

Tech Firms Are Not Sovereigns

ANDREW KEANE WOODS

Aegis Series Paper No. 1813

It has long been argued that the Internet has the capacity to upend state sovereignty. These claims run as far back as John Perry Barlow's 1996 paean to an online utopia, "A Declaration of the Independence of Cyberspace."¹ Barlow wrote about a fictional land called cyberspace—a place where the "Governments of the Industrial World . . . have no sovereignty."² He was not alone in thinking that the Internet would be government-free and sovereignty-busting.³

But it did not happen. As Jack Goldsmith and Tim Wu showed over a decade ago—ten years after Barlow wrote his declaration—this vision of an Internet free from national government control is unrealistic.⁴ It simply cannot be squared with Internet governance today, which features states demanding that data be stored locally (a demand that companies often heed), courts demanding that companies take down web content that does not comply with local law, and companies generally tailoring their products in many distinct ways to comply with different rules in different markets around the world.

Today, few would argue that the Internet is free from sovereign control. But who are the sovereigns? It is increasingly common to hear that the sovereigns that reign over the Internet are Internet firms—the companies that set user policies and wield enormous influence over the day-to-day functioning of the Internet. The user bases of these firms can be larger than many countries.⁵ They have foreign policy teams.⁶ They have even engaged in experiments with user-driven self-governance.⁷ In many ways, they look like states.⁸

But firms are not sovereigns. *Some* public-facing Internet firms may find it expedient to resist *some* states, *some* of the time on *some* issues. But this does not mean that Internet firms are a serious and lasting threat to state sovereignty. If anything, we might draw the opposite conclusion: the fact that states have managed to bring hugely powerful corporations to heel suggests that state sovereignty is alive and well. This is not an academic point; it has considerable implications for how policy makers think about trade-offs as they craft policies that either recognize that sovereignty or challenge it, thereby forcing states to aggressively assert their sovereign power.

This short essay proceeds in three parts. The first part interrogates the idea that state sovereignty is threatened by Internet firms. The second part reveals that state control over the Internet is alive and well. The question is not *whether* states can enforce their laws online, but *how* best to do this. The third part outlines several barriers to meaningful Internet governance policy reform.



Internet Firms Are Arbitrageurs, Not Sovereignty-Busters

The view that Internet firms pose a threat to state sovereignty might rest on two assumptions: (1) that Internet firms *oppose* state sovereignty and (2) that Internet firms *weaken* state sovereignty. Let us consider the first assumption.

Do Technology Firms Oppose State Sovereignty?

If technology firms pose a challenge to traditional notions of state sovereignty, they certainly do not do so uniformly. Not all firms resist state power. And those that do resist state power may not do so all the time, and they may act differently with different states—appeasing one while challenging another. The only thing that can be predicted about Internet companies is that they are strategic actors that will act more or less rationally in ways that are thought to benefit the firms.

Not all firms Even if some technology firms oppose state surveillance some of the time, not all of them do. In fact, we can draw important distinctions between at least a few sorts of companies. Firms that primarily sell hardware will likely take a different posture than those that sell data services. Likewise, consumer-facing firms may maintain a different posture than enterprise firms. For example, while Apple resists government efforts to unlock iPhones, other companies offer to provide the government with exactly that service. Cellebrite, among other companies, offers to help law enforcement agents gain access to locked iPhones, including those that Apple will not unlock.⁹ This is partly a natural result of the firms' different customers. Firms that make most of their money selling tools to law enforcement agencies may be naturally less resistant to law enforcement demands than firms that make their money selling goods or services to the general public—especially at a time when the public at large may be suspicious of state efforts to gain access to digital data. Some of the differences in firms' conduct may also be attributed to different histories and attendant firm cultures. For example, some technology firms have long histories of accommodating law enforcement demands. Verizon and AT&T, for example, have built extremely robust regimes for accommodating law enforcement requests for data. Some of this is simply a result of the fact that laws like the Communications Assistance for Law Enforcement Act require these carriers to build lawful intercept capabilities into their networks.¹⁰ Whatever explains the difference between different firms' attitudes toward law enforcement, the difference is there.

