caution and suggests reasons to resist the PCIF solution. The next two sections seek to show that privacy will be better protected, both for Americans and for the world at large, if we resist the lure of a privacy-conscious international framework.

III. Implications for Americans

A comparison of the privacy safeguards available to Americans under current law to those that would apply in a PCIF regime faces at least three hurdles. First, American law is both unclear and in flux. Second, the same is true with respect to the EU member states, not to mention other nations that might be candidates for inclusion in an international treaty. Third, the shape of any agreement that might emerge from multilateral negotiation is inevitably speculative.

Despite this complexity, a few generalizations are broadly accurate and sufficient to move the present discussion forward. First, with respect to national security surveillance, American law -- for all its worrisome flaws -- is unquestionably more detailed and more protective of privacy than its current counterparts anywhere else in the world. This point should not be misread as self-congratulatory American triumphalism. The operational infrastructure and

13 See notes 8-9, supra.
resources dedicated to surveillance by the American intelligence community dwarf those to be found elsewhere, and accordingly the need for limitation and oversight is many times more pressing in the American case. Second, emerging surveillance law reforms, though especially promising in the EU, almost certainly will not alter this basic picture: national security surveillance will continue to be regulated more tightly under American law than it is elsewhere.

This section briefly documents these two benchmarks. The next section then considers the implications of an international agreement that harmonizes divergent national regimes.

A. National Security Surveillance under Current American Law

American surveillance law features six especially important safeguards: (1) judicial oversight, (2) particularized probable cause for threshold authority to gather intelligence, (3) proportionality (absence of less intrusive alternative means of investigation) and (4) generally equal treatment of U.S. citizens and foreign nationals present within the United States.\(^\text{14}\) Fifth, for national security matters of a purely domestic character, the identical requirements apply, with no relaxation of the restrictions governing the investigation of ordinary crime.\(^\text{15}\) Finally, \textit{even when national security has an international dimension}, American law imposes restrictions that remain roughly faithful to these principles of antecedent judicial approval, probable cause, proportionality, and largely parallel requirements for surveillance of in-country foreign nationals.

With respect to “U.S. persons” (both American citizens and foreigners permanently resident in the U.S.), electronic surveillance for national security purposes must be authorized in advance by a judicial warrant based on probable cause to believe that the target is (or “may be”) committing a foreign intelligence crime, such as espionage or international terrorism. Moreover,

\(^{14}\) Identical in ordinary law enforcement and in security matters that have no international dimension. Minor differences in connection with foreign intelligence surveillance, see note xx infra.

\(^{15}\) Keith, Keith dicta and FISA
U.S. persons enjoy these protections in an identical way (at least in theory) regardless of whether they are within the United States or outside U.S. borders. Wherever they may be, they cannot be targeted for surveillance except on the authority of a prior judicial warrant issued on probable cause.\(^\text{16}\) Non-U.S. persons are subject to surveillance under a similar regime of judicial authorization and a particularized (though more relaxed) conception of probable cause\(^\text{17}\) -- but in their case those protections apply only while they remain within American borders.\(^\text{18}\) Relative to the requirements (if any) that other nations impose in national security matters, this is an exceptionally specific and restrictive regime of oversight.

American law nonetheless suffers from three notable weaknesses. First, it extends little-to-no privacy protection to non-U.S. persons who are outside American territory.\(^\text{19}\) Second, it tends to de-emphasize or ignore use restrictions on intelligence once it is gathered. To be sure, American law, unlike that of most other countries, forbids the use in court of illegal intercepts and any of their proximate fruits.\(^\text{20}\) But the “minimization” principles applicable to legally gathered intelligence are not stringent, and in foreign intelligence matters, they are largely secret to boot.\(^\text{21}\) Finally, American law affords radically diminished protection for metadata and other information held by third parties. At least for the moment, Supreme Court jurisprudence places such information beyond constitutional protection.\(^\text{22}\) Statutes fill parts of this gap, but statutory requirements nonetheless stop far short of the limits on acquisition and mechanisms of oversight that apply under U.S. law outside the third-party context.\(^\text{23}\)

