Massachusetts Institute of Technology
Center for International Studies

Secrecy, Surveillance, Privacy, and International Relations

Workshop Papers

April 2015

The array of issues raised by the revelations by Edward Snowden has shaken the worlds of journalism and think tanks, academia, politics, and even popular culture. It is more than simply shocking, however: the scale of secrecy and surveillance has rocked relationships with key allies like Germany and Brazil, has rattled the reputation of the United States as the leading exponent of democratic values in the world, and has raised a host of issues around privacy, corporate responsibility, and the rationales for secrecy and surveillance. The "Snowden Effect"—the attention and probing that his revelations spurred—is as much an issue of international relations as it is of civil liberties. Indeed, it comprises a set of issues in which political principles of privacy interact dynamically with international relations.

The MIT Center for International Studies convened a distinguished group of scholars and practitioners to address these and other questions pertaining to secrecy, surveillance, privacy rights, and international relations in a workshop at MIT's Endicott House in April 2015. The conferees explored the growth and rationale for secrecy and surveillance, the norms of privacy as necessary to social comity and democratic vigor, how other institutions are affected by the growth of secrecy and surveillance, the costs and benefits of leaks to national security, and how different political systems and societies regard government secrecy in particular. We also consider the technology in use (and the involvement of technology corporations) and how it drives the capacity of states to enforce secrecy, eavesdrop, collect data, synthesize it, and act upon it.

The aforementioned leads to a probe of the international relations dimensions of the controversy, which incurs not only reputational costs but the expectations of benefit in a comprehensive secrecy and surveillance system that can reach the far corners of the globe. How does a "wired" world impact the normal conduct of foreign relations? We examine the norms of privacy in relation to a specific collective need—namely, security—and assess their different and sometimes clashing claims to primacy. Relevant questions include how sovereign states draw red lines against or create openings for surveillance cooperation, and the overreach by states that undermines the implicit bargain of the privacy *v*. security equation. It is already documented that the

security envelope—both secrecy and surveillance—has expanded dramatically, which some argue is without compelling necessity. The temptation to keep snooping and classifying beyond what had been established as reasonable for counter-terrorism not only violates privacy rights, but may aggravate the anarchy of the international system by breaching rules of conduct, alienating allies, empowering adversaries, and intensifying security dilemmas. This international dynamic is primarily what we seek to understand.

::

The conference memos are intended to raise questions and suggest some research and hypotheses. They are not fully formed articles. **Those wishing to cite these papers should ask permission of the authors first**. The papers are in one document, in alphabetical order:

Domestic Politics and the Transparency Norm

Memo prepared for Workshop on Secrecy, Surveillance, Privacy, and International Relations
MIT Center for International Studies, April 16-17, 2015

Daniel Berliner
Assistant Professor, University of Minnesota
Beginning August 2015: Assistant Professor, Arizona State University
danberliner@gmail.com

Transparency has become a powerful international norm over the past several decades, spurred by international advocates, domestic civil society movements, growing recognition in international law, and rapid adoption of access to information policies by governments and international organizations around the world. Access to information is on the verge of being embraced as one of the United Nations' Sustainable Development Goals, successors to the Millennium Development Goals. The Open Government Partnership, launched only in 2011, already has 65 member countries. Even many repressive or semi-democratic regimes pay lip service to transparency in principle, even as they increasingly restrict media and civil society.

But transparency also creates political winners and losers. It has distributional consequences for access to information between groups in power, and groups out of power. Transparency is a thorn in the side of those in power, empowering their opponents, hindering their ability to keep secrets, and increasing the risks of costly scandals.

Under circumstances of limited transparency, groups in power can maintain privileged control over government information for themselves and their allies, thereby monopolizing opportunities to benefit from corruption in public procurement, and minimizing opportunities for oversight that might lead to scandals over negative policy outcomes or outright misuse of office. Full transparency, in theory, means equal access among all individuals and groups – whether in power or not – to government information, thereby leveling the playing field for access to public procurement and tools to monitor officials and hold them accountable. Transparency is thus more valuable to groups out of power than to groups in power. As such, political parties or elite groups in power should be expected to oppose, resist, and delay transparency, unless presented with some countervailing incentives.

Thus, although transparency has enormous rhetorical and symbolic power, and virtually no political actors are willing to speak out in opposition to it *in principle*, those in power routinely delay and resist meaningful transparency reforms, and seek to roll them back when they can. While many examples of the passage of national access to information laws (also called freedom of information or right to information laws) have been hailed as victories for international and/or domestic civil society, there are numerous examples of lengthy delays in the face of concerted campaigns. Such campaigns went without success for years or even decades in countries ranging from Brazil, Indonesia, and Nigeria to Japan, Spain, and the United Kingdom. Other countries, like the Ghana, the Philippines, and Tanzania, continue to delay passing access to information

laws despite repeated promises to do so and increasing pressure from both civil society and international initiatives like the Open Government Partnership.

In many cases, political parties that championed transparency when out of power soon changed their tune once they were in power. Olusegun Obasanjo promised transparency in his 1999 presidential campaign in Nigeria (and had even been on Transparency International's advisory board), but ended up resisting meaningful reforms and even vetoed a freedom of information bill in 2007. The British Labour party demanded transparency reforms throughout the 1990s and, while they did pass the 2000 Freedom of Information Act, it did not come into effect for a full five more years, and Tony Blair ultimately called the law his biggest regret from his time in office.[1] In the United States, the contrast between the Obama administration's promises and its actions in terms of transparency needs little explication.

However, many countries and organizations *have* embraced the norm of transparency and adopted new policies like access to information laws and others. This perspective calls for attention to the countervailing incentives that can outweigh the risks and costs of transparency to those in power. In some cases, international "sticks" or "carrots" fulfill this role. For example, many countries adopted access to information laws in response to pressure from international institutions like the European Union or the World Bank (although in many such cases, the resulting information regimes have been weak in practice). The United States Millennium Challenge Corporation aid program includes freedom of information as one of its criteria.

But in many other cases, the incentives for institutionalizing transparency were endogenous to political interactions in the domestic political system. One important potential incentive for ruling groups to embrace transparency is *insurance*: to ensure that, in case they should lose power in the future, they will not be shut out of access to government information by those who take their place. Since transparency is more valuable to groups out of power, if a group in power expects to be out of power in the future, or faces substantial uncertainty over future political control, then they will face more of the expected benefits (and fewer of the expected costs) of increased transparency in the future.

I have investigated this idea in two empirical studies of the timing of adoption of access to information laws – both cross-nationally (Berliner 2014), and sub-nationally among states in Mexico (Berliner 2015). In both cases I found that adoption was more likely, and occurred sooner, in more politically competitive contexts – where groups in power faced greater uncertainty over their future control of office. In ongoing work, I have also found a similar relationship at the local government level in South Africa: more politically competitive municipalities have better implemented and complied with the requirements of the 2000 Promotion of Access to Information Act (Berliner 2015). Similar findings have emerged in studies of fiscal transparency across countries (Wehner and De Renzio 2013) and among U.S. states (Alt et al. 2006).

[1] "Freedom of Information. Three harmless words. I look at those words as I write them, and feel like shaking my head till it drops off my shoulders. You idiot. You naive, foolish, irresponsible nincompoop. There is really no description of stupidity, no matter how vivid, that is adequate. I quake at the imbecility of it" (Blair 2010, 511).

Two brief examples, from Canada and Mexico, highlight the utility of this perspective. Canada's 1982 Access to Information Act was passed ahead of the Conservative party's widely expected defeat of the sitting government, and at the time was called Prime Minister Pierre Trudeau's "gift" to his successor. This was because "Trudeau would not have to live with the consequences of the legislation produced by his government, but his successor, Brian Mulroney, would" (Savoie 2003, 49). More recently, many attribute the success of recent attempts to limit transparency and weaken the Information Commission to the political dominance of Stephen Harper's Conservative party, which has been in power for nearly ten years.[2]

Mexico's 2002 access to information law was passed two years after the PAN party first took the presidency from the long-ruling PRI, and ultimately developed into a strongly institutionalized transparency regime, used by hundreds of thousands of individuals each year and safeguarded by the independent information commission IFAI. Ten years later, after the PRI retook the executive office in the 2012 elections, the law now ensures continues access to information by PAN supporters, now that they are out of power at the national level. The transparency regime has so far been sufficiently institutionalized to withstand several attempts to weaken it by expanding exemptions from disclosure and limiting IFAI's independence and authority.[3]

There are other possible political incentives for transparency besides insurance, often focusing on benefits to groups in power arising from mechanisms of inter-governmental monitoring. One such possible purpose is to establish decentralized "fire alarm" monitoring (McCubbins and Schwartz 1984) of lower levels of government. This has been offered as an explanation of China's surprisingly robust Open Government Information regulations (Distelhorst 2012, Lorentzen et al. 2014, Piotrowski et al. 2009). The Chinese central government needs cost-effective ways of ensuring that local officials do not threaten social stability through unacceptable levels of corruption, pollution, or abuses of power, and so can rely on information requests from citizens to alert it to such problems. Another possible incentive is for the leading party in a coalition government to monitor its coalition partners, as Michener (2015) has argued in the case of Brazil and other Latin American countries.

Applications to International Relations and Security

While my research has emphasized the domestic political origins of state commitments to transparency, this approach also has implications for understanding the roles of transparency in international relations and security issues.

First, it offers a cautionary warning to studies seeking to analyze the effects of transparency on outcomes like foreign policy, security, or corruption. Transparency is not a "randomly assigned treatment," but rather comes about as a result of political incentives and interactions. If scholars compare political units or contexts with different levels of transparency, and identify differences

[2] See http://www.ipolitics.ca/2014/12/12/the-harper-government-is-killing-access-to-information-slowly.
[3] Just last month, for example, the government introduced 81 last-minute amendments to a new access to information law, but ultimately withdrew 77 of them after domestic and international outcry. See http://www.freedominfo.org/2015/03/mexican-senate-approves-new-access-legislation; http://www.freedominfo.org/2013/08/groups-condemn-amendments-passed-by-mexican-house; http://www.freedominfo.org/2013/08/mexican-house-passes-foi-bill-with-altered-amendment.

in outcomes like foreign policy success or corruption levels, they should exercise extreme caution in attributing such differences to transparency itself. Equally possible, if not more likely, is that the very circumstances that gave rise to increased transparency are also responsible for the differences in outcomes.

Second, this approach highlights the fact that the domestic and international consequences of transparency and secrecy are rarely separable from each other. Most transparency or secrecy policies, whether pursued for domestic reasons, international reasons, or a combination, serve to either enable or inhibit access to information by *both* internal and external actors, and on topics relevant to *both* domestic and international politics. This international-domestic nexus in which transparency and secrecy policies operate means that there will be frequent "spillover" of consequences from one context to the other – often in unintended ways. Scholars and policymakers should also be wary of claims based on the necessity of international secrecy that may mask goals oriented primarily around limiting domestic transparency.

Attempts to enhance the domestic accountability of government to its public can rarely be prevented from also generating unwanted disclosures about foreign policy or national security, or increasing the information available to outsiders. Even though access to information laws around the world all include national security exemptions from disclosure, they are often used nonetheless to reveal scandals about military spending and procurement, or controversial policies like the United Kingdom's role in the CIA's rendition program.[4] China's Open Government Information regulations, while arguably driven by domestic goals of maintaining social stability, have also created new avenues for scholars to gain insight on inner workings of the country's political system (Distelhorst and Hou 2014, Meng et al. 2014).

On the other hand, international threats often spark (or are used to justify) attempts to protect national security by reducing transparency, broadening exemptions to disclosure, making it easier to classify documents, reducing protections for whistleblowers, and increasing penalties for the media. While their impetus may be international, such policies clearly have implications for domestic transparency and accountability as well. This is clear in the recent example of Japan's secrecy bill, which has been called a response to growing international threats from China, but will also empower political groups in power to better keep secrets for their own ends.[5]

Lastly, this approach has implications for attempts to further promote the transparency norm and related issues like whistleblower protections, through new initiatives like the Open Government Partnership and the Tshwane Principles on National Security and the Right to Information. We should expect to see governments' and political actors' commitment to these initiatives and principles driven as much by their own parochial political needs and incentives as by any commitment to the norm of transparency itself, or by pressure from domestic civil society or international advocates.

---

[4] See http://www.theguardian.com/world/2014/aug/16/uk-ambassador-senators-hide-diego-garcia-rendition-cia.

[5] See http://www.bloomberg.com/news/articles/2013-12-06/japan-s-abe-seeks-to-pass-secrecy-bill-that-sapped-popularity; http://www.nytimes.com/2013/11/29/world/asia/secrecy-bill-could-distance-japan-from-its-postwar-pacifism.html.

References

Alt, James, David Dreyer Lassen, and Shanna Rose. 2006. "The Causes of Fiscal Transparency: Evidence from the US States." *IMF Staff Papers*. 53: 30-57.

Berliner, Daniel. 2014. "The Political Origins of Transparency." *The Journal of Politics*. 76(2): 479-491.

Berliner, Daniel. 2015. "Local Government Compliance with South Africa's Promotion of Access to Information Act." Working Paper.

Berliner, Daniel, and Aaron Erlich. 2015. "Competing for Transparency: Political Competition and Institutional Reform in Mexican States." *American Political Science Review* 109(1): 110-128.

Blair, Tony. 2010. *A Journey: My Political Life*. New York: Alfred A. Knopf.

Distelhorst, Greg. 2012. "Publicity-Driven Accountability in China: Qualitative and Experimental Evidence." MIT Political Science Department Research Paper Working Paper 2012-24. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2153057.

Distelhorst, Greg, and Yue Hou. 2014. "Ingroup Bias in Official Behavior: A National Field Experiment in China." *Quarterly Journal of Political Science.* 9(2): 203-230.

Lorentzen, Peter, Pierre Landry and John Yasuda. 2014. "Undermining Authoritarian Innovation: The Power of China's Industrial Giants." *The Journal of Politics*. 76(1): 182-194.

McCubbins, Mathew, and Thomas Schwartz. 1984. "Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms." *American Journal of Political Science*. 28(1): 165-179.

Michener, Gregory. 2015. "How Cabinet Size and Legislative Control Shape the Strength of Transparency Laws." *Governance*. 28(1): 77-94.

Meng, Tianguang, Jennifer Pan, and Ping Yang. 2014. "Conditional Receptivity to Citizen Participation: Evidence from a Survey Experiment in China." *Comparative Political Studies*. Forthcoming.

Piotrowski, Suzanne J., Yahong Zhang, Weiwei Lin, and Wenxuan Yu. 2009. "Key Issues for Implementation of Chinese Open Government Information Regulations." *Public Administration Review*. 69: 129-135.

Savoie, Donald J. 2003. *Breaking the Bargain: Public Servants, Ministers, and Parliament*. Toronto: University of Toronto Press.

Wehner, Joachim, and Paolo de Renzio. 2013. "Citizens, Legislators, and Executive Disclosure: The Political Determinants of Fiscal Transparency." *World Development.* 41: 96-108.

Secrecy, Diffusion, and Democracy

Clifford Bob
Duquesne University and Transatlantic Academy

This memo argues that the ordinary processes through which norms, policies, and laws are generated, institutionalized, and diffused in democratic societies work poorly with regard to secrecy. This poses major problems for democratic accountability and democracy itself.

In the memo, I use the terms norm, policy and law interchangeably (although my preference is to avoid the vague term "norm"). To begin, it is important to distinguish two broad types: substantive and procedural. Most of the international relations literature has focused on the former—e.g., those concerning poison gas, landmines, whaling, etc. By contrast, laws on secrecy are primarily procedural. They affect who is allowed to know certain information and therefore whether and to what extent certain substantive issues may be debated. In this, they resemble meta-level principles regarding participation, which affect who may engage in debate and where. In both cases, they cut across substantive issues—in the case of secrecy, all issues that can be related to "national security." Notably in the United States that term has recently expanded beyond near-term threats to the nation. It now includes long term threats and threats to individual citizens, i.e., Ebola, global warming, terrorism.

Below I first discuss the "normal" process of public debate and diffusion for substantive policy, then examine how these processes are limited in the area of secrecy.

Substantive Laws

Policy and legal change in democratic societies involves contestation among groups with differing views. A legislative or policy outcome—whether stasis or change—happens when sufficient political power is exerted by one or another side. Conflict over major policies occurs at many levels simultaneously—local, national and international. It involves diverse institutions including not just familiar branches of government but also the media, schools, and more. It unfolds over long periods, with particular outcomes only waystations in evolving conflicts that continue indefinitely.

Much of this is open and public. The contending forces conduct campaigns seeking to rally forces, convince undecided sectors, weaken opponents, shape institutions, and engage in long-term "education" favoring their views. The main subjects are the "problem" prompting the debate and the content and effects of the "solution," whether status quo or new policy. Similarly public are the institutional processes through which at least the overt manifestations of policy—the text of new laws—are created (even if key deals may be made in backrooms). After a new policy is

established, there is also ongoing public contestation to promote and demote it. The "losers" seldom give up after their "defeat" (see: continuing conflict over Obamacare). Instead, they and the "winners" seek to shape a policy's interpretation and implementation, sometimes seeking to "capture" the institution charged with executing the policy. They monitor, litigate, and assess it—all from partisan standpoints and to position themselves for the next round of conflict.

Although most of these contentious processes are public, some are secret. Most commonly, rival groups keep their campaigns' evolving strategy secret, to obtain an advantage over the other side and keep their foes from preemptively undermining them. Other aspects of campaigns are hidden to greater or lesser degrees including: the real goals driving the campaigner (as opposed to publicly stated ones); and the use of certain negative tactics against one's foe such as wedge issues, dog-whistle issues, and voter suppression.[1] In addition, in most policy debates, there are information asymmetries at play. It is usually easier for a concentrated player (corporation, NGO, agency) to maintain secrecy than for a broad social movement or "the public" to do so.[2]

The locus of the foregoing processes is the state. In some cases, however, international processes and institutions matter to some degree. This is clearly the case regarding international conventions, although a crucial aspect—implementation—occurs through national-level institutions and contestation. On a more regular basis, international diffusion processes affect domestic policymaking. Transnational NGOs and international organizations seek to influence national processes. Domestic interest groups reference other countries' experiences or demand that their state emulate others. In all these cases, however, the international processes are secondary to and weaker than domestic ones.

Secrecy

In the case of secrecy, contestation is far more limited. Of course, it is important to acknowledge that normal democratic practices such as those sketched above may have established secrecy laws in the first instance.[3] Elected executives and legislatures approved the creation of foundational secrecy regimes and granted significant discretion to national security agencies. Judiciaries have developed or ratified doctrines such as political questions and state secrets that limit their role in particular cases.

---

[1] Secrecy is sought here because these tactics are most powerful when not associated with the campaigner.

[2] The decentralized nature of movements makes them relatively spontaneous, meaning that their strategy may be "secret" because it is always evolving.

[3] In some cases, however, democratic processes may have simply ratified already-existing "emergency" practices.

But even if that is true, the development of secrecy differs significantly from that of other policies. First, it is often difficult to determine the scope or even the precise identity of the problem for which secrecy is the proposed solution. Typically it is framed most broadly as a national security matter for which secrecy is one answer.[4] But unlike military measures directed toward a foe, secrecy affects one's home population as much as the enemy.[5] It limits the ability to debate issues and may make major foreign policy errors more likely (see: Iraq War). This is compounded by the fact that whereas unauthorized leaks violate the secrecy regime and are rare, authorized "leaks" are frequent and biased. Yet in the long run, secrecy and authorized leaks may harm national security more than they help. Fuller public debate could save money and lives. Certainly, the question remains open. Yet the "answer"—secrecy—has already been found and is seldom questioned.

Second, information asymmetries are large, whether debating particular national security issues or the proper amounts of secrecy overall. One of the key parties is highly concentrated—executive and intelligence agencies. The other is the public. The rationales provided by secrecy proponents are themselves shrouded, deliberately, in secrecy. It is said that a particular document should be classified because it is necessary to protect national security, but actual evidence to that effect is seldom provided—because it will threaten security. At a more abstract level, the same argument is made about the entire classification system: it is necessary to protect security. But proof is not offered, and the costs of secrecy are not added to the calculus. For instance, the costs of *not* disclosing information about Saddam's supposed WMDs, a major rationale for the Iraq War, appear huge and growing. Similarly huge are the costs of *not* disclosing information about Qaddafi's ostensible genocide in Benghazi, a key reason for the disastrous Libyan regime change.

Conversely, transparency is claimed to threaten national security, but evidence is rarely provided. In the most obvious cases, leaks, there is much handwringing about alleged damage. But seldom is evidence produced showing actual damage, ostensibly because it must be kept secret in the name of security. Under certain existing statutes forbidding disclosure, there is no need to present evidence of damage or intent.

At a broader level, the content of national security and the threat thereto is seldom analyzed—something that would seem essential in deciding the extent of secrecy or whether particular disclosures should or should not be welcomed. For instance, if it could be shown through the ordinary risk analysis regularly applied to other government programs that terrorism's risk to human life is minuscule, then the

---

[4] Of course for opponents of this view, secrecy is the problem and threatens our security as a *democratic* nation.

[5] Arguably, more so: If we assume that enemies engage in monitoring, they will know everything that citizens know. If we assume that they engage in espionage, they may know more about national security issues than a nation's own citizens.

secrecy (and huge spending) on counter-terrorism would seem inappropriate. Instead, even a small threat is used as the basis for huge amounts of secrecy.

Third, after a secrecy policy is established, continuing oversight is sharply curtailed, primarily to internal executive/intelligence inspectors general and to small numbers of senior legislators. In such circumstances, bureaucratic capture and groupthink are major dangers. Judicial "oversight" through particular cases in controversy is also limited by the doctrines noted above. Thus, the critical feedback loops through which political contestation continues after a policy is established are nearly inoperative with regard to secrecy. Independent monitoring and ordinary democratic debate are limited significantly by the self-interested gatekeepers of secrets.

As a result, secrecy policy includes a powerful ratchet mechanism, leading toward ever greater secrecy. Recent American history exemplifies this, with increases in classification even in the face of reduced threats (see: collapse of Soviet Union) and moves toward greater governmental openness in other areas (FOIA). For those who oppose these trends, fighting them is difficult because of the secrecy surrounding their specifics. One of the few things *not* kept secret are high profile prosecutions and harsh punishments of those who break secrecy rules without authorization (or powerful friends; see: David Petraeus). This is deliberate and intended to bolster the secrecy regime through deterrence of unauthorized disclosures and whistleblowing.

