Safe and Free: National-Security Surveillance and Safeguards Across Rule-of-Law States

Jordan Schneider ⋮ 12-15 minutes

Published by The Lawfare Institute
in Cooperation With

In the decade since Edward Snowden began leaking classified documents from the National Security Agency, scholars and policymakers around the world have debated how to ensure that intelligence agencies respect civil liberties and privacy and follow the law. Intelligence oversight, once an arcane topic with little visibility, now features regularly in U.S. congressional debates and even presidential politics.

The U.S. and other rule-of-law democracies have passed major intelligence reforms since Snowden's leaks. Germany adopted a statutory charter for its main foreign intelligence agency, the BND. Canada created a new oversight commission. The United Kingdom adopted a "double-lock" requiring for the first time that judges approve surveillance warrants.

There are obvious reasons for citizens to care about their own governments' intelligence-related policies and protections. After all, we have the most to fear from those who wield coercive power over us.

But why study how *other* governments oversee their intelligence agencies? A new Strauss Center project, "Safe and Free: National Security Surveillance and the Rule of Law Across Democratic States," aims to spur the comparative study of surveillance and to move that field beyond the narrow, often rivalrous transatlantic comparisons of the post-Snowden era. Instead, the Safe and Free series harnesses comparative study to gain insight about oversight structures, transparency, legal remedies, and political and technological trends affecting many rule-of-law democracies.

Since the Snowden leaks, cross-border surveillance debates have often been driven by litigation over the European Union's requirement of "adequacy." Without a finding by the European Commission that the destination country's law provides an adequate level of protection, European data cannot be seamlessly transferred outside of the EU—including, importantly, to the United States.

The United States has now adopted a more modest version of the EU's adequacy requirement. President Biden's Executive Order 14086 requires the attorney general to decide which other countries' laws are sufficiently protective of Americans' data to merit designation as "qualifying states." Unlike the EU's adequacy rule, this new U.S. mechanism does not apply to data flows. Instead, designation as a qualifying state gives those countries' citizens access to a surveillance redress process, which includes a new Data Protection Review Court within the Justice Department.

"Adequacy" may make sense as a legal and diplomatic tool, but it is a poor aid to deeper understanding. Comparisons driven by adequacy requirements are inherently competitive. Does *your* system meet *my* standards? Whose is better? The narrow lens of adequacy, where differences are viewed as potentially suspect, omits much of what makes comparative research valuable.

Learning From Surveillance Practices and Safeguards Across Rule-of-Law States

Fortunately, the competitive dynamic that adequacy requirements have created is beginning to lose its grip.

Most notably, in a landmark 2022 Declaration on Government Access to Personal Data Held by Private Sector Entities, the member states of the Organization for Economic Cooperation and Development (OECD) established seven shared principles for surveillance under the rule of law. The principles reflect "commonalities drawn from" OECD countries' "existing laws and practices." And they "distinguish" *all* OECD member states, American and European alike, from "other countries whose law enforcement or national security access to personal data are inconsistent with democratic values and the rule of law."

It is in this spirit that the Robert Strauss Center on International Security and Law at the University of Texas at Austin has launched a new major effort to stimulate comparative study of surveillance laws, institutions, and safeguards across rule-of-law states.

The Safe and Free series aims to promote genuine comparative study, generating insights to help improve surveillance law, oversight, and transparency globally.

To do that, the Strauss Center has commissioned papers by academics and experts from 10 rule-of-law countries across three continents, with papers from other countries to come. The papers reveal fundamental similarities but also salient differences in how each country has worked to reconcile secret intelligence with democracy and privacy. Examples of these intriguing findings include the following:

- Independent oversight bodies are proliferating, from the United States's Privacy and Civil Liberties Oversight Board (PCLOB), to the Netherlands's Review Committee on the Intelligence and Security Services (CTIVD), to Canada's National Security and Intelligence Review Agency (NSIRA). But their powers differ in important ways.

  Some, like the United States's PCLOB, must rely on a statutory right to receive information from intelligence agencies, rather than direct access to the agencies' systems. The board's requests for information are then fulfilled by the agencies themselves.

  Some of the PCLOB's counterparts, in contrast, do enjoy direct access to intelligence agencies' systems: The Dutch CTIVD, as Peter Koop explains in his paper on electronic surveillance norms in the Netherlands, "has access to the buildings of" the principal Dutch intelligence services "and is allowed to question [their] employees and look into their files, computer systems, and archives." Similarly, Thorsten Wetzling notes that Germany's Independent Control Council (UKR) "enjoys comprehensive access to all BND premises and to all its IT systems as long as they are under the sole direction of the BND."

- The quality of legislative oversight varies widely: In the United States, "[t]he most powerful and important oversight bodies are in Congress." By contrast, Stephanie Carvin explains that in Canada, the opportunity for parliamentary "committees to engage in robust scrutiny is limited." Overall, she notes, such parliamentary scrutiny "plays a less important role in the Canadian context relative to Canada's Five Eyes partners."

