7-2016

Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights

Peter Margulies
Roger Williams University School of Law, pmargulies@rwu.edu

SURVEILLANCE BY ALGORITHM: THE NSA, COMPUTERIZED INTELLIGENCE COLLECTION, AND HUMAN RIGHTS

Peter Margulies[*]

Abstract

ISIS's cultivation of social media has reinforced states' interest in using automated surveillance. However, automated surveillance using artificial intelligence ("machine learning") techniques has also sharpened privacy concerns that have been acute since Edward Snowden's disclosures. This Article examines machine-based surveillance by the NSA and other intelligence agencies through the prism of international human rights.

Two camps have clashed on the human rights implications of machine surveillance abroad. The state-centric camp argues that human rights agreements like the International Covenant on Civil and Political Rights (ICCPR) do not apply extraterritorially. Moreover, the state-centric camp insists, machine surveillance is inherently unintrusive, like a dog seeing a human step out of the shower. Surveillance critics respond that machine and human access to data are equivalent invasions of privacy and legal protections must be equal for individuals within a state's borders and non-nationals overseas. In a controversial recent decision, *Schrems v. Data Protection Commissioner*, the European Court of Justice appeared to side with surveillance's critics.

This Article argues that both the state-centric and critical positions are flawed. This Article agrees with surveillance critics that the ICCPR applies extraterritorially. Machine access to data can cause both ontological harm, stemming from individuals' loss of spontaneity, and consequential harm, stemming from errors that machines compound in databases such as no-fly lists. However, the *Schrems* decision went too far by failing to acknowledge that human rights law provides states with a measure of deference in confronting threats such as ISIS. Deference on overseas surveillance is particularly appropriate given U.N. Security Council resolutions urging states to deny terrorists safe havens. But deference cannot be absolute. To provide appropriate safeguards, this Article recommends that machine searches abroad be tailored to compelling state purposes, scientifically validated, and subject to independent review.

---

* Professor of Law, Roger Williams University School of Law; B.A., Colgate University, 1978; J.D., Columbia Law School, 1981. I thank Sudha Setty and participants at a workshop at Western New England University School of Law for comments on a previous draft.

INTRODUCTION

Searching for a needle in a haystack is a metaphor for human futility, but searching for a fact in a haystack of data is just more code for a computer.[1] Nevertheless, appreciation for the computer's prowess has not translated into applause for automated surveillance. Concerned commentators invoke Jeremy Bentham's panopticon, in which minders perpetually keep tabs on inmates.[2] Others assert that automated surveillance designed to detect overseas terrorists such as Islamic State of Iraq and Syria (ISIS) recruits[3] is ineffective, echoing humans' ill-fated

1. *See* IAN H. WITTEN ET AL., DATA MINING 21–22 (3d ed. 2011) (discussing private sector data mining of Internet usage patterns).

2. *See, e.g.*, BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 32 (2015); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 92–93 (2007).

3. ISIS, also known as ISIL or the Islamic State, is fighting the Assad regime and Western-backed forces in Syria, gaining control of territory in Iraq, and inspiring recruits to violence

haystack dives.[4] Suppose, however, that technological progress makes computer (machine) searches effective tools in locating overseas terrorists.[5] That promise should prompt inquiry into machine searches' status under human rights law.[6]

In the international realm, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary intrusions on privacy.[7] This Article argues that states should receive a measure of deference in using scientifically validated machine searches to collect overseas intelligence, subject to both substantive and procedural constraints. Privacy objections to machine searches are not wholly misplaced. However, such objections should be tempered by awareness of the positive role safeguards can play and the advantages that properly cabined automated surveillance provides.

This safeguard-centered approach to machine access contrasts with both a state-centric approach and the position of critics of state surveillance. A state-centric approach might view international machine access as entirely appropriate, even without meaningful safeguards. In keeping with this view, the U.S. position is that the ICCPR does not bind states parties extraterritorially.[8] A state-centric view regards machine

---

worldwide. *See* Anne Barnard & Michael R. Gordon, *Goals Diverge and Perils Remain as U.S. and Turkey Take on ISIS*, N.Y. TIMES (July 27, 2015), http://www.nytimes.com/2015/07/28/world/middleeast/us-and-turkey-agree-to-create-isis-free-zone-in-syria.html.

4. *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1661 (2010).

5. The term "machine search" refers to a search conducted by a computer or computer network at human initiative or under human direction. When using a machine search, human analysts may not review all the data accessed by the machine but may only view a far smaller set of data outputs. Professor William Banks acknowledges that machine searches of massive troves of data, sometimes called "data mining," may be effective as a "preliminary screening method" in identifying terrorists. *See id.*; NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS 4, 77 (2008) (discussing risks and possible benefits of counterterrorism data mining). Given the difficulty in identifying violent extremists and the risks posed by false negatives (here, terrorists erroneously classified as innocents), even a "preliminary" detection method has promise.

6. While this Article touches on the domestic use of machine searches, it leaves extended discussion of Fourth Amendment issues to others. *See, e.g.*, SLOBOGIN, *supra* note 2, at 21–47 (providing a comprehensive approach to new technology); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 388–92 (2015) (cataloguing risks and benefits of new technology and its effect on the Fourth Amendment). In searches abroad, targeting persons with no ties to the United States, the Fourth Amendment does not apply. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265, 274–75 (1990).

7. International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171, 177 [hereinafter ICCPR].

8. *See* U.S. DEP'T OF STATE, SECOND AND THIRD PERIODIC REPORT OF THE UNITED STATES OF AMERICA TO THE UN COMMITTEE ON HUMAN RIGHTS CONCERNING THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, ANNEX I (2005) [hereinafter STATE DEP'T PERIODIC

access as inherently free of the intrusiveness of human access.[9]

In contrast, critics of state surveillance in general and U.S. surveillance in particular posit what this Article refers to as the equivalency thesis. The thesis contains three interrelated propositions. First, surveillance critics claim that machine and human access are equivalent invasions of privacy.[10] Second, critics assert that the United States' technological capabilities—not the law—drive government surveillance practices.[11] Third, critics claim that human rights law requires equivalent protections for both U.S. and non-U.S. persons.[12]

This Article argues that both the state-centric and equivalency thesis are wrong. Taking issue with the state-centric approach, this Article

---

REPORTS]; *see also* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 307 (2015) (observing that the "United States has long interpreted the ICCPR not to apply extraterritorially"); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2143 (2014).

9. *See, e.g.*, Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 254 (2008) (arguing that machine searches do not intrude on privacy because computers are not "sentient beings"). For a more nuanced critique of privacy advocates' assumptions, see William H. Simon, *Rethinking Privacy*, BOS. REV. (Oct. 20, 2014), http://bostonreview.net/books-ideas/william-simon-rethinking-privacy-surveillance (asserting that privacy advocates derive their views from an illusory baseline in which individuals form their identities uninfluenced by the views of others).

10. *See* SCHNEIER, *supra* note 2, at 130 (arguing that surveillance conducted via computer algorithms is materially identical to human surveillance in terms of intrusiveness).

11. In other words, the U.S. and other states will generally do whatever they are technologically capable of doing. *See* Ryan Devereaux et al., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, INTERCEPT (May 19, 2014, 12:37 PM), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (quoting Michael German, former American Civil Liberties Union counsel and former FBI agent, as observing that intelligence officials "have this mentality—if we can, we will"); *cf.* Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM. & TECH. L. REV. 317, 319–22 (2015) (arguing that surveillance conducted by National Security Agency (NSA) is driven by technological capabilities and unconstrained by provisions of relevant law).

12. *E.g.*, David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013, 12:48 PM), https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/ (critiquing U.S. surveillance policy overseas as inconsistent with human rights); *see also* Ben Emmerson (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism), *Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, ¶ 43, U.N. Doc. A/69/397 (Sept. 23, 2014) (asserting that states are "legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction"); Jennifer Granick, *Foreigners and the Review Group Report: Part 2*, JUST SECURITY (Dec. 19, 2013, 12:47 PM), https://www.justsecurity.org/4838/foreigners-review-group-report-part-2/ (welcoming a Review Group's recommendation to limit U.S. surveillance of non-U.S. persons). A U.S. person within the meaning of this Article refers to a U.S. citizen or lawful resident, or an individual of any nationality or immigration status who is physically present in the United States.

demonstrates that the ICCPR applies extraterritorially. Moreover, unfettered machine access abroad would violate the ICCPR's prohibition on arbitrary intrusions on privacy. At the same time, this Article argues that the equivalency thesis's propositions each miss the mark. Consider the proposition that human and machine access are equally intrusive. Although unfettered machine access is problematic, computers' lack of consciousness suggests that cabined machine access is consistent with human rights law.[13] Safeguards that limit human access can ensure that some level of machine access passes muster.

This Article also identifies flaws in the equivalency thesis's second assertion, which this Article calls the technological imperative: government practice will inevitably extend to the limits of government capabilities.[14] While advances in technology can exert a powerful gravitational pull on operations, the technological imperative fails to reckon with the robust safeguards, such as search filters, that technology can impose on both human and machine searches. In addition, surveillance critics who embrace the technological imperative as a descriptive matter ignore legal safeguards that limit state surveillance. Dismissing current safeguards may impose too high a bar for reform, since any protections that are likely to be adopted may also earn critics' disdain. Critics eager to proclaim the virtues of freedom and progress[15] do not always grasp Voltaire's observation that the perfect is the enemy of the good.[16]

The equivalency theorists' second assertion also fails to address a paradox that emerges from the interaction of accuracy and transparency in machine data analysis. A nuanced account would distinguish between directed techniques using keywords submitted by human analysts and autonomous techniques in which analysts input data and machines then

---

13. *See, e.g.*, SLOBOGIN, *supra* note 2, at 195 (explaining that machine searches accompanied by restrictions on analysts' queries of the resulting database could preserve anonymity and therefore reduce intrusions on privacy).

14. Surveillance critics use this assertion for descriptive purposes; as a normative matter, they argue vigorously that the government *should not* collect everything it *can* collect. *See, e.g.*, SCHNEIER, *supra* note 2, at 92–98 (addressing privacy rights and abuse of government surveillances).

15. *See, e.g.*, *id.* at 97–98.

16. However, privacy advocates are right to assert that the temptations posed by the technological imperative require further privacy safeguards, including independent review of intelligence collection and a public advocate at the United States' Foreign Intelligence Surveillance Court (the FISC) who will provide a voice opposing the government's surveillance requests. *See* Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* JUST SECURITY (Nov. 4, 2013, 1:34 PM), https://www.justsecurity.org/2873/fisa-special-advocate-constitution/ (discussing the Privacy and Civil Liberties Oversight Board's "special advocate" proposal).

find patterns independent of explicit human commands.[17] Autonomous techniques give rise to what this Article refers to as the transparency paradox: these searches use "hidden layers" of computing power to group myriad variables more accurately.[18] However, because the layers assess so many variables, analysts cannot provide a substantive verbal explanation for courts or other legal gatekeepers seeking an articulable justification for individual searches. As a result, the law could preclude more accurate techniques, while embracing techniques that produced more errors but provided the familiar comforts of a verbal explanation. Surveillance critics avoid this issue by dismissing the accuracy of autonomous searches in the counterterrorism context.[19] If they are wrong about accuracy, however, the transparency paradox becomes too important to ignore.

The equivalency theorists' third proposition—a state must accord the same rights to its nationals and persons overseas—also ignores both practicality and precedent. The ICCPR, as the European Court of Human Rights (ECHR) acknowledged in *Weber v. Germany*,[20] gives states greater leeway in surveillance of transnational communications than in surveillance of domestic communications.[21] Transnational surveillance with safeguards can assist in vindicating international norms, such as the framework of cooperation against ISIS and other terrorist groups established in United Nations Security Council resolutions 2178[22] and 1373.[23] Measured overseas surveillance can compensate for the ability of extremist non-state actors to find safe havens in weak states. In addition, while transnational surveillance can diminish privacy, it can also *enhance* privacy by combating rogue cyber states and non-state actors who breach

17. *Cf.* STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE 694–95 (3d ed. 2010) (describing the three types of feedback that determine learning: unsupervised learning, reinforcement learning, and supervised learning).

18. *See* WITTEN ET AL., *supra* note 1, at 467, 469.

19. *E.g.*, SCHNEIER, *supra* note 2, at 136–39.

20. 2006-XI Eur. Ct. H.R.

21. *See id.* at paras. 87–88; Sarah St. Vincent, *International Law and Secret Surveillance: Binding Restrictions upon State Monitoring of Telephone and Internet Activity*, CTR. FOR DEMOCRACY & TECH. (Sept. 4, 2014), https://cdt.org/files/2014/09/CDT-IL-surveillance.pdf. The ECHR's deferential approach suggests that European and U.S. legal analysis of the intersection of privacy and national security may not be all that different, despite differences in rhetoric; *cf.* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 632–33 (2007) (noting parallels in European and U.S. conceptions); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004) (arguing that the United States protects privacy to safeguard liberty, while Europeans view privacy as central to dignity, which they define as sparing the individual from unwelcome public attention).

22. S.C. Res. 2178, paras. 2–4 (Sept. 24, 2014).

23. S.C. Res. 1373, paras. 1–3 (Sept. 28, 2001).

privacy protections.[24] Moreover, overseas surveillance can be appropriate under the law of armed conflict (LOAC) as a form of reconnaissance.[25]

In light of these concerns, this Article defends a measure of deference for states' overseas machine surveillance. Just as the ECHR has accorded states a "margin of appreciation" in taking steps that protect security and public safety,[26] the proportionality inquiry underwritten by the ICCPR Article 17 arbitrariness standard should be deferential. However, a measure of deference does not entail a blank check.

This Article proposes three elements of accountability for machine surveillance: First, surveillance must be for a compelling purpose, such as national security,[27] and should be tailored to that goal. For example, bulk collection of the content of another state's communications should be prohibited, unless the state whose data is collected is involved in an armed conflict with the collecting state. Under this test, the United States could continue to engage in bulk collection in Afghanistan for the duration of the armed conflict there but could not engage in bulk surveillance of content in the Bahamas, where the United States reportedly conducts bulk surveillance of all communications to reach the far smaller set of narcotics and human traffickers.[28] Second, searches should be reliable and subject to accepted techniques for validation. To deal with the transparency paradox that affects autonomous searches, this Article argues that human rights law should accept a methodological

---

24. *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 229 & n.38 (2016).

25. Michael N. Schmitt, *Unmanned Combat Aircraft Systems and International Humanitarian Law: Simplifying the Oft Benighted Debate*, 30 B.U. INT'L L.J. 595, 595–98 (2012) (analyzing surveillance and reconnaissance in the context of using drones for targeted killing during an armed conflict).

26. Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A), paras. 47, 66 (1976) (regulating public dissemination of information about human sexuality to protect children). The ECHR's use of the margin of appreciation in cases involving free expression provides an *a fortiori* case for the margin's materiality in adjudicating surveillance.

27. These include the limits that President Barack Obama outlined in Presidential Policy Directive No. 28 (PPD-28), which restricted bulk collection of content abroad to specific purposes, such as countering terrorism, espionage, arms proliferation, cybercrime or other international lawbreaking, or evasion of lawful sanctions. *See* Press Release, Office of the Press Sec'y, Presidential Policy Directive – Signals Intelligence Activities (Jan. 12, 2015), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28]. The U.S. government distinguishes between bulk and targeted collection. *Id.* Bulk collection obtains virtually *all* communications content or other data for subsequent analysis, while targeted collection obtains only data that corresponds to certain specific identifiers. *See* PPD-28 Section 4 Procedures, USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons, at 7 n.1–2 (Jan. 12, 2015) [hereinafter PPD-28 Supplemental Procedures].

28. *See* Devereaux et al., *supra* note 11.

explanation of a machine search's validity in place of a substantive verbal explanation.

Third, review must be independent. Decisions by the ECHR[29] and the Court of Justice of the European Union (CJEU), including the 2015 decision in *Schrems v. Data Protection Commissioner*[30] and the 2014 decision in *Digital Rights Ireland Ltd. v. Ireland*,[31] require some level of independent review of surveillance.[32] The United States provides judicial review of much of its surveillance through the Foreign Intelligence Surveillance Court (FISC).[33] To complement the FISC, it should also create an executive branch agency to review surveillance under Executive Order 12,333, a Reagan Administration measure that authorizes the collection of intelligence.[34] The new agency should be shielded from political influence to the maximum degree possible under the U.S. Constitution. The agency should address complaints by individuals that their personal data has been wrongfully collected, retained, or disseminated. Moreover, the FISC should have input from a robust voice that opposes government surveillance requests. The provision for amici curiae in the newly enacted USA Freedom Act[35] improves the situation. So does the provision for a State Department ombudsperson in Privacy Shield, the EU–U.S. data transfer agreement that replaces the agreement invalidated by the CJEU in *Schrems*.[36] However, more improvement is needed.

This Article proceeds in five Parts. Part I explains the way in which machine searches operate and the sources of U.S. legal authority for their use. Part II considers both deontological and consequentialist arguments on whether machine access is less intrusive than human access. It concludes that while machine access is less intrusive on both deontological and consequential grounds, safeguards are necessary for deploying it. Part III considers surveillance critics' claim that a state's surveillance capabilities dictate its surveillance practices. This Part, while

29. *See, e.g.*, Zakharov v. Russia, Eur. Ct. H.R., para. 147 (2015); Kennedy v. United Kingdom, Eur. Ct. H.R., paras. 79–80 (2010).

30. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R.

31. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Comm'r, 2014 E.C.R.

32. *See* Banks, *supra* note 4, at 1661; Deeks, *supra* note 8, at 358.

33. *See Foreign Intelligence Surveillance Court*, FED. JUD. CTR., http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html (last visited Mar. 18, 2016).

34. Exec. Order No. 12,333, 46 Fed. Reg. 59,941–42 (Dec. 4, 1981).

35. 50 U.S.C. § 1803(i) (2012); *see also* Stephen I. Vladeck, *The FISA Court and Article III*, 72 WASH. & LEE L. REV. 1161, 1179 (2015) (suggesting that "special advocate" in FISC proceedings who would oppose government requests in a wider range of cases would ameliorate concerns that the provisions for FISC review of surveillance procedures under § 702 violate Article III of the U.S. Constitution, which governs the role of federal courts).

36. *See* European Comm'n, *Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU–U.S. Privacy Shield* 26 (Feb. 2016) [hereinafter EC Adequacy Decision].

acknowledging that the technological imperative to expand capability influences surveillance practice, notes that privacy advocates unduly discount both technology's potential to protect against intrusive searches and the power of legal safeguards to curb abuses.

Part IV considers the state-centric view that human rights agreements like the ICCPR do not apply extraterritorially and shows that the ICCPR's language and purpose support extraterritorial application. Part V suggests a normative framework for machine surveillance overseas, in light of the ICCPR's prohibition on arbitrary intrusions. This framework is deferential because of the need to accommodate conflicting international norms, including Security Council resolutions against terrorism and LOAC, as well as the privacy benefits of surveillance targeting international cyber criminals. However, the framework's deference is not absolute. To ensure accountability, the model requires that states tailor surveillance to a compelling purpose, demonstrate the reliability of their machine surveillance through commonly accepted scientific methods, and provide for independent review and recourse. These safeguards will allow governments to utilize machine searches to protect the public while also protecting privacy.