\(^{16}\) FAA 701. Note targeting limitation and realities of incidental collection.
\(^{17}\) FISA, expl more relaxed definition of probable cause.
\(^{18}\) Compare FAA 702.
\(^{19}\) FAA 702.
\(^{20}\) Mapp, statute and Warshak with respect to email.
\(^{21}\) Expl minimization.
\(^{22}\) Smith; Jones.
\(^{23}\) At one end of the spectrum, there are strong safeguards for email in transit, though without an exclusionary rule in case of violations. For email content in storage, weaker limits apply, and statutory limits on acquiring metadata,
B. National Security Surveillance Law Elsewhere

No attempt will be made here to canvas surveillance law worldwide. For present purposes, it will suffice to single out the laws of the UK and the EU, as those are the most plausible partners for multilateral negotiation among parties who have some hope of finding common ground.24

EU surveillance law appears to mirror the American picture in two respects but is the opposite in most others. Like the United States, the EU protects foreign nationals in-country but not when they are outside EU borders. Where the regimes differ, EU law appears to be more protective in two respects -- its ambitious use restrictions and its rejection of anything like the American third-party doctrine. But conversely, EU law is weaker than the American in three respects, and UK law may well be weaker across virtually all the relevant dimensions.25 UK/EU law generally does not insist on judicial oversight of surveillance.26 [comment on legislative oversight] UK/EU law is more permissive with respect to surveillance without probable cause.27 And most important for present purposes, UK/EU law for the time being appears to impose virtually no restrictions whatever on surveillance for national security purposes.

This last conclusion is somewhat formalistic. Current UK/EU law may already embody substantial limits on national security surveillance -- limits that are immanent in the ECHR and financial records, health records and the like are weaker still. See Stephen J. Schulhofer, Rethinking the Patriot Act (2005).

24 A few democratic nations outside the EU (e.g. Canada) appear to have strong restrictions on electronic surveillance, but even in those countries, national security exceptions seem to be much broader than those now available to security services in the U.S. And for the great majority of non-EU states, restrictions on national security surveillance are either notably weaker than current or emergent restrictions in the US/EU or are simply non-existent.

25 With respect to use restrictions, UK law is stronger in one respect, in that in categorically prohibits the use of intercept evidence in criminal prosecutions. But UK law apparently does not impose other use restrictions, and even in the context of criminal prosecutions, UK law apparently allows the ample use of intercept evidence as leads to evidentiary fruit that can be admissible.

26 Klass etc.

27 Id.
ICCPR but as yet lack specific legislative and doctrinal recognition. However that may be, it is uncontroversial that UK/EU national security law has no current counterpart to the detailed specificity of U.S. FISA; for now, any UK/EU restrictions on national security surveillance are merely implicit and therefore inevitably speculative by comparison those of the U.S. The next section considers the extent to which these contrasts should be amended in light of the ways that these regimes might be expected to evolve in the foreseeable future.

C. Forthcoming Change

Emerging American developments suggest significant progress in the three areas where U.S. law is weak. The Supreme Court may soon rein in the third party doctrine, at least to some extent. Following on the heels of the Snowden revelations, reports from the U.S. Privacy and Civil Liberties Oversight Board and the recommendations of the President’s Panel of Experts, the President has promised (and Congress may require) greater care with respect to data retention and data-base queries without individualized suspicion; similarly, the President has promised to extend to foreigners abroad most of the safeguards available to U.S. persons. Nonetheless, reasonably foreseeable future developments afford little confidence that the three prominent weaknesses in American surveillance law will be entirely remedied any time soon.

With respect to UK and other European laws governing national security surveillance, emerging ECtHR jurisprudence (and other potential sources of law) probably will impose some safeguards on this hither-to unregulated domain. It is reasonable, however, to predict that such safeguards will likely be less restrictive -- and certainly will be no more restrictive -- than the EU standards applicable outside the national security context. That is, they will -- at best -- mirror ECtHR jurisprudence with respect to ordinary law enforcement, focusing on formal “rule of law”

---
principles rather than substantive limitations. They will emphasize the need for legislative
definition of surveillance powers, but grant member states a wide margin of appreciation and
tread lightly on substantive judicial review of necessity and proportionality. The changes now
on the European horizon are unlikely to meet justifiable concerns for the preservation of needed
privacy in global communication.

In sum, it is oversimplified but largely accurate to state that in the distinctive domain of
national security, the safeguards Americans enjoy against surveillance by their own government
-- however porous or inadequate they may be -- are now and are likely to remain stronger than
those which restrict national security surveillance by the intelligence services of other nations.