  Yet Canada's system involves parliamentarians in oversight by other means. Instead of relying on direct parliamentary oversight, Canada has created the National Security and Intelligence Committee of Parliamentarians, which is made up of parliamentarians but housed within the executive branch. Similarly, Sébastien-Yves Laurent explains that four members of France's CNCTR, a nine-member independent oversight body, are drawn from Parliament.

- As in the United States, the rise of populist movements and low social trust influence the political and social contexts in which intelligence agencies currently operate around the globe. Artur Gruszczak discusses the effects of Poland's period of "democratic backsliding" since 2015. That experience, he explains, has had "considerable impact on Polish intelligence and security services in terms of their organization, institutional arrangements, human resources, professionalism, and … legality of their activities."

  Romania has made considerable progress since the days of the dreaded communist-era Securitate. But as Aitana Radu explains, the country's intelligence arrangements continue to

"reflect its recent history" and habits inherited from "its Communist past." Despite efforts "towards increasing transparency," intelligence in Romania "remains very much outside public scrutiny, with little to no information available on either the technological capabilities of the intelligence agencies or the effectiveness of human rights safeguards."

- Countries are responding differently to the challenges and opportunities presented by the volume of data available in the digital area. German law, for example, limits how much data can be collected from a given medium. When conducting "strategic foreign intelligence collection," the BND may ingest no more than 30 percent of total network traffic. In absolute terms, however, the scale of collection appears quite large, with the BND reportedly using hundreds of thousands of selectors (distinctive identifiers such as email addresses) to copy trillions of internet protocol (IP) connections per day from the DE-CIX internet exchange in Frankfurt. Much of this vast collection, Wetzling's paper clarifies, is conducted at the request of liaison services, potentially including the U.S. National Security Agency.

  The United Kingdom's Investigatory Powers Act 2016 permits bulk interception, bulk acquisition of communications metadata, and bulk interference (that is, hacking). Agencies must make a heightened showing when seeking approval to use these bulk powers. But as Ian Leigh notes, the act's language nonetheless allows "a high degree of generality in the authorization of bulk powers, and a number of the controls governing how analysts can query databases of collected data remain in the form of internal procedures rather than legal requirements."

- Transparency in the intelligence context has improved dramatically in many countries. In others, however, progress has been slower. Australia is somewhat of a mixed bag in this respect. Its "electronic surveillance regime is highly codified by a suite of legislation that has been laid down over the past fifty years and routinely refined by Australia's Parliament." Yet, "agencies' use of electronic surveillance is still somewhat opaque." William Stoltz elaborates that "[f]or law enforcement agencies, annual reporting provides the overall numbers of authorisations that are approved or refused, but little insight is given into the typical basis for refusal or key factors driving approval." And for "intelligence agencies, even the numbers of authorisations are hard to discern, let alone more contextual information that might help Australians understand the typical nature of the targets or the urgency with which surveillance is undertaken."

  France's CNCTR publishes detailed annual statistical reports regarding domestic surveillance. Sébastien-Yves Laurent notes "that terrorism and organized crime are the two main crimes that justify the bulk of individual surveillance (from around 59% to around 70%, depending on the year)." There is less transparency, however, about investigations of foreign espionage, presumably for security reasons.

- Many countries now offer a redress mechanism, though their precise features vary. In Sweden, both residents and nonresidents can submit complaints to the Defense Intelligence Inspection (SIUN), which oversees the principal foreign intelligence agency, the National Defence Radio Establishment (FRA). Iain Cameron cautions, however, that while the door to the redress mechanism is open, "nonresident foreigners are likely to receive the same bland information as citizens and resident foreigners: namely, that SIUN has investigated the allegation and found no violation of the law."

  Complainants before the United States' new redress mechanism, which culminates in review by the Data Protection Review Court, will receive the same neither-confirm-nor-deny response as complainants to Sweden's SIUN. Yet the Data Protection Review Court's door is not quite as open as the SIUN's. The new redress process is available to complainants whose data was allegedly transferred to the U.S. from "qualifying states"—currently the U.K. and the member states of the EU and European Economic Area (EEA). In most circumstances, however, Americans cannot use this new redress mechanism, and access to federal court remains limited by the constitutional "standing" doctrine, which bars courts from hearing speculative complaints.

Moving the Comparative Study of Surveillance Beyond "Adequacy"

“Adequacy” remains the law of the EU and has now been adopted, in a more modest form, by the United States. But approaching comparative study through a competitive lens misses much of what makes comparative research valuable. Instead of asking whether the other side is “good enough,” Safe and Free poses different questions: What can we learn from one another? What can common challenges tell us about broader social and technological trends? And how can we improve together?

Read the full series: safeandfree.io