Not all the time Even those firms in the headlines today for resisting law enforcement demands for access to customer data were not always so obstinate. Indeed, many of the firms that are the most resistant to state surveillance efforts today were much more amenable to those efforts before Edward Snowden's revelations in 2013.¹¹ In the wake of those disclosures, the political calculus changed. It became politically costly to be seen to cooperate with the state.¹² It may also have been suddenly expedient to decry government intrusions into user privacy, shifting attention away from industry practices that have come

under increased scrutiny by privacy advocates. Before Snowden, technology firms were not seen as serious barriers to state efforts at surveillance. Had the Snowden disclosures not occurred, perhaps nothing would have changed—and today’s technology firms would not have the same desire to resist state surveillance efforts as strongly as they do. This suggests that those technology companies that oppose state surveillance efforts are not always or inherently opposed, but rather are opportunistic actors who are for or against a particular state action depending on the relevant political and market calculus.

Not all states Even if a firm opposes one state’s surveillance efforts, it may cater to another’s. Apple resisted granting the FBI access to one of its phones, but the next year it built a data center in China to be sure it was fully compliant with Chinese cybersecurity laws—laws that enable the state’s considerable surveillance efforts.¹³ While we can surely distinguish between the two examples, taken together they suggest that Apple, like other global technology firms, is willing to take extreme measures to appease one government—including, in China, developing a first-ever joint venture with a government-run entity—but not another. So even if Apple is in fact a threat to state sovereignty, it is not the same threat to all states.

What can we conclude from this? Simply that Internet firms are not all inherently opposed to state sovereignty and in fact regularly take steps to accommodate it. Why? Because over the long run, they have little choice.

What Are Firms Really Up To?

If Internet firms do not represent an ironclad and industry-wide challenge to state power, what are they up to? The answer, of course, is: making money. Firm resistance to state regulatory authority happens all the time for different reasons. For example, in the surveillance context, one simple reason that firms resist state surveillance efforts is because it is good for the brand. In the wake of the Snowden disclosures, customer trust in Internet companies was ebbing.¹⁴ One way to restore that trust, some Internet firms seemed to calculate, was to push back on state efforts to access customer data, even where that access was lawful.¹⁵

The other reason firms evade state regulatory efforts is because those efforts are costly. For as long as there have been borders, there have been businesses that seek to exploit arbitrage opportunities across borders. This includes, of course, regulatory arbitrage: taking advantage of differences in the laws between two states. Apple, to pick a well-known example, exploits differences in the tax regimes between different countries.¹⁶ But arbitrage can also be done with data. Firms choose where to store data based on costs, latency speeds, environmental concerns, and more. Whether a state’s legal regime is favorable or not to the company’s handling of huge amounts of customer data is sure to factor into the equation. Regulatory arbitrage is not new. Neither is corporate resistance to regulation. Businesses—especially



those that cross national borders—will frustrate states by resisting unwanted regulations, either directly or indirectly by strategically organizing the business in ways that advantage the firm and disadvantage states seeking to regulate it. This strategic exploitation of differences between different countries' laws may increase a state's law enforcement costs, but it does not ultimately threaten its sovereignty.

State Sovereignty Is Alive and Well

Even if they wanted to, Internet firms do not have the capacity to threaten state sovereignty over the long run. The fact that some firms find it to their benefit to oppose some state efforts at control, some of the time, does not mean that the state cannot get what it wants. It simply means that at times the costs are higher.

An Analogy

Imagine a country whose economy is in transition. As the country's economy develops, businesses become larger and more complex. What were once many local mom-and-pop-style family businesses have now become a few large, publicly traded firms like Costco and Target. Some agents of the state—like, say, tax collectors—find their jobs harder to do. These big firms have many lawyers, lobbyists, and offshore shelters. Compared to the mom-and-pop shops, the corporate behemoths have more power to avoid compliance with the law and more power to change the law. They have more power—full stop. And in some ways that makes the state's job harder.