If domestic mechanisms for development and contestation over secrecy norms are short-circuited, it is all the more so for weaker international diffusion mechanisms. It is notable that even NGO promulgators of the Tshwane Principles acknowledge their limits. They claim only that the Principles will be "highly persuasive" with countries that "aspire to comply, and to be seen by the international community to comply, with international law."[6] They "do not think that the Principles will have much impact, at least in the short-term" on countries, including major ones such as the U.S., China and Russia, that have "not shown much interest in compliance with international law, or in the laws and practices of other countries." Even in countries that "aspire to comply," however, the envisioned mechanisms are weak: playing "a role in supporting civil society demands" and "where at least some reformers in government" care about IL compliance. By implication there will be others in government—and civil society—who disagree. The fact that the Principles were established as a result of a long-term processes involving wide consultations—or that certain states adopt them—will (unfortunately) be of little persuasive value to those who oppose them. It is of course possible that long term change in public perceptions about national security and secrecy will change this. But it is hard to

[6] All quotations in this paragraph from Open Society Institute briefing paper, "Understanding the Tshwane Principles," June 12, 2013, http://www.opensocietyfoundations.org/briefing-papers/understanding-tshwane-principles

see how this will happen, and such changes will be fought by those who support the status quo or greater secrecy.

On the other hand, expansion of secrecy through international diffusion among intelligence agencies occurs easily. At the most superficial level, they may emulate one another's classification terminologies and public rationales. But the actual ways in which these are implemented would seem to be secret, limiting the effectiveness of emulation alone. On the other hand, there is much scope for more direct diffusion, through the tight ties that exist among certain intelligence agencies (i.e., Five Eyes; Mossad and U.S.). Coordination and intelligence sharing among them would seem to require covert coordination regarding secrecy norms. Otherwise, potential sharers in one country would fear disclosure in a country with a weaker secrecy regime. This is a powerful mechanism both for direct diffusion of secrecy norms and for continual ratcheting up of secrecy. In other words international diffusion processes, like domestic ones, seem more likely to increase than decrease secrecy, with attendant threats to democracy.

Working Draft for Discussion Only: 6 April 2015
Not for Quotation or attribution or for distribution outside this conference

PRIVACY, SECRECY, SURVEILLANCE: EMERGING ISSUES IN INTERNATIONAL RELATIONS

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CENTER FOR INTERNATIONAL STUDIES
ENDICOTT HOUSE CONFERENCE
APRIL 161-17, 2015

BY JOEL BRENNER

Differences about the meaning and limits on privacy, secrecy, and intelligence gathering, and related conflicts over network security, IP theft, and the governance of electronic networks and information flows have emerged prominently in international relations. These issues, formerly of domestic interest only, are now reflected in international forums, in bi-lateral and multi-lateral negotiations among nations, in the flow of international commercial transactions, and in the application of international trade and competition law. Because these questions involve the rights of nations as well as persons, companies, and groups, they have implications for the exercise of sovereign power both internally and across borders. The meaning of sovereignty in cyberspace, the governance of the internet (which has until now been heavily influenced the United States, which invented it[1]), and the ability to impose legal restraints on the availability of personal information to governments and private actors are all contentious issues, as is the ability of the international trade regime to restrain the theft of intellectual property (IP). Emerging international norms also raise the prospect, for the first time, that intelligence activities may be subject to international norms based in part on the national laws of friendly target countries.

The relationship of communications and information to international security has been on the UN agenda since 1998 and since then has been the subject of regular meetings of a Group of Governemntal Experts (GGE).[2] The topic is also of concern to various governmental and non-governmental

---

[1] By "internet" I refer strictly and only to the system by which data may be exchanged via TCP/IP protocols. The World Wide Web, which enabled the commercialization of internet applications, was the brainchild of Tim Berners-Lee of the United Kingdom.

[2] See United Nations Office of Disarmament Affairs, "Developments in the Field of Information and Telecommunications in the Context of International Security," [n.d.], at http://www.un.org/disarmament/topics/informationsecurity/, accessed April 3, 2015.

institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union (ITU, a U.N. agency), the Shanghai Cooperation Organisation, the European Community (EU) and its various agencies, and companies such as Google, Facebook, and Apple in Silicon Valley. As the most recent report of the GGE notes, "Information and Communication Technologies (ICTs) have reshaped the international security environment."[3] I have not detected any strategic thinking on this topic in the U.S. intelligence community, which is nevertheless much concerned with it at a tactical level.

The aim here is not to delve at length into each of these areas – a large undertaking indeed – but rather to emphasize the existence of a rapidly evolving nexus of issues in international relations that deserves further academic attention. As nations become more enmeshed with each other socially as well as economically, the globalization of information flows is producing two different effects. Among advanced post-industrial nations with a relatively liberal political and social order, it arguably tends to produce a convergence of norms relating to privacy and secrecy – though that is a point to be proven, and the convergence is unlikely to be complete. As between those nations and nations with a high degree of state control over the political and economic order, the globalization of information flows is a source of conflict that threatens the ability of the state to control information within its borders.

The early days of the internet were characterized by a vehemently libertarian, even anarchic, ideology. According to Google's Eric Schmidt, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."[4] The internet connects people and organizations, transforms markets by eliminating middlemen, and subverts hierarchy. Many of its early evangelists asserted its autonomy from external authority or regulation of any kind. It did not take many years for that worldview to be exposed as an anarchic fantasy, but it continues to have hard-core adherents. Cyber "space" is at any rate a powerful

---

[3] GGE, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Report A/68/98, June 24, 2013, at http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98, accessed April 3, 2015.

[4] The quotation is frequently attributed to Schmidt without reference to place or occasion. See, e.g., http://www.brainyquote.com/quotes/quotes/e/ericschmid102325.html. See also "The Cluetrain Manifesto at http://en.wikipedia.org/wiki/The_Cluetrain_Manifesto#Theses_41.E2.80.9352:_Intranets_and_the_impact_to_organization_control_and_structure.

metaphor. It describes an experiential reality not only for players of fantasy games but also for quite normal people in their daily lives. It also describes an actual, not virtual, "domain" of military operations, now fixed in U.S. military doctrine.[5] Yet cyberspace remains a metaphor. As Jack Goldsmith and Tim Wu pointed out in their account of the birth and shattering of "illusions of a borderless world," every part of the internet is owned by someone: servers, routers, wires, transmission towers, switches – everything that makes the internet work, everything that creates the lived illusion of cyber "space" is a physical thing subject to some government's jurisdiction.[6]

Networks are both a means of communication and a means of affecting the physical world. (The current unconscious assumption that the movement of electrons in space or over wires is anything other than physical is likely to be seen as a passing historical curiosity.) The networks themselves and the behavior they enable must be amenable to legal constraint, at least in principle, to the same extent as any other human activity. Whether and to what extent they are technologically amenable to constraint is nevertheless an open question. And the extent of *appropriate* constraint is a proper subject of contention internationally and within democratic nations.

Here are several specific areas of international interest that involve one or more aspects of privacy, secrecy, and surveillance and that would merit academic attention.

1. The governance model

No one owns the internet and no one runs it, exactly. But it would not work without universally agreed technical protocols that permit packets of information to be disassembled, routed, reassembled, and delivered where they are meant to go. The technical maintenance of this system is performed by the International Corporation for Assigned Names and Numbers (ICANN), a not-for-profit California corporation. Among other things, ICANN operates the top-level domain system (authorizing domains such as ".com," ".org," etc.) and the Internet Assigned Numbers Authority (IANA). When you type in an internet address such as www.mit.edu, for example, it must be resolved into a numerical IP address, 172.230.242.131, in order to make the connection. ICANN, through its IANA division, controls that process. ICANN operates under contract with

[5] [TK]

[6] Jack Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (New York: Oxford University Press, 2006).

the U.S. Department of Commerce. Corruption of the IANA system could lead to havoc in international communications.

ICANN has been under systematic attack for its relationship with the U.S. government. While the attack has been spearheaded mainly by members of the Shanghai Cooperation Organisation (SCO), composed of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan, it has also resonated with some U.S. allies. No one seriously suggests that the Commerce Department has interfered with ICANN; its stewardship has been remarkably benign. But the Snowden leaks did nothing to dampen that argument that the internet should be completely separated from any single government. Russia has advocated an enhanced role for the ITU, which has heretofore had nothing to do with the internet. The ITU operates on a one-country-one-vote principle, like the U.N. General Assembly. The Russians favor this because they believe that most developing nations prefer government control over communications. The U.S. and its allies disfavor it for the same reason. Indeed, if it actually occurred, the internet would probably quickly fragment. This issue came to a head at the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, in December 2012, where the U.S. and allied group was heavily outvoted. Without the support of this group, no change could occur, but the result was a significant diplomatic embarrassment. Subsequent meetings of the Net Mundial Multi-Stakeholder Group in Sao Paolo in May 2014, and in Busan, South Korea, in December 2014, produced quite different results but still left a serious cleavage between the democracies and countries such as Russian, China, Iran, and many others that favor further government control and less U.S. involvement in internet governance. At the extreme, Russia has enunciated a doctrine of "information aggression," meaning that the free flow of information into a nation, against the wishes of that nation's government, would constitute a form of aggression under international law. Less radically, the SCO has proposed a Code of Conduct with a "particular focus … on fighting the 'three evil forces' of terrorism, separatism, and extremism.'"[7] These nations define "security" very differently than does the United States, which for that reason no longer uses the term in international negotiations. Russia has also declined to engage with the United States even in the narrow area of crime control on the ostensible ground that it prefers to negotiate over a far wider, and, to the U.S., objectionable, range of issues.

Fifteen years ago, the great majority of internet users were American. This is no longer true. The Chinese are now the largest group of internet users. Because connectivity in the United States is nearly saturated, future growth will

[7] See the SCO website at https://ccdcoe.org/sco.html.

occur mostly in the developing world. The argument for maintaining U.S. control, or at least trusteeship, of ICANN will therefore be difficult to maintain. Against this background, and in an effort to retain the unity of the Western group on matters of internet governance, the U.S. last year agreed in principle to relinquish formal control over ICANN *if* a suitable alternative could be found.[8] The move was immediately criticized from the political right.

Potential Project: Write the concise history of these events, including the evolution of the GGE, and draft strategy and policy recommendations for U.S. government consideration. In the long term, perhaps the medium term, the realistically defensible goal may be to protect the integrity of the system rather than to maintain U.S. control, which to date has been exercised chiefly to protect ICANN from interference. ICANN already has a heavily international governing board.

Potential Project: Many parts of the U.S. government, and different parts of the Department of State, have a stake in this issue. U.S. diplomatic efforts in the lead-in to Dubai were widely seen as poorly prepared. Efforts leading up to Busan, on the contrary, seemed well prepared. How did the government organize itself to focus effectively on this issue? What role, if any, did the NSC staff play?

2. Effect of the governance model on capitalizing internet infrastructure

"Net neutrality" is politically contentious in the United States because it would require a degree of regulation over internet communications not previously seen. But net neutrality involves a free-rider problem because under prevailing technological arrangements, internet content is chiefly delivered over a telecommunications infrastructure capitalized solely by the telecoms. Content providers are dependent on this infrastructure and profit from it but don't pay for it. This issue seems even more acute in the developing world than it is in developed nations, because in many developing nations the problem is not so much *re*-capitalizing the infrastructure but capitalizing it to begin with. Moreover, most global internet content delivery companies are American. To the extent they sell content in foreign markets, wealth is transferred from those markets to the United States. In the developing world, local telecoms tend to be either nationalized or nationally sanctioned monopolies, so their governments can be expected to reflect their viewpoint.

---

[8] [TK]

Potential Project: Is the U.S.'s preferred multi-stakeholder model of internet governance consistent with the interests of these nations? If not, how might that fact affecting the U.S.'s ability to solicit support for that model and for ICAAN? How will these issues be affected (in all nations) as the technology by which content is delivered changes, possibly making delivery possible other than through a telecomm?

3. "Information sovereignty" and data localization

One form of backlash from the Snowden leaks was a movement in a number of countries to "localize" data in order to protect it from U.S. intelligence agencies. There was also a related effort to move business from dominant U.S. companies to non-U.S. companies, preferably domestic. To some degree these efforts reflected genuine concern about surveillance; they also represented opportunities for foreign firms to take market share from U.S. companies. By one assessment, these efforts have cost U.S. business about $120 billion.[9] There are at least two different but related policy challenges here from the viewpoint of a foreign government: to protect information from U.S. intelligence services, and to protect information from U.S. legal process (not necessarily the same thing).

Potential Project: Would the medicine address the perceived illness? The idea that putting data in a foreign commercial server would insulate it from *any* skilled sigint service is mildly amusing, though it would insulate it from U.S. legal process (assuming the server were owned by a foreign corporation with no U.S. presence). The loss of efficiency would seem to be significant, however. Could that loss be quantified? Would the arrangement be even feasible for, say, a U.S. company with operations in both the U.S. and the foreign nation, which would require seamless worldwide operations? A related concern would seem to arise if the recently reported Chinese effort to control foreign connectivity of its scientific community[10] were implemented; for that measure would affect that community's access to foreign information and its ability to engage creatively with the world scientific community. Could that effect be quantified, or at least described in ways that would make its cost appear concrete?

4. The encryption dilemma

[9] [TK]
[10] [TK]

Apple now encrypts communications on users' devices but does not retain a key. Apple's website states:[11]

> Your iMessages and FaceTime calls are your business, not ours. Your communications are protected by end-to-end encryption across all your devices when you use iMessage and FaceTime, and with iOS 8 your iMessages are also encrypted on your device in such a way that they can't be accessed without your passcode. Apple has no way to decrypt iMessage and FaceTime data when it's in transit between devices. So unlike other companies' messaging services, Apple doesn't scan your communications, and we wouldn't be able to comply with a wiretap order even if we wanted to. While we do back up iMessage and SMS messages for your convenience using iCloud Backup, you can turn it off whenever you want. And we don't store FaceTime calls on any servers.

Other companies may adopt similar policies. The government is concerned that widely available communications channels will not be amenable to search even with a judicial warrant.[12] The British government is similarly concerned.[13] The Chinese government is most unlikely to permit such a practice. The possibility of creating a widely available channel of unsearchable communications, which would undoubtedly be a boon to criminals as well as for everyone's privacy, thus creates a clash between powerful imperatives. On the one hand, the government has the power to regulate behavior and enforce order for the general welfare. The prohibition in American constitutional law against depriving persons of life, liberty, or property without due process of law implies that government can deprive persons of those things with due process of law. This is a bedrock proposition of a civilized legal order. On the other hand, many citizens are concerned about the scope of government surveillance of private communications, and the companies that drive the U.S. economy – Apple recently replaced AT&T in the Dow Jones Industrial Average – fear losing business overseas (now their largest markets) as a result of the Snowden leaks. For these companies, demonstrating independence from the U.S. government is a commercial imperative.

---

[11] Apple website at https://www.apple.com/privacy/privacy-built-in/, accessed April 6, 2015.

[12] See, e.g., the statement of FBI Director James Comey, October 16, 2014, FBI Website at http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course, accessed April 6, 2015.

[13] Alex Hern, The Guardian, January 15, 2015, at http://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws, accessed April 6, 2015.

In evaluating these competing interests, one should examine the U.S. situation in context. It would seem rash to believe that the French, Russian, Chinese, British, or Israeli government cannot access encryption developed in those countries. As a practical matter, realistic third-country nationals may well have to determine which nation's government they'd prefer to have easier access to their communications, and on what terms. Markets behavior is not necessarily rational, however; which is why U.S. companies are so afraid of appearing to be the handmaidens of government surveillance. This issue is therefore beginning to look like a replay of a similar but not identical furor in 1996, when the U.S. government decided to permit the export of fairly high-grade encryption on the grounds that if it did not, the world would adopt non-U.S. standards and products. In other words, encryption could not be prevented, so we might as well have the world using American crypts. Susan Landau is an expert on this.

Potential Project: Comparing the current conundrum to the 1996 decision would be enlightening. The situations are similar but not identical. We still do not permit the export of military-grade encryption, for example. Apart from the difficult policy choice, the problem has a technological aspect. Will the type of encryption offered by Apple remain unbreakable? For how long? Assuming how much computing power?

5. Prudent limits on sovereignty?

Microsoft has been served with a warrant under the Stored Communications Act from a federal court in New York to produce the metadata and communications of an Irish citizen. Microsoft nevertheless asserts that the matters sought to be produced are stored on servers in Ireland and that the government should proceed under Irish and E.U. law to obtain what it wants. Under U.S. law, however, a party is personally subject to U.S. jurisdiction if it is physically present here, which Microsoft certainly is. And a party subject to jurisdiction can be order to produce things under its custody and control, even if located outside the jurisdiction. Not surprisingly, the district court held for the government. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 13 Mag. 2814 (SDNY 04/25/14). The case is now on appeal.

The issue is enormously significant, however, because it implicitly presents the question whether the United States would apply the same principle in the mirror-image case. That case is not likely to remain hypothetical for long, because Alibaba, the giant Chinese communications company, has announced

plans to open a data center in California.[14] It is only a matter of time before the Chinese government serves Alibaba with a demand to produce, in China, the communications of U.S. citizens inside the United States and stored by Alibaba in California. For a U.S. court to acquiesce in such a demand (assuming Alibaba challenged it) would be remarkable. But if it did not, the result would be "cognitive dissonance"[15] hardly supportable by a world trading power. The case therefore presents the appellate court with the question of the prudent limits of U.S. jurisdiction. However it comes out, cases like this are driving the re-nationalization of communications control. Microsoft and Amazon already offer enterprises choices about where to store their data.

Potential Project: Measuring the extent to which firms are either intentionally off-shoring, or intentionally on-shoring, data in order to protect it from, or subject it to, a chosen jurisdiction's reach would be illuminating.

Potential Project: Can a principled case be made to distinguish cases like *Microsoft* from black letter jurisdictional doctrine? If not, can we frame a principle of comity or restraint? Should we?

6. Security as a driver of protectionism

The Committee on Foreign Investment in the United States (CFIUS) is an interagency body staffed by Treasury. It is authorized by statute to review transactions in which a foreign party acquires control of a U.S. business to evaluate the potential effect of the transaction on U.S. national security. Observers of CFIUS generally agree that the definition of "national security" has become much more expansive than formerly, particularly as data control and connectivity have become genuine security issues. Many more kinds of cases are caught in the CFIUS net as a result, ranging from a large travel agency to the Waldorf-Astoria Hotel in New York City to the Dubai Ports deal. The available data are skimpy but may support the view that CFIUS' reach has expanded. (CFIUS review does not necessarily imply that CFIUS will object to a deal.) Security

---

[14] Paul Mozur, "Alibaba Expands in Silicon Valley With Its First U.S. Data Center," *New York Times*, March 4, 2015, at http://bits.blogs.nytimes.com/2015/03/04/alibaba-to-open-data-center-in-silicon-valley/?_r=1

[15] Paul Rosenzweig, "Alibaba and the Cognitivie Dissonance of American Data Policy, Techcrunch, March 25, 2015, at http://techcrunch.com/2015/03/25/who-says-alibaba/, accessed April 6, 2015. For Microsoft's view, see the conversation between Jonathan Zittrain and Microsoft's general counsel, Brad Smith, at min. 22-27: of http://cyber.law.harvard.edu/events/luncheon/2014/11/Smith, accessed April 6, 2015.

concerns nevertheless appear to be driving a more protectionist, even mercantile, trade policy, and the process accelerates as the Chinese mirror our measures with a vengeance. That tendency is contrary to the open trade policies of a liberal international order, on which U.S. policy is built. There appears to be developing a conflict between national security imperatives and the commercial imperatives of the world's largest economy.

Potential Project: After describing these developments, and quantifying to the extent that available data permits, it would be useful to propose a principle for limiting the damage. Otherwise the national security exception to the basic policy of open trade would threaten to swallow the basic policy. This problem is difficult, serious, and currently important.

7. Limitations on Espionage-Privacy

In its simplest form, this is the Angela Merkel episode. The German chancellor was communicating in the clear on a Nokia cell phone and by a widely accepted but now disputed account, NSA was picking up the conversations.[16] So, presumably, were the Russian, French, and other services, without objection. Nor did the Germans object to the fact that their leader was communicating in the clear. However, they did object vehemently to the fact that their friends the Americans were listening. For reasons too obvious to require explanation, this was obviously very, very bad. So President Obama telephoned the Chancellor and promised not to do it anymore.

It has always been a basic principle in the intelligence business that intelligence agencies are in business to steal secrets and that they do so by breaking the laws of other nations. It is also an observable tendency, if not a principle, that as nations become more enmeshed with one another commercially, they obey common norms of commercial behavior. From there it is a small step to say that as nations become more enmeshed socially with one another, they will expect one another to obey common norms of behavior regarding the privacy (or not) of their citizens' communications. I have described this convergence elsewhere like this:

> There are no friends among nations, only convergences of interest. This is especially true among intelligence services. It's

[16] For an explanation of why NSA might have been collecting Merkel's communications, see Joel Brenner, "N.S.A.: Not (So) Secret Anymore," at http://joelbrenner.com/n-s-a-not-so-secret-anymore/, accessed April 6, 2015.

> well known, for example, that the NSA and Britain's GCHQ have uniquely close relations in signals intelligence, or Sigint, but the relationship between certain other agencies is stand-offish. (My friends in the business would put it more colorfully.) Our intelligence relationship with the French services has been mostly excellent when it comes to dealing with terrorism, but our Sigint services have historically not got along well. That may be starting to change, and it should. Our interests and those of the French coincide much more than they diverge, and both countries have wasted resources in mutual distrust. Germany is not as aggressive in collecting intelligence as either Britain or France – the Nazi period left Germans with an abiding distaste for all manner of surveillance – but German leaders know better than the German public that as a result of German legal restrictions, German security services have been unable to prevent major terrorist attacks in Germany without American help. That's why the German government is likely to become more measured in seeking changes in U.S. collection practices.
>
> It's time to get closer to both the Germans and the French, but that will require substantial movement on all sides, not just ours. Some have suggested the way to do it is to bring these nations into the "Five Eyes" treaty under which the United States, Britain, Canada, Australia, and New Zealand share intelligence and do not collect against one another. That's a non-starter. The Five Eyes nations share a common language, common legal traditions, and united wartime experiences. They also work side-by-side in in one another's agencies. These arrangements have no parallel and are based on a century of deep trust and experience. It is unrealistic to imagine that Germany and France would suddenly be admitted to the club. A deal with these nations, and perhaps also with the Netherlands and Denmark, should move in stages and begin more modestly, but it is in the interest of all sides that it begin.

Since I wrote that, the Germans have rejected a U.S. proposal for closer cooperation and substantial limitation, saying they wanted a complete "no spy" agreement or nothing at all.

Potential Project: There are four points where convergence may be observable. The first is in negotiations over the "safe harbor" provisions of the current E.U. data regulation regarding commercially held information. The second is in arrangements between E.U. nations and the United States over government-to-government information sharing. Those arrangements may be further affected by a pending E.U. directive on this subject. The third is in negotiations over the Transatlantic Trade and Investment Partnership, known as TTIP. The fourth pertains to a series of multilateral assistance agreements for information exchange (MLATs). The procedures under these agreements are cumbersome and time-consuming and hinder investigations of terrorism and cyber crime. There have been proposals to amend them in both Europe and the United States.

