

Choosing Both: Making Technology Choices at the Intersections of Privacy and Security

Alexander W. Joel*

Advanced technology and its creative application remain a comparative advantage for the United States, but we fear that the Intelligence Community is not adequately leveraging this advantage And this problem affects not only intelligence collection; we also lag in the use of technologies to support analysis.¹

It's six minutes before midnight as a surveillance society draws near in the United States. With a flood of powerful new technologies that expand the potential for centralized monitoring . . . we confront the possibility of a dark future where our every move, our every transaction, our every communication is recorded, compiled, and stored away, ready for access by the authorities whenever they want.²

[T]he [Intelligence Community] must *exemplify America's values*: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people.³

["Buridan's ass"]: a paradox whereby a hungry and thirsty donkey, placed between a bundle of hay and a pail of water, would die of hunger and thirst because there was no reason for him to choose one resource over the other.⁴

When you come to a fork in the road, take it.⁵

Technology plays a critical role in intelligence activities, enabling intelligence agencies to pursue their national-security mission more effectively and efficiently. The United States has long been a leader in

* Alexander Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI). The views expressed in this Article are his own and do not imply endorsement by the ODNI or any other U.S. government agency.

1. COMM. ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES 326 (2005), *available at* http://www.gpoaccess.gov/wmd/pdf/full_wmd_report.pdf.

2. AM. CIVIL LIBERTIES UNION, *EVEN BIGGER, EVEN WEAKER: THE EMERGING SURVEILLANCE SOCIETY: WHERE ARE WE NOW?* 4 (2007), http://www.aclu.org/files/pdfs/privacy/bigger_weaker.pdf.

3. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *THE NATIONAL INTELLIGENCE STRATEGY 2* (2009), *available at* http://www.dni.gov/reports/2009_NIS.pdf.

4. *THE OXFORD DICTIONARY OF PHRASE AND FABLE* 180 (Elizabeth Knowles ed., 2006), *available at* <http://www.encyclopedia.com/doc/1O214-Buridansass.html>.

5. YOGI BERRA, *THE YOGI BOOK: "I REALLY DIDN'T SAY EVERYTHING I SAID!"* 48 (1998).

technological innovation,⁶ and the Intelligence Community⁷ (IC) has recognized the importance of leveraging American technological advantages.⁸ Calls for the IC to make better use of technology are not uncommon, nor are complaints about its failure to capitalize on the latest technological developments;⁹ this is particularly true following news of a major event that the IC did not anticipate.¹⁰ Such calls often raise concurrent concerns about the civil liberties and privacy implications of placing powerful new capabilities in the hands of intelligence operatives, where they might be used in potentially unanticipated ways, cloaked from public scrutiny by rules that protect “sources and methods” from disclosure.¹¹

Intelligence officers and policy makers standing at the intersection of security and privacy can find themselves presented with a conundrum: how to make prudent technology choices? Moving in one direction seems imperative for accomplishing important national-security missions, yet raises red flags about potential impacts on privacy and civil liberties. Moving in another direction seems necessary to protect civil liberties, yet raises alarms about potentially dangerous security gaps. This dilemma calls up the image of Buridan’s ass, caught between two competing and compelling

6. EDMUND B. FITZGERALD, *GLOBALIZING CUSTOMER SOLUTIONS: THE ENLIGHTENED CONFLUENCE OF TECHNOLOGY, INNOVATION, TRADE, AND INVESTMENT* 23 (2000).

7. The term “Intelligence Community” is defined in § 3(4) of the National Security Act of 1947, 61 Stat. 495 (codified as amended at 50 U.S.C. § 401(a) (2006)), in relatively general terms. The specific members of the IC are listed in the Director of National Intelligence’s guide. NATIONAL INTELLIGENCE: A CONSUMER’S GUIDE 9 (2009), available at http://www.dni.gov/IC_Consumers_Guide_2009.pdf. There are seventeen elements of the IC: Office of the Director of National Intelligence; Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; Federal Bureau of Investigation National Security Branch; National Reconnaissance Office; National Geospatial-Intelligence Agency; Drug Enforcement Administration, Office of National Security Intelligence; Department of Energy Office of Intelligence and Counterintelligence; Department of Homeland Security Office of Intelligence and Analysis; Department of State Bureau of Intelligence and Research; Department of Treasury Office of Intelligence and Analysis; Air Force Intelligence; Army Intelligence; Coast Guard Intelligence; Marine Corps Intelligence; and Naval Intelligence. *Id.*

8. See Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM. RTS. & DEV. L.J. 143, 153 (1999) (asserting that developed states leverage their technological advantages in areas such as information management).