One place to which privacy advocates have turned for help is international human rights
law, particularly the right to privacy enshrined in article X of the ICCPR. Scholars have found in
article X a plausible basis for insisting that internet surveillance meet strong threshold predicates
for access to private communication, respect known limits on the retention and use of personal
data, and be subject to independent oversight.\(^2^9\)

Though not to be undervalued or discouraged, this effort will fall short for several
reasons. First, the U.S. government is notoriously inattentive to robust conceptions of human
rights as understood in the international community. Moreover, the international law
scholarship, even on its own terms, is often incomplete, because much of it is framed in terms
applicable to ordinary law enforcement, without taking on board the extra flexibility and secrecy
that is arguably “necessary in a democratic society” in the case of surveillance for national
security purposes.\(^3^0\) And relatedly, to the extent that human rights norms are informed by
prevailing practice in the international community, a fair account of requirements applicable to

\(^2^9\) See, e.g., ECHR art. 8, 213 U.N.T.S. 221, 230 (1950).

\(^3^0\)
national security surveillance would have to acknowledge that the level of protection commonly respected worldwide in this domain is quite minimal. Paradoxically, although much of this recent work has been precipitated by the exposure of massive NSA spying, its conclusions may have only indirect and limited application to that domain.

Perhaps for that reason, privacy advocates have not placed all hopes on international human rights law but instead have urged the negotiation of a privacy-sensitive multilateral framework that signatory states would accept as binding. What, however, can be the expected shape of such an agreement, and where will it leave Americans and others once its provisions enter into force?

### IV. The Dangers of Multilateralism

One obvious obstacle to a broad international agreement is the wide -- probably unbridgeable -- gulf between privacy commitments in the West and in many undemocratic governments. But even within the framework of a narrower US-EU negotiation or one among Western democracies, the complexity of the issues and the diametric opposition between U.S. and other Western approaches suggest that reaching common ground on essential specifics will be arduous and slow. But a more fundamental concern is whether the goal -- an international agreement -- is even worth working for. To be sure, the international perspective is normally more balanced and progressive than the one that dominates in the domestic American setting -- a contrast that helps give “American exceptionalism” its bad name. But the human rights advantages of internationalism are unlikely to be realized in a multilateral national-security negotiation. The concerns are not only the obvious risk of regression to the mean, but also institutional dynamics and the merger of floor and ceiling.
A. Regression to the mean (or below it).

In an international negotiation, conferees might conceivably accept on each issue the most privacy-protective features to be found in any participant’s national regime. They might enshrine the American preference for judicial oversight and probable cause, together with the British proscription against evidentiary use in criminal cases, the broader EU use restrictions and EU norms concerning protection of data held by third parties. Such an outcome is plausible, however, only if each negotiating team puts privacy above other concerns and sets aside its own nationally shaped assumptions about the need to gather national security intelligence.

That does not seem a plausible scenario. The norms emerging from any international negotiation will almost inevitably be situated somewhere between the most protective and least protective conceptions of the participants.

The risks in a truly global negotiation are especially pronounced. The most likely platform for such a negotiation, the International Telecommunications Union, is a UN agency with a membership of 193 countries, including China, Russia, Saudi Arabia and many others whose governments do not share Western commitments to human rights. Any other broadly inclusive framework will similarly include authoritarian regimes determined to preserve their freedom of action with regard to surveillance. The Brown-Halperin proposal, if it envisages a broadly based international accord of this sort, seems especially in need of modification. Cole and Fabbrini are surely right that any agreement tolerably protective of privacy will have to be confined to a US-EU framework, with the possible addition of such Western democracies as Canada, Australia and New Zealand.

31 (as well as over 700 private-sector entities and academic institutions).
In a negotiation among Western democracies, where are the compromises likely to be struck? No one can be certain, but if we are to see the implications of such an accord, informed speculation is imperative. One way to foresee the likely outcome is to focus on the institutional dynamics that would shape multilateral negotiations.

B. Institutional Dynamics

The prospect of an international data-privacy agreement evokes memories of the process that produced the ICCPR and similar human-rights milestones. That picture no doubt contributes to the appeal of a multilateral approach. But responsibility for framing national security surveillance principles will not be entrusted to human rights specialists in the State Department and their counterparts in European foreign ministries. The dynamic will be quite different.