8. The Problem of State-Sponsored IP Theft

Late last year I argued that state-sponsored IP theft is a plague on post-industrial economies that offends accepted principles of the international trading order, as enshrined in the portion of the World Trade Organization Treaty of 1996, known as TRIPS. TRIPS deals with "Trade-Related Aspects of Intellectual Property Rights." I proposed measures aimed at strengthening the multilateral system of political norms that apply, or should apply, to state-sponsored IP theft.[17] On April 1, President Obama issued an executive order that could provide relief against some forms of cyber crime and theft of IP.[18] The order permits the government to freeze the assets of anyone who engages in, *or who is complicit in*, cyber attacks from abroad that harm or attempt to harm organizations "in a critical infrastructure sector."

Potential Project: In what kinds of cases would relief under the executive order become practically available? If the Treasury secretary took action under the order, and if an affected nation took the United States to the WTO on a complaint, would the action stand scrutiny under the treaty?

Conclusion

These issues, which are hardly exhaustive, are playing out in bi-lateral and multi-lateral agreements, including the GGE, WTO, national courts, and various forums devoted to internet governance. They are affecting trade – the impending E.U. case against Google will certainly do so – and they are subtly influencing cooperation among intelligence agencies. While some of these issues have a technical legal side, they are fundamentally policy challenges, and they will be dealt with most effectively through diplomacy. Many of these issues offer opportunities to bring policy, technical, and legal expertise together in interesting ways.

---

[17] Joel Brenner, "The New Industrial Espionage," *The American Interest*, December 10, 2014, at http://www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/, accessed April 6, 2015.

[18] The White House, Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Actvities," at https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m, accessed April 6, 2015. See Joel Brenner, "Bringing out the Big Stick," at http://joelbrenner.com/bringing-out-the-big-stick/, accessed April 6, 2015.

Surveillance law in the UK

Prof. Ian Brown, Oxford Internet Institute, University of Oxford, UK

The UK does not have a codified constitution setting out citizens' rights, or allowing a constitutional challenge to government surveillance. These protections – and public authorities' powers to access, share and use personal data – come mainly from the statutes described in this memo, alongside EU and international law.

1.1 Data Protection Act 1998

The main legislation controlling access to and use of personal data is the Data Protection Act 1998, which implements the EU's Data Protection Directive. All personal data processing (by both government and private sector organisations) must comply with the eight principles in Schedule 1 of the Act, which mirror the OECD "fair processing" principles.

There is an almost complete exemption for matters certified by Ministers as relating to national security, a term that has been broadly interpreted in UK law. In a leading case, the Court of Appeal agreed with a government submission that it "is a protean concept, 'designed to encompass the many, varied and (it may be) unpredictable ways in which the security of the nation may best be promoted'."[1]

Data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty, is exempt from the first data protection principle (conditions for processing data), the subject access provision, and the non-disclosure provisions (principles 2-5) to the extent they would be likely to prejudice these matters (s.29).

1.2 European Convention on Human Rights and the Human Rights Act 1998

The UK is a signatory to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Article 8 protects private and family life, homes and correspondence.

Under general principles of the Convention, any restrictions on rights must be based on published, clear and specific legal rules; serve a legitimate aim in a democratic society; be "necessary" and "proportionate" to that aim; not involve discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, nationality, property, birth or other status; not confer excessive discretion on the relevant authorities; and be subject to effective safeguards and remedies.[2]

Ministers must certify whether bills introduced into Parliament are compliant with the Convention rights. The senior UK courts may declare that a statute is incompatible with a Convention right, requiring Ministers to consider and potentially change the statute – but this declaration "does not affect the validity, continuing operation or enforcement of the provision in respect of which it is given" (s.4).

---

[1] *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153

[2] D. Korff and I. Brown (2010) *New Challenges to Data Protection*. European Commission: DG Justice, Freedom and Security.

1.3 EU Charter of Fundamental Rights and the European Communities Act 1972

The UK must comply with the Charter of Fundamental Rights when it is acting within the fields of EU law. Articles 7 and 8 of the Charter protect privacy and data protection rights. This obligation is strongly constrained in relation to national security by Article 4(2) of the Treaty on European Union, and less emphatically in relation to preventing and detecting serious crime, and protecting the economic well-being of the UK.

1.4 Regulation of Investigatory Powers Act 2000

Part I Chapter 1 of the Regulation of Investigatory Powers Act 2000 (RIPA), as amended by the Data Retention and Investigatory Powers Act 2014 and Counter-Terrorism and Security Act 2015, allows a Secretary of State to authorise the interception of the communications of a person or premises over a public telecommunication system.

An interception warrant may be requested by the Security Service (domestic intelligence), Secret Intelligence Service (foreign intelligence), Government Communications Headquarters (signals intelligence), National Crime Agency, the police, HM Revenue and Customs (taxation), Defence Intelligence or other national government bodies under a treaty obligation.

A warrant need not specify a person or premises if it relates to the interception of communications external to the UK, which is the mechanism by which the government authorizes GCHQ to undertake broad automated searches of communications that originate or terminate outside the British Islands. This includes the transmission of data to or from servers outside the UK.

Documents leaked by Edward Snowden show that such warrants are wide-ranging. They can cover classes of traffic such as ‘all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe’, with the Secretary of State then issuing a certificate describing in general terms which information should be extracted from the resulting intercepted communications. It has been reported that ten “basic” certificates exist, covering broad categories of data such as “fraud, drug trafficking and terrorism”. This allows intelligence officials to undertake automated searches through this information looking for specific keywords.

Interception must be undertaken for one of the following purposes:

1) in the interests of national security;
2) for the purpose of preventing or detecting serious crime;
3) for the purpose of safeguarding the economic well-being of the United Kingdom;
4) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

Intercepted information is expressly excluded from legal proceedings (s.17) to prevent interception methods being revealed in court. It can only be used for intelligence purposes.

Access to "communications data"—metadata such as subscriber information, records of calls made and received, e-mails sent and received, websites accessed, the location of mobile phones—is regulated under Part I Chapter II of RIPA. A very large number of central and local government departments are able to access communications meta-data by having a senior official authorise a request to a Communications Service Provider. The Interception of Communications Commissioner commented in his 2004 report that: "In addition to the agencies covered by Chapter I of Part I of RIPA, and the prisons (138 in number) there are 52 police forces in England, Wales, Scotland and Northern Ireland and 510 public authorities who are authorised to obtain communications data, all of whom will have to be inspected. This is clearly a major task."[3] In 2013, 514,608 requests for communications data were approved.[4]

Section 37 of the Protection of Freedoms Act 2012 requires that local councils obtain judicial approval from a magistrate before accessing communications data.

Communications data can be accessed for the following purposes under s.22(2) of RIPA:

a) in the interests of national security;

b) for the purpose of preventing or detecting crime or of preventing disorder;

c) in the interests of the economic well-being of the United Kingdom;

d) in the interests of public safety;

e) for the purpose of protecting public health;

f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

h) for any purpose [not falling within paragraphs (a) to (g)] which is specified for the purposes of this subsection by an order made by the Secretary of State.

It is not yet completely clear how monitoring of social media fits into this framework, but it has been suggested that public authorities monitoring private information in public media spaces – for example, building a detailed profile of a user from several openly available sources – would need authorisation for "directed surveillance", and those using fake or anonymous accounts, especially to elicit information, for "covert human intelligence".[5]

1.5 Other surveillance powers

Physical interference with property to plant a bug must be authorised by the Secretary of State under s.5 of the Intelligence Services Act 1994 (for MI5, MI6 and GCHQ) or senior police or HM

[3] The Right Honourable Sir Swinton Thomas, *2004 Annual Report of the Interception of Communications Commissioner*, HC 549, London: The Stationary Office, Ordered by the House of Commons to be printed 3 November 2005, p. 5.

[4] The Right Honourable Sir Anthony May, *2013 Annual Report of the Interception of Communications Commissioner*, HC 1184, Ordered by the House of Commons to be printed 8 April 2014, p.22

[5] J. Bartlett, C. Miller, J. Crump and L. Middleton, *Policing in an Information Age*, London: Demos, March 2013, pp. 27—30, at http://www.demos.co.uk/files/DEMOS_Policing_in_an_Information_Age_v1.pdf?1364295365

Revenue and Customs officers under Part III of the Police Act 1997. When material of a legally privileged, confidential or journalistic nature could be acquired, a Surveillance Commissioner must approve police authorisations under s.97.

Agencies are also able to remotely break into computer systems to access communications and other types of data on those systems. Section 10 of the Computer Misuse Act 1990 (CMA) exempts law enforcement powers of inspection, search and seizure from its prohibitions on unauthorized access to computer material.

Section 94 of the Telecommunications Act 1984 allows the Secretary of State to give public electronic communications networks "directions of a general character as appear…to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom". Very little is known about the use of this broad power. The Interception of Communications and Intelligence Services Commissioners appointed under RIPA have both told the UK Parliament they do not oversee its use.[6]

[6] Home Affairs Committee – Seventeenth Report, *Counter-Terrorism*, 30 April 2014, §175, available at: www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

The Tshwane Principles on National Security and the Right to Information: Their Origins, and Steps Towards Norm Development

for Workshop on Secrecy, Surveillance, Privacy, and International Relations,
MIT Center for International Studies, April 16-17, 2015

Sandra Coliver, Senior Legal Officer, Freedom of Information & Expression
Open Society Justice Initiative, Open Society Foundations
www.opensocietyfoundations.org/search?key=coliver www.right2info.org

The Tshwane Principles on National Security and the Right to Information set out detailed guidelines for those engaged in drafting, interpreting or implementing laws or policies relating to the state's authority to withhold information on national security grounds or to punish the disclosure of such information.[1] They were issued by a group of 22 civil society organizations and academic centers in June 2013. Since then, they have been endorsed by several intergovernmental bodies and experts, and have been credited with influencing secrecy legislation in a few countries.

This paper provides a summary of the process that led to their drafting, and how they are expected to shape future policy. An annex provides information about the substance of the Principles.

Origins of the Tshwane Principles

In 2010, the Justice Initiative, an operational program of the Open Society Foundations, began to explore how it could best help civil society groups around the world that were trying to prevent adoption of overbroad state secrecy laws and gain access to information of high public interest (including about the CIA's extraordinary rendition program) that governments were keeping secret.

A number of countries had recently adopted, or were in the process of adopting or revising, state secrecy, classification and related laws, sparked by several developments. Perhaps most significant had been, and continues to be, the rapid adoption of access to information laws since the fall of the Berlin Wall, when only 13 countries had such laws, with the result that, as of the date that the Principles were issued, more than 5.2 billion people in 95 countries around the world enjoyed the right of access to information, at least in law, if not in practice.[2] People in these countries were—often for the first time—grappling with the question of how provisions on national security secrecy should be interpreted and applied given the new presumption set forth in most access to information laws that information held by public authorities should be available to the public. States also have been considering ways to tighten controls on sensitive information in response to post-9/11 security-related threats. Some states have claimed that the US and other countries have conditioned intelligence sharing on more stringent information control practices.

International law on these issues is not well developed. While the main UN and regional human rights treaties state that the right to freedom of information may be restricted where

[1] For the text of the Principles, papers that support them, and endorsements of them *see* http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-6.
[2] As of April 2015, 104 countries have access to information laws in force. See http://www.right2info.org/laws/constitutional-provisions-laws-and-regulations.

necessary to protect national security, neither the treaties, nor authoritative interpretations, nor case-law has provided guidance on what constitutes national security for purposes of restricting information, or on how the competing interests should be weighed. Cases that have addressed the issue have simply deferred to executive claims of national security-based necessity.

The most relevant guidance on these issues, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, had been drafted in 1995 by a group of some three dozen experts convened by Article 19, the International Center Against Censorship.[3] However, in 1995 the international right of access to information was in the early stages of its development, and thus only eight of the Johannesburg Principles deal with access to information and only in broad terms.

After consulting with Article 19 and several other groups and experts, the Justice Initiative decided that a set of principles with norm-creating potential could be valuable if:

1) sufficiently detailed to be useful to those engaged in drafting, revising or interpreting laws and policies;
2) practical, in that they should not impose undue burdens on those tasked with implementing them; and
3) based on international and national law, standards and good practices (understood to refer to those practices that aim to give effect to the right to information held by public authorities to the maximum extent possible, while also protecting legitimate national security interests).

The Drafting Process

The Justice Initiative embarked on a drafting process that was widely consultative in order to make the principles as clear and useful as possible to people working in different regions and contexts; strengthen their legitimacy; and increase the number of people and organizations that would work to get them endorsed and implemented.

At the outset, the Justice Initiative invited nine academic centers and international and national NGOs with relevant expertise to join as co-drafters. As the drafting progressed, they collectively invited another 12 to join. They decided not to invite the main human rights advocacy organizations (such as Human Rights Watch and the ACLU), in order not to alienate government officials and professional associations who might otherwise be interested in the project. They did, however, consult these groups, which well understood the reasons for their exclusion; most of them have already referenced the Tshwane Principles in relevant publications and advocacy campaigns.[4]

---

[3] I was Article 19's Law Program Director at the time, and coordinated the drafting of the Principles, drafted a commentary setting forth their basis in international and national law and practice, and co-edited a book of papers that provided support for the Principles. *See* Secrecy and Liberty: National Security, Freedom of Expression and Access to Information (Martinus Nijhoff Pubs. 1999). The Johannesburg Principles were welcomed and circulated by the UN Rapporteur on Freedom of Expression, translated into more than a dozen languages, and widely cited by NGOs and academics and even a few courts. UN offices continue to transmit these Principles to governments when requested to provide advice concerning the drafting of laws or policies concerning the classification of information.

[4] In the end, Amnesty International was invited to join as a co-drafter because of the extensive engagement of Amnesty's staffers in helping to draft Principle 10, concerning the presumption, and in some cases the requirement, that information about human rights violations should be disclosed.

Over a period of two years, the drafters held a total of 14 meetings around the world with more than 500 civil society activists, former and current government officials and security professionals, academics and other experts. The Justice Initiative commissioned more than two dozen papers from experts in Africa, the Americas, and Asia, in order to identify trends and good practices;[5] and worked with a Danish academic to conduct a comparative study of law and practice in 20 European states.[6]

The drafting period lasted nearly two years in part in order to increase the engagement of security and intelligence professionals, many of whom expressed interest precisely because they were consulted during the drafting process rather than confronted with a fait accompli. Some of these security professionals are now talking with the Justice Initiative about how to promote and implement key principles, including a colonel in the Senegalese Armed Forces tasked with working to improve civil-military relations and security sector governance in West Africa, and some former intelligence officials in South Africa.

Resolution of Disputes Concerning Concepts and Language

Almost every one of the 50 Tshwane principles was debated extensively. Following are a sampling of questions with which the drafters grappled:

- Should the document be crafted as a set of principles, practical recommendations, or best practices? Should any of the principles be phrased as mandatory?
- How should "information of public interest" be defined?
- Should "national security" be defined? At the least, should a negative definition be included of what "national security" does not include?
- Should the Principles include a list of information that may legitimately be withheld from the public? If yes, should the list be exclusive or illustrative? If exclusive, should information about a state's economic well-being be included?
- If information about human rights and humanitarian law violations should never be classified on should be proactively released, how can the privacy of victims be protected?
- Should whistleblower protections be available only for people who disclose information tending to show wrongdoing, or also information important for public debate? Should good faith be a requirement to avail oneself of the public interest defense?
- How should the Principles address the concern that a public interest defense is unworkable given that it affords civil servants and members of the armed forces discretion to decide what information is in the public's interest to be made public?

At the meeting to finalize the Principles held in Tshwane, South Africa, working groups addressed these and other questions, and were able to achieve consensus on most of them. The Justice Initiative was authorized to make decisions in the few cases where consensus could not be reached.

---

[5] See Papers in support of the Tshwane Principles, at http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-6.

[6] Amanda L. Jacobsen, National Security and the Right to Information in Europe (2013). Individual country questionnaires: Albania, Belgium, Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, United Kingdom.

Endorsements and Expectations for Impact

Efforts to promote the impact of the Principles are in their early stages but appear to be progressing. The aim, ultimately, is for the Principles to influence states – governments, legislatures, courts – in drafting, interpreting and applying laws, regulations and policies that advance the right of the public to information of public interest to the maximum extent while protecting legitimate national security interests. The strategy is first to obtain endorsements from individuals, inter-governmental bodies, professional associations, and other organizations that are likely to have influence in persuading states to incorporate some of the principles into national law; and then to work with in-country actors in states that are most likely to be susceptible to such influence to reform laws consistent with the Principles – the "low hanging fruit" approach. States are most likely to be amenable to influence where a) leading officials are interested to comply, or be seen to comply, with international standards and best practice; b) a few key actors (in one or more branches of government) were engaged, or familiar, with the Tshwane Principles process, or respected one or more of the co-drafters; and c) legislation is being debated in the country, or challenged in court, that would affect practices addressed by the Principles.

The Justice Initiative thus decided to engage all of the relevant Special Experts – on freedom of expression, media freedom and counterterrorism measures – of the UN, OAS, OSCE and African Commission on Human and Peoples Rights in the drafting process. Two of them participated actively in the finalization meeting. When the Principles were launched, all five experts issued statements endorsing them, and several have since referenced them.

Also at the finalization meeting, and at the main European regional meeting, was a staff member of the legal secretariat of the Parliamentary Assembly of the Council of Europe (PACE), comprised of 318 parliamentarians chosen from and by the parliaments of the Council's 47 member states. Largely through his efforts, the PACE endorsed the Principles in October 2013 and, among other things, "call[ed] on the competent authorities of all member States of the Council of Europe to take them into account in modernising their legislation and practice concerning access to information." In March 2014, the Parliament of the European Union endorsed the Principles for guidance both on transparency as a component of democratic oversight in the field of intelligence and on protection for unauthorized disclosures of national security information. The PACE will consider, and is expected to pass, a resolution in June of this year calling on the United States to allow Edward Snowden to return home "without fear of criminal prosecution under conditions that would not allow him to raise the public interest defense."[7]

The Tshwane Principles are also being used in the Open Government Partnership process. The reviewer of Guatemala's national action plan called on the state to incorporate relevant Tshwane Principles in order to reform its national security classification system.[8] The Illustrative Commitments on Security Sector Transparency, included in an Open Government Guide to suggest the sorts of commitments that would be appropriate depending on a country's level of development, are based on the Tshwane Principles;[9] and the Illustrative

[7] See Coliver, "Europeans Urge United States to Allow Edward Snowden a Public Interest Defense," Mar 19, 2015 http://www.opensocietyfoundations.org/voices/europeans-urge-us-allow-edward-snowden-public-interest-defense.

[8] Report on Guatemala's national action plan: http://www.opengovpartnership.org/country/guatemala/progress-report/report.

[9] See Open Government Guide, Security Sector, at http://www.opengovguide.com/topics/security-sector/.

Commitments on Whistleblower Protection reference the Tshwane Principles concerning security sector whistleblowers.[10]

The UN Resource Guide on Good Practices in the Protection of Reporting Persons, soon to be released by UNODC (UN Office of Drugs and Crime) will include excerpts of, and recommend, relevant Principles in a section on national security whistleblowing.

The UN Human Rights Committee, in its 2011 General Comment No. 34, provides an authoritative interpretation of the right to freedom of expression and information. It asserts emphatically, reflecting comments submitted by several of the Tshwane drafters, that states may not, consistent with international law, "suppress or withhold from the public information of legitimate public interest that does not harm national security." That statement marked a significant advance over previous, norm-creating UN statements. Moreover, states may not "prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information." It is implicit that this duty extends even to information that has been formally classified.

The Principles have already played a role in influencing legislation in at least two countries. In South Africa, the Right to Know Campaign, supported by some 400 organizations and 30,000 individuals, credit the Tshwane Principles with having considerably strengthened their advocacy to mitigate problematic aspects of South Africa's Protection of State Information Bill, introduced to the National Assembly in June 2010. Becoming the most controversial Bill pushed by the Zuma administration, it was actively debated for more than three years before finally being adopted with significant reforms – although far from adequate in the view of many civil society organizations – in December 2014. It is expected to be signed into law by President Zuma within the next few months. Several factors account for the Tshwane Principles' influence, even while they were still being drafted. First, a respected research center, the Institute for Security Studies, co-hosted a meeting to discuss an early draft of the Principles with current and former justice and security officials, including Mandela's still highly respected first Minister of Intelligence Ronnie Kasrils, academics and civil society researchers in Cape Town in October 2010. One of the intelligence officials who participated, and whose attitude changed from defensiveness to collegial engagement, then became the government's chief point person on the Bill. Second, the Principles were seen as an elaboration of the Johannesburg Principles, which have particular salience in South Africa, given their provenance. Third, South Africa's 1996 Constitution, reinforced by decisions of the Constitutional Court, makes clear that courts and other bodies are to be guided by international law and norms, and the interpretation placed on these norms by international courts and other institutions; and may, as well, consider foreign law.[11]

---

[10] See Open Government Guide, Whistleblower Protections, at http://www.opengovguide.com/topics/whistleblower-protection/.

[11] Sec. 233 of the 1996 Constitution reads: "When interpreting any legislation, every court must prefer any reasonable interpretation of the legislation that is consistent with international law over any alternative interpretation …." Sec. 39(1) of the Constitution reads: "When interpreting the Bill of Rights, a court, tribunal or forum (a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom; (b) must consider international law; and (c) may consider foreign law." The Constitutional Court has interpreted these provisions liberally. See, e.g., S v. Makwanyane 1995 (3) SA 391 (CC), at 413-14: "In the context of section 35(1) [changed to 39(1) in the 1996 Constitution], public international law would include non-binding as well as binding law. They may both be used under the section as tools of interpretation."

In Japan, after the administration of Prime Minister Abe introduced the Designated State Secrets Law (DSSL), Japan's Federation of Bar Associations and other civil society groups used the Tshwane Principles in their advocacy campaigns as evidence of international norms requiring greater protection of the right of the public to access information. While Abe challenged the authority of the Principles, the media and other opinion makers seemed to accept them as a statement of global norms. Their credibility was enhanced owing to endorsement by US security expert Morton Halperin, who made two trips to Japan to discuss the Principles including with government officials and parliamentarians, was quoted extensively in Japan's media, and made a detailed, formal submission concerning the DSSL's implementing regulations.[12]

The Principles have now been translated into ten languages, including Japanese, by, or at the request of, civil society organizations that wanted to use the Principles in advocacy campaigns.[13] For instance, in Poland, the Polish Helsinki Foundation used the Principles as the basis for a two-day, closed-door meeting with security professionals and government officials that has led to further in-depth conversations about security sector reform.