I. INSIDE THE MACHINE: COMPUTERS AND SURVEILLANCE

Because "Big Data" is too big for humans to process, machine searches are increasingly important in both government and the private sector.[37] Such searches can entail different methods of gaining access to data, which in the United States typically have different sources of legal authority. This Part distinguishes between scanning and collection; it then divides the latter into bulk and targeted collection.

Different types of machine searches can also entail more or less human involvement. This Part describes directed machine searches, which require supervision from a human analyst. It then describes autonomous searches, where humans feed data to a machine, permit the machine to find patterns on its own, and then validate the results. Each method has trade-offs. This Article defines one of these crucial trade-offs as the transparency paradox: in autonomous searches, accuracy often improves at the expense of transparency. Machines that are fed enough data can discern patterns that humans would miss. However, because of the volume of data involved in such searches and the number of variables that the machine analyzes, humans cannot offer a substantive, verbal

37. *See* Jorge Garcia, *Machine Learning and Cognitive Systems: The Next Evolution of Enterprise Intelligence (Part I)*, WIRED, http://www.wired.com/insights/2014/07/machine-learning-cognitive-systems-next-evolution-enterprise-intelligence-part/ (last visited Mar. 18, 2016).

explanation of the machine's reasoning path. This raises a legal issue that this Article addresses in subsequent Parts: ranking transparency and accuracy, when enhancing one value will sacrifice the other.[38]

A. *Scanning Versus Collection*

If one analogizes machine access to living arrangements, scanning is like a quick visit, while collection resembles a lengthy stay. Scanning intrudes on privacy in passing, while collection contemplates the storage of data by the collecting entity. The differences between scanning and collection matter less in the private sector, where scanning of internet users' data is ubiquitous and recurring. Those differences have higher stakes for the government's machine access.

1. Scanning in Government and the Private Sector

Scanning involves the recurring inspection, usually by machine, of information from individuals, but it does not entail the storage of all the information by the scanning party. A private firm or government agency, respectively, can scan a user's email, as Google does with Gmail, or gain access to interchange points in the transmission of internet communications, as the U.S. government does pursuant to statute.[39] For example, in scanning pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act,[40] the NSA's machines gain access through a buffer, cache, or other device that temporarily stores transnational communications in the course of transmitting them to their destination. Scanning is by definition a process that allows machines to gain access to a huge volume of communications, the vast majority of which are substantively irrelevant. In the process of scanning, the machine selects material that is relevant and designates that material for collection and subsequent analysis.

In the commercial internet space, scanning is not a *part* of the business model; it *is* the business model.[41] Google's computers use algorithms devised by Google's own engineers or searches crafted by the firm's computers to scan users' web-browsing histories and the contents of

38. *See infra* Section I.C.

39. *In re* Government's Ex Parte Submission of Reauthorization Certification for 702 Program, 2011 WL 10945618, at *5, *19–20, *23 (Foreign Intell. Surveillance Ct. Oct. 3, 2011) (describing government's use of designated "facilities" and "selectors" with links to terrorism or other foreign intelligence information, including not only communications to or from phone numbers or e-mail addresses, but also communications "about" these identifiers).

40. 50 U.S.C. § 1881a (2012).

41. SCHNEIER, *supra* note 2, at 49 (noting that "[s]urveillance is the business model of the Internet"); *see also* Ferguson, *supra* note 6, at 358–59 (discussing the commercial rationale for corporate data mining).

individuals' emails.[42] Private firms engage in such scanning for two key reasons. First, firms refine their knowledge of users' aggregate browsing practices, which Google then uses to make its searches and search rankings more precise.[43] Second, Google and other firms gather information about particular users, which firms use to tailor web-based advertising to that user's habits and interests.[44]

The U.S. government uses scanning internationally but not domestically. Both the Constitution and various statutes preclude the government from scanning the content of purely domestic communications—communications between two individuals located within the United States.[45] However, under FISA, the U.S. government scans devices such as buffers and caches used in international communications—communications between a person in the United States and a person that government officials reasonably believe to be located overseas.[46] Under Section 702 of the FISA Amendments Act of

---

42. *See* Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, GUARDIAN (Apr. 15, 2014, 8:24 AM), http://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarif; Steven Levy, *Exclusive: How Google's Algorithm Rules the Web*, WIRED (Feb. 22, 2010, 12:00 PM), http://www.wired.com/2010/02/ff_google_algorithm/. Private sector scanning is premised on either express or implicit consent by internet users. *See In re* Yahoo Mail Litig., 308 F.R.D. 577, 584–85 (N.D. Cal. 2015); *cf.* BENJAMIN WITTES & GABRIELA BLUM, THE FUTURE OF VIOLENCE 135 (2015) (arguing that users' web data "tends to be material we have disclosed to others, often in exchange for some benefit and often with the understanding . . . that it will be aggregated and mined for what it might say about us").

43. *See* Levy, *supra* note 42.

44. *See* Gibbs, *supra* note 42.

45. *See* Riley v. California, 134 S. Ct. 2473, 2490, 2494–95 (2014) (in holding that a digital search of a suspect's cell phone is not a search incident to arrest and therefore requires a warrant, the Court described the cell phone as a "cache of sensitive personal information"); *cf.* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 291–92 (2015) (discussing case law on the effect of borders on Fourth Amendment rights). *But see* Jennifer Daskal, *The Un-territoriality of Data*, 125 YALE L.J. 326, 364–66 (2015) (arguing that national borders are an artificial and outmoded basis for determining Fourth Amendment limits on data searches). Government scanning of *domestic* communications content for data mining on terrorism would be problematic on legal, ethical, and policy grounds. *Cf.* James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1466–67 (2004) (warning of the adverse privacy consequences of government data mining of domestic records for pattern-based searches).

46. PPD-28 Supplemental Procedures, *supra* note 27, at 7 n.2 (permitting temporary acquisition of data "to facilitate targeted collection, such as search and development activities . . . or the processing of a signal that is necessary to select specific communications for forwarding for intelligence analysis"). Some have argued that intelligence agency access to international data outside the purview of bilateral Mutual Legal Assistance Treaties (MLATs) is problematic. This Article focuses on human rights issues, and the role of MLATs is beyond its scope. It is worth noting that the ECHR has held that transnational surveillance of another country's nationals does not violate the sovereignty of that country because no physical intrusion occurs. *See* Weber v. Germany, 2006-XI Eur. Ct. H.R. para. 81; Joris V.J. van Hoboken & Ira S.

2008, which Congress enacted with votes from liberal legislators, including then-Senator Barack Obama, the United States can gain access to such communications.[47] However, Section 702 and policies implementing the statute impose limits on the government's collection of such data.[48] Describing those limits requires unpacking the distinction between targeted and bulk collection.

2. Targeted and Bulk Collection

Targeted collection entails the use of particularized identifiers or selectors to winnow out irrelevant scanned data. Under Section 702, U.S. intelligence agencies can *store* the content of calls between persons in the United States and those reasonably believed to be located outside the country only if scans have revealed that such communications include specific selectors, such as phone numbers, email addresses, and discrete topics related to national security or foreign affairs.[49] The FISC approves procedures under Section 702, although it does not approve specific selectors in advance.[50]

Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 ME. L. REV. 487, 490 (2014). A country's consent to another state's surveillance would address concerns about sovereignty but would not trump human rights. *See Weber*, 2006-XI Eur. Ct. H.R. at para. 25.

47. *See* 50 U.S.C. § 1881a(a) (2012); *see also* David R. Shedd, Paul Rosenzweig & Charles D. Stimson, *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, HERITAGE FOUND. (May 13, 2016), http://www.heritage.org/research/reports/2016/05/maintaining-americas-ability-to-collect-foreign-intelligence-the-section-702-program (noting § 702's effectiveness at producing foreign intelligence); Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings* (Hoover Inst. Series Paper No. 1604, 2016), https://www.lawfareblog.com/defense-faa-section-702-examination-its-justification-operational-employment-and-legal-underpinnings (same).

48. *See* 50 U.S.C. § 1881a(b).

49. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 32–33 (2014), https://www.pclob.gov/library/702-Report.pdf; *cf.* PPD-28 Supplemental Procedures, *supra* note 27, para. 3.4, at 6 (noting that United States can collect "foreign private commercial information or trade secrets" for limited purposes, such as detecting violations of fair trade laws or sanctions, but not to supply U.S. firms with a competitive advantage).

50. 50 U.S.C. § 1881a(g)–(i) (noting that the Attorney General and the Director of National Intelligence must file certifications under Section 702 with FISC for review). Professor Daphna Renan has helpfully analogized the FISC's role to that of an administrative agency setting parameters for a regulated industry. *See* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1103–08 (2016); *cf.* Zachary K. Goldman, *The Emergence of Intelligence Governance*, in GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 207, 230–32 (Zachary K. Goldman & Samuel J. Rascoff eds. 2016) (discussing role of courts in framing incentives for executive action and forcing greater transparency); Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633 (2016) (discussing role of the President in coordinating principled and collaborative approach to

In contrast, bulk collection involves the collection of a mass of data, which analysts subsequently query using selectors or other methods.[51] In bulk collection, much of the data collected is by definition substantively irrelevant. Suppose that the government wishes to sort through the content of communications in a foreign state to uncover individuals' efforts to join ISIS, Al Qaeda, or the Taliban. Despite ISIS's popularity in some quarters, in any state only a tiny minority of communications will concern ISIS recruiting—most will deal with countless other more mundane issues, from personal, family, and business matters to entertainment, recreation, and so on.[52] However, collecting these substantively irrelevant communications is nonetheless relevant methodologically to a state's efforts to protect its nationals or those of other countries from ISIS.[53] Bulk collection ensures that the government has a database that is comprehensive when it searches for specific content about ISIS recruiting. While scanning is evanescent because information is not stored, collection gives the government access to communications over time. That enables the government to search more effectively for evolving patterns in ISIS's communications. For example, if ISIS uses different forms of encryption or code to hide its communications, collecting information in bulk will allow the government to trace the evolution of ISIS's tradecraft. In contrast, relying on scanning or targeted collection fails to reckon with ISIS's ability to transform its tactics.

---

intelligence oversight); Carrie Cordero, *A Response to Professor Samuel Rascoff's* Presidential Intelligence, 129 HARV. L. REV. F. 104 (2016) (observing that the importance of speed and secrecy in collecting intelligence to serve national interests will pose challenges for any comprehensive regulatory scheme, and that position of Director of National Intelligence provides requisite professionalism in intelligence collection together with insulation from politics).

51. PPD-28 Supplemental Procedures, *supra* note 27, at 7 n.1 (defining bulk collection); *see also* David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y 209, 217–18 (2014) (discussing the bulk collection of domestic call record data and use of identifiers to query such data under the USA Patriot Act prior to the effective date of the 2015 USA Freedom Act that reformed this program in the wake of Edward Snowden's revelations).

52. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 78 (observing that "terrorists and terrorist activity are rare" and "[d]ata specifically associated with terrorists . . . are sparse"); Dempsey & Flint, *supra* note 45, at 1470 (noting that agencies searching for patterns linked to terrorists "have a very small sample set on which to base their predictions").

53. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things, B.R. No. 15-75, 2015 WL 5637562, at *7 (FISC June 29, 2015) (holding that the collection of metadata under the pre-USA Freedom Act provision of the USA Patriot Act was "designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities"); Kris, *supra* note 51, at 235 (discussing FISC's conception of relevance under pre-USA Freedom Act statutory provision, Section 215 of USA Patriot Act, which has now been amended to bar government collection of metadata and require the government to seek a court order to obtain call records from telecommunications firms). *But see* ACLU v. Clapper, 785 F.3d 787, 815–16 (2d Cir. 2015) (holding that Section 215 defined information that was "relevant" to an investigation in a narrower manner that did not authorize government collection of metadata).

The United States has used bulk collection in two principal contexts. First, before the USA Freedom Act became fully effective, the government, with authorization from the FISC, collected most domestic land-line call records (metadata, as opposed to content) detailing both phone numbers called by persons in the United States and the duration of the calls.[54] After government officials brought overreaching to the attention of the FISC in 2009, intelligence analysts restricted queries to specific identifiers, such as phone numbers, that triggered a reasonable and articulable suspicion (RAS) of links to terrorism.[55]

Second, even more importantly for this Article's present discussion, Executive Order 12,333 (EO 12,333), enacted during the Reagan Administration, empowers the President, acting pursuant to a presidential finding, to order surveillance abroad.[56] While the Executive Branch has

54. Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 13 (2014); *see also* Kris, *supra* note 51, at 235 (noting the government's argument that "the telephony metadata must be available in bulk to allow NSA to identify the records of terrorist communications because without access to the larger haystack of data, it cannot find the needles using the much narrower querying process"). Relying on the third-party doctrine, the Supreme Court has held that government access to metadata, as opposed to content, does not pose a Fourth Amendment problem. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979). That doctrine holds that individuals who voluntarily make information available to third parties, such as phone companies that need metadata to complete calls, have no reasonable expectation of privacy in such data. *Id.* at 743–44. *But see* SLOBOGIN, *supra* note 2, at 156–58 (criticizing the third-party doctrine); Jonathan Mayer, Patrick Mutchler & John C. Mitchell, *Evaluating the privacy properties of telephone metadata*, 113(20) PROCEEDINGS NAT'L ACAD. SCI. 5536 (May 17, 2016) (using digital research and probabilistic analysis to demonstrate that collection of metadata can have serious privacy consequences); *cf.* Robert S. Litt, *The Fourth Amendment in the Digital Age*, 126 YALE L.J. F. 8, 13–16 (2016) (suggesting that courts should replace both third-party doctrine and "reasonable expectation of privacy" test articulated in Katz v. United States, 389 U.S. 347 (1967), with inquiry focusing on how government handles data and the data's intended use).

55. Margulies, *supra* note 54, at 45–46; *cf.* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 104–05 (2016) (criticizing the program's intrusiveness); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 897–900 (2014) (criticizing the statutory and constitutional predicate for the program); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1757–58 (2014) (suggesting that Congress's authorization for the program may have been adequate under the applicable statute but arguing that courts should revive delegation theory to curb executive discretion over the program's nature and scope).

56. Exec. Order No. 12,333, 46 Fed. Reg. 59,941–43 (Dec. 4, 1981). EO 12,333 mirrors provisions of the National Security Act that authorize covert action abroad based on a presidential finding. *See* 50 U.S.C. § 3093 (2012); Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARV. NAT'L SECURITY J. 629, 640–41 (2011); *cf.* Amos Toh, Faiza Patel & Elizabeth Goitein, *Overseas Surveillance in an Interconnected World*, BRENNAN CTR. FOR JUSTICE (Mar. 16, 2016), https://www.brennancenter.org/publication/overseas-surveillance-interconnected-world (expressing concern about intrusiveness of collection under EO

historically been reticent about operations conducted under EO 12,333, the unprecedented openness ushered in by President Obama's post-Snowden January 2014 speech and the issuance of Presidential Policy Directive 28 (PPD-28)[57] support the inference that the government engages in bulk collection of information abroad under an unspecified authority *not* linked to FISA, which after all permits only targeted collection. The most plausible inference from PPD-28 is that the authority for bulk collection abroad stems from EO 12,333.[58]

Since the government defines "bulk" collection as the acquisition of data without the aid of "specific" selectors,[59] it is reasonable to assume that bulk collection efforts overseas will have varying geographic and temporal parameters. For example, bulk collection might include using StingRay or comparable technology[60] to collect all telephonic signals within a neighborhood near a U.S. embassy abroad for twenty-four hours because of otherwise unspecified reports of an imminent terrorist attack. At the other pole of collection efforts, reports indicate that the United States has collected in bulk the content of *all* telephonic traffic in Afghanistan, where the United States today is still engaged in an armed conflict with Al Qaeda and the Taliban. To combat drug and human trafficking, U.S. government agencies also apparently collect the contents of mobile phone traffic in the Bahamas.[61] In PPD-28, President Obama barred collection for particular purposes, such as suppressing speech critical of the United States, discriminating against racial, religious, or ethnic groups, or gaining a competitive advantage for U.S. companies.[62]

12,333). *See generally* Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SECURITY L. & POL'Y 539, 543 (2012) (providing background on the statutory authority for covert action).

57. *See* PPD-28, *supra* note 27, at sec. 2.

58. *See* PPD-28 Supplemental Procedures, *supra* note 27, at 7 n.1 (defining bulk collection as the collection of "large quantities of SIGINT [signals intelligence] data that, because of technical or operational considerations, is acquired without the use . . . of specific identifiers or selection terms").

59. *Id.*

60. *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 14–15, 34, 55–56 (2014) (describing StingRay as a portable device that gathers mobile phone signals within a relatively narrow area).

61. *See* Jacob Kastrenakes, *The NSA Is Capturing Nearly Every Phone Call in Afghanistan, WikiLeaks Claims*, VERGE (May 23, 2014, 9:41 AM), http://www.theverge.com/2014/5/23/5744616/nsa-capturing-nearly-all-afghanistan-phone-calls; Devereaux et al., *supra* note 11.

62. *See* PPD-28 Supplemental Procedures, *supra* note 27, at 5–6.

B. *Breaking Down Machine Searches*

Having established that states can collect data in a targeted or "bulk" fashion, this Article next considers how intelligence analysts search through data. Searches can be either directed or autonomous. A directed search sorts through data using keywords or other discrete pieces of data, such as phone numbers, email addresses, URLs, or Internet Protocol addresses.[63] Analysts choose the "selectors" or "identifiers" used, and the machine then dutifully searches the data available.[64] Autonomous searches are different. This Article uses the term autonomous to connote searches in which machines do not merely execute searches formulated by humans but instead engage in calculations that closely resemble human reasoning.[65] Commercial firms engage in autonomous searches under the broad rubric of "data mining."[66] While there is no evidence that the government has engaged in data mining of domestically collected metadata,[67] there are reasonable bases to infer that states, including the United States, use autonomous data mining techniques on transnational communications.[68]

To see how autonomous learning works, consider a setting familiar to most lawyers: discovery.[69] Suppose that plaintiffs had sued manufacturers of air bags used in cars, claiming that the air bags deployed

---

63. *See* Kris, *supra* note 51, at 216.

64. *See id.* at 216–18.

65. The term autonomous has been used to describe technological advances such as self-driving cars and computerized weapons systems that can operate independently of humans. *See* George R. Lucas, Jr., *Automated Warfare*, 25 STAN. L. & POL'Y REV. 317, 324 (2014). This Article adapts the term to the context of searches.

66. Danielle K. Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 5, 26 (2014); *see also* SCHNEIER, *supra* note 2, at 43 (listing AOL and Netflix as examples of commercial firms that engage in autonomous searches).

67. Querying domestic metadata without RAS-approved identifiers would violate FISC orders that govern domestic bulk collection. *See* Margulies, *supra* note 54, at 12–14.