9. See, e.g., AMY B. ZEGART, *SPYING BLIND: THE CIA, THE FBI, AND THE ORIGINS OF 9/11* 137 (2007) (noting how inefficiently the FBI adopted new technology, including FBI Director Louis Freeh removing his computer from his office in 2000 for lack of use).

10. Indeed, soon after the attempted attack on December 25, 2009, on Flight 253, the White House announced that “[t]he U.S. government had sufficient information to have uncovered and potentially disrupted the December 25 attack . . . but analysts . . . failed to connect the dots that could have identified and warned of the specific threat . . . Information technology . . . did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information.” Press Release, White House, White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack (Jan. 7, 2010), <http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack>.

11. See, e.g., Martin E. Halstuk & Eric B. Easton, *Of Secrets and Spies: Strengthening the Public’s Right to Know About the CIA*, 17 STAN. L. & POL’Y REV. 353, 354–56 (2006) (asserting that after *CIA v. Sims*, 471 U.S. 159 (1985), the CIA has been shielded from public scrutiny).

considerations.¹² It also brings to mind Yogi Berra's famous advice on encountering a fork in the road: when forced to choose between security and privacy, find ways to "take it"—to have it both ways.¹³ Through it all, intelligence agencies must remember this: protecting privacy and civil liberties is not optional. The question they face is not *whether* to provide such protections—agencies are obligated, by law and duty, to provide them. Rather, the question is *how* to provide them while accomplishing the intelligence mission.

I. The Broader Context

The paradoxical directive that the IC use technology more aggressively because of its potential to make agencies more effective at their missions (which includes, of course, "spying"), yet refrain from using technology because of its potential intrusiveness, is a recurring one. Concerns that authorities for "espionage" might be abused if not properly overseen, given the advent of new capabilities, find eloquent expression in Justice Louis Brandeis's dissent in a 1928 Supreme Court case. In discussing wiretapping and the invention of the telephone, Justice Brandeis warned:

Subtler and more far-reaching means of invading privacy have become available to the Government The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.¹⁴

Fifty years later, the Church Committee echoed Justice Brandeis's concerns, warning that at a time when "the technological capability of Government relentlessly increases, we must be wary about the drift toward 'big brother government.'" The potential for abuse is awesome and requires special attention to fashioning restraints which not only cure past problems but anticipate and prevent the future misuse of technology.¹⁵ Privacy and civil liberties advocacy groups, academic commentators, and others have similarly raised such concerns over the years.¹⁶

12. See *supra* note 4 and accompanying text.

13. See *supra* note 5 and accompanying text.

14. *Olmstead v. United States*, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

15. S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-755, at 276 (1976).

16. See *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) (statement of James X. Dempsey, Center for Democracy and Technology), available at <http://www.judiciary.house.gov/hearings/pdf/Dempsey100505.pdf> ("[I]t is clear that the balance among . . . the individual's right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust . . . has been lost as

Public discourse is complicated in the IC arena by information disclosure restrictions and inhibitions that have traditionally gone hand-in-hand with intelligence activities.¹⁷ In part due to this lack of public transparency, popular imagination, as reflected in and fueled by fiction, television, and movies, is free to take leaps in different directions, uninhibited by the constraints—legal, policy, technical, operational, budgetary, and cultural—under which intelligence agencies operate. Satellites that peer around corners, analysts who can instantaneously access data from any source by tapping on a laptop, watch centers that can redirect surveillance cameras at any point on the globe to follow an individual running through a crowded square, supercomputers that can contact someone on his cell phone and then send him a message on an electronic billboard—these are the capabilities commonly portrayed in books and movies. Even while knowing that creative imaginations are at work, commentators focus on the imagery emerging from these works for the insights they may provide into potential intelligence capabilities, and concomitantly, potential abuses.¹⁸

Whether fact or fiction, such imagery can affect public perceptions, and thus expectations, of the IC's capabilities. Some may wonder whether agencies could deploy technology to instantaneously and precisely detect, identify, and track a terrorist before an attack.¹⁹ To achieve that capability, should the government acquire more computing power, access more data, and deploy more surveillance equipment? This vision of a technologically enabled future obscures bothersome details about technology that do not

powerful new technologies create and store more and more information about our daily lives"); Neil M. Richards, *Intellectual Privacy*, 87 TEXAS L. REV. 387, 394 (2008) (arguing that courts should use the First Amendment to protect the people from the government).

17. See 50 U.S.C. § 403-1 (2006) (directing the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure); *CIA v. Sims*, 471 U.S. 159, 177 (1985) (upholding the CIA's decision to withhold its sources and methods from a disclosure request under the Freedom of Information Act).