But in other ways, these conglomerates make the state's job easier. Compared to smaller businesses, their bookkeeping is more professional and more thorough. This is helpful to state efforts at auditing and tax collection. The conglomerates' lawyers are more accustomed to dealing with federal regulators, easing negotiations and settlements. Moreover, because of aggregation, the state must only interact with a few larger firms, all of whom are repeat players, rather than many smaller firms who may be dealing with state agents for the first time.

Would we conclude, in this hypothetical market transition from smaller businesses to larger conglomerates, that state sovereignty has been eroded? From the perspective of the state's ability to accomplish its aims, the shift from small businesses to larger conglomerates has made things both harder and easier. But has sovereignty been eroded? I think not. Ultimately, although the costs have gone up, the state can achieve its aims. Now, in any participatory democracy, state control is somewhat more fragile than in an authoritarian government. The government can be lobbied by people and corporations, which can influence state action. But the key thing is that the corporations must do the lobbying; the corporation does not set the rules, but rather must petition the state to embrace rules the corporation likes. The state is still the final word, and that makes the state sovereign.¹⁷

The same goes for Google and Facebook. Why should we think that Google is a threat to state sovereignty in a way that Walmart is not?¹⁸ What is so different about data intermediaries from, say, banks and health care organizations? These are organizations that could, if they sought to, seriously hinder state efforts at law enforcement. Indeed, sometimes they do just that. If one thinks Google and Facebook are the new sovereigns, then surely one also must conclude that companies like Walmart and Coca-Cola are sovereigns too.

State Control

The case for state sovereignty over the Internet is not so different from state sovereignty over anything else. It is the ability to achieve the state's aims. Internet firms take considerable steps to appease states. Their opposition to state power is strategic, rather than inherent—temporary, rather than permanent. But even if these firms were committed to opposing state power with all their might, they can be brought to heel. This fact suggests that they do not actually represent the threat to state sovereignty that some think.

Those firms that want to do business in China must do so on terms set by the Chinese government.¹⁹ Firms that do not like those terms can choose not to do business there, as Google famously did. There are some creative work-arounds: American firms using partnerships, like Facebook's rumored partnership with a Chinese company to get a sense of the market without tarnishing the brand.²⁰ But at the end of the day, the Chinese government is largely able to get what it wants. One does not imagine that the Chinese government feels as if its sovereignty has been eroded by Internet firms. If anything, these firms present a nice opportunity to reaffirm state power.

The same story can be told about the United States, even when law enforcement does not get what it wants. The fact that Apple declines to hand over encryption keys in a particular dispute with the FBI or that Microsoft refuses to hand over Irish-held data does not mean that the FBI cannot ever get that information. It means that the FBI must convince a judge or legislature that it is entitled to that data. In other words, the FBI must petition the state. And what are we to make of the pro-privacy lobby—the civil liberties groups that will fight any efforts by law enforcement agents to pass particular laws? Suppose that the Department of Justice proposes a bill to allow greater law enforcement access to data held abroad.²¹ Suppose that civil society groups oppose the bill.²² If the bill fails, would we conclude that state sovereignty has been eroded? Hardly! Regardless of what Congress does, or the courts do, or the president does, the government has the final say. There will be times when particular actors within the executive branch are frustrated by company or civil society resistance, but that is not a loss of sovereignty. Rather, that is an affirmation of it. The state—reflecting citizens' wishes—reigns supreme.

In a democracy, there is a difference between (1) state sovereignty and (2) cops getting everything they want. When it becomes harder for the police or national security experts



to do their jobs as a result of a loss of public trust, that is a sign that state sovereignty is alive and well—not proof of its death.