In Africa, the Justice Committee of the Pan-African Parliament, expressing interest in the Tshwane Principles, has scheduled a civil society briefing on them for its August session. The Special Rapporteur of the African Commission on Human and Peoples Rights, Advocate Pansy Tlakula, is working this year to develop a Protocol on Access to Information to the ACHPR Declaration of Principles on Freedom of Expression. She has stated her intent to rely on the ACHPR Access to Information Model Law, the African Platform on Access to Information, and the Tshwane Principles.

The Principles' drafters do not expect that the Principles will have influence in countries, such as the United States, China and Russia, that have not shown much interest in complying with international human rights law and standards, or in being guided by good practices of other countries. But, they do seem to be having an effect in influencing debates at the international and national levels triggered by a range of current events, from adoption of access to information laws to Edward Snowden's revelations. The strategy of a prolonged consultative and inclusive drafting process seems to have succeeded in developing principles that are at the right level of detail to be useful for people working in a range of regions and contexts; and that have broad legitimacy. Groups in different parts of the world are invoking the Principles in their advocacy campaigns and court briefs and working to persuade regional bodies to endorse them. Very interestingly, there have been virtually no challenges to the legitimacy of the Principles overall, or to the language of particular principles, from intergovernmental bodies, civil society organizations, or scholars.[14]

---

[12] For a discussion of Halperin's main points, including the relevance of the Tshwane Principles, see Morton Halperin and Molly Hofsommer, Japanese Secrecy Law and International Standards, September 2014, at http://www.right2info.org/exceptions-to-access/national-security#section-3.

[13] The Principles have been translated into Arabic, Dari, French (booklet PDF), German, Japanese (pdf), Mandarin (pdf), Polish, Portuguese, Serbian, and Spanish (booklet PDF).

[14] For academics and civil society organizations that have discussed the Principles *see* Pozen, David, The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information. 127 Harv.L.Rev. 512 (2013) (cites the Principles at fns 515, 517 and 522; and Transparency International, Security Classification in 15 Countries, February 2014.

ANNEX:

THE TSHWANE PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION - KEY PRINCIPLES

The Principles are grouped into seven substantive sections:

(I) General principles
(II) Information that May be Withheld on National Security Grounds, and Information that Should be Disclosed
(III) Rules Regarding Classification and Declassification of Information, and Handling of Requests for Information
(IV) Judicial Aspects of National Security and Right to Information
(V) Bodies that Oversee the Security Sector
(VI) Public Interest Disclosures by Public Personnel
(VII) Limits on Measures to Sanction or Restrain the Disclosure of Information to the Public

Here are 15 key points included in the Principles:

1. The public has a right of access to government information, including information from private entities that perform public functions or receive public funds. (Principle 1)

2. The government bears the burden of proving the necessity of restrictions on the right to information. (Principle 4)

3. Governments may legitimately withhold information in narrowly defined categories, such as information about defense plans, weapons development, and the operations and sources used by intelligence services. Also, they may withhold confidential information supplied by foreign governments that is linked to national security matters. (Principle 9)

4. But governments should never withhold information concerning violations of international human rights or humanitarian law, including information about the circumstances and perpetrators of torture and other grave crimes, and the location of places of detention. This includes information about past abuses under previous regimes, and any information they hold regarding violations committed by their own agents or by others. (Principle 10A)

5. The public has a right to know about policies concerning surveillance, and the procedures for authorizing surveillance. (Principle 10E)

6. No government entity may be exempt from disclosure requirements—including security sector and intelligence authorities. The public has a right to know about the existence of all security sector entities, the laws and regulations that govern them, and their budgets. (Principles 5 and 10C)

7. Whistleblowers should not face retaliation if the public interest in the information disclosed outweighs the public interest in secrecy. But they should have first made a

reasonable effort to address the issue through official complaint mechanisms, provided that an effective mechanism existed. (Principles 40, 41, and 43)

8. Criminal action against those who leak information should be considered only if the information poses a "real and identifiable risk of causing significant harm" that overrides the public interest in disclosure. (Principles 43 and 46)

9. Journalists and others who do not work for the government should not be prosecuted for receiving, possessing or disclosing classified information to the public, or for conspiracy or other crimes based on their seeking or accessing classified information. (Principle 47)

10. Journalists and others who do not work for the government should not be forced to reveal a confidential source or other unpublished information in a leak investigation. (Principle 48)

11. Public access to judicial processes is essential: "invocation of national security may not be relied upon to undermine the fundamental right of the public to access judicial processes." Media and the public should be permitted to challenge any limitation on public access to judicial processes. (Principle 28)

12. States should not be permitted to keep state secrets or other information confidential that prevents victims of human rights violations from seeking or obtaining a remedy for their violation. (Principle 30)

13. There should be independent oversight bodies for the security sector, and the bodies should be able to access all information needed for effective oversight. (Principles 6, 31–33)

14. Information should be classified only as long as necessary, and never indefinitely. Laws should govern the maximum permissible period of classification. (Principle 16)

15. There should be clear procedures for requesting declassification, with priority procedures for the declassification of information of high public interest. (Principle 17)

Knowledge Legitimation in Contemporary World Politics

Henry Farrell
George Washington University
henry.farrell@gmail.com

Martha Finnemore
George Washington University
finnemor@gwu.edu

Draft memo for April 2015 MIT Meeting – Please Don't Circulate or Cite Without Permission

The politics of Wikileaks and the Snowden disclosures have highlighted how structures for legitimating public knowledge are changing. National and international politics have always been characterized by a plethora of information representing multiple viewpoints and approaches to the truth, often contradictory, and of varying reliability. Societies, if they are to function at all, need to reduce a wilderness of confusing and contradictory information down into something tractable. One of the important functions of modern states has been to turn contending sources of information into more authoritative 'knowledge' (i.e. information that is socially legitimated and recognized among key actors as being appropriate to understanding a topic) by, for example, creating national statistics and indices. Yet non-state actors can play an important role in creating and legitimating knowledge too – whether these be international organizations, NGOs, credit rating agencies or businesses.

In this memo we discuss only one, albeit important, set of questions about the politics of knowledge. In modern societies, mass media play a crucial role in turning (some) information into public knowledge. It shapes the facts that are in broad circulation and it also legitimates that information by giving it a journalistic stamp of approval, thus substantially influencing the broad contours of politics.

It is unsurprising then, that the relationship between national media and national political decision makers has historically been quite intimate. Those plotting coups typically try to seize broadcasters so as to ensure that their preferred information becomes publically accepted knowledge, perhaps helping to create a self-fulfilling prophecy. Authoritarian and semi-authoritarian governments often try to retain direct control of mass media, or institute censorship regimes. They may try to ensure that key media are owned by political allies or engage in active disinformation campaigns.

Democracies are not immune to this mutual dependence and cross-influence. Media organizations like to describe themselves in public as fearless and apolitical advocates of the truth, but they are usually well aware of their political role. Governments try to influence the public knowledge produced by media organizations, and often succeed, especially where this knowledge involves security

matters. Editors know that publishing highly sensitive information can have unexpected fallout for their organizations, and perhaps for national security, and the most influential outlets take these risks seriously. They understand that part of what makes them (and their news) authoritative and respected is precisely their reputation for good judgment and forbearance in the "public interest." Editors understand that journalistic independence, alone, is not sufficient to ensure credibility. Some larger commitment to public values is also required if newspapers are to retain their legitimating role.

In the US, the result has been a complicated ballet between the media organizations (such as *The New York Times*) that play a key role in legitimating public knowledge, and the state. As described by former *New York Times* editor Bill Keller, the media organization lets the administration know that it has a sensitive story, and provides the administration an opportunity to make representations. Depending on those representations, the newspaper may decide to publish, change or bury a particular story based both on their perception of the story's journalistic merits, and their sense of the politics. It is through these professional judgments that the information is legitimated and turned into public knowledge. Sometimes these judgments are contested – as when the Bush administration reproached the *New York Times* for publishing details of US surveillance of the international financial industry, or when left-leaning critics reproached the *Times* for failing to publish other national security relevant stories. But these editorial judgments are contested and criticized precisely because they are powerful. In other democracies with a less robust history of press freedom, media organizations may have to fear more direct forms of censorship and legal repercussions and, of course, non-democracies may impose quite strict censorship. These varied rules may change the type of dance done with national authorities, but all governments have relationships, formal and informal, with major national media outlets, relationships both sides value and cultivate.

It is unsurprising that both non-democratic and democratic states try to shape processes of knowledge legitimation. The knowledge that is legitimated helps shape the contours of the politically possible. Our interest here is in how the developments of the last several years are reshaping these processes and weakening democratic states' influence over knowledge legitimation. Social entrepreneurs like Julian Assange and the various actors with access to the Snowden files have succeeded in creating legitimated knowledge that would likely have either not appeared at all, or appeared only in publications with less legitimacy in a previous era. Elite US news organizations would probably not have published revelations about the extent of US spying abroad, to take one example, ten, or even five years ago.

The consequential developments in this story are not – or not simply – artifacts of the Internet easing the cost of publishing information. Information that is simply published on the Internet without legitimation is unlikely to have major consequences for world politics. It can muddy existing narratives and challenge existing knowledge, but has had a hard time generating coherent and broadly

compelling alternatives. While Internet based amateurs are creating their own knowledge sifting structures (which range from the proprietary algorithms of companies such as Google and Facebook to online knowledge generation projects such as Wikipedia and StackExchange) they do not yet possess the kinds of independent legitimacy as sources of political news that would allow them to change political debate. (Wikipedia relies heavily on the authority of external sources).

Instead, we argue that there are two major factors at work, changing the way knowledge is legitimated. First is the development of a densely linked cross-national network of activists and journalists that are less interested in working with traditional national political structures than in developing a shared cross national agenda. Second is the ability of activists to arbitrage different national media sources and different rules in order to pursue their agenda.

The first of these has received significant attention, but relatively little serious analysis. A loose but relatively coherent network of hackers (in the broad sense of the term), NGOs, independent journalists, and politicians has formed over the last decade in response to September 11, interested in pursuing cross national civil and human rights issues. Unlike the transnational networks that pursued rights abusers in Latin America in the 1980s, these networks do not pursue a 'boomerang' model of publicizing transgressions in order to embarrass a more powerful state to push its weaker allies into behaving better (Keck and Sikkink 1998). This would be hard, since the new transnational networks have identified the US – the most powerful state in the system – as a major target. Instead, they seek to reshape domestic politics within the US to make it less likely to trample privacy and civil rights, and to shift politics within US allies to make them less likely to cooperate with the US. This network has had limited success with its US agenda, but has managed to play an important role elsewhere, for example in German domestic politics as well as helping to reshape EU level discussions of privacy.

This network has been able to achieve the successes that it has achieved through tapping into a variety of elite national media to publish stories aimed at embarrassing the NSA, the US administration and other foreign agencies (especially spy agencies) that regularly cooperate with the US or otherwise conduct large scale surveillance. Activists such as Julian Assange initially believed that they did not require the help of these media; all they had to do was release information to spur political change. However, events of the last several years have shown that Assange (and his allies) were wrong, and were obliged to reach accommodations with traditional journalists to analyze and legitimate their information and get their story out. Both the Wikileaks activists and those associated with Snowden have used media organizations such as the *Guardian*, the *New York Times* and *Spiegel* to get their story out to the public. It is not clear that their efforts to build an international presence are economically sustainable (it would be interesting, for example, to think about how the Snowden story might have transpired if the Guardian had not had

funding from the Scott Trust) but the traditional outlets did provide a platform that has allowed activists and activist journalists to pursue a cross national agenda.

This new "complex interdependence" among diverse governments, traditional media of varied nationalities, and transnational internet-empowered activists presents a very different environment for public knowledge construction. No longer constrained by national media markets, this new environment has allowed the activists to shop transnationally for legitimating media outlets, They can also leverage differences in national laws to get their information out, and they can now do this in new, potentially potent ways. On the one hand, they can tailor revelations (e.g. of US spying) to specific national audiences. On the other, they can arbitrage differences in national laws to maximize the impact and minimize the risks of their activities.

For example, many activists and journalists have moved to Berlin, in part because of a privacy-friendly political system. Many of the most important revelations have been published in *Spiegel* – legitimizing them, and allowing them to circulate through the broader journalistic ecosystem. When the *Guardian* was faced with the threat of legal action over leaked information that it held, it moved this information to the US where press protections are stronger. The Austrian activist Max Schrems has used the Irish and EU legal systems to pursue claims aimed at undermining US surveillance. In a sense, activists are arriving to these strategies a little late – both terrorists and intelligence agencies have been adept at exploiting the loopholes created by regulatory interdependence. Yet they are using them quite effectively.

Over the longer term, this activist arbitrage is substantially weakening the ability of states to control structures of knowledge legitimation. States like the United Kingdom face a generalized version of the *Spycatcher* problem that they first confronted three decades ago – they cannot control how actors outside their jurisdictional grasp publish information, and outside sources (such as the *New York Times* or *Spiegel*) are far more accessible than they were. States like the US can no longer assume that informal conversations with editors will allow them to shape the publishing process in ways that are conducive to national security. Not only do they now face foreign journalists, whom they cannot appeal to in the traditional ways, but domestic publications such as the *New York Times* are less likely to grant deference than they once were, since they worry about losing legitimacy (and perhaps readership) if they suppress stories.

One should not exaggerate these problems – but they are real. As national media spaces start to become interpenetrated so that national media faces (some) competition from international sources, media organizations are likely to become less responsive to purely national concerns. This can in turn be exploited by activists whose aims and interests are explicitly cross-national. There is no very strong international public sphere – but the structures of political knowledge production are no longer as determined by national borders as once they were.

This is not a simple story in which globalization undermines systems of authority leaving nothing in its stead. Instead, it is a conflict over legitimacy between existing national systems and newer, cross-national relations with their own logic. On the one hand, national authorities appeal to traditional notions of national interest, and a sharp division between the domestic and international politics of surveillance. On the other, activists and associated journalists reject the claim that they should be beholden to national interests, instead seeing themselves as defending cross-national civil liberties and human rights that are being undermined by an ever-proliferating web of surveillance and tacit cooperation between different national security authorities. Both sets of actors have their own understanding of social legitimacy, and which kinds of information it is appropriate to legitimize as knowledge. The conflict between these understandings is both inevitable and important.

Independent Oversight of National Security Surveillance

Elizabeth Goitein, Co-Director, Liberty and National Security Program, Brennan Center for Justice at NYU School of Law

It goes without saying that much of what intelligence agencies do must be done in secret – i.e., without disclosure to the public. It is equally obvious, but perhaps less widely understood, that multiple incentives, unrelated to national security, will lead agency officials to classify and withhold more information than they should. (This is the topic of the Brennan Center's report *Reducing Overclassification Through Accountability*.) And it is surely beyond dispute that the ability to exercise powerful authorities in secret creates a significant potential for abuse – potential that was fully realized during the early decades of the Cold War and documented in the findings of the Church Committee.

Because of these distinct features, independent and robust oversight is far more important in the national security context than in other areas of governance. It alone ensures that information is not hidden for reasons other than national security (thus impeding democratic self-government) and that intelligence authorities are not abused for reasons political or personal. And yet, several factors undermine the effectiveness of intelligence oversight in the U.S. The current system may even be counterproductive in one sense, as it perpetuates the appearance of checks and balances where few exist, thus serving to legitimize executive activities that trench on the rule of law.

Congressional oversight is weak by design. The intelligence committees were established in the wake of the Church Committee, and the National Security Act of 1947 was amended in 1991 to require the Director of National Intelligence and other agency heads to "keep the congressional intelligence committees fully and currently informed of all intelligence activities, other than a covert action..." For covert actions, defined as undertakings "to influence political, economic, or military conditions abroad" and expressly excluding "activities the primary purpose of which is to acquire intelligence," notification in some cases may be limited to the so-called "Gang of Eight": the chair and ranking members of the intelligence committees, as well as the party leadership in each house.

These notification provisions contain a critical loophole, however. They are preceded by the words: "To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters…:" In other words, the executive branch may modify or disregard the notification requirements upon a unilateral determination that its activities are too sensitive to report as required. Thus, many intelligence activities that do not qualify as "covert operations," and thus should be briefed to the full committees rather than the Gang of Eight, are instead briefed only to a "Gang of Four" – the chairs and ranking members of the intelligence committees – a procedure that exists nowhere in the statute. The full list of instances in which the executive branch decided it could not afford to notify *any* member of Congress is unknown and unknowable.

Even without this loophole, the notification system is insufficient. Oversight is not an end in itself; members of Congress must be able to act on the information they receive. Individual

members can do little on their own, however. Meaningful action generally requires the full committees and often (where legislation is involved) the full Congress. The National Security Act states that "each of the congressional intelligence committees shall promptly call to the attention of its respective House, or to any appropriate committee or committees of its respective House, any matter relating to intelligence activities requiring the attention of such House or such committee or committees." This requirement is honored in the breach (and many members lack the security-cleared staff required to take advantage of it, in any event). Moreover, the executive branch takes the position that it may prohibit members of the smaller "gangs" from disclosing information to others, and the members have acquiesced in this apparent departure from the statute.

There also is the fundamental question of how effective secret oversight can be. Any regulatory body runs the risk of "capture" by the entity it regulates; publicity usually serves to hold this dynamic at least somewhat in check. Intelligence committees are particularly prone to capture given the insular nature of the national security establishment – when "read into" a classified program, members become part of an elite club – and there is no publicity to discourage this phenomenon. Furthermore, as Jack Goldsmith has written, the intelligence committees have little incentive to pick secret battles with the executive branch. There are no political rewards to these fights – no legislative "goodies" to dole out to donors, no victories to splash across newsletters to constituents. On the other hand, there are political risks: if a major terrorist act were to occur, any actions members had taken to limit the executive branch's exercise of national security authorities surely would come to light.

One might expect more effective oversight from the judiciary because the political forces are less salient. In fact, courts have provided little oversight over surveillance activities. A key barrier to judicial oversight has been standing; because the subjects of foreign intelligence surveillance generally do not receive notice of the surveillance even after the investigation has ended, plaintiffs in civil suits have struggled to establish the requisite injury. In recent years, the Supreme Court has been notoriously stingy in its reading of standing requirements, and has denied standing to plaintiffs who reasonably feared surveillance and incurred costs to avoid it.

The law does require the Justice Department to inform criminal defendants when using evidence obtained or derived from foreign intelligence surveillance authorities. Until recently, however, the Department did not comply with this requirement, and agencies continue to avoid the notification requirement by engaging in the practice of "parallel construction" – reconstructing evidence using other authorities. In the few cases in which defendants have received notice of foreign intelligence surveillance, neither they nor their attorneys have been permitted to see the government's surveillance application, rendering any challenge to the surveillance an exercise in shadow-boxing.

Moreover, apart from issues of standing and notification, lower courts often view national security matters as beyond the scope of their expertise or even their jurisdiction. With few exceptions, courts have accepted governmental invocations of the state secrets privilege. This acquiescence is particularly problematic because under the past two administrations, the Justice Department has used the state secrets doctrine not as an evidentiary privilege (as the Supreme Court has described it) but as a jurisdictional bar. It has argued that courts must dismiss lawsuits

challenging surveillance at the pleadings stage because litigating the case would be impossible without revealing state secrets. Rather than test this prediction by allowing discovery to proceed and requiring the defendant agency to invoke the privilege for specific items of responsive evidence, courts have accepted the executive branch's characterization of such lawsuits as non-litigable.

In theory, the Foreign Intelligence Surveillance Court (FISC) provides *ex ante* judicial oversight of foreign intelligence surveillance. In practice, FISC oversight in recent years has been reduced to near-nothingness. Under the 2008 FISA Amendments Act (FAA), which governs the acquisition of communications between foreign targets and Americans, the court has no role in approving the targets of surveillance. Its sole responsibility is to pre-approve agencies' general procedures for assessing whether targets are indeed foreigners overseas (not a straightforward task in the digital era) and for "minimizing" the retention and dissemination of Americans' information. The FISC is charged with determining whether these broad procedures, which leave enormous discretion to the officials implementing them, are constitutional, despite having no information about their actual application in specific cases. In the Brennan Center's report *What Went Wrong with the FISA Court*, we argue that this role may not even comport with Article III, let alone provide a sufficient check on executive action.

Given the legal and practical constraints on oversight by Congress and the judiciary, mechanisms for "independent" oversight *within* the executive branch have taken on increased importance. Each major intelligence agency has an inspector general, and there is a presidentially appointed inspector general for the intelligence community at large. These officers are served by independent counsel and report to Congress as well as to the heads of their respective agencies. As Shirin Sinnar at Stanford Law School has pointed out, certain investigations by inspectors general after 9/11 exposed government misconduct that otherwise might never have been publicly revealed. A good example is the investigation by the Justice Department's inspector general into the FBI's use of so-called "exigent letters" to circumvent the requirements of National Security Letters.

As Sinnar also has noted, however, there are systemic limitations on the effectiveness of inspector general oversight. Inspectors general are not fully independent; they may be removed by the president without cause. While they can make recommendations, they have no authority to remedy government misconduct, whether by compensating victims, holding officials accountable, or changing agency policy. Perhaps most significantly, the heads of agencies involved in national security matters are authorized to block investigations or reports involving sensitive national security matters. The threat of this authority likely obviates the need for its exercise, as inspectors general quickly come to know where the limits are.

Even when acting inside these limits, inspectors general are, to a significant degree, at the mercy of their agencies. Last year, 47 inspectors general signed a letter to congressional leaders noting that certain agencies were improperly asserting "privilege" to refuse requests by inspector generals to examine documents. In January, the CIA's inspector general resigned, almost certainly under pressure, after CIA director John Brennan expressed displeasure with his office's finding that the CIA improperly monitored the computer activity of Senate intelligence

committee staffers. It is unsurprising, under these circumstances, that Sinnar has found a wide range in the rigor of inspector general oversight.

A final source of independent oversight is the Privacy and Civil Liberties Oversight Board (PCLOB), a bipartisan, five-member commission charged with providing reports and recommendations on executive counterterrorism policies. Congress enacted legislation establishing the PCLOB in 2004, yet the board stood vacant for years, and President Obama only fully staffed it in 2013. The PCLOB in theory has greater independence and access than inspectors general, and in the two years since the Snowden disclosures, it has been able to obtain the declassification of significant information about surveillance programs. Nonetheless, the Board is hampered by partisan division and by resources that are paltry compared to those of inspectors general, even though it oversees the entire national security establishment. In this fiscal year, the PCLOB had 13 staffers and a budget of $8 million, compared to 474 staffers and $86.4 million for the Justice Department's Office of the Inspector General.