68. *See, e.g.*, Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 447 (2008); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 262–63 (2008); see Bignami, *supra* note 21, at 633–34.

69. The case law on using autonomous searches to comply with electronic discovery obligations is growing rapidly. *See, e.g.*, Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 261–62 (D. Md. 2008); William A. Gross Constr. Assocs. v. Am. Mfrs. Mut. Ins. Co., 256 F.R.D. 134, 136 (S.D.N.Y. 2009); Nat'l Day Laborer Org. Network v. Immigration & Customs Enf't Agency, 877 F. Supp. 2d 87, 109–10 (S.D.N.Y. 2012); Moore v. Publicis Groupe, 287 F.R.D. 182, 186–87 (S.D.N.Y. 2012); Jason R. Baron, *Law in the Age of Exabytes: Some Further Thoughts on 'Information Inflation' and Current Issues in E-Discovery Search*, RICH. J.L. & TECH., Spring 2011, paras. 18, 20–21; *cf.* John Didday, *Informed Buyers of E-Discovery: Why General Counsel Must Become Tech Savvy*, 5 HASTINGS SCI. & TECH. L.J. 281, 306–07 (2013) (discussing the promise of advanced machine learning in e-discovery).

unpredictably, causing substantial injuries to passengers. Manufacturers had millions of documents on air bags, but only a relatively small number of documents were actually relevant to the plaintiffs' claims. Inspection by human beings would be time-consuming and inefficient given the number of documents. A directed search using keywords would generate large numbers of errors. For example, a keyword search could generate an unmanageable number of false positives—documents that the search flagged as relevant, even though the documents were useless.[70] Searching for a phrase such as "air bag" might yield thousands of documents dealing with the different consumer warranties applicable to the vehicle or labor relations in the factory that produced the item. By the same token, a keyword search could produce many false negatives—omitting documents because they did not fit the criteria humans had chosen, even though those documents were in fact highly relevant.[71] For example, because of fear about litigation or regulatory action, the manufacturer's employees might have coyly discussed air bag issues as "our problem" or "the question on the table." Keyword searches are not effective at ferreting out code, vague terms with specific connotations, or other evasive or deceptive stratagems.[72]

---

70. *See* Gregory L. Fordham, *Using Keyword Search Terms in E-Discovery and How They Relate to Issues of Responsiveness, Privilege, Evidence Standards and Rube Goldberg*, RICH. J.L. & TECH., Spring 2009, para. 10.

71. *See* Fordham, *supra* note 70, at para. 10; *Nat'l Day Laborer Org. Network*, 877 F. Supp. 2d at 110.

72. Fourth Amendment cases on protocols for digital searches of laptops pursuant to lawfully obtained warrants are instructive on the deception that criminals use to hide their handiwork. *See, e.g.*, United States v. Stabile, 633 F.3d 219, 238–39 (3d Cir. 2011) (suggesting that law enforcement officials conducting digital searches pursuant to warrants need broad latitude to address deceptive tactics used by criminals in labeling and storing files); United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010) (observing that "[u]nlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents"); United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (declining to take a rigid approach to search protocols used to investigate a laptop covered by a warrant, pertaining to deceptive labeling of computer files); Wolf v. State, 266 P.3d 1169, 1173–75 (Idaho Ct. App. 2011) (allowing an officer broad discretion to search a computer based on an affidavit describing that officer's prior experience in child pornography investigations); *cf.* United States v. Schesso, 730 F.3d 1040, 1050 (9th Cir. 2013) (cautioning that judicial inclusion of detailed search protocols in warrants authorizing laptop searches may unduly constrain law enforcement efforts to unravel criminals' deceptive data practices); Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1123 (2009) (discussing the advantages of narrowly focused search protocols in laptop searches at U.S. border entry points). *But see In re* Appeal of Application for Search Warrant, 71 A.3d 1158, 1182 & n.23 (Vt. 2012) (barring "sophisticated search techniques" beyond keyword searching absent specific evidence that the suspect had tried to hide laptop files); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1255–58 (2010) (arguing that "[t]he search protocol must forbid the use of tools that would discover illegality relating to evidence outside the scope of the warrant"); *see also* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179–80 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) (recommending that judges

Autonomous searches can do a far better job.

An autonomous machine search will typically include four steps: training, testing, application, and validation.[73] In the first step, a programmer will feed the machine data.[74] In our air bag scenario, the programmer will find both relevant data, including data that would not show up on keyword searches, and irrelevant data. Feeding the machine sufficient data trains the machine on the patterns that distinguish relevant from irrelevant items.[75] Programmers design the training process to enable the machine to search not only for documents that match those in the training set, but also for documents with patterns that are parallel or analogous.[76]

In this space of analogous pattern detection, the machine exhibits a human capacity to draw inferences and craft analogies, along with the capacity to absorb and analyze vast amounts of data that far exceeds human abilities.[77] To ascertain whether the machine has been properly trained, the programmer will test the machine on another data set.[78] If the machine can properly generalize lessons from the training set and apply them to the data set, it passes the test.[79] The machine is then put into operation. In the air bag scenario, the computer would analyze the vast trove of documents available to find patterns that matched those in the training set. Programmers would then validate the machine's performance,[80] perhaps by comparing the machine's outputs to the results of a sample of documents inspected by humans. If error levels were adequate, the machine would be used again.[81] If error levels were too high, programmers would either scrap the machine search or refine it.[82]

Autonomous searches can be either supervised or unsupervised.[83] The search described in the air bag scenario is a supervised search, in which programmers have certain objectives in mind and devise training and test sets to meet those objectives.[84] In unsupervised searches, a machine

include specific methodological criteria in warrants for laptop searches).

73. STÉPHANE TUFFÉRY, DATA MINING AND STATISTICS FOR DECISION MAKING 304 (2011).

74. *See id.*

75. *See id.* at 305–08; Steven M. Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 N.Y.U. J.L. & LIBERTY 556, 590–91 (2013).

76. *See* Bellovin et al., *supra* note 75, at 591.

77. *See id.* at 590–91.

78. *See* Lina Zhou et al., *A Comparison of Classification Methods for Predicting Deception in Computer-Mediated Communication*, 20 J. MGMT. INFO. SYS. 139, 152 (2004).

79. *See* TUFFÉRY, *supra* note 73, at 542.

80. *See* PETER FLACH, MACHINE LEARNING 19 (2012); RUSSEL & NORVIG, *supra* note 17, at 735; Bellovin et al., *supra* note 75, at 590–91 (2014).

81. *See* TUFFÉRY, *supra* note 73, at 542.

82. *See id.*

83. *See* Bellovin, *supra* note 75, at 591.

84. *See* RUSSELL & NORVIG, *supra* note 17, at 695.

might be given a massive amount of data, such as data from internet users' search histories, and tasked to find patterns that linked individual users.[85]

C. *The Search Deepens: Primary Machine Search Strategies*

Understanding autonomous searches and how they might work in national security intelligence collection requires more detail on the types of searches that machines can perform. These include decision trees, neural networks, and support vector machines. This Section briefly discusses each in turn.

1. To Tree or Not to Tree: Decision Trees and Machine Learning

Decision trees are useful in making predictions and ascertaining causation. In preparing a decision tree, a machine analyzes the factors behind certain decisions or outcomes.[86] A leaf in a decision tree represents a causal factor and identifies how examples with and without that attribute fared in achieving a particular outcome.[87] A decision tree will deliver an output that is consistent with the rule of Ockham's Razor: an explanation that is as simple as possible, given the data, with leaves pruned away if they were unnecessary for prediction.[88] For example, a decision tree analyzing the Titanic shipwreck of 1912, in which almost 1500 people died, would establish that out of the countless variables possessed by the passengers, gender and ticket class were the most significant determinants of survival.[89] A decision tree modeling web-surfers' choices for reading online posts might suggest that visitors are more likely to read a post when the author is known, the thread is new, and the post is short.[90] Decision trees that search for relevant documents in a large document database would consider the presence of certain words and word combinations.[91] For example, a decision tree that identified documents on sophisticated financial transactions would look for the word "swap" and then determine if the document flagged also

85. *See* FLACH, *supra* note 80, at 47.

86. *See* RUSSELL & NORVIG, *supra* note 17, at 698.

87. *Id.*

88. *Id.* at 696.

89. *See* TUFFÉRY, *supra* note 73, at 315–16. Gender was relevant because the Titanic's captain ordered that women and children move first to the lifeboats on board. *Titanic: 'Iceberg Right Ahead,'* ULTIMATE TITANIC, http://www.ultimatetitanic.com/the-sinking/ (last visited Nov. 18, 2016). Ticket class was relevant because first class passengers had quarters closest to the ship's main deck, where lifeboats were located. *Id.*

90. *See 7.3.1 Learning Decision Trees*, ARTIFICIAL INTELLIGENCE: FOUND. OF COMPUTATIONAL AGENTS, http://artint.info/html/ArtInt_177.html (last visited Mar. 23, 2016).

91. *See* Maura R. Grossman & Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review*, 7 FED. CTS. L. REV. 1, 13–14 (2013).

contained the word "credit," suggesting that the document discussed "credit-default swaps," one kind of complex transaction.[92]

A decision tree could also model what types of individuals abroad are most likely to become ISIS recruits.[93] Some of the variables would be relatively obvious: the model would predict that recruits were more likely to be young, male, and Muslim. However, these factors do not hold true for all ISIS recruits[94] or adequately separate that cohort from the far larger population of non-ISIS recruits. To find ISIS recruits, a decision tree might rely on other factors, such as employment history (to detect the disaffected or alienated), information from facial recognition software regarding attendance at events sponsored by radical clerics, search history data showing visits to violent extremist sites, and social media posts, texts, emails, or phone calls with known ISIS recruits.[95]

2. Machines and the Transparency Paradox: The Hidden Life of Neural Networks

Artificial neural networks are more useful than decision trees in performing certain search or identification tasks. However, technological improvements are not a free lunch. The autonomous steps called "hidden layers" that enhance these searches' utility come at transparency's expense.

a. Artificial Neural Networks: Mimicking the Brain

Artificial neural networks are useful for discerning patterns between individuals, groups, and objects or behaviors.[96] Neural networks are software applications that mimic the functioning of the human brain.[97] The human brain works through neurons, which are the fundamental functional unit of the nervous system.[98] Fibers called dendrites branch out

92. *See id.*

93. Professor Stuart J. Russell and Peter Norvig, Google's Director of Research, model a more everyday, lower-stakes decision: whether to wait for a table at a crowded restaurant. RUSSELL & NORVIG, *supra* note 17, at 698 (discussing the importance of common-sense factors such as alternative restaurants, price, hunger, and estimated wait). The authors use this example because of its familiarity. Their broader point, however, is that decision trees can also be a useful strategy for more complex decisions. *See id.*

94. *See* Katrin Bennhold, *Religion Meets Rebellion: How ISIS Lured 3 Friends*, N.Y. TIMES, Aug. 18, 2015, at A1 (describing ISIS's recruitment of three teenage girls in Britain).

95. A directed search using identifiers could pinpoint contacts of known ISIS operatives; programmers could then integrate these outputs with an autonomous search looking for fresh patterns.

96. Michael Aikenhead, *The Uses and Abuses of Neural Networks in Law*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 31, 35–36 (1996).

97. *Id.* at 32; *see* RUSSELL & NORVIG, *supra* note 17, at 728.

98. *See* Aikenhead, *supra* note 96, at 34–35.

from each neuron to others, as does a long fiber called the axon.[99] The interchange between neurons is called a synapse.[100] As in the human brain, neurons in an artificial network are interconnected but distinct, enabling the neurons to break down complex problems into more manageable component parts.[101]

In the human brain, all neurons fire at the same time—all neurons in the human brain simultaneously send signals.[102] Some signals might transmit visual or auditory cues, while others may transmit bits of context and memory.[103] This simultaneous firing allows the human brain to readily perform certain tasks, such as distinguishing between two small, red, round, and organic objects, one of which is an apple and the other a tomato. In contrast, even complex software that seeks to mimic the human brain will generally not allow all artificial neurons in a network to fire at once. For that reason, using neural networks for visual pattern recognition is a sophisticated task, albeit one which has seen remarkable progress.

i. Training Neural Networks

Neural networks use inductive learning algorithms that allow a machine to draw inferences based on massive amounts of data.[104] One builds a neural network by deciding how many nodes or units are required for a task, how to connect those nodes, and how to initialize the synaptic "weights" that comprise a neural network's primary means of long-term storage.[105] As with any form of machine learning, neural networks are first trained with examples that the network digests with the aid of a learning algorithm.[106] Certain types of neural networks can then generate outputs that find patterns between a new stimulus and data in the training set.[107] For example, suppose the training set for the neural network consists of photos of suspected terrorists. Suppose further that the network receives a new stimulus in the form of a small piece of one photo from the training set. The network will readily reproduce the entire photo, including that small piece.[108]

---

99. *Id.*

100. *See id.*

101. WITTEN ET AL., *supra* note 1, at 232–33.

102. *Neurons and Their Jobs*, NAT'L INST. ON AGING, https://www.nia.nih.gov/alzheimers/publication/part-1-basics-healthy-brain/neurons-and-their-jobs (last updated Jan. 22, 2015).

103. *Id.*

104. *See* Aikenhead, *supra* note 96, at 34.

105. *See* WITTEN ET AL., *supra* note 1, at 235; Aikenhead, *supra* note 96, at 35.

106. *See* Aikenhead, *supra* note 96, at 35.

107. *See id.* at 35–36, 36 n.11.

108. *See, e.g.*, *Human Face Recognition Found in Neural Networks Based on Monkey Brains*, MIT TECH. REV. (Feb. 13, 2015), http://www.technologyreview.com/view/535176/human-face-recognition-found-in-neural-network-based-on-monkey-brains/ (explaining how

Neural networks connect inputs and outputs through hidden layers.[109] Software engineers use multiple hidden layers because breaking down the sorting of data into multiple steps allows greater precision than one-step sorting. Each layer performs a function that sorts out data from the previous step.[110]

Consider how a neural network performs facial recognition—detecting faces in a massive number of video images.[111] Facial recognition software breaks up that task, first searching for facial features, such as eyes and noses. To detect eyes, software engineers will use at least three hidden layers, each trained with image data.[112] The first layer will search for short edges in an image.[113] Eyes have short edges compared to larger inanimate or inorganic objects, such as buildings or trucks. However, another layer is necessary to categorize the particular

---

scientists have created a neural network based on a monkey's brain that is able to recognize faces and then match the face to an identity).

109. Zhou et al., *supra* note 78, at 149–50.

110. *See* RUSSELL & NORVIG, *supra* note 17, at 729. Hidden layers are also a feature of another machine learning technique, support vector machines (SVMs). *See* WITTEN, ET AL., *supra* note 1, at 191–92. One virtue of SVMs is that they deal effectively with data that has many variables, and therefore many "dimensions" that an SVM can plot in space, using hyperplanes that cleanly separate disparate groups. *Id.* at 223–25. Linear modes of data analysis such as graphs can only plot two variables at a time, including the intersection of mass and acceleration to compute force or age and education to help predict an individual's likelihood of voting. *Id.* In contrast, the hyperplanes derived by SVMs can separate groups along twenty or more variables. *Id.* Using hidden layers, SVMs discern relationships between variables that humans would miss. To illustrate how an SVM could aid in counterterrorism, consider the identification of ISIS recruits through the relationship of a large number of variables, each of which alone might be useless. For example, ISIS recruits might cite particular commentaries or interpretations of sacred texts as authorizing violence. In addition, ISIS recruits might refer to such religious commentaries or to operational and logistical details using code. A directed search would find only codes already known to government officials. In contrast, a SVM could also find uses of language that were analogous to known codes in syntax, frequency of word choice, and similar factors. The SVM might detect new codes by grouping the incidence of certain word choices with other individual behaviors, such as frequent visiting of chat rooms advocating violent extremism, use of specific kinds of encryption, or patronage of stores selling burner phones. In this fashion, ISIS recruits that would escape detection by humans, directed searches, or other autonomous searches would "pop" in SVM outputs.

111. *See, e.g.*, *Human Face Recognition Found in Neural Network Based on Monkey Brains*, *supra* note 108. Use of facial recognition technology in either the domestic or transnational context requires safeguards; for example, no state should use such technology to identify or target political opponents. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 545–48 (2012).

112. *See, e.g.*, *Human Face Recognition Found in Neural Network Based on Monkey Brains*, *supra* note 108.

113. *Id.*

short edge detected in the first layer.[114] Depending on the perspective in an image, a short edge could be part of an eye or part of a large inanimate object, such as a truck, building, or rock formation, whose image had short edges because it happened to be far away from the camera. This second layer distinguishes between short edges that fit together in the distinctive oval pattern typical of eyes and images in a more straight-edged pattern that might indicate the presence of a distant inanimate object.[115] This layer is "hidden" because software engineers do not impose specific quantitative parameters on the machine in this layer. Instead, they feed the machine enough images to train the computer to recognize distinctions between eyes and inanimate objects.[116] A third layer could search for a particular kind of face or even the face of an individual.[117]

ii. Neural Networks and the Transparency Paradox

Hidden layers create a trade-off in machine learning. Given sufficient data to sort through, hidden layers that rely on autonomous learning can be extraordinarily accurate, yielding more true positives and fewer false positives than directed searches.[118] For example, a neural network with hidden layers and a robotic arm can, given enough tries, learn to pick up a ball as it generalizes from information that is available about the weight and size of the ball and other factors.[119] This task is elementary to humans but actually involves a significant number of discrete steps. Combining the ability to learn with the ability to absorb huge amounts of data, a

---

114. *See id.*

115. *See id.*

116. *See* Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* 17–18 (Lancaster Univ. Mgmt. Sch., Working Paper No. 2010/030, 2010), http://eprints.lancs.ac.uk/49012/1/Document.pdf. Another layer might perform a similar operation to detect composed edges typical of the human nose. A further layer would combine this search with the search for eyes. Similar image data can also train machines to recognize other elements of human anatomy, such as arms and legs.

117. My goal here is to concisely explain how hidden layers work, not to explore the latest developments in the fluid field of facial recognition, including the detection of individual faces. For a discussion of recent developments, see Introna & Nissenbaum, *supra* note 116, at 16–18; Kirill Levashov, Note, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 167–70 (2013).

118. The benefit of hidden layers is the networks' greater capacity to learn autonomously, compared with other machines such as decision trees. A machine that learns autonomously with a large amount of data will typically outperform a machine with less data, even when the second machine has been programmed with a workable algorithm. *See* RUSSELL & NORVIG, *supra* note 17, at 756–57.