The problem with describing technology companies as sovereigns is not so much that it is wrong, but that it obscures the true challenge in Internet governance: determining which states influence how the Internet operates and where. The fundamental policy challenge of global Internet governance is not so different from other global policy challenges. The challenge is for states to coordinate to develop sensible global policy while also managing domestic political concerns. The challenge, in other words, is a two-level game.²³ Companies are a part of that dynamic, naturally. State goals are often achieved by regulating technology companies, and companies play an important role in managing user experiences and thereby citizens' expectations around the world. But technology companies are not directly setting state policy, except insofar as they manage to influence the political process.

To be sure, some states will choose not to assert their power too brutally. But firms will eventually face a choice: comply with state law or leave the market. The open empirical question is: How far can firms push before states will assert that power? The only answer I can offer here is that eventually, over the long run, some determined states will recognize—as China has—that it is possible to assert that authority without approval or support of foreign service providers. The data localization trends we're seeing suggest the limits of firm resistance to state power and the limits of states' patience. Before we can announce that state sovereignty is dead and what matters is platform power, states will rear up and remind us of their power.

The Real Barriers to Reform

The global governance challenges of the Internet call out for sensible policy reform. Yet the current debate suffers from several challenges. Rather than propose fantastical solutions to these problems—a global treaty? Internet-based global governance?—it might make more sense to sketch some of the barriers to thoughtful policy reform in this space. Each of these barriers reflects the fact that the organizations best situated to make policy on a given topic—legislators, firms, civil society groups—often have incentives to serve an audience whose interests do not align with the foreign stakeholders most affected.

Lawmaker Incentives

Those most directly affected by cross-border jurisdictional problems are often foreigners—actors with limited ability to influence policy in the place where it is needed. For example, the problem of jurisdictional barriers to law enforcement access to data stored abroad is felt most acutely by law enforcement *outside* the United States. These are actors with no effective voice in the US legal system. If Indian police cannot effectively conduct criminal investigations, American lawmakers do not have compelling incentives to care. The Indian

law enforcement agents are left with two options. The first option is to put diplomatic pressure on the United States to change its laws to incentivize American firms to comply with foreign laws in foreign markets. This would require considerable coordination: law enforcement officers in India would need to band together to convince their superiors that it is worth their time to negotiate with their American counterparts and that this particular issue is more important than other issues, like trade, military affairs, and whatever else might be on an Indian diplomat's agenda. It is conceivable that that will happen, but it is not the first thing that will happen.

The second option available to foreign law enforcement is considerably more direct than the first: pressure American firms to comply with local laws. Arrest the employees of US firms, search their offices, throttle their services—make life difficult—and those firms will have an incentive to lobby American lawmakers to change the law. This is perhaps the most logical pathway to developing policy change for law enforcement outside the United States but it is, to say the least, not ideal. One of the reasons it is not ideal is that it encourages more regulatory arbitrage by firms. If firms continue to tell one state they will pursue change in another state, they may—or they may not. This brinkmanship is the kind of thing that leads states to turn toward developing more local forms of control over the Internet.

Tech Firm Incentives

Firms have enormous incentives to play regulatory arbitrage across jurisdictions. If Brazil seeks to enforce its laws against Google, for example, that firm has considerable incentives to avoid complying up until the moment that noncompliance carries real costs. But what is that moment? Only when the firm's product is taken offline, its employees arrested, or its offices raided. These are rather extreme measures. State efforts at law enforcement can be frustrated—and American Internet firms can make money without differentiating their product for each market in order to comply with local law—for quite some time before frustration boils over into one of these measures.

Now, it is entirely sensible for the state to seek to enforce its rules on a foreign company operating within its borders, and it is not at all crazy to expect a global company with enormous resources to have regulatory compliance teams all over the world. But while the state gathers the political will to determine how to treat a noncompliant foreign company, firms can make money. From a firm's perspective, the less money spent on local lawyers, local servers, or other compliance measures, the better. Of course, brinkmanship and arbitrage are short-term strategies that may be good for a firm in a given moment but bad for the industry over the long run. That is, it may be beneficial to a firm in the short run to resist state efforts to enforce local laws, but over the long run this accelerates the harmful state processes described above—processes like forced data localization and exceptional access.