In short, due to a shortage of both will and resources, none of the existing independent oversight mechanisms serves as an effective check on government surveillance practices. The current state of affairs presents a perplexing question: has the intelligence establishment become too big to oversee? This part of the government has experienced dramatic growth since 9/11 and today comprises seventeen organizations with a disclosed $70 billion budget and employees and contractors numbering in the hundreds of thousands. Providing effective oversight of such a behemoth ultimately may require either a commensurate growth in the size, resources, and powers of independent oversight bodies, a scaling back of the intelligence agencies, or both.

Technology and Local Norms and Practice – Surveillance and Censorship in China

Shirley Hung
MIT/ CSAIL
April 2015

It is easy to think of Internet technology as being universal – bits and computers and fiber are the same everywhere. Yet local laws, norms, and conditions shape how technologies are used, just as those technologies affect local policies and practices differently. A common example is of the 'open', free-wheeling Internet the West that serves as a mechanism for free speech, commerce, maintaining relationships, and entertainment versus the 'closed', restrictive Chinese Internet, locked behind the Great Firewall. The irony is that the Internet serves the same functions in China, just in a different and continually evolving form due to the pressures of the censorship regime. This raises a broad policy question of how (or if) we are to manage or tolerate those differences across countries: we may not like Chinese censorship, but what if anything should we do about it? What should our policies be when Chinese actions affect US or multinational corporations? Does it matter if those companies were operating on Chinese soil at the time, or if they (or their servers) were firmly on US soil? Do we protect US corporations as we would US citizens? These questions obviously are not limited to China, but it is a place to start the discussion.

The Great Firewall is something of a misnomer, in that it implies a monolithic, impenetrable, unchanging barrier. Instead, it is a complex system that relies on technical components (false or incorrect DNS addresses and restricting access to servers, control of routes, IP blocking of sites and ports, deep packet inspection, TCP resets, etc), human operators (manual review/ deletion and manipulation of discussions), targeting of specific individuals and organizations both online (spearfishing, hacking into accounts) and offline (intimidation, jailing), and the panopticon effect. The system is supported by a far-flung bureaucracy at national (State Information Office and the newly formed Cyberspace Administration), provincial, and local levels that incorporates quasi-NGOs, industry groups, and citizen volunteers. Together they have a variety of tools of control at their disposal ranging from licenses and registration to internal third-party monitoring within companies. The control regime is further undergirded by state ownership of infrastructure, including ISPs with connections to the foreign Internet backbone, and the blocking of popular foreign-owned sites and applications such as Google, Facebook, and Twitter combined with promotion of domestic alternatives (Baidu, Renren, Weibo). Of all of these, however, despite the plethora of DPI boxes and virtual army of censors (estimates range from 30,000 to 100,000), the panopticon effect is the tool officials rely upon most. In private discussion, officials admit they do not expect to prevent everyone from accessing forbidden information; deterrence of the majority is enough, and the average citizen knows he is being constantly surveilled in his online activity. To add a level of complexity, much of Internet usage in China is conducted on mobile devices – and SIM cards must be registered with the government, which has admitted that it uses location tracking data to monitor large groupings of people in an effort to curtail protests.

Clearly, the Great Firewall is clearly not impenetrable. Estimates of the percentage of users who circumvent the restrictions range from 3-10%. Rapidly changing Web 2.0 applications such as Weibo (a microblogging service similar to Twitter) and the next generation of social media services, including as enhanced IM-style services such as WeChat, have posed ongoing challenges to Chinese officials who struggle to keep up with policies and means of monitoring and censoring activity on these platforms. Moreover, users continually find ways of getting around restrictions while working within the system – character substitutions, puns, jokes, videos, and images/ cartoons all make it harder for censors to pick up on 'inappropriate' content quickly.

And perhaps most interestingly, the Great Firewall changes. This ongoing evolution – the cat-and-mouse game – is what presents the most interesting policy questions. For example, in recent months, China has cracked down on VPNs, a common mode of circumventing censorship, leading to protests from foreign companies dependent on the ability to VPN back into their headquarters networks. Multinational corporations deal with differing regulations based on jurisdiction all the time, but how should they cope with one that interferes with their ability to connect back to headquarters securely?

Just in the past two weeks, details of Chinese man-in-the-middle attacks on GitHub, dubbed the "Great Cannon", to 'encourage' the removal of two sites mirroring banned sites, the anti-censorship service Greatfire.org and the Chinese edition of the New York Times, have emerged as well. In this attack, malicious code was injected into the traffic of people from outside China who visited websites using Baidu (a Chinese search engine) analytics software, which caused their computers to essentially launch a DDoS attack against the targeted GitHub pages. As researchers at CitizenLab note in their report, this is "a significant escalation in state-level information control" – it targeted users outside China to attack servers outside China in service of Chinese censorship regulations. And it did so by using Baidu servers, which is the star of the Chinese Internet economy. How should companies such as GitHub respond? How should the US?

In addition, Google and Firefox removed CNNIC (China Internet Network Information Center), an administrative agency of the Chinese government, as a trusted root certificate authority on April 1. CNNIC had issued an intermediate CA certificate to an Egypt-based firm that then used CNNIC keys to issue unauthorized digital certificates for Google domains. Root CAs are built into browsers, which means that CNNIC is trusted by almost all browsers and operating systems. The implications of corrupting this chain of trust are significant and affect almost anyone who uses a browser to access the Internet. It is unclear exactly what happened in this incident, but it does raise the question of how to protect the security of certificates in the future.

This summary of the Chinese Internet's censorship and surveillance system is nowhere near complete nor comprehensive, but hopefully it offers a starting point for discussion.

Two Cryptographic Tales — and Their National-Security Implications

Susan Landau

Following Edward Snowden's disclosures on NSA surveillance, some Internet companies sought to protect data through a more widespread use of encryption. Some of the protections, such as standardly encrypting company inter-data-center communications, left in place the companies' ability to access user content in the clear. This also the ability for governments to access content under legal authority. Other technical solutions, such as Apple's and Google's plans to have mobile phone data encrypted by default with only the user holding the key, do not.

The response has included strong statements by the UK Prime Minister David Cameron and FBI Director James Comey on the difficulties the use of encryption raises for law-enforcement and national-security investigations, and threats to restrict its use. The British Prime Minister stated that, "If I am prime minister I will make sure that it is a comprehensive piece of legislation that does not allow terrorists safe space to communicate with each other." [Cameron] NSA Director Mike Rogers has said, "I think we can work our way through this" [Peterson] — meaning enabling access to encrypted content — without being explicit about what the technical solutions would be.

These issues echo the "Crypto Wars," a time when governments, especially the United States, battled industry and academia over encryption [Levy]. These disputes came to a head during the 1990s as commercial enterprise developed over the Internet. In 1999 the EU relaxed its controls on the export of computer and communication systems with cryptography, and the US did so in 2000, but the legacy of the controls remain, and affect computer security to this day.

Cryptography is mathematically complex, but it is also the multiple uses to which cryptography can be put that has made use of the technology complicated. Cryptography's most well-known use is confidentiality, and this is the cause for conflict over the technology's deployment. Cryptography can also be used for integrity, ensuring that there has been no tampering of a message, and authenticity, confirming that the origin of a message is who it claims to be; these uses do not raise the US government's objections. But controlling a technology's use in one way inevitably impacts its capabilities elsewhere.

Cameron and Comey's objections to technologies that secure Internet communications may well lead to attempts to place controls on encryption implementations. It is thus appropriate to examine the impact of such controls. In this brief memo, I look at an example of how 1992 export controls on the strength of cryptography used for confidentiality has continued to undermine Internet security two decades later.

Information security relies on encryption, the encoding of communications and data at rest that is done in a way that only the intended user of the information can read it. In the nineteenth century, Auguste Kerckhoff established the principle that if a system has more than a handful of users, the encryption algorithm should be public, and the security should rely on the key.

Private-key systems, also known as symmetric-key systems, use the same key for encryption and decryption. Because they have been studied for decades, there are many such trusted and efficient systems. Perhaps the most popular is the Advanced Encryption Standard (AES), which was chosen as a cryptographic standard by the National Institute of Standards and Technology in 2001. A cryptographic algorithm is considered strong if the most efficient way to decrypt encoded communications is essentially no faster than brute force examination of all possible keys. AES works with key sizes of 128, 192, and 256 bits; even at its smallest key size, it is considered secure. That is, of course, based on current technology and the length of time the cryptographic system is intended to keep information confidential. Computers are always increasing in speed; as this occurs, the strength of cryptographic systems decreases.

One of the complexities of secure communication is key transmission. This issue is especially important over the Internet, which is an insecure communications channel. In 1975 public-key cryptography, a system whose security is based on the mathematical difficulty of inverting a particular computation, was proposed as a way to solve this problem.

Several number-theoretic and algebraic problems provide the basis for public-key cryptographic algorithms; one example is multiplication and its inverse, factorization into primes (while multiplication of large integers can be done efficiently, the fastest known algorithms for factoring an integer are exponentially slower). In public-key cryptography, one key is made public and is used to encrypt communications, the other, called a private key, is used to decrypt the communications. Only the intended recipient of the communications knows the private key. [Diffie-Hellman]

Public-key cryptography also provides another, extremely useful functionality: digital signatures. This technology, which uses the private key to encrypt a message, embodies both integrity and authenticity. Since the public key is public, the message is easily decrypted; however, no one but the owner of the private key could have encrypted the communication. This ensures the message's integrity and authenticity.

Prior to the development of public-key cryptography, cryptography research and development was essentially the domain of the intelligence agencies; in the US, this was the National Security Agency (NSA). There was conflict between the US government and industry and academia from the mid 1970s to the late 1990s, first

over private-sector research in cryptographic algorithms and then later over implementations of cryptographic tools in computer and communication systems.

In the early 1970s, the US government realized that the increasing use of computers for civilian data required cryptography to secure communications. NSA would have been the natural choice to develop such a system, but because of concerns about exposing its design methodologies, the intelligence agency was unwilling to provide an algorithm that would be used by the public. In 1965 the National Bureau of Standards (later renamed the National Institute of Standards and Technology, or NIST; I will refer to it here by the latter acronym) had been placed in charge of establishing Federal Information Processing Standards, standards that manufacturers had to meet in order to sell equipment to the government. Thus NIST was a natural agency to determine this new cryptography standard. NIST put out a call for a cryptographic system, and IBM, which had developing a system for banking, submitted a proposal. Technical expertise lay at NSA, which went to work on this proposal. In some ways, the revised algorithm, known as the Data Encryption Standard (DES), was made more secure, but in others, specifically by decreasing key length from 64 bits to 56, made the system easier to break. This action created much distrust of NSA, and of the US government process.

In 1987 the Computer Security Act put NIST firmly in charge of developing non-national-security US government cryptographic standards, but the agency was to consult with NSA on technical aspects of such standards. Tension over the development of US cryptographic standards continued through the 1990s. In the latter half of the decade, NIST began work on a DES replacement, the Advanced Encryption Standard (AES). In contrast to the DES effort, the competition was highly public and international. The result was that industry had confidence in the security of the chosen algorithm, and the algorithm was widely adopted. The other result was that the private sector developed confidence in NIST's ability to promulgate security cryptography standards.

Standards had been one way that the US government controlled cryptographic development; the government also controlled deployment. This was done through a prohibition on the export of strong cryptography in computer and communication equipment. The purpose of the export-control regime was ostensibly to prevent the deployment of strong cryptography abroad, but this action indirectly contributed to weak cryptographic — and thus weak security — systems domestically.

While the export-control system allowed export of cryptographic tools for purposes of authentication, the same cryptographic tools could also provide other functionality, including confidentiality. Thus it happened that authentication systems were either weakened prior to export or sometimes export was prohibited altogether.

The growth of the Internet and a globalized economy created an increasing need for secure communications. In 1992 the government arrived at an arrangement in

which systems using 40-bit keys for symmetric-key algorithms and 512-bit keys for public-key systems were permitted for export without undergoing the slow and laborious licensing process. Such key lengths provided a modicum of security while nonetheless enabling access under a determined national-intelligence effort.

Tensions over the encryption controls grew as Internet use expanded. For a number of reasons, including business needs, the export-control regime largely ended in 2000. Exports of systems to governments and telecommunications providers with strong cryptography and custom-built systems remained controlled, but export of systems were largely no longer subject to controls. [Commerce]

Doing business on the Internet is very different from conducting the business in the bricks-and-mortar world. One important distinction is in how easy it is to be sure of exactly where you are in the Internet. In the offline world, it is relatively easy to determine, for example, when you are in an Apple store: the stainless steel walls, glass stairs, and "Genius Bar" provide clear signals. On the Internet, such assurances fail. In particular, accessing http://www.apple.com can be subject to a "man-in-the-middle" attack. This is an attack in which an interceptor presents a webpage that appears to be the Apple page but is actually an identical looking page that is under the control of the attacker. Certificates and PKI infrastructure are used to authenticate websites and secure communications between the user and the site. That allows a customer to be sure that they are at the correct website and to send over confidential information — a credit card number, instructions on transferring money between accounts, etc. — securely. A more technical description appears in the appendix.

The 1990s export controls meant that cryptography intended for export had to obey the 40-bit key rule for symmetric-key algorithms (later a 56-bit rule) and the 512-bit rule for private keys; this included the software in browsers. By the time that requirement was lifted in 2000, this encryption strength was considered weak. With the relaxation of export controls, the keys used in browsers went to using 128 bits for symmetric-key cryptography and 1024 bits in public-key cryptography (the 1024-bit standard is being phased out in favor of 2048 bits). These should be secure enough.

Engineering intrudes. A basic principle of communication system design is that all systems should be backwards compatible, that is, newer systems should work with older, less advanced ones. That's why modern smart phones and old-style rotary phones can connect. In the world of browsers, the impact is that the old protocols of 40-bit symmetric keys and 512-bit public keys were in current browsers and thus were, under certain circumstances, available for use.

The weak cipher suites should not be cued during the exchange. But recent research demonstrates an attack that causes the browser and the server to agree to use the weak keys required by 1990s export-control regulations. These weak keys can then

be factored to enable an interceptor — the same "man-in-the-middle" who caused the negotiation to default to the weak keys — to read all the traffic.

Who is vulnerable to this attack? When the attack was first made public, 9.6% of the https servers at the top 100 million domain names were; that number has now gone down, but originally included Groupon, NPR, MIT. Browsers that were vulnerable included Chrome on Mac OS and Android, IE, and Safari on Mac OS and iOS (patches are now available) [FREAK].

One of the more disturbing Snowden revelations was that NSA had tampered with the cryptographic standards development process. The algorithm in question, Dual EC-DRBG, is a "pseudo random bit generator" and was on a list of recommended NIST algorithms for taking a short random string and producing a longer, "pseudo-random string." Such strings are used for many purposes, including as the basis for cryptographic keys.

The algorithm was insecure, but in a very clever way. Such a system should be designed so that the output of the pseudo random bit generator is unpredictable. However, with a priori knowledge of the relationship between several parameters of Dual EC-DRBG — something the NSA apparently had — it would be possible to figure out the output. Thus keys computed through this method would be insecure. It appears that at the time NIST recommended the use of Dual EC-DRBG, the standards agency had been unaware that Dual EC-DRBG had been compromised in this fashion.[1]

In September 2013, the compromise of Dual EC-DRBG and the NIST cryptographic recommendation process became known as a result of the NSA disclosures. One problem, that of removing Dual EC-DRBG from the list of recommended NIST pseudo-random-number generators, was easily handled. The far more difficult problem of restoring faith in NIST as an honest broker of cryptographic standards remains. A diminished role for NIST as an international purveyor of cryptographic standards would have a severe negative impact on global information security.

Cryptography is one part of secure communication. Information in communications leaks in many ways. Communications metadata, including the who, when, where of a message, is well known to reveal much information, including organizational structure, activities, plans, etc. It is the foundation of signals intelligence work and

[1] After the problem was revealed, NIST conducted several reviews to understand how the agency might have recommended a flawed algorithm that had a cryptographic backdoor. In one review, the agency observed, "When evaluating Dual_EC_DRBG, NIST asked itself "Do we think there is a trapdoor?" when it should have asked, "Should we include an algorithm in our standards that could have a trapdoor?"[NISTReview]

has been a basic tool of the military since at least World War I. Thus in order to communicate securely, anonymity — hiding the communications endpoints — is at least as important as confidentiality.

Thus it should not be surprising that the US Naval Laboratory developed a system for anonymous communication: The onion routing network, or Tor. This technology — a collection of servers with encryption and decryption software — protects against traffic analysis through deployment of an overlay network that hides the communication path from attacker. An eavesdropper who is able to view the entire network at once can use timing correlations to learn about particular communications. Without such capabilities, deanonymizing Tor is very difficult. Browser and IM communications can be done via the Tor network.

If the only users of an anonymity system belong to a particular organization (e.g., are employees of the US military), then even though particular users cannot be uncovered, the fact that they are on the system identifies them as members of the organization. Anonymity works best when there are many users on a system, and thus the Tor network is available to the public at large.

The Snowden disclosures prompted many to seek more secure forms of communication. Google, which had begun efforts to secure inter data center communications, increased its efforts, and Yahoo and Microsoft began similar implementations. Individuals sought protection in implementing Tor, whose usage went up sharply. Google and Apple said that they would make secure encryption on Android and the iPhone the default.

In response, US law enforcement and GCHQ began a very public effort to urge that communication systems be built in such a way as to ensure authorized access was possible. NSA Director Mike Rogers also weighed in with similar suggestions. The problem is that there are no easy ways to do this.

Escrowing the encryption keys was tried in the 1990s and was highly unsuccessful. We now have a highly globalized economy, making a new effort in this direction even less likely to succeed. Complicating matters include that other nations would also press for access.

Escrowing communications would create an even more complex and more difficult to manage system, and thus is also unlikely to succeed.

That leaves the choice of weaker forms of security, the situation that was described above. As the situation with server certificates show, such a choice creates serious long-term security risks. And the situation with Dual EC-DRBG, and its consequent impact on trust in NIST's cryptographic development standards process, may have created greater insecurity in cyberspace, not less. That is also not in the US national-security interest.

When discussing communications surveillance, it is important to keep in mind that it is in fact extremely difficult to be anonymous in modern society. One can do without smart phones and use the Internet only in public places, but even such behavior as using travel passes paid for with cash enables a modicum of tracking. Consider the 2005 case of the assassination of former Lebanese Prime Minister Rafik Hariri in Beruit. The planning behind the assassination was well hidden. But studying the patterns of cell phone traffic in Beruit and other locations around the time of the assassination revealed the plot. It showed several distinct groups of users traveling around the city tracking Harari and communicating amongst each other while obeying strict rules to keep the groups largely separate (only the heads of each group communicated with other groups) and also not using the phones for other communications. Despite this care, the communication patterns, including locations, identified the users. [Bergman]

One can live without access to modern communications (Osama bin Laden did so in the final years of his life). Doing so comes at high cost in terms of effectiveness. In addition, lack of access to modern communications often makes the person stand out. One can use the modern technologies. But even with great care, there is information leakage. In the Harari plot, for example, minimal slips of using a phone in a plotting subnetwork to call outside allowed identification of users.

The fact is that the world where national intelligence was tens of years ahead of the general public in communications technology is gone. That does not mean that the intelligence agencies are lost; the success in Stuxnet, an extremely impressive effort in terms of engineering and tradecraft, shows successes in surveillance and subsequent action are still quite possible.

This, then, is the context for the discussion of secure communications technologies.

Bibliography

[Bergman] Ronen Bergman, "The Hezbollah Connection," *New York Times Magazine*, February 10, 2015.

[Cameron] David Cameron, Speech, January 12, 2015, http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg

[Diffie-Hellman] Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654.

[FREAK] "Tracking the FREAK Attack," https://freakattack.com/

[Levy] Steven Levy, *Crypto: How the Code Rebels Beat the Government — Securing Privacy at the Same Time*, Viking, 2001.

[NISTReview] Report and Recommendations of the Visiting Committee on Advanced Technology at the National Institute of Standards and Technology, *NIST Cryptographic Standards and Guidelines Development Process*, July 2014.

[Peterson] Andrea Peterson, "Here's How the Clash between the NSA Director and a Top Yahoo Executive Went Down," *Washington Post*, February 23, 2015.

[Commerce] US Department of Commerce, Bureau of Export Administration: 15 CFR Parts 734, 740, 742, 770, 772, and 774, Docket No. RIN: 0694-AC11, Revisions to Encryption Items. Executive January 14, 2000.

Appendix

If a browser seeks to establish a secure connection with a website — what is called an "https" connection — the first step is that the browser sends a request to the server to establish a connection and also requests that the site identify itself. In its initial request, the browser includes information on what version of the authentication software (SSL/TLS) it is running and what cryptographic suites the browser supports.

The system is designed so that the server picks the strongest cryptographic system that the two systems — server and browser — support and transmits that choice to the browser. The server also sends a *certificate*, a document that establishes the authenticity of the server's identity and also binds this identity to the server's public key. Certification is accomplished through public-key cryptography. The certificate contains the certificate issuer's name, the subject name (the name of the site that is being validated), the subject's public key, and the dates during which the certificate is valid. The important point is that this set — issuer name, subject name, subject public key, dates of validity — are signed with the certificate issuer's private key.

Every browser has a list of valid Certificate Authorities (in Firefox these can be found in Preferences > Advanced > Certificates). The browser checks the validity of the certificate by checking the signature of the certificate; using the public key for the certificate issuer, the browser ascertains that the certificate is valid, and that the subject name matches the site. If it is, then using the server's public key, the browser encrypts a random string using that key, and sends this to the server. This is used as the basis for determining a secret key through which the browser and server will communicate securely.

Note that the certificate might not be signed by a Certificate Authority found in the browser, but by an authority whose own certificate is signed by an authority whose certificate is in turn signed by an authority whose, ..., etc. So the browser may have to do this recursively, that is going through a chain certifying parent certificates until it reaches a certificate that it can directly check (one for which it has direct evidence that it is a Certificate Authority).

Aryeh Neier
March 16, 2015

Whistleblowing

Whistleblowing may be defined as an attempt by an insider, such as an employee of a business or a government body, to disclose publicly information that is otherwise unavailable that shows wrongdoing. Edward Snowden is the best known whistleblower of our time and, perhaps, the best known whistleblower of any time. His disclosures not only have provided a great deal of information that was previously kept secret on the surveillance practices of the National Security Agency within the United States and internationally. In addition, Snowden's revelations directly contradicted the recent testimony of the Director of National Intelligence at a Congressional hearing with respect to surveillance of the electronic communications of Americans. Snowden demonstrated that the testimony was false. As a result of his disclosures, Snowden faces prosecution on charges of violating the Espionage Act that could result in a lengthy prison sentence. Although the United States has laws and regulations that appear intended to protect whistleblowing, and to recognize its significance as a means of making wrongdoing publicly known, these protections do not apply to Snowden. Accordingly, Snowden has sought refuge in Russia and probably will not voluntarily return to the United States unless and until he is able to negotiate a plea with the United States Department of Justice that limits the amount of time he would spend in prison to what he considers a tolerable period.