119. Dana S. Rao, Note, *Neural Networks: Here, There, and Everywhere—An Examination of Available Intellectual Property Protection for Neural Networks in Europe and the United States*, 30 GEO. WASH. J. INT'L L. & ECON. 509, 512–13 (1996–1997).

neural network can also autonomously discern patterns in photographs, voice recordings, or other types of data[120] with a level of efficiency that no human could possibly match. However, the superior accuracy of such autonomous layers comes at the cost of humans' ability to substantively explain the inferential reasoning that occurs in each layer.[121] Since the hidden layer's search is autonomous, not directed, the human analyst cannot cite specific parameters that the analyst programs into the machine.[122] As noted, the analyst refrains from imposing such parameters because they would yield results that are less accurate.[123]

In the absence of a substantive explanation, the analyst can only offer a methodological explanation: the network's hidden layers have searched for patterns that distinguish most accurately between human eyes and other image components.[124] An analyst can also describe how she has validated the autonomous machine search's results.[125] The law governing searches must decide if machine learning's validated accuracy, accompanied by a methodological explanation, outweighs the lack of a specific, articulable substantive explanation.

The contrast between substantive and methodological explanations of machine searches becomes most salient in searches designed to predict human conduct, including criminality or terrorism. To satisfy U.S. statutory or constitutional requirements, a government official would

120. *See* Dave Gershgorn, *These Are What the Google Artificial Intelligence's Dreams Look Like*, POPULAR SCIENCE (June 19, 2015), http://www.popsci.com/these-are-what-google-artificial-intelligences-dreams-look (explaining Google's approach to teaching an artificial neutral network what a fork is).

121. *See* Zhou et al., *supra* note 78, at 150–51; Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 906 (2016).

122. *See* Zhou et al., *supra* note 78, at 150–51 (explaining that because of hidden layers' role in connecting inputs and outputs, which gives neural networks a "highly nonlinear structure," there is no definitive way "to easily interpret the relative strength of each input to each output in the network"). This confluence of accuracy and difficulty in substantive explanation is not confined to machines. It extends to other nonhuman search aids. For example, drug-sniffing dogs are often extraordinarily accurate in detecting traces of contraband. Humans, whose sense of smell is laughably crude by comparison, lack any detailed substantive or scientific explanation of the physiology behind dogs' uncanny olfactory accuracy. *See* Rich, *supra* note 121, at 911–12. A warrant application or a legal justification of a warrantless search based on a drug-sniffing dog's reaction will not try to quantitatively classify a smell as so many parts per million. Instead, the legal justification will be methodological in nature. The justification will describe the dog's reaction, on the theory that the canine reaction alone is sufficient demonstration of the presence of drugs. A methodological explanation is sufficient based on validated scientific techniques that using dogs works.

123. *See* Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1519–20 (noting that in many cases using only techniques that would permit a substantive, verbal explanation of the machine's calculations would reduce the accuracy of the search).

124. *See id.*

125. *See id.* at 1520.

generally need to present substantive reasons in favor of a warrant.[126] Authorization for a search would depend on probable cause or a reasonable suspicion that the subject of a search had committed or was in the process of conspiring to commit a specific criminal act.[127] For example, the government might seek to show that an individual was conspiring to provide material support, including money, arms, or more intangible assistance, to ISIS or another foreign terrorist group.[128] The warrant application would include specific substantive information bolstering this conclusion, such as a conversation between the subject and a government informant.

In contrast, an autonomous machine search for ISIS recruits would typically not yield such a substantive justification. Instead, an autonomous search—even one of publicly available databases not protected by the Fourth Amendment—would find patterns that might include an individual's opinions, associations, and types of behavior. Given enough data, an autonomous search could infer a reasonable risk that a given individual was an ISIS recruit based on myriad patterns that might include expressions of political opinion in chat rooms, a recent report of a lost passport (indicating an attempt to conceal a visit to a terrorist training camp in Afghanistan or Pakistan), attempts to use or deploy a common encryption technique, and patronage (picked up through public video surveillance and facial recognition software) of a store specializing in pre-paid cell phones.[129] This convergence of variables might be predictive of terrorist activity but would likely not in itself be sufficient to satisfy the U.S. Constitution's probable cause standard.[130]

126. United States v. U.S. District Court, 407 U.S. 297, 320 (1972).

127. *Cf.* United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010) (requiring showing of probable cause to obtain the contents of emails); United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015) (en banc) (holding that locational data was available upon individualized statutory showing, requiring "specific and articulable facts showing reasonable grounds to believe the records [or other information sought] are relevant and material to an ongoing criminal investigation," while noting that this statutory showing was less rigorous than probable cause).

128. *See* 18 U.S.C. § 2339B (2012); *see also* Holder v. Humanitarian Law Project, 561 U.S. 1, 8 (2010) (upholding the constitutionality of material support statute against vagueness and First Amendment challenges); Peter Margulies, *Advising Terrorism: Material Support, Safe Harbors, and Freedom of Speech*, 63 HASTINGS L.J. 455, 486–93 (2012) (defending the *Humanitarian Law Project*'s decision that upheld limits on active relationships with foreign terrorist groups, based in part on the difficulty of gaining information about such groups' activities abroad).

129. Let us suppose that either the machine or a human analyst assessing search results would also apply a test for false positives, such as information that a particular individual flagged by the search was a lawyer, journalist, academic, or human rights researcher.

130. *See* Illinois v. Gates, 462 U.S. 213, 238–39 (1983) (holding that probable cause is a fair probability that contraband or evidence of a crime will be found in a particular place).

Moreover, in an unsupervised learning mode, the machine would use hidden layers to analyze multiple variables.[131] Because of the number of variables that the hidden layers crunched, an analyst would not be able to retrieve a substantive, verbal explanation of how those variables interacted to generate a particular result. Indeed, assuming enough inputted data, the machine's search would be valuable precisely to the extent that it detected patterns that would have eluded a human analyst. Even then, however, a definitive conclusion about a positive result from a particular machine search would benefit from follow-up investigation by counterterrorism officials.[132] Moreover, for every "true positive"—a bona fide ISIS recruit—identified through such follow-up, several false positives might emerge: individuals flagged by the machine search who were in fact not ISIS recruits.

In this scenario, a paradox emerges. Let us take the best-case scenario in which a follow-up investigation identifies otherwise undetected ISIS recruits, with a minimal number of false positives. Let us assume that a machine search of this type will yield results that are superior to sole reliance on either human intelligence or a directed search using contacts of known terrorists. Human access to the search results might still be arbitrary under international human rights law, if one defined a non-arbitrary search as one entailing a substantive verbal explanation of the factors giving rise to the search. After all, as previously noted, the machine search's hidden layers would preclude just such a substantive verbal explanation. However, finding human access to such search results to be arbitrary would create an anomaly: *less* accurate results, such as those based on the assertions of an informant with an axe to grind, would comply with human rights norms, while *more* accurate results would not. This Article resolves the transparency paradox in Part V; the goal here is to simply flag the problem.

D. *The Accuracy of Machine Learning as a Counterterrorism Tool*

The discussion above regarding the accuracy of certain machine learning techniques raises an issue that is as hotly debated as any in the study of counterterrorism surveillance law and policy: the accuracy of machine learning in the national security space.[133] Privacy advocates, including those with significant technical expertise, claim that machine learning in this context is ineffective because data is insufficient—the needles are too small and the haystack too large.[134] As this Article shows

131. *See supra* notes 109–17 and accompanying text.

132. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 206.

133. *See, e.g.*, *id.* at 207–09 (highlighting policy makers' decision-making strategies when evaluating the "trade off" between privacy and accuracy in data mining).

134. *See, e.g.*, SCHNEIER, *supra* note 2, at 136–38 (quoting former NSA Director General

below, however, critics of counterterrorism machine searches sometimes skew the definitions of outputs to reinforce their arguments. Other technologists, however, while acknowledging the difficulties of machine searches in this context, also concede that these searches could have "substantial benefits."[135] If one believes that technology improves exponentially over time, this latter view provides the basis for cautious optimism about the role of national security machine searches.

Any candid analysis of machine learning in counterterrorism must acknowledge a crucial problem: to be effective, machine searches need data to compare and analyze. Terrorism, although a huge problem with devastating consequences, is relatively rare.[136] Terrorists do not need to command the allegiance of the majority of the population to have an impact; if they did, ISIS, which probably has no more than 30,000 armed fighters,[137] would be a paltry force in the Middle East, which is home to more than 200 million people.[138] Since, by any count, terrorists are relatively rare, mobilizing the data to input into machines is a major challenge.[139]

If data is insufficient, machine searches are likely to "overfit" the training data.[140] That is, a machine will simply "memorize" the characteristics of known terrorists, including those that are irrelevant to the subject's terrorist status.[141] When a sample is large, irrelevant characteristics will likely be evenly distributed among true positives and negatives. However, when the sample is small, chance may create a spike in certain irrelevant factors. For example, in a small sample, a disproportionate number of individuals labeled as positives might have a common birthday or might be left-handed. These attributes clearly have no bearing on whether the individual is an ISIS recruit. A machine might "overfit" its training data, however, by treating such irrelevant factors as

---

Keith Alexander arguing that "you need the haystack to find the needle"); *see also* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 13 (noting that a massive amount of data must be analyzed to distinguish between terrorist activities and legitimate ones, and that innocent people's data will be collected, resulting in a privacy issue).

135. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 196.

136. SCHNEIER, *supra* note 2, at 137.

137. *See* Jim Michaels, *New U.S. Intelligence Estimate Sees 20-25K ISIL Fighters*, USA TODAY (Feb. 4, 2016, 5:35 PM), http://www.usatoday.com/story/news/world/2016/02/03/isil-fighters-new-estimate-25000-iraq-syria/79775676/.

138. *See Population: Middle East*, INDEX MUNDI, http://www.indexmundi.com/map/?v=21&r=me&l=en (last visited Mar. 25, 2016).

139. SCHNEIER, *supra* note 2, at 136–38.

140. FLACH, *supra* note 80, at 6; RUSSELL & NORVIG, *supra* note 17, at 709, 736; WITTEN ET AL., *supra* note 1, at 18–19, 29.

141. *Cf.* FLACH, *supra* note 80, at 6 (explaining a phenomenon called overfitting, where a machine will learn all the characteristics of past information but cannot generalize it to new, future information).

part of its working hypothesis for predicting terrorist status. That would make the hypothesis a poor basis for generalizing about the presence of terrorism in a larger population. Programmers can address overfitting, but in the absence of enough data, a machine still lacks the ingredients for an accurate search. For the most ardent critics of surveillance, this problem is insurmountable.[142]

While the surveillance critics raise strong points, particularly on the effect of data on accuracy,[143] their arguments are less persuasive than they might appear. First, machine searches could be very effective at pinpointing confluences of facts that suggest terrorist plots, such as contact between an individual that facial recognition technology showed was taking photographs of New York City landmarks and another individual buying large quantities of explosives.[144] Moreover, the critics stack the deck when they posit that a machine search must uncover imminent attacks to be considered effective.[145] The critics are right that imminent attacks are rare, once one leaves sites of armed conflict such as Afghanistan. However, in a conflict zone, attacks are more frequent. The United States and other states have a legitimate interest in detecting planned attacks in conflict zones.[146] In addition, the thousands of ISIS recruits that have traveled or conspired to travel to the Middle East[147] are a more substantial group than the isolated ring of conspirators that surveillance critics posit. Fortunately, the number of ISIS recruits does not approach the numbers of Amazon customers or Gmail users that private firms mine.[148] However, the cohort of active ISIS recruits may be big enough to provide generalizable data. Indeed, ISIS's reliance on social media[149] may actually make its adherents more like the commercial internet users that private firms mine for purchasing habits. As surveillance critics concede, data mining is good at finding mutual tastes

142. *See, e.g.*, SCHNEIER, *supra* note 2, at 139 (asserting that the problems with data mining for terrorists "cannot be fixed").

143. *Cf.* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 812–16 (2015) (discussing the application of the *Daubert* test on scientific evidence to validate machine searching techniques).

144. *See* PEDRO DOMINGOS, THE MASTER ALGORITHM 232–33 (2015) (noting that machine searches of contacts and records can uncover patterns of criminal activity, even when specific data points seems "innocent enough in isolation").

145. *See, e.g.*, SCHNEIER, *supra* note 2, at 138.

146. *See, e.g.*, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 115.

147. Eric Schmitt & Somini Sengupta, *Thousands Enter Syria to Join ISIS Despite Global Efforts*, N.Y. TIMES (Sept. 26, 2015), http://www.nytimes.com/2015/09/27/world/middleeast/thousands-enter-syria-to-join-isis-despite-global-efforts.html?.

148. *See* Sean Madden, *How Companies Like Amazon Use Big Data to Make You Love Them*, FAST COMPANY (May 2, 2012, 8:30 AM), http://www.fastcodesign.com/1669551/how-companies-like-amazon-use-big-data-to-make-you-love-them; Gibbs, *supra* note 42.

149. Schmitt & Sengupta, *supra* note 147.

and detecting joint participation in events.[150] Keeping track of who attends ISIS's virtual recruitment fairs may in fact play to machine searches' strengths.

In addition, if the actual data set of ISIS recruits is still not large enough, that does not necessarily mean that counterterrorism officials must write off data mining. Creative programmers can find work-arounds, including populating a data set with "synthetic" data: virtual replicas of actual terrorists that can augment sample size and permit rudimentary validation of a machine search.[151]

Moreover, the experience of the government thus far reinforces the case for cautious optimism about machine searches. While some programs have ended in futility, some specialized government data mining programs, such as those focused on fraud, have established a niche.[152] The government's USA PATRIOT Act (Patriot Act) metadata program, although it did not catch any terrorists on the brink of an attack, supplied a useful lead in an investigation of a plot to bomb New York subways.[153]

Finally, the trove of documents leaked by Edward Snowden, which one would assume are "Exhibit A" for surveillance critics, in fact suggest that machine learning may be helpful.[154] Consider the targeted surveillance reports on conversations between an Australian, who wished to join the Taliban, and his girlfriend.[155] While critics claim that the girlfriend was a false positive, her conversations with her aspiring Taliban-member boyfriend reveal his deepening radicalization and the streak of male control fixation that accompanied it.[156] That window into the Australian's motives, which might generalize to other terrorist recruits, reinforces the value of overseas intelligence collection. True, it appears that the conversations between the aspiring Taliban and his

150. SCHNEIER, *supra* note 2, at 140 (finding that "political dissidents are likely to share a well-defined profile").

151. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 81.

152. *Id.* at 235–36.

153. *See* Margulies, *supra* note 54, at 15. The metadata program first supplied this lead, although it might have been available from other sources. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 150 (2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

154. *See id.* at 1.

155. Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

156. *Id.*

girlfriend were collected as part of the targeted Section 702 program,[157] not an autonomous search. However, it seems reasonable to assume that some of the selectors used in the Section 702 program, which largely belong to persons outside the United States, first came to light through autonomous search techniques.

II. MACHINE VERSUS HUMAN ACCESS TO DATA

Now with a basic grasp of how machine searches work, this Article can address a normative question: how intrusive are machine searches? Surveillance critics state two normative objections to machine access to data. The deontological objection frames privacy as a right that inherently protects the individual against all manner of intrusions, whether by people or machines.[158] In contrast, the consequentialist objection cites the risk that governments, corporations, or other individuals will misuse personal information.[159] Champions of a state-centric approach discount the deontological implications of computer access and the risks of adverse consequences.[160] In contrast, government critics and privacy advocates argue that under either a deontological or consequentialist reading, machine and individual access pose risks of equivalent severity. This Article argues for a middle ground that recognizes that, while machine access poses both deontological and consequentialist risks, appropriate safeguards can address these concerns.

A. *The Deontological Objection to Machine Access*

Many privacy advocates' arguments suggest that machine access violates central aspects of personhood. Professor Julie Cohen, for example, has written that pervasive machine access by private sector firms tracking individuals' internet use intrudes on humans' sense of control and self.[161] According to Professor Cohen, certain types of

157. *Id.*

158. While the deontological view is an important touchstone in thinking about privacy, many contemporary legal scholars deal with either direct or more intangible consequences of privacy intrusions. *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1909–10 (2013) (discussing theories of the self, while also linking privacy with participation in democratic governance); *cf.* SLOBOGIN, *supra* note 2, at 94–95 (surveying research suggesting individual's knowledge of ubiquitous surveillance may limit spontaneity). *But see* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1145 & nn. 342–44 (2002) (citing sources while rejecting the deontological view).

159. *See, e.g.*, Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1945–47, 1951 (2013) (discussing the importance of privacy in the ability to think freely without government intimidation); Solove, *supra* note 158, at 1151 (arguing that protecting privacy prevents "exercises of power employed to destroy or injure individuals").

160. *See, e.g.*, Posner, *supra* note 9, at 249–51.

161. Cohen, *supra* note 158, at 1910–11, 1916–17 (discussing spontaneity and play in the

machine access, such as scanning email to tailor behavioral advertising to individual users, inhibit individuals' capacity to develop their own values and preferences through trial and error.[162] Burdened by the awareness that machines are monitoring the content of their communications, individuals will be less spontaneous—less willing to make mistakes.[163] If the freedom to make mistakes is an essential ingredient of personal autonomy, then for Professor Cohen machine access abridges that autonomy.

A state-centric account would take the opposite tack. On this view, machine access alone, uncoupled from human access, has no deontological privacy implications.[164] This view holds that only beings with a certain level of consciousness can intrude on privacy.[165] Forms of life such as animals lack consciousness in the human sense and therefore cannot intrude. No one regards a dog or cat as intruding on his privacy, even if it saw him without clothes.[166] A computer, on this reading, is similarly unintrusive, as long as it is uncoupled from human access.[167]

Intuitions about privacy do not entirely square with the deontological objection to machine surveillance. Most privacy advocates rely, either expressly or implicitly, on the metaphor of the "gaze." Professor Jeffrey Rosen, for example, in his groundbreaking work, *The Unwanted Gaze*, repeatedly uses examples of privacy intrusions such as the public disclosures of Monica Lewinsky's sexual history with then-President Bill Clinton[168] and the disclosures of individuals' sexual histories and communications in sexual harassment litigation.[169] In each of these instances, the intrusion on privacy arose from the knowledge acquired by other people and the prospect of others' amusement, pity, or disdain.

That said, the state-centric dismissal of the equivalency theory also is too facile. While one cannot fully quantify or predict the costs to self of ubiquitous machine access, it seems reasonable to assume that such

development of selfhood, and suggesting that systematic intrusions by the government and corporations adversely affects such development).

162. *Id.* at 1916–18.

163. *Id.*

164. *See* Posner, *supra* note 9, at 254.

165. *See id.*

166. Ross Andersen, *An Eye Without an 'I': Justice and the Rise of Automated Surveillance*, ATLANTIC (June 14, 2012), http://www.theatlantic.com/technology/archive/2012/06/an-eye-without-an-i-justice-and-the-rise-of-automated-surveillance/258082/.

167. Dan Froomkin, *The Computers Are Listening: How the NSA Converts Spoken Words Into Searchable Text*, INTERCEPT (May 5, 2015, 10:08 AM), https://firstlook.org/theintercept/2015/05/05/nsa-speech-recognition-snowden-searchable-text/ (quoting Kim Taipale, Stilwell Center for Advanced Studies in Science and Technology Policy, as noting that "[a]utomated analysis has different privacy implications" than access to data by human analysts).