1. The American dimension. Consider first the U.S. side of the negotiating table. Who would lead the American team? The answer is unambiguous and, for privacy advocates, chilling. This will be a job for the national security establishment -- FBI, NSA, the Director of National Intelligence and the White House National Security Council. Hopefully, a State Department representative will be allowed round out the team, but the voices of civil liberties will be at the far edges of discussion. Neither Congress nor the courts will have significant influence on American negotiating priorities. And an executive agreement in the exercise of the President’s Article II commander-in-chief powers arguably could enter into force without legislative involvement or approval at all.32

---

32 If presented as a formal treaty, such an agreement would require ratification by a two-thirds vote of the U.S. Senate; pro-privacy legislators accordingly could hold veto power and would have to be accorded a substantial role in the negotiations. But U.S. practice no longer favors the treaty route in situations of this sort. And an executive concerned to marginalize civil liberties resistance would be sure to avoid it. The alternative to a multinational “treaty” -- and the one certain to be used in this context -- is the “executive agreement.” This path at most requires congressional approval by simple majority, and, as the text above explains, many features of such an executive agreement could enter into force without congressional approval at all.
These pessimistic conclusions require some qualification. Since the President’s Article II powers are not exclusive in this domain but rather are shared with Congress, international standards more permissive than statutes like FISA would have no effect without statutory endorsement. But an ostensibly privacy-conscious framework, once negotiated and agreed upon at the international level, would trigger nearly irresistible momentum for legislation to bring stricter FISA safeguards into conformity with the new multilateral regime.

Another consequence of the U.S. President’s executive-agreement power is even more troubling. For many matters at the center of international concern, FISA does not mandate particular safeguards; rather it delegates responsibility to the Executive. These issues include targeting procedures and other programmatic features of part-foreign/all-foreign interception, as well as minimization, data-retention, and use restrictions for both domestic and foreign interception. A common international framework on these issues would not expressly conflict with FISA and therefore would enter into force without legislative approval. To be sure, Congress is already sidelined to a degree on these matters, but with an important qualification: Both the FISA court and the Congressional Intelligence Committees currently have oversight authority in these areas that they could lose if more porous standards were enshrined in an international agreement. (The next section explains why internationally agreed standards that dilute judicial oversight would override any independent judicial role that might otherwise be constitutionally mandated.)

The upshot is that on the U.S. side, a multilateral approach will give even greater primacy than usual to the national security establishment and marginalize the strongest sources of pro-privacy leverage in the American political and constitutional system. At least from the selfish

---

33 Cf. Hamdan.
34 FISA.
35 See infra.
perspective of Americans concerned to protect *their own* privacy, there is strong reason to prefer a more parochial, go-it-alone strategy.

2. *The European dimension.* An detailed analysis of institutional dynamics on the European side is beyond the scope of this paper, but I will briefly note several parallels and one significant contrast. In rough accord with the American picture, privacy-conscious voices are strong in the UK House of Commons, in the Strasbourg parliament and in the most relevant court -- the ECtHR. In contrast to America, however, a powerful executive body, the European Commission, has shown itself a dedicated and proactive advocate of data-privacy safeguards.

The problems for privacy protection on the European side, however, are the limitations and uncertainties concerning the competency of the Commission relative to that of Member States. Even in “internal” security and law-enforcement matters, and especially with regard to “external” concerns, Commission authority is circumscribed. As a result, any US-EU negotiation would likely be dominated on the European side by Member-State governments -- meaning the Interior Ministries and security services such as MI-5, GCHQ, and their German, French and Spanish counterparts. And even if allowed a leading role, the Commission would be constrained to act under instructions laid down by the Council of Ministers. Either way, the security services will likely exercise considerable control over EU negotiating objectives and the terms of any acceptable multilateral accord.

Would the safeguards resulting from such a process be more permissive than those applicable in the absence of an international agreement? Would Strasbourg, the national parliaments and the ECtHR exercise greater influence on norms articulated at the national and EU levels than they would on international standards negotiated by Member-State governments?

---

36 Reports.
37 Site.
Perhaps there would be no discernable difference, given the dominant power that the security services are likely to exercise in either scenario. But my imperfectly informed guess is that EU institutions are likely to achieve higher levels of privacy protection in a framework internal to the EU than they can realize in a multilateral negotiation dominated on all sides by the security services of the participating States.