18. For example, *EAGLE EYE* (DreamWorks Pictures 2008), directed by D.J. Caruso, is about a secret Department of Defense computer system that uses its ability to both access and control nearly all networked computers and devices to surveil and direct the actions of an ordinary American. A leading advocacy organization noted that "beneath the fast-paced, action packed plot are looming questions about the future of technology and the importance of government accountability." ELEC. PRIVACY INFO. CTR., EPIC ALERT, June 22, 2009, http://epic.org/alert/EPIC_Alert_16.12.html. Similarly, *ENEMY OF THE STATE* (Touchstone Pictures 1998), directed by Tony Scott, about a rogue cell within the National Security Agency (NSA) that uses NSA's surveillance technology to track every move and conversation of an American (portrayed by Will Smith), leading him at one point to disrobe to avoid surveillance, has been cited in discussions about domestic surveillance. See, e.g., Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375, 376 n.7 (2002) (noting the Orwellian themes of the movie).

19. See, e.g., 24 (Fox Broadcasting Co. 2001) (portraying government agencies as using a variety of sophisticated technology to identify suspects, prevent terrorism, and apprehend criminals); *MINORITY REPORT* (Twentieth Century Fox & Dreamworks Pictures 2002) (telling the story of a world in which technology allows police to see the future and arrest potential offenders before the "precrimes" are committed).

always get comparable screen time.²⁰ Technology functions imperfectly resulting in the potential for error. Moreover, as technology enables access to more data, it increases demands on human analysts to review and act on that data. Thus, even without considering the ways in which fiction writers have imagined that the government could abuse such technologies, we should be concerned with the less dramatic aspects of these technology-enabled visions, such as false positives and increased “noise” in the system.²¹

Conversely, fictional imagery of the IC’s technological prowess may cause others to fear that such powerful capabilities could be abused or misused and to question how these types of capabilities could ever be properly controlled.²² Is the answer simply to prevent intelligence agencies from using advanced technological capabilities so as to minimize the risk of an Orwellian future? Or would there be consequences to outright prohibitions, affecting how well intelligence agencies can perform their authorized missions?

These contrasting visions of technology’s promise and peril may play a role in the paradoxical signals sent to the IC: do both more and less with technology. As the Church Committee put it thirty years ago in the midst of documenting what it characterized as a “massive record of intelligence abuses”:

We must acknowledge that the assignment which the Government has given to the Intelligence Community has, in many ways, been impossible to fulfill. It has been expected to predict or prevent every crisis, respond immediately with information on any question, act to meet all threats, and anticipate the special needs of Presidents. And then it is chastised for its zeal.²³

20. See, e.g., NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 88 (2004) (describing problems of technology development including its cost, tendency to fail, and use by terrorists for their own purposes, but concluding that in spite of all of this “Americans’ love affair with [technology] leads them to also regard it as the solution”).

21. See, e.g., *Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs Before the S. Judiciary Comm.*, 110th Cong. 12 (2007) (statement of Kim Taipale, Executive Director, Center for Advanced Studies in Science and Technology Policy) (discussing false positives in data mining); ROBERTA WOHLSTETTER, PEARL HARBOR: WARNING AND DECISION (1962) (discussing the failure to anticipate the Japanese attack on Pearl Harbor as a failure to identify “signals” from the “noise,” with “signal” meaning a sign of an enemy move, and “noise” meaning competing signals that are useless for predicting that move).

22. See, e.g., JAY STANLEY & BARRY STEINHARDT, AM. CIVIL LIBERTIES UNION, BIGGER MONSTER, WEAKER CHAINS 1–3 (2003), available at http://www.aclu.org/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (using George Orwell’s writings and the movie *Minority Report* to illustrate the real-world pervasiveness of surveillance systems and the fact that such systems “rarely remain confined to their original purpose”).

23. S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-755, at 290 (1976).

II. Keeping the Scale Balanced

Faced with these competing considerations, the obvious way ahead is to strike a balance: capitalize on America's technological prowess while protecting privacy and civil liberties through safeguards and oversight. Even the use of the term "balance," however, presents difficulties, returning us to the imagery of either/or choices. It raises the specter of a government official using a scale to make a decision about whether to deploy a program, where the official metaphorically weighs the benefits for national security that a new technology has to offer against the costs to privacy or civil liberties that using the technology might entail. In this vision, if the security benefits outweigh the liberty costs, the official approves the program. Alternatively, if there are only slight security benefits but heavy liberty costs, the official disapproves the program. Inherently, this view assumes a tradeoff between security and liberty—what weighs down one side of the scale necessarily causes the other side to go up—with no compromise options.²⁴