168. JEFFREY ROSEN, UNWANTED GAZE 4–6, 8 (2000).

169. *Id.* at 88–94.

comprehensive surveillance would make people more wary of making mistakes. That reticence would lead to less experimentation and perhaps less personal growth. Universal machine access might also induce an anxiety that undermined personal well-being, even when more tangible indicia of welfare showed improvement.

In addition, the deontological objection to full machine access may reflect developments in artificial intelligence that have brought computers closer to human beings. It is unlikely that computers possess even the consciousness and affective attributes, such as anger or fear, attributable to household pets. However, every day researchers add to the repertoire of judgments that computers can make. It is now routine to subject machines performing searches or other autonomous activities to penalties for exceeding certain parameters and to reward machines for good performance.[170] Those penalties and rewards may not produce emotions such as guilt or shame, but they indicate that computers can respond to stimuli. Indeed, the extraordinary progress in machine learning over the past few decades has far exceeded humans' ability to change. If providing information to an entity that can process that data in a sophisticated fashion instills perceptions of loss of control, machine access may undermine perceptions of control far more readily than access by other humans, let alone dogs or cats.

B. *The Consequentialist Objection*

Machine access also draws consequentialist objections. For example, machines may be largely responsible for implementing certain counterterrorism tools, including no-fly lists.[171] These lists have a significant number of errors, including both false positives and false negatives.[172] Inclusion on a no-fly list can hamper individuals' ability to travel to the United States and possibly to other countries. Because officials may overestimate a machine's accuracy,[173] they rarely remove individuals from such lists.[174] When hidden layers reduce the

170. *See* FLACH, *supra* note 80, at 131 (discussing the use of a penalty for a machine that set predictive criteria that were too complex to efficiently generalize to future cases).

171. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 214.

172.The late Senator Ted Kennedy was sometimes delayed in boarding because his name matched one on the list. *See* PETER MARGULIES, LAW'S DETOUR: JUSTICE DISPLACED IN THE BUSH ADMINISTRATION 44–45 (2010). Errors in the no-fly list have attracted greater attention after the June 2016 ISIS-inspired mass shooting at an Orlando nightclub because of legislative proposals to bar those on the list from buying guns. *See* Molly O'Toole & Paul McLeary, *Here's How Terrorism is Scrambling America's Gun Debate*, FOREIGN POL'Y (June 21, 2016), http://foreignpolicy.com/2016/06/21/heres-how-terrorism-is-scrambling-americas-gun-debate/.

173. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 206.

174. *See* Latif v. Holder, 28 F. Supp. 3d 1134, 1161 (D. Or. 2014) (holding that the Department of Homeland Security's process for correcting the erroneous placement of travelers

transparency of machine outputs, these problems multiply. While such searches *can* be more accurate than other types, flaws in inputted data will compromise outputs.[175] Some of these concerns are best addressed through a robust framework for correcting errors.[176] Nevertheless, such concerns reinforce the consequentialist objection to machine access.

Errors in machine searches may prompt further harms. For example, states might detain individuals because of outputs from machine searches. Prolonged detention based solely on a machine search would be arbitrary and hence a violation of the ICCPR. An individual could also be subject to counterterrorism sanctions because of a flawed search.[177] In addition, flawed search results could affect targeting decisions by states engaged in armed conflicts with violent extremists. In a provocative and intentionally hyperbolic remark, former NSA (and CIA) Director General Michael Hayden asserted, "We kill people based on metadata."[178] In fact, the process used by the United States for targeted killings is far more

---

on the no-fly list left them stranded on the list indefinitely and violated their procedural due process rights); Ibrahim v. Dep't of Homeland Sec., 62 F. Supp. 3d 909, 929–31 (N.D. Cal. 2014) (same); Irina D. Manta & Cassandra Burke Robertson, *Secret Jurisdiction*, 65 EMORY L.J. (forthcoming 2016) (discussing litigation over no-fly lists and finding that "[w]hile people like Ted Kennedy did not remain on the no-fly list for long, less connected individuals like Rahinah Ibrahim and many others were not so lucky, receiving recourse after many years, if at all"); *cf.* Abdelfattah v. Dep't of Homeland Sec., 787 F.3d 524, 529–43 (D.C. Cir. 2015) (detailing lawful resident plaintiff's difficulties with repeated security checks that information in government databases may have prompted and holding that plaintiff could seek relief under both the Privacy Act and the U.S. Constitution, but denying relief because the plaintiff had not established a factual basis, including tangible harm, for the relief sought).

175. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 76 (discussing errors when machine searches inspect multiple databases, each of which may have incorrect inputs).

176. Peter M. Shane, *The Bureaucratic Due Process of Government Watch Lists*, 75 GEO. WASH. L. REV. 804, 810 (2007). The government has established a program to directly handle complaints about difficulties in boarding aircraft that may be due to erroneous inclusion on a terrorist watch list. *See DHS Traveler Redress Inquiry Program (DHS TRIP)*, U.S. DEP'T OF HOMELAND SEC. (Sept. 11, 2015), http://www.dhs.gov/dhs-trip. Recently, the government expanded the information it would provide to travelers who encountered such difficulties. *See* Dibya Sarkar, *Justice Department Revises Procedures for Individuals on No-Fly List Seeking Redress*, FIERCEGOVERNMENTIT (Apr. 16, 2015), http://www.fiercegovernmentit.com/story/justice-department-revises-procedures-individuals-no-fly-list-seeking-redre/2015-04-16. A program like DHS TRIP is a useful supplement to, but not a substitute for, a program that would address complaints about wrongful data collection and retention. Wrongful collection or retention or flawed data inputs that conflate an innocent with a terrorist can manifest themselves in a range of harms; difficulty in boarding an aircraft is just one of them. In such cases, it is more effective to address the problem at the source. The DHS TRIP program shows that such redress is feasible.

177. *See* Peter Margulies, *Aftermath of an Unwise Decision: The U.N. Terrorist Sanctions Regime After Kadi II*, 6 AMSTERDAM L.F. 51, 52–53 (2014).

178. Lee Ferran, *Ex-NSA Chief: 'We Kill People Based on Metadata,'* ABC NEWS (May 12, 2014), http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/.

diligent, methodical, and comprehensive than the general's off-hand remark suggested.[179] Despite concerns about autonomous weapons, no one claims that the United States or any other state targets individuals based solely on a machine search. That said, if flawed machine outputs play a role because individual officials are unwilling or unable to follow up, that deficit should also figure in the consequentialist calculus.

In sum, while surveillance critics overstate the force of the deontological objection to machine access, this objection cannot be completely dismissed. Similarly, consequentialist objections to machine surveillance have some foundation. This does not mean that human rights law should preclude machine surveillance or treat it as equivalent to human access in all contexts. However, the risk of deontological and consequential harms points toward the need for safeguards.

III. AGAINST THE TECHNOLOGICAL IMPERATIVE: STATE CAPABILITIES NEED NOT DRIVE MACHINE SEARCH PRACTICES

With the above discussion as a predicate, this Article now examines the flaws in the second equivalency proposition, which this Article calls the technological imperative: the descriptive claim that in matters of surveillance, a state's capabilities determine its practices.[180] Viewed in a more modest light, this claim is sound; indeed, in a speech announcing reforms in overseas intelligence collection, President Obama acknowledged the "inevitable bias [in government] . . . to collect more information about the world, not less."[181] However, as an ironclad prediction about state practice, the technological imperative fails to deliver because it unduly discounts technological, legal, and political constraints on democratic governments.

The technological imperative reflects an incomplete acknowledgment of technology's role in privacy matters. While privacy advocates often view increasing technological sophistication solely as a threat to privacy, this perspective is too limiting. Technological advances such as search filters can preserve privacy by regulating government surveillance

179. Gregory S. McNeal, *Targeted Killing and Accountability*, 102 GEO. L.J. 681, 685 (2014) (concluding based on document review and interviews that U.S. targeting decisions involved elaborate analysis engaged in by dozens or even hundreds of officials); *cf.* Ferran, *supra* note 178 (indicating that General Hayden did not make his remarks about metadata in the course of describing U.S. targeted killing procedures but instead highlighted that the Patriot Act domestic metadata program required directed searches based on identifiers linked to terrorism and did *not* allow autonomous machine searches).

180. *See supra* note 11 and accompanying text.

181. *Transcript of President Obama's Jan 17 Speech on NSA Reforms*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

officials.[182] For example, search filters can prevent analysts from gaining access to machine-generated data unless the analysts use pre-approved queries. Software can also monitor analyst's online work to ensure that analysts do not try to circumvent such safeguards or otherwise overreach.[183]

As a descriptive matter, the technological imperative also unduly discounts the force of law. In an unprecedented summary of norms governing intelligence collection, NSA officials implementing President Obama's PPD-28 guidance to respect privacy worldwide declared that signals intelligence scanning, collection, processing, and retention should be "as tailored as feasible."[184] NSA has also stated that it will prioritize reliance on "diplomatic and public sources."[185] Admittedly, these guidelines preserve much of the intelligence agencies' flexibility, since the terms "feasible" and "prioritize" do not expressly preclude other options. Nevertheless, it would be glib to dismiss the importance of such constraints.

Guidelines such as those implementing PPD-28 start a conversation, which in itself is valuable in the often-closed world of intelligence collection.[186] In the future, if intelligence agencies give in too readily to the temptation to "collect it all" that the technological imperative describes, privacy advocates can cite the government's own guidelines in seeking positive change. Legislators as well as bodies such as the Privacy and Civil Liberties Oversight Board (PCLOB) can provide oversight. In

182. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 72; *cf.* John DeLong, *Aligning the Compasses: A Journey through Compliance and Technology*, IEEE Security and Privacy, at 85, 86–88 (July–Aug. 2014) (discussing importance of technology that promotes compliance with legal rules); Litt, *supra* note 54, at 18 (same).

183. *See id.* (discussing individual audit records that compile all queries and permit comparison between analysts to detect anomalies that might indicate overreaching); Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795, 1853 (2010) (same); *see also In re* Production of Tangible Things, No. BR 08-13, 2009 WL 9150913, at *5, *7–8 (FISA Ct. Mar. 2, 2009) (discussing technological safeguards); Margulies, *supra* note 54, at 44 (same); Pozen, *supra* note 24, at 236–38 (same); Gellman et al., *supra* note 155 (including comments by Robert Litt, General Counsel for the Director of National Intelligence, on technological safeguards).

184. PPD-28 Supplemental Procedures, *supra* note 27, para. 3.5, at 6.

185. *Id.*

186. *See, e.g.*, *Transcript of President Obama's Jan 17 Speech on NSA Reforms*, *supra* note 181. For an argument that intelligence agencies and their lawyers prior to Snowden's disclosures failed to model this kind of proactive conversation, see Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015); *cf.* Shirin Sinnar, *Institutionalizing Rights in the National Security Executive*, 50 HARV. C.R.-C.L. L. REV. 289, 340–41 (2015) (discussing virtues and risks of establishing units in the U.S. Executive Branch to promote internal compliance with civil and human rights).

addition, the proposal advanced below[187] would empower an independent body to decide if the government was adopting the measured outlook captured in the guidelines. Officials may still push the envelope, but they will get pushback if they do.

Skeptics about the government's ability or willingness to live within the law on surveillance also too quickly discount the government's track record in the three years prior to Snowden's revelations. Consider the post-2009 record of the government on the pre-USA Freedom Act domestic metadata program that limited analysts' access to call record information. In 2009, the FISC took charge of enforcing limits that required an intelligence analyst to use only RAS-approved identifiers (RAS stands for "reasonable articulable suspicion") in queries of the database.[188] Diligent media efforts in the post-Snowden period have uncovered only a handful of violations of the RAS standard out of the billions of call records the government acquired.[189]

As noted above, skeptics about the U.S. government's focus on tailored collection abroad do not fully reckon with the government's track record of retrieving such tailored intelligence. Consider again the report by journalists working with Edward Snowden describing surveillance on the Australian national who tried to join the Taliban and conversed with his girlfriend during his quest.[190] Much of the conversation recorded dealt with the Taliban aspirant's motivations for extremism, which would be relevant. In addition, as the girlfriend acknowledged to reporters, she was troubled about the target's extremist bent. This attitude would make her a possible informant if the target ever decided to resume his quest for a more active role with the Taliban. If the technological imperative were an adequate description of U.S. practice, surely journalists with access to Snowden's copious files could have come up with a better example.

In addition, privacy advocates arguing that state capabilities necessarily drive intelligence practices do not pay sufficient attention to their own efforts, or to other forces countering the state. In the post-Snowden era, privacy advocates will have a seat at the table on

187. *See infra* Section V.C.

188. *See In re* Production of Tangible Things, No. BR 08-13, 2009 WL 9150913 at *2. The FISC became involved because intelligence community officials disclosed to the FISC in early 2009 that the NSA had earlier used non-RAS-approved identifiers. *See* Margulies, *supra* note 54, at 45–48.

189. *See* Ryan Gallagher, *How NSA Spies Abused Their Powers to Snoop on Girlfriends, Lovers, and First Dates*, SLATE (Sept. 27, 2013, 11:19 AM), http://www.slate.com/blogs/future_tense/2013/09/27/loveint_how_nsa_spies_snooped_on_girlfrgirlf_lovers_and_first_dates.html (detailing that the NSA, through lie detector tests routinely given to employees, uncovered twelve instances since 2003 in which analysts spied on intimate partners or engaged in other collection activities barred by agency procedures).

190. *See* Gellman et al., *supra* note 155.

surveillance policy.[191] Moreover, U.S. companies eager to dispel the impression that they are mere vassals of the U.S. intelligence community will also push back. Finally, other countries will make their voices heard.[192]

The claim that technology determines state surveillance is most plausible as a warning of what will happen if adequate safeguards are not in place. A more modest version of the technology-determines-practice claim might generate less heat in mobilizing privacy advocates, but it would also shed more light.

IV. EQUIVALENCY AND EXTRATERRITORIALITY

Now comes the third component of the equivalency thesis: the proposition that a state must accord equivalent rights to persons within its own borders and persons located overseas with no ties to that state.[193] Here, there is also a statist counterpart: the claim that the ICCPR does not apply extraterritorially.[194] As in the other issues previously discussed, both the statist and equivalency claims miss the mark. This Part addresses the statists' claim, which conflicts with the ICCPR's language, structure, and purpose.[195]

The statist view finds support in a superficial reading of the ICCPR's language. Article 2(1) of the agreement obligates each state party "to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant."[196] The

191. *See generally* JACK GOLDSMITH, POWER AND CONSTRAINT (2012) (analyzing both President Bush's and President Obama's counterterrorism programs and finding that presidents act with greater discretion and secrecy during times of war).

192. *See* Deeks, *supra* note 8, at 330.

193. *See* Emmerson, *supra* note 12, para. 43, at 16.

194. This is the U.S. position. *See* STATE DEP'T PERIODIC REPORTS, *supra* note 8, at Annex 1; Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AM. J. INT'L L. 119, 124–26 (2005) (defending the U.S. view). The United Kingdom's Investigatory Powers Tribunal shares this view. *See* Human Rights Watch v. Sec'y of State, paras. 52–63 (Investig. Powers Trib. 2016), http://www.bailii.org/uk/cases/UKIPTrib/2016/15_165-CH.html.

195. In this Section, this Article addresses the equivalency theorists' claim that the U.S. must accord identical rights to those within and without its borders. *See infra* notes 196–213 and accompanying text.

196. ICCPR, *supra* note 7, art. 2(1) (emphasis added). For more detailed explanation of this and other textual arguments, see Margulies, *supra* note 8, at 2143; *see also* Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 85 (2015) [hereinafter Milanovic, *Human Rights Treaties and Foreign Surveillance*] (supporting extraterritorial application of the ICCPR); Marko Milanovic, *From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties*, 8 HUM. RTS. L. REV. 411, 429 (2008) (same); Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change*, 90 INT'L L. STUD. 20, 57–59 (2014) (same). *See generally* Sarah H. Cleveland, *Embedded International*

Vienna Convention on the Law of Treaties requires interpreting a treaty "in accordance with the ordinary meaning . . . [of its] terms."[197] Under the "ordinary" meaning of two conditions linked by the conjunctive "and," a state incurs a duty only when *both* conditions are met.[198] In other words, a state incurs obligations under the ICCPR only to individuals who are both "within its territory" *and* "subject to its jurisdiction." This reading of the ICCPR's language precludes extraterritorial application.

However, ordinary rules of textual interpretation provide reasons to question the statist view.[199] First, this reading makes the verb "respect" redundant.[200] Generally one assumes that the drafters of a treaty, statute, or constitution did not intend mere surplusage or superfluity—each of the words used should add something to the agreement's meaning.[201] The statist position clashes with this interpretive rule. Consider that the term "respect" commits a state to refrain from violations. The term "ensure," in contrast, entails both respect in this sense *and* affirmative duties to guarantee rights against incursions by others. Since "ensure" is a far broader term that already encompasses the narrower duty to "respect" rights, expressly mentioning the duty to "respect" would be unnecessary if the statist position is correct that a state is bound to ensure and respect rights only for those individuals within its territory.

In contrast, the position that the ICCPR applies extraterritorially dovetails with the rule against superfluity. On the reading supporting extraterritorial application, a state must respect individual rights regardless of the location of the individuals. However, the state undertakes the larger and more complex obligation to *ensure* rights only regarding those individuals who are both within its territory and subject to its jurisdiction.

Law and the Constitution Abroad, 110 COLUM. L. REV. 225 (2010) (noting that the Supreme Court abandoned the formalistic territorial approach). *But see* J. Andrew Kent, *A Textual and Historical Case Against a Global Constitution*, 95 GEO. L.J. 463, 464–65 (2006) (suggesting caution in extraterritorial reading of the U.S. Constitution).

197. Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S.

198. Margulies, *supra* note 8, at 2143. Satisfaction of either condition would trigger an obligation if the treaty drafters had placed the subjunctive term "or" between the two conditions.

199. The textual arguments against the current U.S. reading were made most comprehensively in a 2010 memorandum by then-U.S. State Department Legal Adviser Harold Koh. *See* Harold Hongju Koh, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights 2 (Oct. 19, 2010) [hereinafter Koh Memorandum].

200. *Id.* at 9.

201. *See* Abbe R. Gluck & Lisa Schultz Bressman, *Statutory Interpretation from the Inside—An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part I*, 65 STAN. L. REV. 901, 930, 934–35 (2013) (noting the canon's importance for courts while reporting that congressional drafters do not necessarily view the canon as central to their work, since legislators prefer surplus language as a way of stressing substantive points).