Among the forms of wrongdoing that may be disclosed by whistleblowing are human rights abuses, corruption, waste, dangers to public health, dangers to safety or harm to the environment. Significant whistleblowers in recent American history include Daniel Ellsberg who made public the

"Pentagon Papers" and, thereby, called attention to the steps that led to American immersion in the war in Vietnam; Ernest Fitzgerald, a Department of Defense purchasing agent who made known the magnitude of cost overruns incurred by the Pentagon in the acquisition of military equipment; Christopher Pyle, a former Army Captain who disclosed that the United States Army had assigned more than a thousand military personnel to engage in political surveillance of opponents of the war in Vietnam; and the unnamed official or former official who made known publicly the United States's invasion of Cambodia and who President Richard Nixon and his National Security Advisor, Henry Kissinger, tried to identify by placing wiretaps without court authorization on the home phones of many persons they identified as suspects. An example of a whistleblower in another country is Dr. Jian Yanyong, the physician in a Chinese military hospital in Beijing in 2003 who disclosed that a number of the patients at the hospital were suffering from a severe respiratory ailment and, thereby helped to alert the world to the onset of the SARS epidemic. Covering up the epidemic had made it impossible to deal with. Disclosure of it, which also involved a Beijing-based business weekly, Caijing, provided the opportunity to get control of SARS and prevent a worldwide disaster.

In certain circumstances, it ought to be possible for governments to limit the disclosure of information and even to invoke criminal penalties as a way to enforce such limits. In the national security area, for example, it is legitimate to provide criminal penalties when the disclosure of information is undertaken with the intent to harm the country or national defense or to aid a foreign power and there is such harm or a likelihood of such harm; or when disclosure of specific information, such as the identities of covert agents, is done with the intent to harm those persons or with knowing disregard of the potential for harm to them, and does not serve a more important public interest purpose.

There have been several recent prosecutions in national security cases that do not meet these criteria. One example of such a case involves John Kiriakou, a former CIA analyst and case officer. In December 2007, he was apparently the first former government official to confirm that waterboarding had been used in connection with prisoners held at Guantanamo, in this case as a means of interrogating Abu Zubaydah. Kiriakou described the waterboarding as torture. In 2012, Kiriakou pled guilty to disclosing information about a fellow CIA officer who had engaged in the waterboarding. The journalist to whom Kiriakou disclosed the identity of the CIA officer who engaged in the waterboarding did not publish the name of that CIA officer. Even so, Kiriakou was sentenced to thirty months in prison and served a prison sentence from February 2013 until February 2015. Needless to say, no one has yet been sent to prison for engaging in waterboarding and other forms of torture, but Kiriakou spent two years in prison for disclosing the practice and for identifying to a journalist who engaged in the practice even though that information was never publicly disclosed. This seems an example where the public interest purpose of whistleblowing should take precedence over even the purpose of protecting the identities of covert agents. Kiriakou is by no means to be compared to Philip Agee whose identification of CIA agents was intended to damage the Agency and whose activities inspired the adoption of the Intelligence Identities Protection Act of 1982.

There may be administrative penalties, such as firing, that are appropriate in certain circumstances for disclosures that fall short of those that are intended to harm the national defense. Such penalties should only be applied, however, if there is written notice of the duty of confidentiality; if there are effective procedures within an organization for consideration of complaints of wrongdoing, if there is protection for the confidentiality of the person blowing the whistle; if there is protection against

retaliation; if there are procedures for conducting good faith investigations of complaints, and for providing information to the complainant about the results of an investigation; and good faith efforts are undertaken to provide remedies when wrongdoing has been shown.

In private businesses, there should be similar procedural protections for whistleblowers. Punitive measures should be permissible only when there is an intent to harm the business, as in the disclosure of trade secrets to a competitor. In addition, of course, there should be public interest exceptions to punishment. For example, an employee who discloses environmental damage or racial, sexual or other invidious discrimination as a result of business practices that have been concealed by the business, and where there are no procedures within the business for dealing effectively with those practices and correcting abuses, should be protected.

In some discussions of whistleblowing, efforts have been made to put Julian Assange and Chelsea Manning into the same category as Edward Snowden. That does not seem appropriate. Assange and Manning released publicly a vast amount of information just because they were able to put their hands on the information. They were not engaged in specific efforts to expose wrongdoing. Some of the information they released may have served valuable purposes. In other cases, it may have done harm. I don't think any purpose is served in providing legal protection for the promiscuous dissemination of confidential information simply on the basis that it has been confidential. Manning may well have been mistreated in detention, but that seems a separate issue. Whether or not Assange warrants prosecution for his part in publishing the information made available by Manning is a separate question, but he is not a whistleblower.

Although Edward Snowden's revelations have attracted a great deal of attention worldwide, the level of outrage that has been generated thus far in the United States and internationally seems relatively modest. What we don't know at this point is whether information collected by the National Security Agency has been used in invidious ways that are not directly connected to protecting the United States against terrorism. Perhaps there has been such use of information, perhaps not. The fact that the information has been assembled and is potentially subject to abuse is not the same as knowing that it has been abused. If the information has been misused, we are most likely to find out about it as a result of disclosures by a future whistleblower. Snowden demonstrated that information that should have been known about the NSA's collection of information only was made known as a result of his efforts. There seems no reason to think that we will learn about possible misuse of the data collected unless and until another Edward Snowden comes along.

Privacy and Secrecy:
The global politics and policy of information exchange and regulation

By

Abraham Newman
Georgetown University
aln24@georgetown.edu

This note has been prepared for the workshop on Secrecy, Surveillance, Privacy, and International Relations, April 16-17, 2015, MIT.

Personal privacy and government secrecy create rules that restrict the flow of information. Interestingly, free speech advocates have derided both as limiting transparency and accountability in a democratic society (Schwartz 2000; Volokh 2000). In part, these criticisms stem from worst-case scenarios in which an absolute right to privacy fosters a Luddite world of technophobes that hampers necessary information exchange. Alternatively, government secrecy run amok leads us down an Orwellian path of state control. While both specters play a useful role in raising the salience of such issues in public debate, they quickly distract from the real policy goal i.e. finding a set of appropriate rules that balance competing interests such as free speech, privacy, and security (Swire and Steinfeld 2001). Rather than placing these competing interests in a zero-sum relationship, such rules ideally create a practical set of standards that allows for their mutual coexistence.

Attempts to balance privacy and secrecy, however, become even more difficult when placed in a global context (Newman 2008; Swire and Litan 1998). With the rise of transborder information flows, citizens' personal data enters the databases of foreign governments. Citizens' must trust that these foreign governments will respect their domestic civil liberties. This bargain becomes increasingly difficult, when these foreign governments make extensive use of secrecy as it undermines trust in such international exchanges (Farrell and Newman 2014). Ultimately, this tension has the potential to degrade the quality of global data as citizens and governments look to ring-fence personal information domestically.

In this quick note, I hope to do four things: (a) lay out the key standards that animate most privacy frameworks, (b) articulate the tensions that arise between such frameworks and demands for government secrecy, (c) examine different efforts to integrate privacy and secrecy concerns and (d) highlight the difficulty of doing this in a global context.

Regulating Personal Information – Fair Information Practice Principles

Data privacy is primarily concerned with the collection, storage, transfer, and use of personal information (Solove, Rotenberg, and Schwartz 2006). It is distinct from other notions of privacy such as bodily privacy such the right to terminate a pregnancy or constitutional privacy associated with the idea of search and seizure. In short, it centers on the rules that govern how governments, firms, and individuals may use personal data in an information society.

Data privacy regulations differ across countries in terms of the scope of their coverage, their stringency, and enforcement mechanisms (A. Newman 2008). On the one hand, countries in Europe and elsewhere have passed comprehensive legislation that regulates the collection, use, and exchange of personal information in the public and private sector. In such comprehensive regimes, independent regulatory agencies – data protection authorities – exist that are dedicated to the implementation and enforcement of data privacy laws. In a smaller number of democracies, including the United States and South Korea, regulation is limited primarily to the public sector and a few key sensitive sectors. In such limited

regimes, oversight and enforcement is often decentralized across a range of agencies and there is no single dedicated privacy regulator.

Despite such cross-national differences in privacy regimes, the basic principles that animate such regulation are surprisingly similar (Bennett 1992). These principles include among others the right to be notified before the collection of information, the right to consent to the further distribution of information, the right to access data held by a data controller, the right to object to incorrect data, and the right to demand erasure of incorrect or disputed information. Labeled the Fair Information Practice Principles (FIPPs), they were first elaborated in national privacy legislation in Sweden and the United States in the 1970s and were latter codified internationally in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 and the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data which came into force in 1985 (OECD 1980). See Table 1.

Table 1: The Fair Information Practice Principles

Collection limitation: personal information collection should be limited and lawful
Purpose: the purpose of data collection should be disclosed and data should not be used for other purposes without consent
Openness: individuals should be informed about privacy policies
Accuracy: data should be accurate, complete, and current
Participation: individuals may request information about data held by organizations and challenge incorrect data
Security: stored data must be secure from theft or corruption

Accountability: organization must be held accountable to measures that implement the above principles

Secrecy and Privacy Tensions

Importantly, government secrecy and data privacy both accept the principle that information flows may be restricted. The key tension arises from the fact that data privacy regulations attempt to offer citizens assurances against unwanted uses of such information. The specter of secret surveillance efforts, however, undermines many of the central tenants of such privacy regulations as they limit the ability of individuals or regulators to know about the existence of data surveillance efforts and in turn hinder efforts to foster the appropriate use of such data (Roberts 2006).

Given the above basic privacy principles, a number of particular tensions arise when governments make extensive secrecy claims. In particular, individuals may not be aware that they are being monitored, breaching openness requirements and raising surveillance concerns. Moreover, it becomes increasingly difficult for individuals to check the accuracy of information held and correct errors when surveillance programs are not disclosed. A core principle of privacy regulation is that information collected should be used primarily for the purpose for which it was collected and not 'secondary' uses. Secret surveillance efforts undermine accountability efforts that are geared towards minimizing fishing expeditions.

Privacy and Secrecy in Practice

These tensions have been recognized in existing privacy regulation in at least one of two ways. In some instances, privacy rules explicitly allow for exemptions in

areas deemed vital for national security. While such exemptions do not eliminate the tension between privacy and secrecy, they recognize the limits of data privacy rights in the face of security concerns. In the European context, the debate is often framed as an issue of proportionality – national security exemptions are permitted but must be weighed in relationship to the extent such exemptions will violate individual privacy.

Even with proportionality balancing tests, however, secret data collection efforts raise a number of issues as there is little guarantee that such proportionality is being conducted according to stated goals and objectives. A second mechanism that has been employed to enhance accountability is to integrate third-party oversight and redress mechanisms. In an increasing number of cases, data privacy authorities or government ombudsmen have been called upon to screen and spot check closed databases. In most cases this is used for disclosed databases in which the information contained in them is restricted to the public. In Europe, for example, there is a large customs and immigration database known as the Schengen Information System. While governments were wary to allow direct citizen rights of access or correction, the Joint Supervisory Authority of the Schengen Information System conducts periodic reviews of the system. Composed primarily of technical experts from national data privacy authorities, the Joint Supervisory Authority conducts spot checks and follows up individual complaints. In its most far-reaching implementation exercise, the Joint Supervisory Authority investigated the use of Article 96 Alerts. These alerts are flagged by customs officials when third country nationals are refused entry to a Schengen country. The Joint Supervisory Authority

had received complaints that these were being used inappropriately and thus undertook a joint review. The JSA made a set of implementation recommendations to improve the system (Joint Supervisory Authority of Schengen 2006). National data privacy authorities, then, investigated individual cases and followed up with their respective governments. The Danish data privacy authority, for example, examined the 443 alerts entered by Danish authorities and found 22 inappropriate alerts. Working with the National Commissioner of Police, the Danish privacy authority got the inappropriate alerts corrected and helped revise the alert procedure (Joint Supervisory Authority of Schengen 2005).

Security and Privacy in a Global Information Society

Global information exchange increasingly places citizens' personal data in the hands of foreign governments. Governments and citizens are put in the position of placing their civil liberties in the hands of foreign governments. Given differences in national privacy rules, this is a difficult political maneuver that requires an extensive amount of trust in the foreign government. Government secrecy further complicates this issue as it attenuates traditional notions of accountability and transparency that states use to bolster public support in international cooperation. Secrecy, then, risks undermining cross-border information sharing and in turn degrading the quality of data available.

A series of disputes between the US and Europe illustrate this dynamic. After the 9/11 terrorist attacks, the US ramped up data collection on foreigners. Some of these efforts were secret (e.g. financial tracking of bank data held by SWIFT or NSA monitoring) while others limited access or disclosure (e.g. the transfer of Passenger

Name Records). When disputes arose between the transatlantic partners, they frequently centered on issues of accountability and oversight (Newman 2011; Farrell and Newman 2014). The US repeatedly claimed that it had procedural checks in place to prevent abuse. As more and more dark networks have been revealed, however, this argument has become increasingly untenable. With the Snowden revelations, governments and firms in Europe have started to question extensive data sharing as well as the outsourcing of information technology processing and infrastructure to US companies that might be forced to turn over personal data to the US government. This issue is complicated even further as the US limited data privacy regime lacks a dedicated privacy authority. Attempts by US officials to pledge third-party oversight have been increasingly re-buffed as Europeans do not see a trusted third-party on this side of the Atlantic.

While tensions clearly exist between privacy and government secrecy, public officials, privacy advocates, and citizens often recognize the importance of their coexistence. In order to facilitate this uncomfortable compromise, governments have stressed proportionality and third party oversight. Unfortunately, dark databases undermine such "trust us" claims. This corrosive effect of secrecy becomes even more pronounced in the international context where governments and citizens are already wary of the intentions of foreign governments with different legal systems and governance institutions.

Bibliography

Bennett, C. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.

Farrell, Henry, and Abraham Newman. 2014. "The New Politics of Interdependence Cross-National Layering in Trans-Atlantic Regulatory Disputes." *Comparative Political Studies*, August, 0010414014542330. doi:10.1177/0010414014542330.

Joint Supervisory Authority of Schengen. 2005. "Article 96 Inspection." June 20.

———. 2006. "Schengen Joint Supervisory Authority Activity Report 2004-2005."

Newman, A. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press.

Newman, Abraham. 2011. "Transatlantic Flight Fights: Multi-Level Governance, Actor Entrepreneurship and International Anti-Terrorism Cooperation." *Review of International Political Economy* 18 (4): 481–505. doi:10.1080/09692291003603668.

OECD. 1980. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: Organization for Economic Cooperation and Development.

Roberts, Alasdair. 2006. *Blacked Out: Government Secrecy in the Information Age*. Cambridge University Press.

Schwartz, Paul M. 2000. "Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence." *Stanford Law Review* 52 (5): 1559–72. doi:10.2307/1229521.

Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz. 2006. *Privacy, Information, and Technology*. Aspen Publishers Online.

Swire, Peter P., and Lauren B. Steinfeld. 2001. "Security and Privacy after September 11: The Health Care Example." *Minnesota Law Review* 86: 1515.

Swire, P., and R. Litan. 1998. *None of Your Business: World Data Flows, Electronic Communication, and the European Privacy Directive*. Washington, DC: Brookings.

Volokh, Eugene. 2000. "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You." *Stanford Law Review* 52 (5): 1049–1124. doi:10.2307/1229510.

Diplomacy in an era of declining secrecy

Justin Rood
Fellow, Information Society Project, Yale Law School

Prepared for the MIT Workshop on Secrecy, Surveillance, Privacy and International Relations, April 16-17, 2015

Successful diplomacy relies on secrecy – for negotiations between countries, for internal deliberations and analysis, and for safeguarding sensitive information on a nation's plans and capabilities. But technology has undermined the ability for nations to keep secrets. It has eroded the privacy of the state, if such a concept can be said to exist, just as it has eroded the privacy of the individual.

In recent years, national security experts have begun to seriously consider that state secrecy may soon be practically impossible.[1] That is not to say that every piece of protected information will be exposed because of technology, but rather governments are becoming less able to predict what information will stay secret and what will be compromised – by a foreign power or criminal hacker; by an insider – a leaker, whistleblower, or inattentive bureaucrat; or by the growing world of open source information. "In 15 years, there will be no more secrets," one CIA official pronounced – in 2008.[2]

Unfortunately, no significant efforts have been made, outside of the occasional roundtable or seminar, to rethink national security strategy in a global environment that has turned increasingly inhospitable towards secrets. This brief memo argues that with some exceptions, technological progress and our capacity for secrecy move in opposite directions, and that should give a sense of urgency to a wholesale re-evaluation of how nations approach diplomacy and national security strategy in general.

Below are three brief examples of recent compromises in national security that were aided by technology. One involves the foreign penetration of sensitive U.S. systems. Another involves the increased exposure resulting from commercial satellite imagery, and the third is a well-known case of a massive leak of sensitive diplomatic cable traffic by an American soldier.

---

[1] See, for instance, "No More Secrets: National Security Strategies for a Transparent World," a March 2011 report resulting from a roundtable convened by the American Bar Association and the Office of the National Counterintelligence Executive.
[2] From "No More Secrets," page 3.

They are each significant, but not unique. Together they illustrate the growing problem of securing diplomatically sensitive information in an age of increasing technology-driven transparency, and underscore the need for developing a national security strategy which does not rely on secrecy for strategic advantage.

1. Presumed Russian hacking of sensitive U.S. email systems

In February 2015, the *Wall Street Journal* reported that hackers believed to be connected to the Russian government had penetrated the State Department's computers in November 2014, and U.S. cybersecurity experts were unable to thwart them.

Two months later, CNN reported the same hackers had compromised unclassified networks at the White House, gaining access to sensitive communications relating to the president's schedule.[3] ABC reported the hackers accessed emails of the White House counsel's office.[4] While not classified, communications and drafts of the White House counsel can be considered privileged and may not be shared with Congress even pursuant to an official request. The reportedly compromised information was non-public, sensitive, and almost certainly contained details of significance to Russia or other foreign powers.

Of the talent of Russian hackers, the *Journal* reported in February:

> Assuming that Russia was involved, U.S. investigators are puzzling over why were they able to detect the breach. American national security officials view Russia's computer warriors as on par with their own and capable of avoiding detection. One person familiar with the incident said that either Moscow wanted to send Washington a message, or it had deployed the 'B-Team.' [5]

The penetrations themselves are enough to challenge our notion of how well the United States can protect sensitive information that may carry foreign policy implications. But the *Journal's* unsourced observation that U.S. officials do not necessarily expect to know if Russian hackers have penetrated their systems is even more jarring. It's one thing to rely on inconsistent security systems; it's another to rely on an inconsistent system when one may not know when and how it is failing.

---

[3] Perez Evan, "How the U.S. thinks Russians hacked the White House," CNN.com, April 8, 2015.
[4] Ross, Brian, "Russian Hackers Have Been in White House System for Months, Officials Say," ABCNews.com, April 7, 2015.
[5] Yadron, Danny, "Three Months Later, State Department Hasn't Rooted Out Hackers," *Wall Street Journal*, Feb. 19, 2015.

2. Open source imagery to model Pakistani nuclear facility

Bryan Lee spent years in nonproliferation at the Defense Department, where his duties included serving as a U.S. inspector of Russian missile facilities under the START treaty. Now an expert with the James Martin Center for Nonproliferation Studies in Monterey, Lee traded in the spy satellite imagery and constrictions of START inspection regimes for Google. What he and his colleagues get from Google, he says, is as good as what he had at the Pentagon, and often superior. In a presentation at Yale Law School in February, Lee gave a few examples.

At the Pentagon in the early 2000s, classified satellite imagery of Russian sites he was given to review before an inspection visit had a resolution of around one meter. Today, Google Earth can give anyone imagery to a quarter-meter resolution, Lee said, a remarkable improvement.

What's more, Google Earth now has embedded geotagged photography of points of interest all over the world, including photographs of sites Lee once inspected. Under START, Lee was prohibited from bringing a camera on an inspection visit or photographing any part of the interior or exterior of a facility.

To illustrate the power of open source imagery, Lee cites the accomplishment of Tamara Patton. As a graduate student in 2011 Patton used commercial satellite imagery, free 3-D modeling software, and some basic trigonometry to generate a surprisingly detailed model of a Pakistani plutonium production facility in Khushab. The model helped her make what is now considered one of the most accurate estimates of the facility's production capabilities at the time.

No espionage or hacking was needed for a student on the other side of the world, armed only with curiosity, high school math skills and an Internet connection, to determine the capacity of a Pakistani nuclear facility – information that can have implications for diplomacy and foreign policy.

3. Release of State Department cables by Wikileaks and Chelsea Manning

In November 2010, the *New York Times* and other news organizations reported on a leaked tranche of over 250,000 sensitive State Department cables, many classified, transmitted mostly during the previous three years. The cables contained details on U.S. intelligence, sensitive observations and analysis on foreign governments and leaders, and more.

Pfc. Bradley Manning, now Chelsea, had exfiltrated from his base the 1.6 gigabytes of sensitive information by copying it onto a CD labeled "Lady Gaga." It was eventually passed to a reporter on a thumbdrive "no longer than a couple of fingernails."[6]

The Manning leaks were a massive exposure of sensitive diplomatic information, and they were largely made possible by technology. Obtaining, storing and sharing that much information would have been much more difficult without today's computers, networks and storage.

The security implications of the cable leaks were proclaimed to be grave. It was reported to have sparked a global diplomatic crisis; former Sen. Joe Lieberman declared the leak was "nothing less than an attack on the national security of the United States."[7] Looking back, some have credited Manning's actions with triggering actions in the Middle East which led to the Arab Spring.

Some observers seized on Manning's fragile psychology to explain his actions: he reportedly had violent outbursts and wet himself, he had shouted at his commanding officers, and some felt he was unfit for duty.[8] "The U.S. Defense Security Service is also investigating why Manning, who had been sent for psychiatric counselling before he was deployed to Iraq, was not screened more fully before he was allowed to work in intelligence," *The Guardian* newspaper reported at the time.[9]

Too often in cases like these, our tendency is to focus on the exceptional nature of the actor: the supremely wily foreign adversary, the particularly bright graduate student, the uniquely troubled leaker. We fail to take into account the consistencies of the cases: in each, and dozens more that preceded them and will follow, technology has not only played a role in but is a critical factor for facilitating the compromise and maximizing its impact.

When the role of technology is considered in these cases, it is often regarded as something that with money and time can be made more secure. In each specific case, and in specific ways, this may be true: software can be patched. Access controls can be restricted. Yet our history with technology suggests that when regarded broadly, the opposite is true. As technology advances, leaks become bigger, hacks increase, and the information available online to the public becomes more plentiful, more timely, and more accurate.