Civil Society Incentives

Civil society groups have played a vital role in developing Internet policy. Indeed, the participation of civil society groups has long been baked into the very multistakeholder model of Internet governance adopted by ICANN (Internet Corporation for Assigned Names and Numbers).²⁴ But this advocacy is extremely Western in flavor. It is almost entirely made on behalf of American (and occasionally European) groups, and very heavily funded by American Internet firms. One consequence of this is that when civil society groups argue for a single model of Internet governance—which they do often—it appears to many as the American model of Internet governance.

The rejection of a state's legitimate interest in regulating how the Internet behaves on state soil is precisely what pushes states closer to efforts at local control. Over the long run, that may be harmful to the users whom civil society groups seek to protect, either because a more local Internet is less privacy-protective—less transparent—or because it compromises on some other key principle. There is room for technology policy groups to advocate for Internet governance policies that recognize real and meaningful differences among states. But so far, that advocacy has been missing.

Conclusion

Internet firms are extremely powerful. But they are not states. Treating them as such is a distraction from the real problem: determining how and within which limits states—real sovereign nations—ought to be able to achieve their aims online. What is the proper scope of one state's authority over the Internet? When that authority extends beyond the state's borders, as it often will with Internet regulations, what kind of deference should affected states grant the extraterritorial regulation? These are the key questions for global governance of the Internet.²⁵ The fact that technology firms wield considerable power is relevant to any account of the political economy of Internet regulations—just as the fact that Walmart is powerful will be relevant to an account of regulation in the retail sector. But little turns on whether tech firms (or Walmart) are state-like in their power. In fact, that assertion distracts from the real question: How is the considerable power wielded by tech firms going to frustrate legitimate policy reform?

NOTES

1 John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, 1996, accessed September 5, 2018, <https://www.eff.org/cyberspace-independence>.

2 Ibid.

3 See, e.g., David R. Johnson and David Post, "Law and Borders—The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367.

4 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford, UK: Oxford University Press, 2006).