C. The Merger of Floor and Ceiling.

To the worry that a multilateral accord could dilute safeguards that would otherwise apply, one possible answer is that an international agreement cannot override minimum constitutional standards as articulated and enforced by U.S. courts and the ECtHR. This answer, however, is inaccurate for three reasons.

First, that answer (that such an agreement would set only a floor of protection), would, if true, defeat the very objective -- inter-jurisdictional uniformity -- that the multilateral accord aimed to produce in the first place. An accord providing only for minimum safeguards would not serve the goals of law enforcement, the security services, and the private-sector ISPs.\footnote{Explain equivalent mechanisms and margin of appreciation.}

To be sure, American ISP executives until now have been forceful voices for data privacy. But that position may not be attributable solely to civil-liberties idealism; American ISPs have commercial imperatives to insure that U.S. privacy safeguards remain robust. Otherwise, the cloud-computing and data-storage business of privacy-conscious consumers will increasingly be dawn to off-shore havens where governments can establish privacy-sensitive regimes for the precise purpose of attracting such business\footnote{Sprigman; examples of this now.} -- the cyber-equivalent of a Cayman Islands tax haven, but in the opposite direction: Inter-jurisdictional variation in tax rates triggers
a race to the bottom, but variation in privacy safeguards will drive a race to the top because the “magic of the marketplace” will tend to draw business to places where data is most secure.  

This commercial dynamic underscores one reason why international uniformity poses such an acute political danger for privacy advocates. So long as surveillance standards vary across jurisdictions, U.S.-based ISPs have a powerful interest in insuring that U.S. safeguards remain as good or better than those of other countries where a competitor could locate. But international or U.S.-EU uniformity would defuse private-sector commercial needs to keep U.S. domestic safeguards strong. That dynamic, in turn, would reinforce other factors that will drive domestic norms downward in a world of uniform surveillance standards.  

One of these is that many salient requirements under U.S. law, though constitutionally inspired, have no firm constitutional pedigree. Safeguards currently mandated under FISA could be relaxed (for example, with respect to minimization and foreign territory interception without raising insurmountable constitutional objections.  

Another factor that connects international uniformity to a downtrend in domestic privacy safeguards is more surprising: Domestic constitutional safeguards would not necessarily trump more permissive international standards, because the domestic constitutional floor would itself migrate downward to reduce discrepancies between the two. This counter-intuitive dynamic is nonetheless likely, because of the peculiarities of the U.S. administrative-search doctrine.  

Foreign intelligence surveillance is a quintessential example of a search that serves “special needs distinct from the ordinary interest in law enforcement.” As such, the Fourth

40 Springman? Forbes?  
41 Of course, any rogue nation seeking to become the Cayman Islands of Privacy would refuse to join a multilateral agreement imposing uniform standards, and that risk is multiplied in the Cole-Fabbrini proposal for an accord between the U.S. and the EU Member States. But the ability of small nations to pursue this strategy would be constrained by the need for a skilled workforce, a cool climate (ruled out the Caribbean) and excellent connectivity not subject to firewalls that ISPs based in the major developed world might be able to deploy.  
42
Amendment’s usual prerequisite of probable cause and a warrant is no longer presumptively applicable; instead the surveillance regime need only satisfy the more flexible criterion of “reasonableness.” Although the Bush administration and the Foreign Intelligence Surveillance Court of Review repeatedly asserted a “foreign intelligence exception” to the warrant requirement, this claim is surely extravagant. The Supreme Court has never approved under the administrative search rubric any warrantless search remotely equivalent in intrusiveness to ongoing electronic surveillance. Any such invasion of privacy could be deemed reasonable only on a strong showing of need and absence of less intrusive alternatives, with ex ante judicial oversight relaxed only to the extent demonstrably necessary. Within this uncontroversial Fourth Amendment framework, something roughly similar to FISA becomes a virtual Fourth Amendment imperative, particularly with respect to surveillance within U.S. borders.