---

[6] Leigh, David, "How 250,000 US embassy cables were leaked," The Guardian, Nov. 28, 2010.
[7] Condon, Stephanie, CBS News, "Congress Lashes Out at Wikileaks, Senators Say Leakers May Have 'Blood on their Hands,'" November 29, 2010.
[8] O'Kane, Maggie, "WikiLeaks accused Bradley Manning 'should never have been sent to Iraq,'" The Guardian, May 27, 2011.
[9] Ibid.

In such an environment, it would be meaningful for the United States – and other countries – to examine how the many functions of diplomacy, from negotiating treaties between nations and enforcing them, to sharing observations and analysis among foreign service officers, to guarding information about a nation's own capabilities, should be conducted absent the assumption that secrecy can be assured.

Rahul Sagar

Who Guards Against The Guardian.com?

In my recent book *Secrets and Leaks* (2013), I argue that unauthorized disclosures—whistleblowing as well as leaking—are consonant with democratic and constitutional values when they help expose wrongdoing. Further I argue that whistleblowing and leaking constitute an especially credible form of oversight since insiders do not typically encounter limitations of information and expertise that hobble lawmakers and judges.

State officials may view these two arguments—that unauthorized disclosures can be legitimate and effective checks on executive power—with some skepticism. It may be mistakenly thought I am essentially espousing or extending the view taken by much First Amendment scholarship. Such a conclusion would be gravely mistaken

I am a non-partisan, and a moderate. For both temperamental and intellectual reasons, I tend to look for important interests on both sides of an issue. My preference is typically to strike a (hopefully refined) balance, based on evidence when it can be had; I am not an ideologue who starts with first principles or premises that brook no opposition or compromise.

What this means in practice is that I devote a significant portion of *Secrets and Leaks* to making the point that First Amendment defenses of whistleblowing and leaking completely fail to acknowledge, much less counter, the possibility that government employees, reporters, editors and publishers can have personal, political, financial, and other motives for disclosing secret information. Such disclosures may be partial, biased, or manipulative, and intended to defeat a policy that is otherwise supported by representatives and representative institutions operating under law. A major concern here is that the government cannot easily confront such malignant disclosures because the relevant evidence may not be suitable for disclosure, thereby leaving the public

misinformed. Alternately, if the government does respond with counter-leaks, the public is left struggling to discern the true picture.

I will not rehash here the cases I discuss there. These include the *New York Times'*s disclosure of the Terrorist Financing Tracking Program (TFTP) and James Risen's disclosure of Operation Merlin. The former it will be recalled was criticized by the *Times*'s own Public Editor, and the latter followed after the *Times*'s decided *not* to publish Risen's story. More recent cases in this vein include indiscriminate data dumps by Wikileaks and Edward Snowden's associates in the media.

What I briefly discuss in this memo are the remedies I examine in *Secrets and Leaks* to temper the press's rashness. The challenge here is that one does not want to throw the baby out with the bathwater. For the reasons outlined above, it is important that the safeguard we devise against rash or manipulative disclosures does not inadvertently strangle legitimate and important disclosures.

How can this be done?

A first step is to clarify what we can reasonably say the press's duty is. I argue in *Secrets and Leaks* that the press has a duty to filter out malicious or misleading disclosures (and when they lack certainty about the intention or content of a disclosure, to do their utmost to inform the public of the source's possible agenda or other conflicts of interest). This claim is, I posit, uncontroversial. It is precisely what the *New York Times* and *Washington Post*, among other outlets, explicitly claim their policy is with respect to 'confidential sources.'

Where things become complicated is when we turn to the second step, namely, enforcing the norm cited above. How can *this* be done? The record on self-regulation is

not heartening. For decades now media critics and ombudsmen (such as those for the *Washington Post*) have openly declared their inability to enforce this norm.

So what are the alternatives?

One alternative is to turn to the law. I show at length in *Secrets and Leaks* that this course of action is fraught with trouble. A law that seeks to compel the press to act as a filter is certain to be confronted by a host of First Amendment challenges. Even a narrowly tailored law may be seen as restricting political speech; the requirement to correct the public record may be deemed as interfering with editorial freedom; and requiring a reporter to reveal his or her source to a judge may be seen as violating reporter's privilege and thereby hindering news gathering. It is a separate matter that the government has been unwilling to take on the press even when it has clear legal support on its side—for instance §798. Then there is the reality that with the rise of the Internet publishing can be done outside the national jurisdiction, as the Snowden (and before that Agee) case shows.

A second course of action would be to bolster self-regulatory mechanisms. This approach has the advantage of avoiding messy—and likely unsuccessful—legal battles. But it is hobbled in two ways of its own. First, given competitive pressures and the constant drilling in of an adversarial mindset, there is little willingness on the part of the news media to corral unauthorized disclosures. Incidental details may be withheld, but juicy scoops are rarely passed up, and when the institutional press passes them up, they still make their way on to the Internet. In short: the media sector is too fragmented to regulate itself.

A second problem is institutional. If we do strengthen internal oversight mechanisms—for instance by empowering ombudsmen to review evidence and punish perpetrators—then we are likely to see media organizations choose 'safe hands' to be ombudsmen.

Alternately, we are likely to see the business of publishing salacious disclosures migrate further to the Internet where such pesky self-regulation is unlikely to exist. In short: internal regulation is more likely to work when the press is institutionalized than when it is freewheeling.

A third approach would be to foster a competitive media environment in the hope that the misuse of anonymous sources will be subject to public rebuke by rival media organizations. Part of the reasoning here is that in a cut throat media market competitors will have an incentive to undermine the credibility and reputability of opponents who can be shown to have engaged in dubious reporting practices. Unfortunately the empirical evidence does not support this view. Media organizations tend to give each other wide berths when it comes to anonymous sources, and in the few cases where blood has been drawn—e.g. the dismissal of Judith Miller—there is no clear evidence of a wider, systemic impact.

This brings me to the final option—the one that I tentatively endorse in *Secrets and Leaks*. I argue there that we must hope that enterprising citizens will establish an independent and well-funded organization dedicated to scrutinizing media performance, which could name and shame reporters and editors who misuse anonymous sources, and the publishers who condone such behavior. This proposal basically echoes what the Hutchins Commission had to say more than half a century ago. Since this proposal proved unpopular with the media establishment, it has been allowed to fade from public consciousness. Now that we have understood why this proposal is so important—because there are so few viable means of regulating the press—I hope this proposal will be revived.

A civil society organization of this kind would have a number of advantages: its advice and reports would not violate the First Amendment as it would not interfere with publication or news gathering; it could be so structured as to have members reasonably

sympathetic to the press; and if done with sufficient gravity or ferocity, its reports could inflict suitable reputational harm on reporters and publishers, including those based overseas and otherwise beyond the reach of the law, hopefully leading them to exercise the sort of self-restraint that would further rather than harm the public interest.

Since I am not much of an optimist I conclude *Secrets and Leaks* by warning that even such an organization is likely to have limited benefit. A fundamental problem American democracy faces is that its consumers of news, especially in an era of 160 character statements, seem to be more drawn to hyperbole than they are to sober or measured reports. So the conglomeration of "armchair media ethicists" envisioned above may find few takers for their reports. Still, it will mark a start, and perhaps we can combat sensation with sensation (the *Daily Show* is surely one of the most important sources of media criticism, showing that such exercises need not be dull or dulling). Ultimately, we have no choice but to persevere: Politics is, after all, "a strong and slow boring of hard boards."

***

Solid Footing for Japanese Democracy?

Richard J. Samuels
Massachusetts Institute of Technology

A Designated State Secrets Law was prepared by Japan's Cabinet's Intelligence Research Office and approved by Prime Minister Abe Shinzo's government in October 2013. In the subsequent year, the law passed the national Diet with multiparty support. It generated significant protest, underwent considerable public discussion and, ultimately, was amended to reflect popular concerns. Postwar Japan's first comprehensive state secrets regime got underway in December 2014, and legislative oversight began last month.

The law replaced ministry/agency specific practices with uniform guidelines across 19 government units for the classification of information in the areas of defense, diplomacy, counter espionage, and counter terror. These categories were further specified in more than 50 sub-classifications, such as military plans, weapons performance data, communications codes, details of negotiations, and specifics relating to intelligence collection and anti-terrorism preparations.

The law also stipulates an initial 30 year period of designation, with the possibility of renewal for an additional 30 years. A third period of 30 years can be designated by Cabinet order if the information concerns weapons systems, is relevant to ongoing negotiations, contains information on collection cryptography, or has been supplied by another country or international organization in which it is subject to a longer designation. In addition, the law establishes a system for background checks of government employees. Violators of the law— malicious leakers and whistleblowers alike— face up to ten years in jail. In a particularly controversial legal stipulation, those who come to learn a designated secret by accident, even in the course of official duties, face up to five years in prison.

This bill became a law with unusual speed and determination on the part of the Abe government. It was debated in Diet for far less time than is normally allotted for major legislation, engendering impassioned criticism of legislative "steamrolling." The anti-Abe *Asahi Shimbun* editorialized that "the ruling coalition railroaded the DSSL through the House of Representatives … in blatant disregard of the will of the people and the opposition camp's call for further deliberation." But even Abe's chief cabinet secretary allowed as how "we should have shown more humility" and acknowledged that an additional 60 hours for public examination could have been added.

samuels@mit.edu

In the event, however, a vigorous debate continued well beyond the legislative process, one that was strikingly different than any before it in this important domain— at least in Japan. All democracies grapple at one time or another with finding the right balance between protecting personal freedoms and control of information, between transparency and secrecy. Indeed, many of the world's most robust democracies, like the United States, the United Kingdom, and the Federal Republic of Germany, are always— or at least are serially— grappling with these choices. Japan has not come late to this issue. In the postwar era it has often engaged it with vigor, but the government had repeatedly failed to enact a comprehensive classification regime that would provide an effective mechanism for intelligence collection or, as Prime Minister Abe discovered during a hostage crisis in Algeria soon after he took office, an effective mechanism for intelligence sharing with allies.

Prime Minister Abe is one of postwar Japan's most conservative prime ministers, and is openly committed to "ending the postwar" and to "taking back Japan." Many understand these slogans as dog whistles to supporters of revisionist understandings of Japan's wartime behavior and to those who would prefer a more muscular and autonomous Japan. It thus surprised no one that he decided to champion state secrets legislation. Abe frequently has argued for enhanced security planning and intelligence capabilities in speeches and essays. Indeed, in his first, short-lived, administration (2006-7), he chaired inter-ministerial meetings on intelligence reform that resulted in a report arguing for secrecy legislation as part of the establishment of a new national security infrastructure. But his government collapsed and his successors directed officials not to issue the report, fearing the public had not yet been adequately primed to receive it.

By the time he returned to power in 2013, Abe was more determined than ever to enhance Japan's security and intelligence infrastructure. And this time he enjoyed an overwhelming majority in the lower house and, with the support of coalition partner Komeitō, a majority in the upper house as well. Abe claims that his "ah ha!" moment regarding the need for a secrets law came during a summit between President George W. Bush and Prime Minister Junichirō Koizumi when their interpreter was subjected to a background check by the U.S. government. But his political allies report that the more direct precipitant was the January 2013 hostage crisis in Algeria, when an Al Qaida-affiliated group took 800 gas plant workers hostage. Ten of the thirty-eight hostages who died in the crisis were Japanese, the largest loss of Japanese life abroad since 9/11 in New York City. The Japanese government found itself operating largely in the dark, with insufficient intelligence of its own and little more supplied by the American, British, or French intelligence services which reportedly were concerned about possible leaks from the Japanese side. Abe was determined to establish a system that would "keep a firm protective lid on information in order to be able to receive high quality information [from allies]." Indeed, this was his primary public justification for the DSSL. He frequently

declared that "without rules on managing classified information, we cannot obtain intelligence from other countries." The DSSL was— along with the establishment of a new National Security Council and the enhancement of Japan's underdeveloped intelligence community— a critical building block in Abe's desire to build entirely new national security architecture.

Until this current round, Japan's debate on classification and espionage had focused less on the universal issues related to secrecy and privacy than on the unhappy peculiarities of Japan's past, a past that has dominated the present in Japanese politics for many decades. Part of the opposition mobilized by stoking the fear that war and totalitarianism lie at the base of any effort to strengthen state power to control information. For these opponents, any law relating to state power vis-à-vis espionage, secrets, and intelligence sits atop a slippery slope to Japan's mid-20th century authoritarian past. Abe's open affection for (and adoption of ideas from) his grandfather, Kishi Nobusuke, an unindicted Class A war criminal and former prime minister, was merely exhibit A in their case.

This time, however, the rhetoric of the slippery slope did not prevail. To the contrary, although the Japanese public was not pleased with the Abe government's handling of the secrecy law, the familiar, Japan-specific, and long dominant "slippery slope" objections faded before more universal concerns about how to ensure that secrecy will be used to enhance national security rather than to conceal abuse of power. Transparency, arbitrary application, press freedoms, whistle blower protection, and even human rights dominated the discourse. All were central to the Tshwane Principles promulgated by the NGO community in South Africa in the months before the Japanese debate. Opponents of the law, including leading freedom of information advocates, participated actively to make it more acceptable and to reassert political control of the bureaucracy.

Measured against the Tshwane Principles, the legal outcome of the Japanese debate was imperfect. But as Tshwane advocates readily acknowledge, their principles are not fully embraced anywhere— and are in some measure resisted as a matter of course by many governments. In Japan, amendments to the law were accepted that protect whistle blowers, that notionally protect against arbitrary classification, and that require review of the law's implementation in five years. Weak oversight commissions were established in each house of the national Diet—no small innovation in a system that is used to bureaucratic, rather than legislative, supervision of all administrative matters It seems no less significant that Japan's discourse on state secrets has migrated from debates about the particular experience of wartime authoritarianism to a more universal concern for the preservation and health of democratic norms. Japanese civil society may have abandoned the slippery slope to find solid footing for vigilant and engaged citizens, many of whom seem to trust that they have a government that hears them.

samuels@mit.edu

Mattathias Schwartz
April 2015 Endicott House Memo Conference
Secrecy, Privacy and International Relations
Mattathias.Schwartz@gmail.com

PRIVACY & SURVEILLANCE NORMS IN ISRAEL

Background

Israel's approach to national security has been defined by a persistent sense of vulnerability. After its foundation in 1948, Israel engaged in several military campaigns, often on its own soil, against hostile neighbors. After years of stalwart U.S. support and Israel's acquisition of nuclear weapons, its relations with the region are considerably more stable. Israel's most pressing security concern is reaching a settlement with the Palestinians over Gaza and the West Bank. But the national culture surrounding transparency and surveillance in Israel reflects the fact that Israel has spent its sixty-six year lifespan on a wartime footing. Israel's $23 billion aggregate military budget of Israel is surpassed by twelve countries; Israel's per-capita military spending is second only to the United States. Military service is compulsory at age 18 for a period of two to three years; many Israelis continue to serve as reservists well into middle age.

The primacy of the military means that most Israelis have some firsthand experience handling sensitive state information, and that Israeli society does not have a separate "civilian" sphere in the same sense as that the U.S. and Western European countries do. A closer analog is South Korea, which also has compulsory enlistment, hostile neighbors, and civil liberties that are unusually circumscribed for a democratic state. While Israeli law grants citizens some control over their personal data in a business context, government surveillance is vast and opaque. The laws protecting government information are strict and the punishments for violating them are harsh. Israel's Penal Law of 1977, and the Emergency Defense Regulations, which have been continuously renewed since 1948, both put a high burden on citizens to be cautious about the possession or

distribution of information that runs contrary to state interests. Paragraph 99 of the Penal Law authorizes the death penalty or life imprisonment for the crime of "delivering information with the intent that it shall fall into the hands of his enemy … with intent to assist the enemy in war against Israel." This applies whether or not the information is classified, whether or not Israel's security is damaged, and whether or not Israel is at war. Harming morale, inciting Israelis not to serve in the army, publishing "seditious" material intended to "raise discontent or resentment," and membership in subversive organizations are also all crimes[1]. Wiretaps and arrests can be undertaken without consulting with a judge. Under the emergency regulations, any police officer with a reasonable suspicion is empowered to make warrantless seizures of "goods, articles, documents or things." In 2007, the Knesset passed the Criminal Procedure Law, which explicitly gives police access to electronic data, including locational data, with minimal judicial oversight. These powers can be used in investigations with no connection to the military. "Israelis are used to being spied on all the time," wrote the Israeli legal blogger Jonathan Klinger. According to Klinger, Israeli police used these new powers more than 9,000 times in 2009 alone.

Israeli newspapers cannot legally operate without a government permit, and sensitive reports by Israeli media are subject to review by a military censor prior to publication. Foreign media must submit to the same process or risk losing their credentials. The Israeli public could (of course) vote to alter this balance of rights-versus-order through parliamentary elections. Thusfar, it has chosen not to. The Association for Civil Rights in Israel has attempted to push back against government surveillance powers through the courts, but with little success.

Snowden and the Memorandum of Understanding

[1] Use of the law against sedition is rare. It was charged by military courts three times during the 1950s, and again in 1990 against Meir Kahane, a Brooklyn-born rabbi and one-time member of Parliament, for calling Arabs "a cancer spreading in our midst" at a rally in Jerusalem.

In September 2013, the *Guardian* published a classified document from Edward Snowden's trove, a five-page Memorandum of Understanding between the National Security Agency and its Israeli counterpart. The document reveals that the U.S. "routinely" sends "raw" signals intelligence in bulk to Israel, data that has not been "minimized" or screened for private information on U.S. citizens, including U.S. leaders. The M.O.U. lays out Israel's privacy obligations regarding the handling of the data, placing the onus on Israel to apply the N.S.A.'s oversight, training, and minimization regime. This suggests that the U.S. trusts Israel to carry out their wishes after data has left their hands, and to handle it with more discretion than Israel is obliged to handle data from its own citizens. Some have argued that this approach is naïve. "Do we really expect the Israelis to … abide by the Fourth Amendment, and the U.S. Constitution, which is what the M.O.U. asks the Israelis to do?" asked Matthew Aid, an intelligence historian.

Indeed, the M.O.U. does evince a belief on the part of the N.S.A. that Israel will self-report breaches of the agreement, and that the ordinary mechanisms of U.S. bureaucracy—management reviews, annual reports, and one N.S.A. "special liaison officer" assigned to Israel—will be sufficient for enforcement. U.S.-enforced agreements about the disposition of nuclear material and sensitive technologies are far more stringent. It's worth asking whether this M.O.U. was actually intended to protect the data of U.S. persons, or whether its purpose was to generate the necessary paperwork to satisfy the N.S.A.'s own internal compliance requirements.

Other documents partially released by Snowden fill out a complex picture of the U.S./Israel relationship. Even as the two countries share facilities, equipment, staff, and intelligence, they also conduct all manner of espionage against each other. One report claims that Israel is the "third most aggressive intelligence service against the U.S.," after Russia and China. Another frets that the intelligence-sharing relationship is "being driven almost totally by the needs of the partner," Israel, but that little can be done due to the importance of Israel to U.S. interests in the region. More recently, Israel has been accused of attempting to disrupt U.S. negotiations with Iran over nuclear weapons by spying on the proceedings and feeding intelligence to Congressional Republicans.

Compared to Western Europe, the Israeli debate over U.S. surveillance practices has been muted, although Prime Minister Benjamin Netanyahu reportedly attempted, without success, to use disclosures about U.S. spying on Israeli soil as a bargaining chip to negotiate the release of Jonathan Pollard. Israel's patriotic culture, strategic vulnerability, more limited civil liberties, and longtime dependence on the U.S. as the guarantor of its security have all contributed to this dynamic. Perhaps the many Israelis who have served in the military have a sense of how their country's security establishment uses domestic intelligence, and this has served to ameliorate concerns about Israeli and U.S. surveillance practices.

The Unit 8200 Controversy

Among the Israeli left, surveillance has generally taken a back seat to more pressing issues—indefinite detention, restrictions on movement and the importation of goods in the Occupied Territories, Arab citizenship and voting rights, and the troubled path to Palestinian statehood. But in September 2014, a little more than a year after Snowden's initial disclosures, and two weeks after the conclusion of Operation Protective Edge in the Gaza Strip, forty-three Israeli veterans published a letter of protest regarding surveillance practices. Unlike Snowden's disclosures, which were mostly informed by documents, not personal experience, the Israeli veterans claimed to be informing the public about abuses that they had witnessed firsthand. All had served in Unit 8200, part of the military directorate of the Israeli Defense Forces, the rough equivalent to the N.S.A. In a letter sent to the prime minister, their military commanders, and published in the *Guardian* and the Israeli newspaper *Yedioth Ahronot*, the Unit 8200 veterans said there was "no oversight" of surveillance conducted against Palestinians in the Occupied Territories, and "no distinction" made by Israel between militants and civilians, innocent and guilty. In an interview, one of the letter's signers said he was instructed to retain compromising information on Palestinians that could be "used to extort/blackmail the person and turn them into a collaborator. At the base we were told that if we find out some 'juicy' detail about them, that it's important to document it … examples of this

were a difficult financial situation, sexual preferences, a person's chronic illness, or that of a relative, and necessary medical treatment." The reservists in the group said they would no longer take part in operations against Palestinians. The letter called on fellow soldiers in Unit 8200 to demand reforms.

Some have described the Israelis who signed the letter as "whistle-blowers," but their actions differ in many respects from those undertaken by Snowden. The Unit 8200 group did not offer any specific anecdotes, let alone documents to back up their charges. While some gave interviews to journalists and a documentary filmmaker and made their full names known to their commanding officer, all chose to remain anonymous to the public. Prior to releasing the letter, the group hired a lawyer and offered their statement to an Israeli military censor for review. Whereas much of Snowden's implied argument is essentially a legal one (the U.S. intelligence community is failing to live up to its obligations under the Fourth Amendment; Congress is failing to perform its oversight functions), Unit 8200 made more of a moral argument, that they had been given orders that they could not carry out in good conscience.

To understand the letter-writers' actions, it may be useful to put them in the context of *Ruach Tzahal*, the extensive ethical code that binds all enlisted Israelis. The code was designed by a committee, including Asa Kasher, a civilian professor of philosophy, in the mid-1990's, at the behest of then-Lieutenant General (and later Prime Minister) Ehud Barak. Among its "Three Fundamental Values," on par with loyalty to and defense of the state, is the obligation to "preserve human dignity." Furthermore, the Israeli military is known to value initiative and improvisation over strict discipline. According to one expert on the Israeli military, "too much emphasis on formal discipline [risks] … weakening the reliance on personal commitment, bravery, and unit pride that has repeatedly brought victory to the I.D.F."[2] Compared to the case of Snowden, who

[2] S.A. Cohen, "Towards a New Portrait of a (New) Israeli Soldier," 1997, as cited by Sidney Shapiro, "Religion and Politics in the IDF," 2010.

reportedly attempted to bring his concerns to superiors, Israel's relative tolerance for dissent within the ranks may have ultimately served the interests of its security forces to protect specific operational details. Both cases, however, are indicative of a larger trend, especially in light of Snowden's claim that he is a sort of freelance ombudsman for the N.S.A. ("I am still working for the NSA right now. They are the only ones who don't realize it.") Secret state organizations are increasingly likely to be troubled by the scruples of disillusioned junior members who believe they are failing to live up to the values they espouse. The specific form that these disclosures take will vary according to national culture, media climate, how the individual construes loyalty to the state's laws and values versus the hierarchical imperatives handed down by its security services. The people at the bottom of the ladder are well-situated to notice any gaps. Technology makes it easier for small groups and individuals to collect and publish vast troves of compromising data. The "insider threat" problem, as some have called it, is essentially driven by hearts and minds. Institutions that offer members a way to "voice" their qualms internally will likely have fewer members who choose to "exit" the obligations of secrecy altogether.