The U.S. position also violates the rules of grammar.[202] Under the U.S. view, a state party must "respect . . . to all individuals within its territory and subject to its jurisdiction the rights" listed in the treaty.[203] Consider on the phrase, "*respect... to* all individuals." That phrase entails an ungrammatical mating of verb and preposition. In English and French syntax, one does not "respect" rights "to" rights holders. Americans might tolerate sloppy drafting in English, but the French would surely insist on flawless French. Massaging the sense of the language could ease the grammar problem. For example, one could respect rights "with regard" to individuals. However, reading the ICCPR in that way adds two words to Article 17. This seems incongruous for a textualist approach that purports to rely on the literal language of the treaty. Textualist canons exclude a reading that depends on adding words, just as they are skeptical of treating some words in the text as superfluous.[204] In sum, the statist position is stuck with a choice of two alternatives that are both flawed from a textualist perspective. Either the drafters used bad grammar, which seems unthinkable for the French, or they inadvertently omitted two words ("with regard") from the provision's text. Each assumption clashes with a textualist reading.

A reading that requires a state to respect rights everywhere but ensure rights only in a more limited area where it has greater control is also consistent with the intent of the ICCPR's drafters, as revealed in the arguments made by U.S. Representative Eleanor Roosevelt. As Roosevelt explained, the United States feared that a broad view of the agreement's territorial scope would require it to guarantee rights within each of the defeated Axis powers that the United States and its allies occupied after World War II.[205] The early wording of Article 2 imposed on a signatory state the duty to "*guarantee* to all persons residing on their territory and within their jurisdiction the rights defined in the present covenant."[206] The term "guarantee" could have created a U.S. commitment to ensure rights in the former Axis states. This commitment would have been burdensome, impracticable, and arguably illegal under U.S. law.[207] To forestall this daunting prospect, Roosevelt told the drafting group that the agreement's language should clearly disavow any duty by states to

202. *See* Koh Memorandum, *supra* note 199, at 10.

203. *Id.* (quoting ICCPR, *supra* note 7, art. 2(1)).

204. *See* Ruth Sullivan, *Statutory Interpretation in the Supreme Court of Canada*, 30 OTTAWA L. REV. 175, 184 (1998–99) (observing that, "[f]or a true literalist, adding words to a clear text is always unacceptable," since it amounts to an "amendment" of the statute).

205. *See* U.N. ESCOR, 6th Sess., 193d mtg. at 13, U.N. Doc. E/CN.4/SR.193 (May 15, 1950).

206. *See id.* (emphasis added).

207. Margulies, *supra* note 8, at 2144–45.

"*ensure* the rights recognized in [the covenant] to the citizens of countries under United States occupation."[208] However, Roosevelt agreed that U.S. forces, wherever in the world their mission placed them, had a duty to *respect* rights under the ICCPR,[209] since imposing a duty on the United States to ensure its own troops' compliance with the treaty was not burdensome or unreasonable.

Finally, the statist view fails to account for the ICCPR's logic and purpose. The ICCPR, drafted by the United States and its World War II allies shortly after the end of that decisive conflict, was a response to the unspeakable persecution unleashed by Nazi Germany.[210] On a statist reading, however, the ICCPR would not bar a recurrence of the prime symbol of Nazi human rights abuses: Auschwitz and the other concentration camps.[211] After all, these death camps were all located outside German territory.[212] A reading of a post-World War II human rights treaty that would not prohibit a repeat of the death camps makes a travesty of the ICCPR's structure and purpose. As Chief Justice John Roberts recently noted with respect to the Affordable Care Act, a plausible interpretation should respect the purpose behind the drafting of a text.[213] Under that standard, the statist view of the ICCPR falls short.

V. A NORMATIVE APPROACH TO AUTOMATED SEARCHES ABROAD

Now having established the applicability of Article 17 of the ICCPR, which bars "arbitrary" intrusions on privacy, this Article can address how that standard affects a state's overseas machine searches. This Part argues that the international law concept of complementarity and the human rights doctrine that accords states a "margin of appreciation"[214] entitle states to a measure of deference in the assessment of their overseas surveillance policies. This measure of deference counters surveillance critics' third equivalency proposition: the claim that a state must provide a person who is overseas and has no ties to that state precisely the same

208. U.N. ESCOR, 6th Sess., 194th mtg. at 5, U.N. Doc. E/CN.4/SR.194 (May 16, 1950) (summarizing statements made by Eleanor Roosevelt regarding the adoption of an amendment to the agreement).

209. *Id.* at 9.

210. *See* Emilie M. Hafner-Burton & Kiyoteru Tsutsui, *Human Rights in a Globalizing World: The Paradox of Empty Promises*, 110 A.J.S. 1373, 1373–74 (2005).

211. *See* Milanovic, *Human Rights Treaties and Foreign Surveillance*, *supra* note 196, at 108–11.

212. *See Nazi Camps*, U.S. HOLOCAUST MEMORIAL MUSEUM, https://www.ushmm.org/wlc/en/article.php?ModuleId=10005144 (last updated Jan. 29, 2016).

213. *See* King v. Burwell, 135 S. Ct. 2480, 2495–96 (2015) (underlining the need to appraise the context and structure of statutes, while conceding, citing Justice Felix Frankfurter, that such assessments are a "subtle business" (quoting Palmer v. Massachusetts, 308 U.S. 79, 83 (1939))).

214. Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A), para. 47 (1976).

privacy rights that the state provides to its citizens or other individuals within its borders.[215]

Three crucial considerations buttress the case for deference. First, overseas surveillance serves substantial international law interests, permitting states to further the intent of U.N. Security Council resolutions, such as Resolution 2178, which the Security Council recently adopted to promote international cooperation against the threat posed by foreign and returning fighters associated with ISIS and other terrorist groups.[216] Second, when used to identify, locate, and deter members of groups such as ISIS engaged in an armed conflict with a state, overseas surveillance is also consistent with the LOAC.[217] Third, surveillance can help states ease privacy threats from cyber criminals and foreign nations.[218]

A. *Deference, Human Rights, and Machine Access*

The first touchstone of any review of state surveillance policies is the measure of deference that states have received from transnational human rights bodies such as the ECHR. This deference is sometimes couched in terms of the complementarity that international tribunals allow to individual state determinations[219] or the "margin of appreciation" that transnational human rights tribunals such as the ECHR show to individual states on matters of security and public safety.[220] Deference is rooted in the structure and logic of international norms.

All international law depends on the cooperation of states.[221] State practice shapes customary international law. In addition, state consent is required for the promulgation of treaties.[222] Failing to allow a measure of deference for state interpretation of treaty terms would discourage future

---

215. *See, e.g.*, Emmerson, *supra* note 12, para. 43, at 16.

216. S.C. Res. 2178, *supra* note 22, at 1–2.

217. *Cf.* Schmitt, *supra* note 25, at 596–97 (noting the importance of intelligence, surveillance, and reconnaissance in war-fighting).

218. *See generally* Pozen, *supra* note 24, at 229 (noting that with a reduction in surveillance, "risk may be shifted not only among groups that suffer privacy harms but also among groups that *cause* harm to a certain privacy interest—among privacy violators as well as victims").

219. Samuel C. Birnbaum, *Predictive Due Process and the International Criminal Court*, 48 VAND. J. TRANSNAT'L L. 307, 337–39 (2015).

220. Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A), para. 47 (1976); *see also* Robert D. Sloane, *Human Rights for Hedgehogs?: Global Value Pluralism, International Law, and Some Reservations of the Fox*, 90 B.U. L. REV. 975, 983 (2010) (noting that the ECHR allows states "a 'margin of appreciation' within which to implement or interpret human rights in ways that may be sensitive or responsive to prevailing social, cultural, and other norms within their polities").

221. *See* William W. Burke-White, *Power Shifts in International Law: Structural Realignment and Substantive Pluralism*, 56 HARV. INT'L L.J. 1, 38 (2015).

222. *See* Duncan B. Hollis, *Why State Consent Still Matters—Non-State Actors, Treaties, and the Changing Sources of International Law*, BERKLEY J. INT'L L. 137, 144 (2005).

treaties and encourage defection from treaty regimes.[223] Moreover, international law bodies have a competence deficit in dealing with the special problems faced by individual states. Navigating the currents of local custom and culture can be perilous. Lending a measure of deference to state officials' efforts ensures that officials with greater knowledge of those institutional and cultural factors can take a first crack at the issue, thereby reducing the mistakes made by transnational bodies lacking such local knowledge.[224]

1. Deference and Harmonizing International Norms

One vital function of deference is giving states the space they need to sort out tensions between disparate international law norms. A rigid approach cannot reckon with the exigencies that shape the implementation of norms. In contrast, granting states a measure of deference can minimize norm conflicts.

Consider U.N. Security Council resolutions enacted after September 11 to address the threat of terrorism. For example, Security Council Resolution 2178 addresses the burgeoning threat of ISIS.[225] Resolution 2178 focuses on the threat of foreign fighters joining ISIS, acquiring safe harbors in states that are unwilling or unable to combat the terrorist group[226] and then returning to their native countries in the West to engage in violence. The Security Council warned specifically about the "increased use by terrorists . . . of communications technology . . . including . . . the internet" as a means of recruitment.[227] To address this concern, the Security Council highlighted the need for member states to cooperate in preventing terrorists from "exploiting technology . . . [and] communications."[228]

Carefully tailored overseas surveillance makes the Security Council's wishes an achievable blueprint, instead of an exercise in airy aspiration. If machine learning can enhance the effectiveness of overseas surveillance, it should be part of the equation. After all, terrorists readily

---

223. *See generally* Laurence R. Helfer, *Overlegalizing Human Rights: International Relations Theory and the Commonwealth Caribbean Backlash Against Human Rights Regimes*, 102 COLUM. L. REV. 1832, 1834 (2002) (raising the question of the point at which the "substantive rules or review mechanism" become "too constraining" on states).

224. *See* Sloane, *supra* note 220, at 982–83; *cf.* Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361, 1364–66 (2009) (analyzing factors influencing U.S. judicial deference to executive decisions).

225. *See* S.C. Res. 2178, *supra* note 22, at 2; *see also* S.C. Res. 1373, *supra* note 23, at para. 3 (urging, in a resolution passed shortly after the September 11 attacks, that states share "operational information . . . regarding actions or movements of terrorist persons or networks" and "use of communications technologies by terrorist groups").

226. *See* S.C. Res. 2178, *supra* note 22, at 1.

227. *Id.* at 2.

228. *Id.* at 3, 7.

cross borders, in both physical and virtual domains.[229] Such groups are not known for their acquiescence to Security Council resolutions.[230] Nor do they advertise their specific plans for violence. Indeed, a crucial aspect of ISIS's tactical advantage is the power of surprise it has gained through its diffuse, decentralized operation.[231]

ISIS has also taken advantage of the weakness and chaos that has afflicted states in the Middle East. A terrorist group that establishes a safe haven in a state that is riven by armed conflict, such as Syria, Iraq, or Yemen, can then mount or inspire operations in other states.[232] Even when those state targets of terror have functioning legal systems and control over their own territory, they are unable to directly regulate terrorist groups that have found safe havens in other countries.[233] Cultivating informants and other sources of human intelligence is difficult when a safe harbor state is unwilling or unable to cooperate with the international community.[234]

Because an international framework is only as strong as its weakest link, safe haven states can undermine global counterterrorism efforts. In the face of terrorists' opportunism in finding safe havens, a target state's ability to conduct surveillance abroad can help bridge the gap in knowledge of terrorists groups' structure, operations, and plans for future violence.[235] Surveillance that harnesses today's technology, but does so with appropriate constraints, can be an equalizer in the battle against ISIS and other groups that practice violent extremism. A rigid definition of international privacy norms that short-circuits this counterterrorism effort would ultimately be self-defeating, leaving the initiative with forces like

---

229. *See id.* at 2.

230. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 30–31 (2010) (detailing terrorist groups' disregard for legal requirements).

231. *See* David Ignatius, *How ISIS Spread in the Middle East and How to Stop It*, ATLANTIC (Oct. 29, 2015), http://www.theatlantic.com/international/archive/2015/10/how-isis-started-syria-iraq/412042/.

232. *See* S.C. Res. 2178, *supra* note 22, at 2.

233. *See Humanitarian Law Project*, 561 U.S. at 34 (upholding a material support statute against First Amendment and vagueness challenges, and observing that deference was important in national security and foreign relations cases because in those areas "information can be difficult to obtain and the impact of certain conduct difficult to assess").

234. *See generally* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483 (2012) (describing the elaborate test a victim state must evaluate before attacking a safe harbor state unable or unwilling to take action against residing terrorists); *cf.* Monica Hakimi, *Defensive Force Against Non-State Actors: The State of Play*, 91 INT'L L. STUD. 1, 12–13 (2015) (explaining that the unable and unwilling standard today applies broadly to non-state actors harbored in unwilling or unable states).

235. Peter Margulies, *Rage Against the Machine?: Automated Surveillance and Human Rights* 4 (Roger Williams U. L. Stud. Paper No. 164, 2015).

ISIS that emphatically reject liberal norms such as privacy. In contrast, a deferential approach would give states the flexibility they need to combat violent extremism, while still demanding constraints that preserve fundamental rights.

2. Surveillance and Armed Conflict

LOAC[236] also counsels for a measure of deference to states on surveillance. Courts need to reconcile the foundational norms of human rights law, including the bar on arbitrary deprivation of the right to life, with the distinctive challenges posed by the existence of armed conflict, including the privilege to use lethal force against other participants in the conflict.[237] LOAC provides more concrete guidance on these issues. Consequently, LOAC's provisions should inform but not displace human rights law,[238] including ICCPR Article 17's prohibition on arbitrary intrusions on privacy. While LOAC does not provide a blanket justification for surveillance, overseas surveillance in the course of an armed conflict has clear implications for LOAC that human rights law should acknowledge.

In *Hassan v. United Kingdom*, the ECHR, addressing international armed conflicts between states, strove to integrate LOAC and human rights norms.[239] *Hassan* addressed the issue of detention in Iraq.[240] The ECHR recognized that under human rights law, an individual has the right to freedom from arbitrary deprivations of liberty.[241] At the same time, the

---

236. For leading literature on international armed conflict law, see YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT (2d ed. 2010); Michael N. Schmitt et al., *The Manual on the Law of Non-International Armed Conflict*, INT'L INST. HUMANITARIAN L. 1, 2, 8 (2006).

237. *See* Legality of the Threat Or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, ¶¶ 95–96 (July 8); Gerald L. Neuman, *Understanding Global Due Process*, 23 GEO. IMMIGR. L.J. 365, 387 (2009) (endorsing "modifying the content of . . . treaty norms . . . by importing relevant rules (if any exist) from the law of armed conflict").

238. *See* Hassan v. United Kingdom, Eur. Ct. H.R. para. 36 (2014). Historically, LOAC has been viewed as *lex specialis*—as law that preempts other otherwise operative provisions of international law. *See* Neuman, *supra* note 237, at 387. However, courts, including the ECHR in *Hassan*, have aimed for a more tempered approach that reconciles LOAC and human rights norms without the wholesale displacement of either corpus of law.

239. *Hassan*, Eur. Ct. H.R. at para. 104 (ruling that in an international armed conflict, human rights norms "continue to apply, albeit interpreted against the background" of LOAC's provisions).

240. *Id.* at para. 3.

241. *Id.* at para. 7. The *Hassan* court interpreted the European Convention on Human Rights, which in Article 5, Section 1 secures the right to "liberty and security of the person" and enumerates specific exceptions, such as detention pending criminal trial or deportation. *Id.* at para. 96. These exceptions do not include detention during an armed conflict. *Id.* at paras. 96–97. The *Hassan* court asserted that the "fundamental purpose of Article 5 § 1" of the European Convention

court recognized that in armed conflict, a state had the legal right to detain combatants whom it had captured to prevent them from reentering the fray.[242] Although detention under LOAC was not expressly enumerated in the European Convention on Human Rights, the *Hassan* court interpreted the Convention to accommodate this venerable aspect of armed conflict.[243]

A similar analysis might govern surveillance. On the one hand, reconnaissance and surveillance of another party to an armed conflict are accepted incidents of war.[244] The law of war does not preclude espionage[245] and permits a wide range of observation of enemy forces. This observation can be clandestine or open. A non-international armed conflict, such as the conflict between the United States and Al Qaeda and associated forces, does not diminish a state's prerogatives to engage in such observation of its adversaries.[246] A rigid application of the ICCPR

---

was "to protect the individual from arbitrariness." *Id.* at para. 105.

242. *Id.* at para. 104.

243. *Id.*

244. *See* Schmitt, *supra* note 25, at 597. Even absent an armed conflict, surveillance of cyber threats might be an appropriate countermeasure for a state injured by another state's failure to control cyber intrusions emanating from the second state's territory. *See* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 705–07 (2014).

245. Jordan J. Paust, *Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect*, 15 CHI. J. INT'L L. 612, 647 (2015) (noting that "widely practiced espionage regarding foreign state secrets is not a violation of international law"). The International Court of Justice has issued preliminary relief barring one state from conducting surveillance on officials of another state in peacetime. *See* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measure, 2014 I.C.J. Rep. 147, ¶ 27 (Mar. 3). That decision turned on the integrity of arbitral proceedings involving the two countries. *See id.* ¶ 42 (asserting that the right of a state to engage in arbitration could "suffer irreparable harm" if the state conducting such surveillance used the information acquired to gain an advantage).

246. Schmitt, *supra* note 25, at 597–98. One question remaining after the ECHR's decision in *Hassan* is the applicability of its holding to *non*-international armed conflicts between a state and a non-state actor, such as Al Qaeda or ISIS. *See generally* Hakimi, *supra* note 234 (discussing the state of the law on armed conflicts against non-state actors). Some language in *Hassan* supports a narrow reading, which would limit authority to detain to traditional international armed conflicts between states. *See Hassan*, Eur. Ct. H.R. at para. 104 (noting that "[i]t can only be in cases of international armed conflict, where the taking of prisoners of war and the detention of civilians who pose a threat to security are accepted features . . . that Article 5 could be interpreted as permitting the exercise of such broad powers"). If this narrow view is correct, in a non-international armed conflict, a state would have to formally derogate from its duties under the governing human rights treaty. This derogation would then be subject to proportionality review. *See* A. and Others v. United Kingdom, Eur. Ct. H.R. paras. 14–17 (2009). This is the view taken by an intermediate-level British court. *See* Mohammed v. Sec'y of State for Defence [2015] EWCA Civ. 843 [¶¶ 242, 246] (Eng.), https://www.judiciary.gov.uk/wp-content/uploads/2015/07/serdar-mohammed-v-ssd-yunus-rahmatullah-v-mod-and-fco.pdf.

that precluded such observation would disrupt LOAC. On the other hand, unchecked overseas surveillance in an armed conflict could lead to the arbitrary intrusions on privacy that the ICCPR prohibits. Given this tension, compliance with safeguards would permit tailored reconnaissance and surveillance, while protecting rights.[247]

3. Overseas Machine Surveillance and Privacy Trade-Offs

Another reason to extend a measure of deference to states is the presence of what Professor David Pozen has called privacy–privacy trade-offs.[248] Nationals of all states face privacy threats not only from their own government, but also from other states and non-state actors. While states wishing to conduct surveillance overseas cannot use this risk as a blanket justification for any surveillance scheme, the need to conduct surveillance to detect and monitor such privacy threats is an added justification for granting states a quantum of discretion.