Enter an international agreement. In the administrative-search framework, a pre-existing Fourth Amendment floor will trump the more permissive requirements of a regulatory surveillance initiative when the latter are unreasonable. If adopted only by Congress, relaxed safeguards could deemed unnecessarily permissive and thus unconstitutional. But in the context of an international accord motivated by the complexities of global data transmission and storage, and by legitimate concerns for inter-jurisdictional uniformity, the constitutional calculus would change; pre-existing constitutional norms would not invariably trump lower standards produced by international negotiation. To the contrary, in an administrative-search analysis, the reduced safeguards – if defensible – would likely to pass muster.45

43
44 Sealed Case
45 The above analysis does not encompass surveillance for ordinary law enforcement purposes; in principle, such surveillance is ineligible for administrative search treatment under U.S. law (see City of Indianapolis v. Edmond, 531 U.S. 32 (2000)), and accordingly is ordinarily permissible only with particularized probable cause and a judicial warrant ex ante. That conclusion, however, is fragile with respect to domains that implicate national security, because its logic requires maintenance of a “wall” between foreign intelligence and ordinary law enforcement. Post-
For Europe, similar considerations presumably would be influential at the ECtHR, where receptivity to the margin of appreciation makes this sort of flexibility even more likely.

If the above dynamics are plausible, then the opportunity to negotiate an international accord could become a “make my day” moment for Western security services. Far from propelling uniform, privacy-sensitive norms for US-EU citizens, such a framework would invite negotiators around the table to impose on themselves a surveillance regime more permissive than any to which they would otherwise be subject. This outcome is perhaps not inevitable, but given the structure of a multilateral negotiation, a race to the regulatory bottom seems far more likely than migration toward the privacy-protective top.

In sum, the seemingly attractive prospect of a privacy-sensitive international agreement poses large risks for internet users throughout the world. The remaining question, however, is whether a go-it-alone strategy will offer greater hope or instead will simply leave undisturbed the loopholes that render so much of the American regulatory apparatus toothless, not only for citizens of other nations but even for Americans themselves.

V. Embracing Sovereignty and American Exceptionalism

The absence of uniform international protection creates loopholes that PCIF proposals aim to address. But international agreement plugging those loopholes could not be achieved quickly, and any accord ultimately reached would likely dilute many safeguards now available. It is worth considering, therefore, whether gaps in protection might be addressed more quickly and more effectively without resort to a multilateral framework.

9/11, such a wall is now deemed inimical to effective counter-terrorism, and as a result, the Supreme Court is likely to relax the Edmond line in the counter-terrorism context; indeed lower courts have already done so. See In re Sealed Case.

46 See supra, specifically exposure to other-country spying, incidental collection, intelligence-service cooperation.
From a purely American viewpoint, reform of domestic legislation is most likely to succeed when it is aimed, at least initially, at tightening the safeguards for U.S. persons. This parochial perspective is obviously unappealing in terms of universal human rights, but it is not merely self-regarding; it is grounded in the concept of privacy itself.

Privacy serves, very roughly, two distinct objectives. One is to protect individual autonomy and enable personal growth. The other is to protect democracy by creating sheltered spaces for investigative journalism, political association and dissent. The former goal is jeopardized by surveillance from any direction, but the latter goal is most strongly implicated when citizens face surveillance by their own government. Bracketing for a moment the problem of inter-jurisdictional sharing of intelligence, U.S. data-collection programs pose a far greater risk of chilling political dissent within the U.S. than of chilling political activity by Germans or Canadians critical of their own governments. Thus, it is not necessarily unjustified to insist on especially effective safeguards when U.S. intelligence agencies spy on Americans.

This seemingly parochial point of departure, however, spotlights the urgent need to address the rights of non-U.S. persons – not exclusively for their own sake but because the foreign-target loophole obliterates large chunks of the protection that the U.S. government is strongly obliged to honor with respect to its own citizens. Incidental collection (intelligence on Americans obtained in the course of targeting foreigners and persons of unknown nationality) has become common, indeed virtually impossible to avoid. In theory, it can be addressed to an extent by restricting the U.S. government’s retention and use of U.S.-person information. At the very least, such “minimization” requirements must be made public (at least in part) and tightened to limit the exploitation of U.S.-person information collected during the unrestricted, unchecked surveillance of foreign targets. But this approach will at best prove a highly porous (if not totally

47 SJS METE.
unworkable) band-aid. American self-interest itself should powerfully motivate efforts to plug the foreign-target loophole.