This is a limited and ultimately unhelpful use of the balance metaphor. While it is true that there are tensions between security and liberty interests, forcing either/or choices is neither helpful to practitioners nor realistic. In practice, programs are frequently adjusted to address concerns during successive review and approval stages. And protecting privacy and civil liberties is not optional; the question is not "whether," but "how." Thus, rather than imagining using a scale to weigh security interests *against* liberty interests in forcing an either/or choice to approve a new technological capability, consider viewing the scale as a means to determine the "weight" that is needed on each side to *keep the scale balanced between security and liberty*. Our focus should be not on which side outweighs the other to inform a go/no-go decision. It should be on giving *equal weight* to security and liberty interests affected by the technology so that the scale *remains balanced*.²⁵

On the security side of the scale, imagine that a new program will add weight to the scale with aspects that are potentially intrusive on privacy or that impact civil liberties.²⁶ We should examine the program to determine

24. When appearing on a PBS Frontline special, a former FBI counterterrorism official stated, "I can give you more security, but I've got to take away some rights. And so there's a balance. Personally, I want to live in a country where you have a common-sense, fair balance because I'm worried about people that are untrained, unsupervised, doing things with good intentions that at the end of the day, harm our liberties."

Frontline: Spying on the Home Front (PBS television broadcast May 15, 2007), available at <http://www.pbs.org/wgbh/pages/frontline/homefront/etc/script.html>.

25. Since program personnel are already focused on the security benefits of the new technology, the net effect of this approach is to provide a methodology for addressing the civil liberties implications of that technology under which those implications are on at least an equal footing with security interests. Of course, if there are legal requirements that apply, those must be followed regardless.

26. For purposes of this use of the balance metaphor, the scale only measures security/liberty interests that are in tension with one another, and thus only records weight on the security side of the scale if a technology program's security measures intrude on liberty interests. The more

whether the degree of intrusiveness occasioned through use of technology is legally authorized, necessary, and narrowly tailored toward achieving a legitimate security purpose. We should also ask whether there is a less intrusive way of achieving the same purpose. The effect of these inquiries is to find ways to add only as much weight to this side of the scale as is necessary and appropriate to achieve legitimate security purposes. On the liberty side of the scale, our inquiry should focus on determining whether and how to add weights in the form of safeguards and oversight to counterbalance the impacts of the added weight on the security side. Certain technologies, then, could add weight to the security side, such as surveillance technologies, while others could add weight to the liberty side—such as anonymization and auditing applications.²⁷

III. Protections for the Liberty Side of the Scale

Of course, this approach to the balance metaphor in evaluating new uses of technology is only helpful if there are effective privacy and civil liberties protections from which to draw to counterbalance any potential new challenges. Public discussion regarding the sources of such protections tends to focus on the Constitution—typically the First and Fourth Amendments—and statutes such as the Foreign Intelligence Surveillance Act of 1978²⁸ (FISA), the Electronic Communications Privacy Act,²⁹ and the Privacy Act of 1974.³⁰ However, the IC operates within an infrastructure for protecting privacy and civil liberties, for which the Constitution and applicable laws lay only the foundation.³¹

Beyond this foundation, the IC conducts its activities under the Executive Branch framework established by Executive Order 12,333.³² It

intrusive the program, the more it weighs down the security side of the scale; a nonintrusive program would add no weight to the scale.

27. The idea of weighing considerations in a manner that avoids a zero-sum decision-making approach has been put forward by others as well. For example, Amitai Etzioni, in *The Limits of Privacy*, discusses four criteria for determining whether privacy concerns and the common good are in balance: Is there a well-documented, macroscopic threat to the common good, not merely a hypothetical threat? Can the threat be countered by non-privacy-intrusive measures? Can the threat be countered by minimally intrusive measures? If privacy-intrusive measures are needed, are there safeguards and measures to address “undesirable side effects”? AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 12–14 (1999).

28. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.).

29. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

30. 5 U.S.C. § 552a (2006).

31. Indeed, all government employees, including intelligence officers, take an oath to support and defend the Constitution, as required by statute. 5 U.S.C. § 3331 (2006). Note that Article VI of the Constitution requires that all “executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution.” U.S. CONST. art. VI, cl. 3.

32. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004),

begins by directing that “[a]ll reasonable and *lawful* means must be used to ensure that the United States will receive the best intelligence possible,”³³ and makes clear that “[a]ll means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used.”³⁴ The Order goes on to provide, “The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.”³⁵

Part 1 then identifies the roles and responsibilities of the national-security and intelligence elements of the Executive Branch. Part 2 enumerates restrictions on the conduct of intelligence activities.³⁶ Section 2.3 governs how IC elements may handle information concerning U.S. persons.³⁷ It provides that:

[IC elements] are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director.³⁸

As further protection, those procedures, some of which are classified, go into extensive detail about what IC elements can do with respect to such information.³⁹ Section 2.3 additionally provides that “[t]hose procedures

Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *reprinted as amended in* 50 U.S.C. § 401 (2006).