Technology Challenges and Technology Solutions for Providing Security and Privacy in Public Clouds

Nabil Schear and Marc Zissman
MIT Lincoln Laboratory
15 March 2015

Cloud computing is a model for deploying software and hardware resources at lower cost and with greater flexibility than typical enterprise computing. Key characteristics include on-demand self-service, broad-network access, resource pooling, rapid elasticity, and measured service. Most of us are daily end-users of cloud-computing environments, e.g., when we make web-based purchases, when we use Google or Apple cloud services, and when we watch web-based entertainment like Netflix.

Commercial cloud providers (e.g., Amazon, Google, Microsoft) focus heavily on providing availability and scalability for very low cost. These providers also have an interest in providing a reasonable level of security and privacy. Unfortunately, commercial cloud security is often proprietary and opaque, both to the cloud tenants (e.g., the company paying the cloud provider for hosting its web-based commerce site) and the tenants' customers (e.g., the consumers placing orders). Tenants typically have no visibility into cloud network security or data provenance. The commercial model is based on trusting the cloud providers, i.e., data are stored unencrypted inside the cloud and all processing is done on unprotected data. The only enforceable guarantees that tenants have are through legal "service level agreements". So, when the adversary strikes, e.g., when he seeks to steal data, to corrupt data or to make data unavailable, cloud tenants do not have timely and controllable mechanisms with which to respond. The customers of the tenants, e.g., the consumers placing orders, are even further "out of the loop" – they may eventually hear on the news or read in the newspaper about some compromise of their data, but that (possibly combined with an offer of two free years of credit report monitoring) is all they get.

So, we need to develop technical means for improving the security and privacy of cloud computing while retaining the many economic advantages it provides. Specifically, the research community should focus on providing solutions to the following four challenges:

- **Secure and Resilient Communication with Provenance** – The goal is to provide end-to-end protection and provenance for all cloud communication. We would like to be sure that data has moved into and out of the cloud while preserving confidentiality, and (ideally) we'd like to be able to track pieces of data through the cloud to understand which processes have read, written and modified them. Among the technical capabilities likely required are cryptographic key management and cloud provenance protocols and analytics.

- **Secure and Resilient Storage** – The goal is to enable both storage and query of encrypted cloud data without the need to decrypt the data (which would leave the data vulnerable, at least for short periods of time). User data should be protected even against a set of malicious actors who are system administrators working for the cloud provider. Approaches would likely leverage novel advanced cryptography and seamless key management. Key management will be

This work is sponsored by Assistant Secretary of Defense for Research & Engineering under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

particularly challenging if we seek to provide the ability of data owners to dynamically manage read/write access to the data dynamically. Additional challenges include managing the trade-offs between functionality, processing overhead, and level of confidentiality.

- **Secure and Resilient Processing** – The goal is to allow arbitrary processing and analytics on encrypted cloud data. Approaches will likely leverage secure multiparty computation and functional encryption. If successful, any computation could be performed on encrypted cloud data without ever decrypting that data. The biggest research challenge at the moment is performing these computations in a reasonable amount of time – current techniques (e.g., homomorphic encryption) are many orders of magnitude too computationally intensive and may not support all possible types of computation. New techniques involving multi-party computation (where one assumes that some fraction of the cloud remains trustworthy even if one doesn't know exactly which parts are the trustworthy parts) hold promise of being a good trade between computational complexity and security/privacy for some types of computation.

- **High Assurance Architecture** – The goal is to provide cloud tenant and provider visibility and control of cloud trust and isolation. Approaches will leverage virtual isolation, situational awareness monitoring, and hardware roots of trust. Tenants would have the ability to verify the correctness of the underlying platform when deploying their software and data to the cloud provider, and they would be able to ensure that the platform remains in a good state for the duration of their computation. One of the challenges will be do provide this type of hardware root-of-trust economically, especially as cloud providers seek to minimize every possible cost associated with their hardware infrastructure.

By advancing the state-of-the-art against each of these four challenges, and by showing that the solutions are practical to implement on a large scale, we assert that the overall security and privacy of cloud computing would be improved. No technology can ensure complete confidentiality, integrity and availability of data, but we should be able to increase substantially the work required by the adversary to compromise our systems and processes.

This work is sponsored by Assistant Secretary of Defense for Research & Engineering under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

Secrecy, Surveillance, Privacy, and International Relations
16 April - 17 April 2015

Bios

Daniel Berliner is an Assistant Professor in the Department of Political Science at the University of Minnesota. Beginning in August 2015, he will be an Assistant Professor in the School of Politics and Global Studies at Arizona State University. He received his PhD in 2012 from the University of Washington, Seattle, and was previously a Postdoctoral Fellow at the Kolleg-Forschergruppe "Transformative Power of Europe" at Freie Universität Berlin. His primary research focuses on the international and domestic politics of transparency and accountability policies, with focuses both on the global diffusion of access to information laws, and on the roles of domestic political competition in their adoption and implementation. His current research seeks to examine these topics in South Africa, Mexico, and Georgia. He has also worked on issues of governance and human rights in global supply chains. His research appears in journals including the *American Political Science Review*, *The Journal of Politics*, *International Studies Quarterly*, and *World Development*.

Clifford Bob is professor of political science and Raymond J. Kelley Endowed Chair in International Relations at Duquesne University. His books include *The Global Right Wing and the Clash of World Politics* (Cambridge University Press, 2012) and *The Marketing of Rebellion: Insurgents, Media, and International Activism* (Cambridge, 2005), which won the International Studies Association Best Book Award and other prizes. Dr. Bob has written for political science, law, and policy journals, and his opinion articles have appeared in newspapers such as the *International Herald Tribune*, *Los Angeles Times*, *South China Morning Post*, *Sidney Morning Herald*, *San Francisco Examiner*, and *Pittsburgh Post-Gazette*. He holds a J.D. from NYU School of Law and a Ph. D. from MIT. This year he is working in Washington, DC as a senior fellow at the Transatlantic Academy.

Joel Brenner is the Robert E. Wilhelm Fellow at MIT's Center for International Studies. He is a lawyer and security consultant specializing in cyber and physical security, data protection and privacy, intelligence law, the administration of classified information and facilities, and the regulation of sensitive cross-border transactions. Mr. Brenner has served as the head of U.S. counterintelligence under the Director of National Intelligence and as the inspector general and later as senior counsel at the National Security Agency, advising Agency leadership on the public-private effort to create better security for the Internet. He has also served as a prosecutor in the Justice Department's Antitrust Division and has extensive trial and arbitration experience in private practice. Mr. Brenner holds a JD from the Harvard Law School, a PhD from the London School of Economics, and a BA from the University of Wisconsin – Madison. He is the author of *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, now in paperback as *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World*. See http:/.joelbrenner.com.

Ian Brown is Professor of Information Security and Privacy at the Oxford Internet Institute. His research is focused on surveillance, privacy-enhancing technologies, and Internet regulation. He is an ACM Distinguished Scientist and BCS Chartered Fellow, and a member of the Information Commissioner's Technology Reference Panel.

Since 1998 Professor Brown has variously been a trustee of Privacy International, the Open Rights Group, the Open Knowledge Foundation and the Foundation for Information Policy Research and an adviser to Greenpeace, the Refugee Children's Consortium, Amnesty International and Creative Commons UK. He has consulted for the United Nations, Council of Europe, OECD, US Department of Homeland Security, JP Morgan, Credit Suisse, Allianz, McAfee, BT, the BBC, the European Commission, the Cabinet Office, Ofcom, and the National Audit Office.

Professor Brown's work has been covered by the BBC, CNN, CBC, Al Jazeera, and numerous newspapers and magazines. He has written for the Financial Times, Daily Telegraph, New Statesman and Guardian. In 2004 he was voted as one of the 100 most influential people in the development of the Internet in the UK over the previous decade.
He has acted as an expert witness for the English High Court, UK Investigatory Powers Tribunal, and European Court of Human Rights; and given evidence to the UK, German, and European parliaments. In 2014/15, he was a Knowledge Exchange Fellow with the Commonwealth Cybercrime Initiative and UK National Crime Agency.

Sandra Coliver has been, since 2005, the Senior Legal Officer for Freedom of Information and Expression at the Open Society Justice Initiative, an operational, non-grant giving program of the Open Society Foundations. She supervises a team of three international lawyers who work on developing global norms, litigating in regional and national courts (outside the US), and helping NGOs obtain information of high public interest, including from the security sectors. In 2011-13, she coordinated the drafting of the Tshwane Principles on National Security and the Right to Information. Previously, she served as the director of the Center for Justice and Accountability, which works to hold human rights abusers accountable in US and other courts; and managed or participated in rule of law programs for more than two decades, including in Bosnia with the UN High Commissioner for Human Rights, the International Crisis Group and the OSCE. As the first Law Program Director (1990-96) of Article 19, she coordinated the drafting of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, and wrote a commentary and edited a book on the Principles. She served for several years on the Faculty of the Summer Program on International Human Rights and Humanitarian Law at American University Washington College of Law.

Henry Farrell is associate professor of political science and international affairs at George Washington University. He has previously been a fellow at the Woodrow Wilson Center for International Scholars, assistant professor at George Washington University and the University of Toronto, and a senior research fellow at the Max-Planck Project Group in Bonn, Germany. He works on a variety of topics, including trust, the politics of the Internet and international and comparative political economy. His recent book, *The Political Economy of Trust: Interests, Institutions and Inter-Firm Cooperation*, was published in 2009 by Cambridge University Press. In addition he has authored or co-authored 25 academic articles, as well as several book chapters and numerous non-academic publications.

Martha Finnemore is University Professor of Political Science and International Affairs at George Washington University in Washington, DC. Her research focuses on global governance, international organizations, ethics, and social theory. She is the co-author (with Michael Barnett) of *Rules for the World: International Organizations in Global Politics*, which won the International Studies

Association's award for Best Book in 2006. She is also author of *National Interests in International Society* and *The Purpose of Intervention*, which won the American Political Science Association's Woodrow Wilson Award as "the best book published on government, politics, or international affairs" in 2004. Her most recent books are *Back to Basics: State Power in a Contemporary World* (Oxford University Press 2013) and *Who Governs the Globe?* (Cambridge University Press 2010). Her articles have appeared in *International Organization*, *World Politics*, *Annual Review of Political Science, Review of International Studies*, *Review of International Political Economy*, *Global Governance, Foreign Affairs* and elsewhere. She is a Fellow of the American Academy of Arts and Sciences, has been a visiting research fellow at the Brookings Institution and Stanford University, and has received fellowships or grants from the MacArthur Foundation, the Social Science Research Council, the Smith Richardson Foundation, and the United States Institute of Peace.

Elizabeth (Liza) Goitein co-directs the Liberty and National Security Program at the Brennan Center for Justice at NYU School of Law, which seeks to advance effective national security policies that respect constitutional values and the rule of law. Before coming to the Brennan Center, Ms. Goitein served as counsel to Senator Feingold, Chairman of the Constitution Subcommittee of the Senate Judiciary Committee, and as a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Ms. Goitein is co-author of the research reports *What Went Wrong with the FISA Court* and *Reducing Overclassification Through Accountability* and author of the chapter "Overclassification: Its Causes and Consequences" in the book *An Enduring Tension: Balancing National Security and Our Access to Information*. Her writing also has been featured in major newspapers including *The New York Times, Washington Post, Wall Street Journal, USA Today, LA Times, Boston Globe, San Francisco Chronicle,* and *Philadelphia Inquirer*. Ms. Goitein graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit.

Shirley Hung is a research scientist at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL). She received her Ph.D. in Political Science from MIT with a dissertation examining regulation of emerging technologies with a focus on commercial encryption and VoIP. She received her AB in Government from Harvard College and was a General Scholar at the Peking University School of International Relations. Her research interests include cybersecurity, Chinese Internet policy, and the interaction of social and political values with Internet technology. She previously worked as a management consultant.

Susan Landau is Professor of Cybersecurity Policy in the Department of Social Science and Policy Studies at Worcester Polytechnic Institute. Landau has been a senior staff Privacy Analyst at Google, a Distinguished Engineer at Sun Microsystems, a faculty member at the University of Massachusetts at Amherst and at Wesleyan University. She has held visiting positions at Harvard, Cornell, and Yale, and the Mathematical Sciences Research Institute. Landau is the author of Surveillance or Security? The Risks Posed by New Wiretapping Technologies (MIT Press, 2011) , and co-author with Whitfield Diffie, of Privacy on the Line: The Politics of Wiretapping and Encryption (MIT Press, 1998, rev. ed. 2007), the latter co-authored with Whitfield Diffie. She has written numerous scientific and policy research papers, and has also published in other venues, including Science, Scientific American, and the Washington Post. Landau has testified in Congress on cybersecurity and on electronic surveillance. Landau currently serves on the Computer Science Telecommunications Board of the National Research Council. A 2012 Guggenheim fellow, Landau was a 2010-2011 fellow at the Radcliffe

Institute for Advanced Study, the recipient of the 2008 Women of Vision Social Impact Award, and also a fellow of the American Association for the Advancement of Science and the Association for Computing Machinery. She received her BA from Princeton, her MS from Cornell, and her PhD from MIT.

Aryeh Neier is president emeritus of the Open Society Foundations. He was president from 1993 to 2012. Before that, he served for 12 years as executive director of Human Rights Watch, of which he was a founder in 1978. He worked 15 years at the American Civil Liberties Union, including eight years as national executive director. He served as an adjunct professor of law at New York University for more than a dozen years, and has also taught at Georgetown University Law School and the University of Siena (Italy). Since 2012, he has served as Distinguished Visiting Professor at the Paris School of International Affairs of Sciences Po.

Neier is a frequent contributor to the *New York Review of Books*, and has published in periodicals such as the *New York Times Magazine*, the *New York Times Book Review*, and *Foreign Policy*. For a dozen years he wrote a column on human rights for *The Nation*. He has contributed more than 200 op-ed articles in newspapers including the *New York Times*, the *Washington Post*, the *Boston Globe*, and the *International Herald Tribune*. Author of seven books, including his most recent, *The International Human Rights Movement: A History* (2012), Neier has also contributed chapters to more than 20 books.

He has lectured at many leading universities in the United States and worldwide. He is the recipient of seven honorary degrees and numerous awards from such organizations as the American Bar Association, the Swedish Bar Association, the International Bar Association and the Committee to Protect Journalists.

Abraham L. Newman is an associate professor at the BMW Center for German and European Studies in the Edmund A. Walsh School of Foreign Service at Georgetown University. He is senior editor at *International Studies Quarterly*. His research focuses on the international politics of regulation and he is the author of *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press 2008) and the co-editor of *How Revolutionary was the Digital Revolution* (Stanford University Press 2006). His work has appeared in a range of journals including *Comparative Political Studies, International Organization, Science,* and *World Politics*. For more information see http://explore.georgetown.edu/people/aln24/

Justin Rood is a fellow with the Information Society Project at Yale Law School, studying national security strategy in an era of declining secrecy. He is also director of the Congressional Oversight Initiative with the Project on Government Oversight, where he works with Congressional committees to enhance and expand their oversight and investigative efforts. Previously Rood served as director of investigations and senior investigator for Sen. Tom Coburn (R-Okla.) on the Homeland Security and Governmental Affairs Committee, and the Permanent Subcommittee on Investigations. Before that he was an award-winning reporter and investigative producer for ABC News, Congressional Quarterly and other outlets, covering intelligence and homeland security.

Rahul Sagar is Associate Professor of Political Science at Yale NUS. He was previously Assistant Professor in the Department of Politics at Princeton University. His work has been published in a

number of edited volumes and peer-reviewed journals including the *Journal of Political Philosophy, The Journal of Politics,* and *Ethics and International Affairs*. His first book, *Secrets and Leaks: The Dilemma of State Secrecy,* published by Princeton University Press in 2013, received the National Academy of Public Administration's 2014 Louis Brownlow Award and was designated a 2014 *CHOICE* Outstanding Title. He has recently begun work on a new book entitled *Decent Regimes* which argues that the United States ought to tolerate, and even support, regimes that may not be fully democratic but nonetheless pursue the well being of their citizens in spite of difficult circumstances.

Richard J. Samuels is Ford International Professor of Political Science and Director of the Center for International Studies at the Massachusetts Institute of Technology. He is also the Founding Director of the MIT Japan Program. In 2005 he was elected a member of the American Academy of Arts and Sciences and in 2011 he received the Order of the Rising Sun, Gold and Silver Star, an Imperial decoration awarded by the Emperor of Japan and the Japanese Prime Minister. He has just been named an Einstein Visiting Fellow at the Free University of Berlin (2015-2017).

Professor Samuels has served as Head of the MIT Department of Political Science, Vice-Chairman of the Committee on Japan of the National Research Council, and as Chairman of the Japan-US Friendship Commission, an independent Federal grant-making agency that supports Japanese studies and policy-oriented research in the United States. He has spent more than a decade doing field research in Japan and Europe and is one of only three scholars (Japanese or foreign) to have produced more than one scholarly monograph recognized by the Nippon Foundation as one of the top "one hundred books for understanding contemporary Japan."
In 2013, Cornell University Press published his book about the political and economic effects of Japan's March 2011 catastrophes: 3.11: Disaster and Change in Japan.
Dr. Samuels' previous book, Securing Japan: Tokyo's Grand Strategy and the Future of East Asia, was named one of the five finalists for the 2008 Lionel Gelber Prize for the best book in international affairs. Another, Machiavelli's Children: Leaders and Their Legacies in Italy and Japan, a comparative history of leadership in Italy and Japan, won the 2003 Marraro Prize from the Society for Italian Historical Studies and the 2004 Jervis-Schroeder Prize for the best book in International History and Politics, awarded by the International History and Politics section of the American Political Science Association.

His 1994 study, "Rich Nation, Strong Army": National Security and the Technological Transformation of Japan won the 1996 John Whitney Hall Prize of the Association of Asian Studies and the 1996 Arisawa Memorial Prize of the Association of American University Presses. His book, *The Business of the Japanese State: Energy Markets in Comparative and Historical Perspective* received the Masayoshi Ohira Memorial Prize in 1988. In 1983, Princeton University Press published his *Politics of Regional Policy in Japan*.

His articles have appeared in *Foreign Affairs, International Security, Foreign Policy, Washington Quarterly, International Organization, The Journal of Modern Italian Studies, The National Interest, The Journal of Japanese Studies, Daedalus,* and other scholarly journals.
Dr. Samuels received his PhD from the Massachusetts Institute of Technology in 1980 and a gold whistle for a decade of service from the Massachusetts State Referee Committee of the U.S. Soccer Federation in 2009.

Mattathias Schwartz is a staff writer at the New Yorker, specializing in national security and state power. "A Massacre in Jamaica," his investigation into the extradition of Christopher Coke, won the 2011 Livingston Award for international reporting. He has also reported for the magazine from Libya, Honduras, Lampedusa, and Zuccotti Park. Between 2002 and 2005, he edited and published the twenty-one-issue run of The Philadelphia Independent, a broadsheet newspaper. He has contributed to Harper's, the London Review of Books, the Wall Street Journal, and Wired, and is a contributing writer at the New York Times Magazine.

Daniel Severson will graduate with joint J.D./M.P.P. degrees from the Harvard Law School and the Harvard Kennedy School in May 2016. He is editor in chief of the *Harvard International Law Journal*. This spring, he will publish an article on U.S. signals intelligence reform in the Journal. Prior to law school, Dan served as a foreign affairs analyst and Council of American Ambassadors Fellow at the U.S. Department of State. He also completed a Fulbright Scholarship in Taiwan. Last summer, he received Harvard's Presidential Public Service Fellowship to support his work at the U.S. Department of Defense. Dan graduated from Bard College with two degrees—a B.A. in Political Studies and a B.M. in French horn performance. He enjoys running and playing the French horn.

John Tirman has been Executive Director and Principal Research Scientist at the MIT Center for International Studies since 2004. Previously, he was program director of the Social Science Research Council, executive director of the Winston Foundation for World Peace, and a reporter for *Time*. In 1999-2000, he was a Fulbright Senior Scholar in Cyprus. He has served as a trustee and chair of several NGOs, including *Mother Jones* magazine, International Alert, and the Institute for War & Peace Reporting.

Tirman has published 14 books, including *The Deaths of Others: The Fate of Civilians in America's Wars* (Oxford University Press, 2011), *Spoils of War: The Human Cost of America's Arms Trade* (Free Press, 1997), and *Dream Chasers: Immigration and the American Backlash* (MIT Press, 2015). His articles have appeared in the *New York Times, Washington Post, Boston Globe, Esquire, Wall Street Journal, The Nation, Bulletin of the Atomic Scientists, International Herald Tribune,* and *World Policy Journal,* among others.

Marc A. Zissman is Associate Head of the Cyber Security and Information Sciences Division. Dr. Zissman joined the Laboratory in 1983, and his early research focused on digital speech processing, including parallel computing for speech coding and recognition, co-channel talker interference suppression, language and dialect identification, and cochlear-implant processing for the profoundly deaf. After working for one year in the Department of Defense under the Intergovernmental Personnel Act program, he expanded his research interests to include cyber security technology. He had responsibility for developing and executing a strategic plan for growing the Laboratory's cyber security research, development, evaluation and technology transfer efforts. In addition to his work at Lincoln, Dr. Zissman served for four years as a U.S. technical specialist to the NATO IST-011/TG-001 task group, which studies military applications of speech technology for NATO. He was elected to and served for four years on the Speech Processing Technical Committee of the IEEE Signal Processing Society. He also served for four years on the Defense Advanced Research Projects Agency (DARPA) Information Science and Technology Study Group. He was part of the U.S. Southern Command (USSOUTHCOM) and Joint Task Force-HAITI team that responded to the January 2010 earthquake in Haiti. Since 2011, he has been serving as a member of the Army Science Board. Dr. Zissman holds an SB degree in computer science and SB, SM, and PhD degrees in electrical engineering all from the Massachusetts Institute of Technology.