- 5 Timothy Stenovec, “Facebook Is Now Bigger than the Largest Country on Earth,” *Huffington Post*, January 28, 2015, accessed September 5, 2018, https://www.huffingtonpost.com/2015/01/28/facebook-biggest-country_n_6565428.html.
- 6 Chrisella Sagers, “Facebook Diplomacy,” *Diplomatic Courier*, June 8, 2011, accessed September 5, 2018, <https://www.diplomaticcourier.com/facebook-diplomacy>.
- 7 Adi Robertson, “Mark Zuckerberg Wants to Democratize Facebook—Here’s What Happened When He Tried,” *The Verge*, April 5, 2018, accessed September 5, 2018, <https://www.theverge.com/2018/4/5/17176834/mark-zuckerberg-facebook-democracy-governance-vote-failure>.
- 8 For the most evenhanded and thoughtful examination of this topic, see Kristen Eichensehr, “Digital Switzerland,” *University of Pennsylvania Law Review* 167 (forthcoming), accessed September 5, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205368.
- 9 “Israeli Firm Helping FBI to Open Encrypted iPhone,” Reuters, March 23, 2016, accessed September 5, 2018, <https://www.reuters.com/article/us-apple-encryption-cellebrite/israeli-firm-helping-fbi-to-open-encrypted-iphone-report-idUSKCN0WP17J>.
- 10 Ryan Knutson, “Why Encryption Fight Divides AT&T and Apple,” *Wall Street Journal*, February 18, 2016, accessed September 5, 2018, <https://www.wsj.com/articles/at-t-verizon-have-different-obligations-than-apple-1455838171> (subscription required).
- 11 See Claire Cain Miller, “Tech Companies Concede to Surveillance Program,” *New York Times*, June 8, 2013, accessed September 5, 2018, <http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html>.
- 12 See Lauren Walker, “NSA Surveillance May Cost U.S. Tech Companies More than \$35 Billion,” *Newsweek*, June 9, 2015, accessed September 5, 2018, <http://www.newsweek.com/nsa-surveillance-may-cost-us-tech-companies-more-35-billion-341168>.
- 13 Paul Mozur, Daisuke Wakabayashi, and Nick Wingfield, “Apple Opening Data Center in China to Comply with Cybersecurity Law,” *New York Times*, July 13, 2017, accessed September 5, 2018, <https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html>.
- 14 Jaikumar Vijayan, “Snowden Leaks Erode Trust in Internet Companies, Government,” *Computerworld*, April 4, 2014, accessed September 5, 2018, <https://www.computerworld.com/article/2489544/data-privacy/snowden-leaks-erode-trust-in-internet-companies—government.html>.
- 15 See Alan Rozenshtein, “Surveillance Intermediaries,” *Stanford Law Review* 70 (2018).
- 16 Charles Duhigg and David Kocieniewski, “How Apple Sidesteps Billions in Taxes,” *New York Times*, April 29, 2012, accessed September 5, 2018, <https://www.nytimes.com/2012/04/29/business/apples-tax-strategy-aims-at-low-tax-states-and-nations.html>.
- 17 F. H. Hinsley, *Sovereignty*, 2nd ed. (Cambridge, UK: Cambridge University Press, 1986), defining sovereignty as “final and absolute political authority in the political community.”
- 18 For those who conclude that these firms *do* erode state sovereignty, then perhaps they conclude that intermediaries like Google do the same. That view is at least consistent, even if it is wrong.
- 19 See Simon Denyer, “China’s Scary Lesson to the World: Censoring the Internet Works,” *Washington Post*, May 23, 2016, accessed September 5, 2018, https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?utm_term=.d70afd3e6b2e.
- 20 See Mike Isaac, “Facebook Said to Create Censorship Tool to Get Back into China,” *New York Times*, November 22, 2016, accessed September 5, 2018, <https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html>.



- 21 David Kris, “U.S. Government Presents Draft Legislation for Cross-Border Data Requests,” *Lawfare* (blog), July 16, 2016, accessed September 5, 2018, <https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests>.
- 22 Statement of Chris Calabrese, Center for Democracy & Technology, Hearing before the US House Committee on the Judiciary, “Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era,” June 15, 2017, accessed September 5, 2018, <https://judiciary.house.gov/wp-content/uploads/2017/06/Calabrese-Testimony.pdf>.
- 23 Robert Putnam, “Diplomacy and Domestic Politics: The Logic of Two-Level Games,” *International Organization* 42, no. 3 (Summer 1988): 427–60.
- 24 Stuart N. Brotman, “Multistakeholder Internet Governance: A Pathway Completed, the Road Ahead,” Brookings Institution report, July 2015, accessed September 5, 2018, <https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf>.
- 25 I address some of these questions in an upcoming paper, “Litigating Data Sovereignty,” *Yale Law Journal* 126 (forthcoming).



The publisher has made this work available under a Creative Commons Attribution-NoDerivs license 3.0. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nd/3.0>.

Hoover Institution Press assumes no responsibility for the persistence or accuracy of URLs for external or third-party Internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Copyright © (2018) by the Board of Trustees of the Leland Stanford Junior University

The preferred citation for this publication is Andrew Woods, "Tech Firms Are Not Sovereigns," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1813 (September 25, 2018), available at <https://www.lawfareblog.com/tech-firms-are-not-sovereigns>.



About the Author



ANDREW KEANE WOODS

Andrew Keane Woods is an associate professor of law at the University of Arizona College of Law, where his research examines cybersecurity, the regulation of technology, and international law. His most recent article is “Litigating Data Sovereignty,” forthcoming in the *Yale Law Journal*.

Working Group on National Security, Technology, and Law

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

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

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

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