33. *Id.* (emphasis added).

34. *Id.* § 1.1(a). The Order defines “United States person” broadly, as “a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.” *Id.* § 3.5(k).

35. *Id.* § 1.1(b).

36. Part 3 defines terminology. Note that the Order was revised significantly in 2008 to align it with the Intelligence Reform and Terrorism Act of 2004. *See* Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008) (citing the Intelligence Reform and Terrorism Act of 2004 as a source of authority for updating Exec. Order No. 12,333, which included striking and replacing the entirety of Part 1).

37. Exec. Order No. 12,333 § 2.3.

38. *Id.*

39. The procedures for the Department of Defense’s intelligence elements and those of the FBI are unclassified. *See* DEP’T OF DEF., DIRECTIVE 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (1982) [hereinafter DOD DIRECTIVE], *available at* <http://www.js.pentagon.mil/whs/directives/corres/pdf/524001r.pdf>; OFFICE OF THE ATT’Y GEN., U.S. DEP’T OF JUSTICE, THE ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS (2008), *available at* <http://www.justice.gov/ag/readingroom/guidelines.pdf>. The FBI has released its comprehensive

shall permit collection, retention, and dissemination of the following types of information,” and lists specific types, including “information that is publicly available,” “information constituting foreign intelligence or counterintelligence,” “information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation,” “information acquired by overhead reconnaissance not directed at specific United States persons,” and “incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws.”⁴⁰

Thus, it is not enough for IC elements to satisfy requirements imposed by the Constitution or applicable statutes when collecting, retaining, and disseminating information concerning U.S. persons. They must also ensure that their actions are consistent with Executive Order 12,333 and the implementing procedures. For example, an IC element’s procedures may require it to review lawfully collected information concerning a U.S. person within a certain time period after collection to determine whether it is “information constituting foreign intelligence or counterintelligence” or whether it meets other collection and retention criteria under the Executive Order.⁴¹ If information fails to meet such criteria, the agency’s procedures may require the agency to destroy the information or transfer it (with no copies retained) to another agency that has proper authority.⁴² These rules are interpreted and applied by agency Offices of General Counsel and by the Department of Justice, and are audited and overseen by agency Offices of Inspector General.⁴³ Possible violations are reported to the Intelligence Oversight Board of the President’s Intelligence Advisory Board.⁴⁴

In addition to Executive Branch protections, there are protections from the other branches as well. For example, the FISA Court issues and enforces orders relating to activities under FISA jurisdiction. Congress conducts

internal guidance under the Attorney General’s guidelines, FBI Domestic Investigations and Operations Guide, which are available at <http://foia.fbi.gov/foiaindex/diog.htm>.

40. Exec. Order No. 12,333 § 2.3.

41. *Id.*

42. *See, e.g.*, DOD DIRECTIVE, *supra* note 39, at 20–21 (describing procedures for retention of information about U.S. persons). Note also that section 2.3 of Executive Order 12,333 authorizes IC elements to collect, retain, and disseminate information concerning U.S. persons “consistent with the authorities provided by Part 1 of this Order.” Even if information is “publicly available,” under section 2.3(a) of the Order, the collection, retention, and dissemination of that information must be “consistent with the authorities” of that IC element. Intelligence officials must always be mindful of tying their activities to their authorized mission, even when dealing with information that is available to the public at large. This point becomes particularly relevant in considering the implications of technological change.

43. Exec. Order No. 12,333 § 1.6.

44. Exec. Order No. 13,462, 73 Fed. Reg. 11,805 (Mar. 4, 2008), *as amended by* Exec. Order No. 13,516, 74 Fed. Reg. 56,521 (Nov. 2, 2009). Section 1.6(c) of Executive Order 12,333 requires IC elements to report to the Intelligence Oversight Board “intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive.”

oversight as a co-equal branch of government.⁴⁵ Congressional oversight is a fundamentally important element of the civil liberties and legal infrastructure for the Intelligence Community, since Congress has access to classified information and can therefore assess the propriety of IC programs and exercise its constitutional prerogatives with respect to such activities, including the power of the purse.⁴⁶

And there are new entities involved in providing privacy and civil liberties advice and oversight in the post-9/11 era, including the DNI's Civil Liberties Protection Officer,⁴⁷ the Privacy and Civil Liberties Oversight Board,⁴⁸ and Privacy and Civil Liberties Officers established under the Implementing Recommendations of the 9/11 Commission Act of 2007.⁴⁹ Nongovernmental organizations also play an important role by providing focused attention, expertise, and advocacy on the intersection of technology, privacy, and national security.