As an example, consider the view expressly held by the U.S. government that China has been responsible for a wide range of cyber intrusions in the United States.[249] To facilitate these intrusions, Chinese operatives may have sought to "spoof" other Internet Protocol addresses based in other states or take over networks of computers in other jurisdictions.[250] While tradecraft of this kind can make it difficult to

---

A broader reading of *Hassan* would argue that the Court's language was dicta because the case concerned an international armed conflict. This view would stress the convergence of the law regarding international and non-international armed conflicts and the functional case for detaining participants in the latter situation to prevent them from engaging in further violence during the pendency of the conflict. *See id.* ¶¶ 205–09, 235–40 (discussing commentary by academics and legal advisers for the International Committee of the Red Cross). The U.S. Supreme Court has held that the conflict with Al Qaeda is a non-international armed conflict, in which both the power of states to detain and the safeguards accorded captives under Common Article 3 of the Geneva Conventions presumptively apply. *See* Hamdan v. Rumsfeld, 548 U.S. 557, 630 (2006) (holding that conflict with Al Qaeda is "not of an international character" and is therefore subject to the Geneva Conventions' Common Article 3); *cf.* Geoffrey Corn & Eric Talbot Jensen, *Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations*, 42 ISR. L. REV. 46, 66 (2009) (contending that the non-international armed conflict designation model is most appropriate for purely internal rebellions or civil wars and that conflict with transnational terrorist organizations like Al Qaeda or ISIS requires a different model).

247. *Cf.* WITTES & BLUM, *supra* note 42, at 200–01 (conceding the risk that U.S. surveillance could target disfavored groups but arguing that safeguards have vastly reduced this risk).

248. *See* Pozen, *supra* note 24, at 222.

249. Randal L. Gainer, *DOD Adopts Interim Cyber Rules as Claims of Chinese Cyber Attacks Continue*, DATA PRIVACY MONITOR (Sept. 14, 2015), http://www.dataprivacymonitor.com/international-privacy-law/dod-adopts-interim-cyber-rules-as-claims-of-chinese-cyber-attacks-continue/.

250. *See* David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SECURITY J. 531, 535 & n.5 (2011); Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELB. J. INT'L L. 496, 503 (2013).

attribute responsibility for cyber intrusions, repeat players at such tasks often use similar tactics over time. These techniques can reveal a signature for the hackers, just as criminals in the analog world acquire a modus operandi that brands their work.[251] However, detecting such tradecraft requires a certain level of surveillance. Machine surveillance that looks for cyber signatures linked to past attacks can deter hackers and provide useful information about cyber-criminals' future plans. Even when such intrusions cannot be stopped, the information acquired can allow the government and prospective private victims of intrusions to improve their resilience and minimize each intrusion's impact. Individual states can judge the need for surveillance to protect against cyber attacks far more accurately than an international body handing down rigid rules.

4. Deference and Post-Snowden Privacy Decisions from European Courts

Recent decisions by the CJEU and the ECHR may at first blush appear to challenge the deferential approach. Both the CJEU's decision in *Schrems v. Data Protection Commissioner*[252] and the ECHR's decision in *Zakharov v. Russia*[253] resulted in the invalidation of regimes that, according to each court, failed to provide adequate safeguards for privacy. Each decision is notable in its insistence that deference cannot be absolute and that any program that authorizes or permits access to personal information by intelligence agencies must have safeguards. However, as this Article points out, *Schrems* dealt only with an important but limited EU agreement on commercial data sharing, not with individual EU states' surveillance programs, which lie beyond the CJEU's jurisdiction. *Zakharov* struck down a surveillance program in Vladimir Putin's Russia that was so fundamentally out of step with the rule of law that the case's relevance is questionable for other states, such as France and the United Kingdom, with more robust democratic traditions and current systems of accountability.

a. *Schrems v. Data Protection Commissioner* and the Need for a More Privacy-Friendly Transatlantic Data-Sharing Agreement

In *Schrems*, the CJEU found that an agreement allowing EU firms to share EU residents' private data with U.S. firms lacked adequate privacy protections.[254] The *Schrems* decision invalidated the so-called "Safe

251. *See* SCHNEIER, *supra* note 2, at 132 (discussing the attribution of responsibility for cyber intrusions based on forensic analysis).

252. Case C-362/14, 2015 E.C.R.

253. Eur. Ct. H.R. paras. 147, 300–04 (2015).

254. Case C-362/14, *Schrems*, at I-4. For commentary on *Schrems*, see Francesca Bignami

Harbor" agreement, under which private firms in Europe could share customer information with U.S. firms to facilitate transnational business transactions.[255] Under the Safe Harbor agreement, U.S. firms self-certified that they had implemented privacy principles, and the U.S. Federal Trade Commission's Consumer Protection Bureau policed firms' privacy practices.[256] The Safe Harbor agreement also included a conclusive presumption that data sharing pursuant to the agreement complied with the privacy protections in Article 25 of the European Charter on Fundamental Rights and Freedoms.[257] This conclusive presumption insulated Safe Harbor from privacy challenges mounted by individual state data-protection authorities.

The *Schrems* case arose after Snowden's revelations when Maximilian Schrems, a law student and Austrian national who maintained a Facebook account governed by a contract with Facebook Ireland, took steps to prevent the transfer of his personal information to the United States.[258] Schrems asked Irish data-protection authorities to stop the transfer of his data. Irish authorities refused, citing the Safe Harbor's presumption of compliance with EU law.[259] The High Court of Ireland affirmed the data commissioner's decision.[260] However, the High Court was concerned that Safe Harbor might violate the European Charter. Accordingly, the High Court referred the case to the CJEU.[261]

The CJEU struck down the conclusive presumption that data shared under Safe Harbor received all of the protections required under EU law,

---

& Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation* 131–32 (George Washington Univ. Pub. Law, Research Paper No. 2015-52, 2015), http://ssrn.com/abstract=2705601 (praising CJEU's upholding of privacy principles); Scott J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's* Schrems *Decision and What It Means for Transatlantic Relations*, SETON HALL J. DIPL. & INT'L REL. (forthcoming 2016) (manuscript at 3), http://ssrn.com/abstract=2680263 (critiquing the decision as failing to offer an accurate account of U.S. intelligence collection); Peter Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, at 10–18 (Ga. Tech. Scheller Coll. of Bus., Research Paper No. 36), http://ssrn.com/abstract=2709619 (pointing out mischaracterizations of U.S. programs such as Section 702 in an opinion on Safe Harbor by EU Advocate General Bot, which CJEU relied on in its opinion).

255. Case C-362/14, *Schrems*, at I-3, I-31.

256. *Id.* at I-9.

257. *Id.* at I-9 to -10.

258. *Id.* at I-19; Juliet Fioretti & Georgina Prodhan, *Schrems: The Law Student Who Brought down a Transatlantic Data Pact*, REUTERS (Oct. 6, 2015, 4:29 PM), http://www.reuters.com/article/us-eu-ireland-privacy-schrems-idUSKCN0S02NY20151006; *cf.* Mieke Eoyang, *Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance* 11–12 (Hoover Inst. Essay Series Paper No. 1603, 2016) (Apr. 2016) (discussing EU indignation about U.S. surveillance post-Snowden that led up to *Schrems* decision).

259. Case C-362/14, *Schrems*, at I-19.

260. *Id.* at I-19 to -20.

261. *Id.* at I-21.

holding that state data-protection authorities could challenge Safe Harbor as not offering an "adequate level of protection" to individuals' private personal information under Article 25 of the European Charter.[262] To support its holding, the CJEU cited Snowden's revelations, asserting that Safe Harbor did not adequately protect individuals' data from the full extent of collection and surveillance by U.S. intelligence agencies.[263] In particular, the CJEU noted that the Safe Harbor agreement did not include a finding that U.S. intelligence agencies, in the course of pursuing concededly "legitimate" objectives, such as national security, had adopted rules to curb "interference" with the privacy rights of EU citizens.[264] The CJEU also cited concerns expressed by the European Commission after the Snowden disclosures that U.S. access to "personal data" exceeded what was "strictly necessary and proportionate" to fulfill those legitimate national security objectives.[265] *Schrems* has structural, substantive, and procedural ramifications for any future EU–U.S. data-sharing agreement.

i. Structure in *Schrems*

The CJEU's decision creates significant collective action problems in the EU by weakening the ability of the EU to agree to terms with the United States on data sharing. Any agreement would have to contain express acknowledgment that the U.S. government, including its security agencies, had enacted safeguards on the use of EU subjects' personal data.[266] Moreover, even if the agreement included a specific description of U.S. government safeguards, *Schrems* seems to leave open the possibility that EU member state data commissioners could challenge the agreement as not providing protections that are "equivalent" to those that the EU provides.[267] Any U.S.–EU agreement would then be subject to a holdout problem, since any single EU member state's data privacy authority could delay the agreement and ask that the CJEU invalidate it.

---

262. *Id.* at I-25.

263. *Id.* at I-31.

264. *Id.* at I-30.

265. *Id.* at I-31 to -32.

266. *See infra* notes 371–78 and accompanying text (discussing prospects for the U.S. enactment of the Judicial Redress Act, which would provide EU residents with protections extended to U.S. persons in the Privacy Act, such as recourse, with exceptions for national security and law enforcement needs, against agencies that improperly collected, retained, or disseminated personal information).

267. *See* Case C-362/14, *Schrems*, at I-33. Ironically, because Safe Harbor provided for review of U.S. participating firms' privacy policies by the U.S. Federal Trade Commission, difficulties in implementing a replacement for Safe Harbor may leave EU residents with *fewer* privacy protections. *See* Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post* Schrems 11, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346.

Imagine if the Framers of the U.S. Constitution had required a unanimous vote from Congress to enact legislation. That chaotic situation was exactly what the Framers wished to overcome when they drafted a Constitution with a strong federal government and robust limits on individual states' power to engage in foreign affairs.[268] *Schrems* appears to invite comparable chaos.

On the structural front, bilateral agreements between states could furnish a "fix" for *Schrems*. The CJEU interprets EU law, which expressly disclaims authority over member states' national security and law enforcement legislation.[269] This carve-out for individual states is part of the bargain that created the European Union. As a consequence, the United States or U.S. firms could reach bilateral agreements or conclude contracts with each member state.[270] The United States has engaged in a similar bilateral strategy in dealing with the International Criminal Court (ICC), concluding agreements with almost one hundred states that they will not refer cases to the ICC involving U.S. personnel conducting activities within those states' borders.[271] However, such agreements are problematic in a number of respects.

First, bilateral agreements can be cumbersome to negotiate[272] and may not be fully binding,[273] particularly if new revelations about U.S. collection practices fuel claims that circumstances have arisen that were not contemplated by the agreements' drafters or included in the agreements' text. Second, even if the CJEU would not have jurisdiction over any such agreements, the ECHR would have jurisdiction over claims that the agreements violated the privacy protections in the European

268. James Madison had warned that the weak federal government of the Articles of Confederation period allowed "any indiscreet member [state] to embroil the confederacy with foreign nations"). *See* THE FEDERALIST No. 42, at 281 (James Madison) (Jacob Ernest Cooke ed., 1961).

269. *See* Case C-362/14, *Schrems*, at I-10 to -12 (citing EU Data Protection Directive, Preamble, 13th recital). "[A]ctivities [such as]... public safety, defence, State security or . . . criminal laws fall outside the scope of [European] Community law . . . ." EU Data Protection Directive, Preamble, 13th recital. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 281) 2.

270. *See* Shackelford, *supra* note 254, at 4 (warning that absent reaching an agreement that will satisfy all EU members and the CJEU, companies will have to resort to "expensive and time-consuming model contracts or other agreements to continue transatlantic data transfers").

271. Stuart W. Risch, *Hostile Outsider or Influential Insider? The United States and the International Criminal Court*, 2009 ARMY LAWYER 61, 80–81 (2009) (noticing that "[t]hese bilateral accords certify that neither signing state will arrest, extradite, or otherwise surrender the other's personnel to the Court").

272. *See* Shackelford, *supra* note 254, at 4.

273. *See* Risch, *supra* note 271, at 82 (stating that "the Bilateral Immunity Agreements (BIAs) do *not* bind the ICC in any way").

Convention on Human Rights.[274] The ECHR might be skeptical of such agreements, viewing them as an expedient rather than a principled approach worthy of deference. Third, and relatedly, U.S. circumvention of *Schrems* might ultimately lead to a diminution in America's "soft power": its ability to persuade other nations of the rightness of its positions through its leadership role.[275] Fourth, political and legal crosscurrents in various EU member states might make the conclusion of such agreements difficult, recreating the holdout problem mentioned above. For example, suppose all states agreed except for Germany. Given Germany's dominant position in Europe's economy, a regime of bilateral agreements that did not include Germany would hardly be worth the cost.

ii. *Schrems* and the Interplay of Substance and Procedure

Because the individual and bilateral fixes for *Schrems* involve significant uncertainty, it is worthwhile to ponder *Schrems*'s substantive and procedural lessons. The CJEU does not clearly separate its substantive and procedural concerns. This Article does so here, with the proviso that both *Schrems*'s posture and the decision's lack of clear separation between substantive and procedural aspects suggest flexibility on the part of the Court that belies the strict privacy-protective rhetoric of the decision.[276]

The posture of the *Schrems* decision leaves the door open to a more flexible approach, since the decision addresses only the threshold

---

274. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(1), Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter Convention for the Protection of Human Rights] ("Everyone has the right to respect for his private and family life, his home and his correspondence."); *id.* art. 8(2) ("There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

275. *See* Risch, *supra* note 271, at 66 (discussing how the United States' bilateralist approach to avoiding jurisdiction of ICC has been costly to America's global reputation and to necessary collaboration with other states); *see also* JOSEPH S. NYE, JR., THE PARADOX OF AMERICAN POWER 35 (2002) (arguing that a failure by the United States to build global consensus will result in the loss of "important opportunities for cooperation in the solution of global problems such as terrorism"); *cf.* Harold Hongju Koh, *On American Exceptionalism*, 55 STAN. L. REV. 1479, 1480 (2003) (highlighting international perception that the United States believes that its global role creates entitlement to exceptions from human rights and other norms).

276. *See* Bignami & Resta, *supra* note 254, at 129 (noting the *Schrem* court's "hardening stance on the right to personal data protection"); *cf.* Google Spain v. Spanish Data Prot. Agency & Costeja, 2014 I.C.J. paras. 20, 99 (May 13) (finding a "right to be forgotten" based on EU privacy guarantees that require internet search firms such as Google to heed requests to delete irrelevant, outdated, and prejudicial material from searchable online data upon an application by an aggrieved party).

question of whether Safe Harbor could bar challenges by individual state data-protection authorities. The CJEU held only that the Safe Harbor agreement was invalid because it wrongly *presumed* U.S. compliance with the European Charter and thus unlawfully precluded challenges by individual EU state data-protection authorities. In the course of supporting that holding, the CJEU engaged in a preliminary and somewhat imprecise discussion of U.S. surveillance in the wake of Snowden's disclosures. However, the CJEU did not rule on any substantive challenge brought by state data-protection authorities. No such challenge was before the court. Instead, the CJEU merely indicated that the Safe Harbor agreement did not provide sufficient safeguards to preclude such a challenge. Viewed in this context, the CJEU's substantive discussion was at best support for a threshold finding that the agreement lacked adequate assurances. A more comprehensive analysis by the court of how U.S. intelligence collection—including post-Snowden reforms[277]—meshed with EU law would have to await adjudication of a challenge brought by state data-protection commissioners.[278]

Turning to the substance of EU privacy protections, the CJEU suggested that U.S. government access to EU residents' data had to be "strictly necessary and proportionate" to the U.S. interest in national security and law enforcement.[279] Yet what this standard might mean in a particular case, including *Schrems* itself, is not exactly clear from the CJEU opinion. The court does not undertake a concrete analysis of major U.S. collection and surveillance programs, including Section 702, EO 12,333, or the domestic collection of metadata. Indeed, the CJEU does not even mention that Congress, in the USA Freedom Act, had enacted a fundamental change in the metadata program as it was authorized prior to Snowden's disclosures, leaving data in private firms' hands subject to specific government requests that the FISC had to approve in advance.[280] The CJEU also did not address the limits in Section 702 or those imposed as part of the United States' PPD-28 process.

Instead of engaging in a specific analysis of U.S. collection and surveillance law, the court appeared to rely on concerns expressed by the European Commission and a Working Group established by the

277. *See* Swire, *supra* note 254, at 10–21 (discussing how the media has misclassified U.S. intelligence collection reforms under Section 702 and how they provide much more protection and oversight than widely believed).

278. The CJEU could also consider an appeal by an individual from a decision by state authorities finding as a substantive matter that the U.S. provided protections equivalent to those in the EU.

279. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-31 to -32.

280. *See* Swire, *supra* note 254, at 26 ("This approach was codified in the USA Act, passed in 2015, which also prohibited the bulk collection of telephone metadata and required the queries to be submitted with court approval to the providers.").

Commission.[281] However, the Commission documents predate passage of the USA Freedom Act and the PPD-28 process.[282] This makes for an unfortunate gap in the court's analysis.

Moreover, even insofar as the EU Commission documents referred to in *Schrems* deal with pre-Snowden collection and surveillance, those documents do not comprehensively address substantive limits that were already in place. For example, the Commission documents cross-referenced in the *Schrems* decision highlight one issue under Section 702: the statutory allowance for collection of information relating to the "foreign affairs" of the United States.[283] The Commission Working Group, as well as privacy advocates on both sides of the Atlantic, viewed this provision as permitting the broad-based collection of information on *any* individual or entity, private or public, that in some attenuated way affects U.S. foreign relations. Viewed in that light, of course, the "foreign affairs" prong of Section 702 would render the other, more specific provisions of the statute meaningless. However, both the provision's text and its apparent application suggest a far narrower meaning.

Section 702 allows collection of intelligence "with respect to a foreign power or foreign territory" relating to the "the conduct of the foreign affairs of the United States."[284] In U.S. intelligence law, the term "foreign power" refers to a foreign government or a non-state entity such as Al Qaeda or ISIS that holds itself out as fulfilling the functions of a state,

---

281. *See* Case C-362/14, *Schrems*, at I-16 to -18.

282. *Id.* at I-17 (noting that EU Commission documents were issued on November 27, 2013, before the announcement or implementation of U.S. reforms).

283. 50 U.S.C. § 1801(e)(2)(B) (2012); see also Peter Margulies, Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy, 72 WASH. & LEE L. REV. 1283, 1285 (2015) ("The 'foreign affairs' language . . . is not a residual clause authorizing all the collection and surveillance precluded by other definitions in the statute. It simply allows the United States to gather information relating to other states' compliance with norms and the prospects for international cooperation on enforcement."). But see Claude Moraes (Rapporteur), Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, 7–8, 11, E.N. Doc. 2013/2188(INI) (Jan. 8, 2014), http://www.statewatch.org/news/2014/jan/-draft-nsa-surveillance-report.pdf (acknowledging analogous exceptions in a report issued before President Obama's speech in January 2014, but arguing that NSA surveillance could be "used for reasons other than national security and the... fight against terrorism, for example economic and industrial espionage or profiling on political grounds" and was not "necessary and proportionate" vis à vis exceptions); Timothy Edgar, Focusing PRISM: An Answer to European Privacy Concerns?, LAWFARE (Oct. 10, 2015), https://lawfareblog.com/focusing-prism-answer-european-privacy-concerns (arguing for narrowing Section 702); Elizabeth Goitein & Faiza Patel, What Went Wrong with the FISA Court, BRENNAN CTR. FOR JUST. 27 (Mar. 18, 2015), https://www.brennancenter.org/publication/what-went-wrong-fisa-court (critiquing Section 702 "foreign affairs" provision).