For similar reasons, a new approach is imperative with respect to the regime that governs multilateral sharing. Attainable reform could encompass threshold requirements limiting when U.S. agencies can accept from other countries information pertaining to Americans, and strict minimization to insure that such information is retained and used only when it is related to a legitimate law enforcement or foreign intelligence purpose. Measures like these are within reach, and they would afford U.S. citizens significant protection even in a world where other governments remained free to spy on them at will.

Major elements of U.S. FISA come up for renewal this year, and at least if current political conditions hold, it is not unreasonable consider legislative fixes like these to be achievable in the reasonably near future -- certainly many years before any international agreement could be reached. A vital remaining question, however, is whether reforms of U.S. domestic law, especially reforms giving privileged protection to Americans, would spread more widely and bring non-Americans within their compass.

The leading reason to expect this to happen is less humanitarian than commercial. American ISPs have a compelling, multi-billion dollar interest in retaining the business of foreign customers. To the extent that foreign companies and individuals can get stronger privacy protection from service providers based in their home countries, they will hesitate to use less-protective U.S.-based ISPs. Indeed, market forces have already created opportunities for cloud-computing and data-storage services to establish themselves outside the U.S.48

This threat to the revenue stream of U.S.-based ISPs (and to an important sector of the U.S. economy) may have been a significant factor in President Obama’s recent (though

48
frustratingly vague) declaration that NSA will extend to foreigners the same safeguards that it respects when it conducts surveillance of Americans.\textsuperscript{49} This competitive dynamic is the flip side of that discussed above in connection with proposals for a multinational approach.\textsuperscript{50} Just as international uniformity mutes the commercial need for robust privacy protection in the home country, jurisdictional differences generate private-sector support for privacy-sensitive reform in the home countries. Conversely, of course, for U.S. security service, the non-citizen loophole represents a powerful \textit{advantage}, one they will no doubt be reluctant to abandon. But their opposition to safeguards for non-citizens will be just as strong in connection with PCIF negotiations, with no offsetting push-back from private-sector ISPs, which lose much of their motivation to support strong domestic privacy safeguards once they are assured that competing businesses in other countries cannot offer anything better.

The same dynamic can fuel a relatively simple solution at the international level - \textit{bilateral parity}. Instead of working toward a comprehensive multilateral framework, as contemplated by PCIF, any nation could negotiate a bilateral agreement with any other, with each party merely committing to extend to citizens of the other whatever safeguards it observed in connection with surveillance of its own citizens. The non-discrimination component creates built-in equity, and since this approach does not require either party to adjust its substantive requirements for surveillance, it can produce agreement without the difficult negotiations needed to find common ground in an area where traditions and practices vary so widely even among the democracies.

The concept of bilateral parity parallels to some extent the approach to fair trial procedure reflected in the Geneva Conventions. The Convention Relative to the Treatment of Prisoners of

\textsuperscript{49} See xxx, supra.

\textsuperscript{50} See xxx, supra.
War establishes no common procedural framework for war-crimes trials; it simply requires each signatory to extend to soldiers of the other the same safeguards it observes in trying its own personnel.51

Insofar as predictions can be made in this complex and politically fraught area, it seems that solutions available at the national level, supplemented when appropriate by bilateral parity commitments, can address the global threat to privacy more quickly, with greater hope of adequately protective substantive content, than can a search for a uniform PCIF.

VI. Conclusion

A robust right to privacy remains essential for personal growth and democratic politics. Yet that right is jeopardized by the globalization of communication, the jurisdictional uncertainties that surround the physical situs of data in transmission or storage, and the virtually universal refusal of governments to extend privacy protection to non-citizens abroad. Ideally, an international accord would set uniform or at least minimum standards to protect this essential human right. But the politics, economics and institutional dynamics that would shape such an agreement suggest that the content of an international accord would tilt heavily in favor of security-service preferences and would likely weaken privacy protections worldwide. Paradoxically, global privacy is likely to be better protected if domestic surveillance laws, especially those of the United States, are left to evolve on their own terms, without resort to a comprehensive multilateral framework.

51 See Geneva Convention Relative to the Treatment of Prisoners pf War (Aug. 12, 1949) arts. 102, 106, 108 (requiring that prisoners of war be tried under conditions identical or broadly similar to those applicable “in the case of members of the armed forces of the Detaining Power”).