IV. Responding to Technological Change: Can Liberty Keep Up?

The importance of this infrastructure of laws, rules, and oversight extends beyond serving as a source from which to draw protections to

45. Congress oversees and authorizes intelligence activities through the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence and appropriates funds for such activities through appropriations committees. Due to the diversity of the community (various elements are nested within other departments, and activities impact areas of concern to multiple committees), various other committees of Congress are also involved in reviewing intelligence activities. Section 502 of the National Security Act of 1947 requires that congressional intelligence committees be kept "fully and currently informed" of all intelligence activities (covert action is covered under section 503), "with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources or methods and other exceptionally sensitive matters." 50 U.S.C. § 413(a) (2006). Moreover, section 501 of that Act requires the President to ensure any "illegal intelligence activity is reported promptly to the intelligence committees." *Id.*

46. While Congress has historically played a role in overseeing intelligence activities since the founding of the nation, the current system of intelligence oversight was explicitly established following the Church Committee era, to work in conjunction with legislation such as FISA and with Executive Branch measures such as Executive Order 12,333 and its predecessors. See RICHARD A. POSNER, *UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM* 195 (2006); Loch K. Johnson, *Governing in the Absence of Angels* (detailing the relatively few times since the 1970s when Congress has devoted significant attention to reforming oversight of the IC), in *WHO'S WATCHING THE SPIES* 57, 60 (Hans Born et al. eds., 2005).

47. The National Security Act states,

[T]he Civil Liberties Protection Officer shall ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures . . . implemented by the . . . elements of the intelligence community . . . and ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.

National Security Act of 1947, 50 U.S.C. § 403-3d(b).

48. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 109-13, § 1061, 118 Stat. 3638, 3684 (codified at 5 U.S.C. § 601 (2006)).

49. Implementing Recommendations of 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801, 121 Stat. 266, 352 (to be codified at 42 U.S.C. § 2000ee).

counterbalance the impact of new capabilities being considered by the IC. Intelligence officers act on—and react to—the world around them, which is changing at ever-increasing rates due to technology.⁵⁰ Staggering amounts of communications and data course through the world’s telecommunications systems and databases, with processing capabilities being added to smaller and smaller devices (themselves networked in new and innovative ways).⁵¹ Consumers now have at their fingertips impressive capabilities to access and process data from public or commercial sources. Seemingly simple query tools—coupled with the profusion of content made available by users, providers, and publishers on the Internet—provides the average computer user access to information that was unimaginable when certain of the IC-related rules just described were originally written.

The explosion of information that the average consumer has access to today—which is also accessible to the average terrorist—has implications for protections on the liberty side of the scale. Rules written with particular technologies in mind, for example, might now be seen to impede intelligence activities in ways that were not originally contemplated; they might be portrayed as weighing down the liberty side in a manner that unduly restricts intelligence capabilities. For example, in supporting the successive FISA amendments (the Protect America Act in 2007⁵² and the FISA Amendments Act in 2008⁵³) government officials stated that proposed amendments were needed to modernize FISA’s provisions.⁵⁴ Conversely, concerns might also be raised that, because technological changes have made so much information available from so many sources, the existing rules are no longer weighty enough to adequately restrict intelligence capabilities in the manner originally intended. For example, commentators have pointed out that the growing amount of data about people’s personal lives now processed and stored by third parties is not protected by the Fourth Amendment (sometimes referred to as the “third party doctrine”).⁵⁵

50. See, e.g., John F. Duffy, *Inventing Innovation: A Case Study of Legal Innovation*, 86 TEXAS L. REV. 1, 66 (2007) (asserting that the electronics and software industries particularly have seen “highly rapid” technological change in the last quarter century).

51. See, e.g., JUNE JAMRICH PARSONS & DAN OJA, *NEW PERSPECTIVES ON COMPUTER CONCEPTS* 304 (2010 ed.) (“[T]he Internet is huge. Although exact figures cannot be determined, it is estimated that the Internet handles more than an exabyte of data every day. An exabyte is 1.074 billion gigabytes, and that’s a nearly unimaginable amount of data.”).

52. Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c).

53. Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of 50 U.S.C.).

54. See, e.g., *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 19 (2007) (statement of J. Michael McConnell, Director of National Intelligence) (“Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA’s scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.”).

55. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1137–38 (2002) (“[I]t is only recently that we are truly beginning to see the profound implications of the Court’s third party doctrine Government information gathering

When confronted with changes in technology that seemingly outpace anything originally contemplated, what should practitioners do? It may be illuminating to briefly reconsider *Olmstead v. United States*⁵⁶ in this context. In that 1928 case, the government used warrantless surveillance to track a “conspiracy of amazing magnitude” involving a network that included financiers, scouts, drivers, and even an attorney.⁵⁷ The surveillance worked: the FBI disrupted the plot. On appeal, the Supreme Court confronted the question of how to apply an “old rule”—the Fourth Amendment’s requirements⁵⁸ with its references to “persons, houses, papers, and effects”—to a “new tool,” wiretapping of telephone wires. The Court upheld the surveillance as legal,⁵⁹ reasoning that “the invention of the telephone . . . and its application for the purpose of extending communications” could not justify expanding the Fourth Amendment “to include telephone wires, reaching to the whole world from the defendant’s house or office.”⁶⁰ In doing so, the Court declined invitations to extend the principles of the Fourth Amendment by analogy to the “invention of the telephone,” rejecting, for example, the analogy of postal mail.⁶¹ Instead, the Court deferred to Congress to address the broader implications of government wiretapping.⁶²

Of course, *Olmstead* is best known for Justice Louis Brandeis’s eloquent dissent. In contrast to the majority, Justice Brandeis found that, just as the Court had previously “sustained the exercise of power by Congress . . . over objects of which the fathers could not have dreamed,” clauses guaranteeing individual protection must also “have a similar capacity of adaptation to a changing world.”⁶³ Justice Brandeis reasoned that “[t]ime works changes [and] brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth.”⁶⁴ Justice Brandeis did not believe that a new constitutional amendment, or legislative action, was called for to address the Fourth

from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times.”).

56. 277 U.S. 438 (1928).

57. *Id.* at 455.

58. The Fourth Amendment provides,

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

59. *Olmstead*, 277 U.S. at 464–65.

60. *Id.* at 465.

61. *Id.*

62. *Id.* at 465–66.

63. *Id.* at 472.

64. *Id.* at 472–73 (Brandeis, J., dissenting) (quoting *Weems v. United States*, 217 U.S. 349, 373 (1910)).

Amendment's use of terms such as "papers" and "effects."⁶⁵ Rather, he reasoned by analogy and found that "[t]here is, in essence, no difference between the sealed letter and the private phone message."⁶⁶

What is the lesson for us? For intelligence professionals facing a landscape where new telephone-type inventions seem to multiply at an ever-increasing rate, pressure may be brought to bear to make a sharp break from prior rules—even technology-neutral ones—and to write new rules for a new era and address changes in technology that were not contemplated when the original rules were developed, particularly where those rules are oriented toward outdated technologies. Perhaps, like the *Olmstead* majority,⁶⁷ we should accept that, for certain new developments, the old rules do not apply and policy makers must develop new ones.

However, when existing rules are based on sound, technology-neutral principles that protect privacy and civil liberties while enabling agencies to pursue their mission, it is not clear that writing new ones will leave us in a better place, even if those who originally crafted the rules did not imagine what technology enables today. Rules can and should be harmonized, clarified, and updated. Where wholesale revision is called for to address technological change, the challenge will be this: technology is complex, difficult to understand and describe, and continues to change rapidly. It is, therefore, a daunting task to pose to lawyers, policy makers, and the rule-making process to capture the essence of technology's implications—in all its richness—and in a way that will enable its effective use while addressing civil liberties implications.

A visualization exercise illustrates the problem. The rate at which technology changes over time can be depicted on a chart as a steep, diagonal line, to show that it changes rapidly.⁶⁸ Indeed, the line might also be jagged, to illustrate how technology can leap ahead in sudden spurts. By contrast, the line showing the rate at which government policies change, be they laws or internal government regulations, would be more horizontal, with periodic step increases to show that policy changes gradually and predictably.⁶⁹ The two lines probably would not intersect—notwithstanding the title of this

65. *Id.*

66. *Id.* at 475. Indeed, he found wiretapping more problematic, since it involved the communications of more people. *Id.* at 476.

67. *Id.* at 465–66.

68. *See supra* note 50 and accompanying text.

69. *See, e.g.,* Ivan K. Fong, *Law and New Technology: The Virtues of Muddling Through*, 19 *YALE L. & POL'Y REV.* 443, 454–56 (2001) (describing courts throughout the twentieth century as "struggling to fit new technologies" into then-existing legal concepts); Bradley C. Karkkainen, *Bottlenecks and Baselines: Tackling Information Deficits in Environmental Regulation*, 86 *TEXAS L. REV.* 1409, 1414 (2008) (reporting that innovative industrial sectors often complain that technology-based regulations are obsolete once promulgated because the industry has moved on to new production technologies).

symposium—leaving a gap between policy and technology at any given point in time.

This exercise illustrates a fairly obvious truth: by the time the lawyers, technologists, privacy officers, and policy makers agree on a new policy to address a technological change, that technology may well have changed again.⁷⁰ If the goal is to update rules to keep pace with such change, the process may be a never-ending one. More specifically, since technologists and lawyers speak different languages, there is a risk of “technical translation error,” that the new policy will get the technology wrong.⁷¹ In addition, it is quite possible that the new policy will use terminology, or assumptions, specific to a particular technology and therefore will quickly become outdated.⁷²

Referring again to the imaginary chart, since it shows a steep line with technology changing quickly and a shallow line with policies changing gradually, we can predict that policies will perpetually lag technologies, leaving a gap. How to fill it? Proceeding without rules is not an option; privacy and civil liberties must be protected. Waiting to deploy the technology while new rules are written (standing there like Buridan’s ass) is no more attractive.

It may be prudent to consider Justice Brandeis’s approach:⁷³ to find the underlying principles animating the existing rules, to reason by analogy,⁷⁴ and to find ways to apply those principles to the new conditions created by technological change (akin to our common law tradition). This can help fill policy gaps while also informing policy makers as they develop new rules, should they determine such rules are called for. Applying these principles to

70. I am referring to policies that require acts of Congress or formal departmental or interagency processes to implement, rather than policies that could be implemented at the operating level.

71. See, e.g., Robert P. Merges, *One Hundred Years of Solicitude: Intellectual Property Law, 1900–2000*, 88 CAL. L. REV. 2187, 2228–31 (2000) (explaining how the Supreme Court’s mischaracterization of computer software as merely an algorithm led the Court to incorrectly ban patents on software for a time).

72. See, e.g., *id.* at 2190 (“Detailed, technology-specific provisions reflecting the passing concerns of a moment have proven difficult to adapt to new technologies.”). Of course, it may well be important to write rules with specific technologies in mind. Yet, excess specificity can have interesting consequences. For example, in conducting oversight, an office’s mission may be to assure compliance with legal requirements, and the office may therefore find it important to require a detailed description of the relevant technology being deployed and the agency’s implementing procedures governing its use. Indeed, the absence of such detail poses problems, since it may otherwise be difficult to ascertain compliance with general standards. However, creating detailed documentation for purposes of oversight risks technical translation errors, which could later result in compliance incidents if the implementation does not match the submitted documentation. Moreover, because technology changes rapidly and unpredictably, if an agency’s procedures are premised on a certain set of external technical conditions and those conditions unexpectedly change, program personnel will need to be alert to submit modifications.

73. See *supra* note 64 and accompanying text.

74. Reasoning by analogy is frequently encountered in judicial opinions. See generally Richard A. Posner, *Reasoning by Analogy*, 91 CORNELL L. REV. 761 (2006) (reviewing LLOYD L. WEINREB, *LEGAL REASON: THE USE OF ANALOGY IN LEGAL ARGUMENT* (2005)).

new situations must, of course, occur under the civil liberties protection infrastructure discussed earlier,⁷⁵ subject to congressional oversight and to judicial supervision where appropriate. Measures to review and enhance elements of this infrastructure, and to provide greater transparency, are in process.⁷⁶ Seen in this context, filling any policy gaps “the Brandeis way” appears to offer a helpful way forward, even in situations where comprehensive rule changes are ultimately deemed necessary.

V. Conclusion

Making technology choices at the intersections of privacy and security does not require tradeoffs. The IC need not stand paralyzed by the choice between its core mission to provide security and its solemn obligation to protect privacy and civil liberties. Instead, we should maintain the balance between security and liberty. We should ensure, on the one side, that a new technological capability is lawful, narrowly tailored to achieve an appropriate security purpose, and that there are no less intrusive means available, while we add, on the other side, counterbalancing privacy and civil liberties protections. We should look to Justice Brandeis’s example, which remains more relevant than ever: find core principles in our tried-and-tested rules, apply them to new changes in the technological landscape, and use those principles to help us clarify and, where necessary, update our rules and develop new protections. In the end, Yogi Berra’s⁷⁷ approach may prove truest of all: when facing a fork in the road between security and privacy, take it.

75. See *supra* note 31 and accompanying text.

76. See, e.g., Exec. Order No. 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010) (“Protecting information critical to our Nation’s security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.”).

77. See *supra* note 5 and accompanying text.