284. 50 U.S.C. § 1801(e)(2)(B).

including defense.[285] Under established principles of construction, the indefinite article "a" preceding "foreign power" also modifies "foreign territory." Bear in mind that courts generally disfavor superfluity in statutory interpretation.[286] If "foreign territory" had the capacious meaning contemplated by privacy advocates, that broader definition would render the preceding statutory term "foreign power" superfluous. There would be no point in expressly authorizing collection "with respect to a foreign *power*" if Congress had already authorized *any* collection that happened to entail a person or entity located outside the United States. To give the term "foreign power" any meaning under the statute, one must also give the term "foreign territory" a more circumscribed meaning than the catch-all connotation that privacy advocates fear.

Viewed in this light, Section 702's authorization of collection regarding a "foreign territory" contemplates two narrowly circumscribed situations. The first connotes a *specific* unit of land that a foreign power has annexed, as Puerto Rico is a territory of the United States. The second use of "territory" entails a specific area that is legally under the sovereign jurisdiction of a foreign power, but as a practical matter that power does not control it (this might describe certain activities within "failed" or "failing" states such as Yemen). Each version or a combination of both ensures some independent meaning for both "foreign power" and "foreign territory," and therefore complies with the canon disfavoring superfluity.

In practice, moreover, the U.S. interpretation of "foreign affairs" includes a more circumscribed definition focusing on foreign governments: activities regarding international agreements, including bribery, collusion, and even the formation of negotiating positions on matters such as sanctions for state sponsors of terrorism.[287] While this information is sensitive, its collection is consistent with longtime international understandings that espionage is not a violation of international law.[288]

---

285. *Id.* § 1801(a) (describing "foreign power" as a "foreign government," a "faction of a foreign nation or nations," an "entity . . . openly acknowledged by a foreign government . . . to be directed and controlled by" a foreign government or governments, or a terrorist group, "foreign-based political organization," an entity "directed and controlled by a foreign government or governments," or an entity "engaged in the international proliferation of weapons of mass destruction").

286. *See* Gluck & Bressman, *supra* note 201, at 934–35 (noting that "the *political interests* of the audience often demand redundancy"); *supra* notes 199–204 and accompanying text (discussing avoiding superfluity in interpreting ICCPR).

287. *See, e.g.*, Charlie Savage, *Book Reveals Wider Net of U.S. Spying on Envoys*, N.Y. TIMES (May 12, 2014), http://www.nytimes.com/2014/05/13/world/middleeast/book-reveals-wider-net-of-us-spying-on-envoys.html (discussing the NSA's role in the diplomatic negotiations leading up to Iran sanctions).

288. *See* Paust, *supra* note 245, at 647 ("Also complicating rational and policy-serving

However, to stem the European concern voiced in *Schrems*, Congress and the Executive Branch should consider either amending the "foreign affairs" prong to promote greater clarity and specificity or conveying an executive branch interpretation in public or private that would vindicate these goals. For example, administration officials could assure their EU counterparts that Section 702 would not permit spying on individual EU residents for purposes that would be barred under EO 12,333, such as suppressing speech critical of the United States; discriminating against racial, religious, or ethnic groups; or gaining a competitive advantage for U.S. companies.[289] These assurances might allay the fears expressed in *Schrems*. Such an effort would be worthwhile as part of the overall process of enhancing transparency that is key to PPD-28.

On the question addressed in this Article—the legality of machine (as opposed to human) access to data—*Schrems* is ambiguous. On the one hand, the court seemed most concerned with the "storage" of data, not with a computer's scanning of such information.[290] Ironically, however, given the court's taking the United States to task for its purported failure to limit surveillance, the court's own description of U.S. programs takes a shotgun approach. That approach breeds uncertainty about the true scope of the CJEU's critique. The CJEU's broad characterization of U.S. intelligence efforts does not fit U.S. intelligence agencies' relatively limited *storage* of transnational communications under Section 702 but may be more accurate as a description of U.S. machine *scanning*.

For example, the *Schrems* court asserted that U.S. intelligence collection entailed

> storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities.[291]

This harsh indictment does not resemble the Section 702 Upstream program. Upstream *scans* a wide range of transatlantic communications as they pass through buffers or caches in communications hubs.[292] Nevertheless, Upstream *entails storage* of only a limited number of

---

choice is the widespread recognition that espionage engaged in by a state within a foreign state can violate the latter's domestic law, but widely practiced espionage regarding foreign state secrets is not a violation of international law.").

289. *See* PPD-28, *supra* note 27, at 3–6.

290. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-32.

291. *Id.*

292. *See* Swire, *supra* note 254, at 18.

communications that are to, from, or about particular selectors linked to Section 702 categories, such as terrorism, espionage, and the limited "foreign affairs" prong discussed above.[293] Perhaps the CJEU viewed scanning and storage as identical intrusions on privacy. However, a court drawing that conclusion should have justified its equation of scanning and storage, which engender disparate risks of human overreaching.

Finally, *Schrems* has a procedural component that builds on the CJEU's prior decision in *Digital Rights Ireland*.[294] Procedurally, *Schrems* calls for two attributes discussed in the normative section of this piece: independent review of surveillance policies and recourse for those victimized by such policies. As the CJEU noted, "The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law."[295] To be effective, the reviewing body must be independent of the agencies whose policies it purports to review. Moreover, each individual should have the right of "access to personal data relating to him" and the right "to obtain the rectification or erasure of such data."[296] In other words, an individual should have a remedy when a government has collected, stored, or disseminated that individual's data wrongfully.

Schrems's emphasis on procedure suggests that there may be a sliding scale with respect to the relationship between substantive and procedural rights and some flexibility within the category of procedural rights.[297] The *Schrems* court might in future cases tolerate more substantive flexibility for U.S. intelligence collection on EU residents in exchange for tighter procedural safeguards. The prospect of independent review, even on a more relaxed substantive standard, would discipline U.S. intelligence agencies, reducing the prospect of egregious intrusions on privacy. The salutary discipline provided by procedural safeguards might assure the CJEU that the rule of law would be observed, permitting a more relaxed reading of the substantive strict-necessity standard. Broader machine collection accompanied by robust restrictions on analysts' access to and use of data might pass muster. That trade-off might actually work better than insisting on a specific level of both substantive and

293. *See id.* at 22 (explaining that the "total number of individuals targeted under Section 702 in 2013 was 92,707, a tiny fraction of total EU or global Internet users").

294. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Comm'r, 2014 E.C.R.

295. Case C-362/14, *Schrems*, at I-33.

296. *Id.*

297. In a familiar example of a sliding scale, courts trade off the irreparability of harm, balance of hardships between the parties, and probability of success on the merits in considering whether to grant a preliminary injunction. *See* Dataphase Sys. v. CL Sys., 640 F.2d 109, 113 (8th Cir. 1981); Jared A. Goldstein, *Equitable Balancing in the Age of Statutes*, 96 VA. L. REV. 485, 487 (2010) (discussing the balance of equities test); *cf.* MATTHEW BENDER, 13 MOORE'S FEDERAL PRACTICE § 65.22(5)(b)–(i) (2015) (analyzing tests in different federal appellate tribunals).

procedural safeguards. Moreover, independence in review mechanisms could be subject to a sliding scale. Administrative, as opposed to judicial review, would be appropriate if the administrative review came with appropriate guarantees of independence, the power to obtain necessary information from intelligence agencies in the course of providing oversight, and the authority to provide necessary relief to enforce compliance with legal requirements.[298]

In February, 2016, the EU and the United States announced a new proposed data-sharing agreement, Privacy Shield, with greater clarity on U.S. substantive and procedural protections of personal data.[299] In the new agreement, the U.S. pledged to create an Office of the Ombudsperson in the State Department to respond to EU complaints about data privacy.[300] As a State Department official, the proposed ombudsperson would be officially separated from intelligence agencies in other U.S. cabinet departments. That separation is an encouraging sign in establishing the independence that *Schrems* mandated. However, like all State Department officials, the ombudsperson would serve at the pleasure of the President. Moreover, the February, 2016 proposal was vague about the precise powers of the ombudsperson, including her access to U.S. intelligence data.[301] Clear description of such powers would be a threshold condition for Privacy Shield's compliance with *Schrems*.[302]

b. *Zakharov v. Russia*: Putin as the Elephant in the Room

The ECHR's decision in *Zakharov v. Russia*, unlike *Schrems*, deals directly with the national security and law enforcement regimes of a particular state.[303] The ECHR in *Zakharov* reiterated its overarching view

298. *See* Zakharov v. Russia, Eur. Ct. H.R., para. 147 (2015) (noting that under CJEU case law review can be by either a "court or by an independent administrative body").

299. *See* EC Adequacy Decision, *supra* note 35; Letter from Robert S. Litt, Gen'l Counsel, Office of the Dir. of Nat'l Intelligence, to Justin S. Antonipillai, U.S. Dep't of Commerce and Ted Dean, Dep. Ass't Sec'y, Int'l Trade Admin. (Feb. 22, 2016) (hereinafter ODNI Letter), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

300. *See* EC Adequacy Decision, *supra* note 36, at 26.

301. This vagueness spurred criticism of the proposed Privacy Shield agreement by EU data protection officials. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision* (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

302. Both the ECHR and the CJEU have found in a different context—the fairness of procedures for designating individuals as terrorist financiers and blocking their assets—that an ombudsperson is not a substitute for more formal judicial review. *See* Al-Dulimi v. Switzerland, (Eur. Ct. Hum. Rts. 2016); Kadi v. Eur. Comm'n (European Court of Justice 2013).

303. *See* Zakharov v. Russia, Eur. Ct. H.R., paras. 1, 3 (2015) ("The applicant alleged that the system of secret interception of mobile telephone communications in Russia violated his right to respect for his private life and correspondence and that he did not have any effective remedy in

that states are entitled to a "margin of appreciation" from the courts on the validity of national security surveillance.[304] In finding that Russia's provisions for domestic surveillance did not comply with Article 8 of the European Convention on Human Rights, the ECHR relied on factors that are specific to Vladimir Putin's Russia.[305] Although some have read *Zakharov* as having broader implications,[306] the court's holding flows largely from glaring flaws in the Russian framework for review of domestic surveillance requests.

The Russian framework found wanting in *Zakharov* combined a robust capacity on the part of Russian authorities to access virtually all domestic telecommunications data[307] with very weak oversight of how law enforcement exercised that capacity. As the court noted, the Russian statute expressly bars a court considering surveillance requests from asking law enforcement authorities for information about undercover operatives or police informants or about how authorities will execute a particular search.[308] These limits on independent oversight effectively made a law enforcement agency the judge of its own case. Deprived of the power to seek information about the reliability of informants or the actual conduct of a proposed search, the reviewing court lacked "sufficient factual basis" for effective oversight.[309] Moreover, although the ECHR noted that the Russian Constitutional Court had held that a reviewing court must find at least a "reasonable suspicion" that a criminal offense has been committed,[310] Russian law and practice did not require that courts of general jurisdiction follow this decision.[311]

---

that respect.").

304. *Id.* at para. 232.

305. *Id.* at paras. 302–05 ("It is significant that the shortcomings in the legal framework as identified above appear to have an impact on the actual operation of the system of secret surveillance which exists in Russia."). Shortly after *Zakharov*, the ECHR reached a similar decision regarding surveillance in Hungary, a former Iron Curtain state with a legal system that suffers from fundamental flaws comparable to Russia's. *See* Szabo v. Hungary, Eur. Ct. H.R. (2016).

306. *See* Carly Nyst, *European Human Rights Court Deals a Heavy Blow to the Lawfulness of Bulk Surveillance*, JUST SECURITY (Dec. 9, 2015, 11:15 AM), https://www.justsecurity.org/28216/echr-deals-heavy-blow-lawfulness-bulk-surveillance/ (suggesting parallels between Russian and United Kingdom surveillance programs); Lorna Woods, Zakharov v. Russia: *Mass Surveillance and the European Court of Human Rights*, EU L. ANALYSIS (Dec. 16, 2015), http://eulawanalysis.blogspot.com/2015/12/zakharov-v-russia-mass-surveillance-and.html (same).

307. *Zakharov*, at paras. 111, 116 (discussing "remote-control" access to data by law enforcement agencies).

308. *Id.* at paras. 37, 261.

309. *Id.* at para. 261.

310. *Id.* at para. 262.

311. *Id.* at para. 263.

The ECHR found that the actual practice of Russian courts entailed merely *pro forma* review.[312] The ECHR noted that law enforcement agency requests routinely lacked *any* supporting materials, that courts "never" requested such materials, and that a mere passing "reference" to national security justifying a search was usually enough to grant a law enforcement agency's request.[313] Moreover, law enforcement authorities were not required to show the *pro forma* approval to telecommunications providers before conducting surveillance.[314] This Potemkin village version of oversight, according to the ECHR, all too predictably led to rampant "arbitrary and abusive surveillance practices."[315] The Russian judge on the ECHR, Judge Dmitry Dedov, concurred in the majority's assessment, observing that a "widespread suspicion" is prevalent among Russia's population that surveillance extends to "human-rights activists, opposition activists and leaders, journalists," and all others "involved in public affairs."[316]

This focus on the special problems posed by Putin's despotic security apparatus limits *Zakharov*'s utility as a template for analysis of surveillance systems in European democracies. However, insistence on crucial safeguards such as independent review will likely figure in those future decisions.

B. *Deferential Proportionality and Article 17 of the ICCPR*

To fashion a standard for assessing a state's machine surveillance, one can combine arguments for reasonable, but not absolute, deference to Article 17's language, which bars "arbitrary" intrusions on privacy.[317] Some form of proportionality review is common in international and human rights cases and may also apply in the case of Article 17.[318] The

312. The ECHR made these findings without expressly mentioning the elephant in the room: Russian President Vladimir Putin, whose commitment to legal niceties such as the separation of powers is open to question. However, that unspoken presence is an important element of *Zakharov*'s context. That element is absent in pending surveillance cases involving the United Kingdom or other states, whatever the excesses.

313. *Zakharov*, at para. 263.

314. *Id.* at para. 269.

315. *Id.* at para. 303.

316. *Id.* at pt. 4 (Dedov, J., concurring).

317. *See* CCPR General Comment No. 16: Article 17 (Right to Privacy), U.N. Human Rts. Comm., The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 32d Sess., para. 1 (Apr. 8, 1988).

318. The Human Rights Committee, which is designated by the United Nations to receive reports from member states on compliance with the ICCPR, has recently advised the United States that intrusions on privacy are subject to "the principles of legality, proportionality and necessity." ICCPR, *supra* note 7, at 10; *cf.* Emmerson, *supra* note 12, at 16 & n.34 (discussing proportionality). To comply with the legality requirement, states must provide individuals with some level of guidance about the state's surveillance practices, although states need not provide

applicable level of proportionality review should be flexible while remaining cognizant of core privacy protections.

Under the Vienna Convention on the Law of Treaties, commonly understood meanings of the term "arbitrary" should inform the type of proportionality review applied.[319] Dictionaries define the term "arbitrary" as referring to an action or decision that is "capricious, unreasonable, [or] unsupported."[320] While this definition does not preclude application of a proportionality standard, it suggests that the standard applied must be capacious enough to uphold a range of reasonable state decisions.[321]

A deferential account of proportionality would be consistent with Article 17's arbitrariness standard and with the reasons for deference outlined above.[322] For an example of a deferential application of proportionality, consider the ECHR's decision in *Zana v. Turkey*[323] interpreting the European Convention's free speech provision, Article 10.[324] Article 10 expressly permits content-related curbs on free speech when those are necessary to protect national security and public safety.[325] The court upheld the criminal conviction of a public official who had described the Kurdistan Workers' Party (PKK), a Kurdish insurgent group, as "legitimate"—Turkey and other states, including the United States, designate the PKK as a terrorist organization.[326] The ECHR cited "serious disturbances" relating to Kurdish insurgency in Turkey.[327] Moreover, the court interpreted necessity in a relaxed fashion. Even

---

notice that will allow targets of surveillance to "adapt" their behavior and thereby frustrate state efforts. *See* Kennedy v. United Kingdom, 52 Eur. H.R. Rep. para. 152 (2010).

319. Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S.

320. *See* David Sloss, *Using International Law to Enhance Democracy*, 47 VA. J. INT'L L. 1, 18 n.76 (2006).

321. *Cf.* Paust, *supra* note 245, at 633–34 (viewing proportionality as reasonable balancing of rights and "just requirements of morality, public order and the general welfare in a democratic society" (quoting Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/810, at art. 1 (1948))).

322. For an example of such a standard, see Martin Lutern, *The Lost Meaning of Proportionality*, *in* PROPORTIONALITY AND THE RULE OF LAW: RIGHTS, JUSTIFICATION, REASONING 21, 34 & n.39 (Grant Huscroft, Bradley W. Miller & Gregoire Webber eds., 2014) (discussing the need for the ECHR to show deference in terrorism-related cases brought under the European Convention on Human Rights to minimize future violations of human rights by non-state actors; the European Convention, tellingly, does not expressly include the ICCPR's arbitrariness language but, according to the author, should nonetheless be read as incorporating a relaxed proportionality standard); *cf. id.* at 35 (noting the frequency of cases that hinge on "many subjective features of particular states and societies, of which a reviewing court (especially an international court) will have no significant knowledge").

323. 27 Eur. H.R. Rep. 667 (1997).

324. *Id.* at 678–81.

325. Convention for the Protection of Human Rights, *supra* note 274, at 11.

326. *Zana*, 27 Eur. H.R. Rep. at 667–68, 679.

327. *Id.* at 688.

though the official's statement in support of the PKK was ambiguous, since the official opposed the targeting of civilians, the court viewed his conviction as "necessary" to deal with the "pressing social need."[328] Citing the margin of appreciation, the EHCR held that preventing speech favorable to terrorist groups was "proportionate" to legitimate state aims.[329] The ECHR arrived at this conclusion despite the absence of evidence that the speech at issue caused any concrete violence.[330] A similar standard should apply to overseas machine surveillance.

C. *Applying the Deferential Proportionality Standard*

Even a relaxed proportionality standard should have some bite. Absolute deference would provide no check on the false positives that rightly worry privacy advocates. To address this concern, machine surveillance should be tailored to compelling state purposes, scientifically validated, and subject to independent review. This Section discusses each safeguard in turn.

1. The Purpose of Machine Surveillance

A deferential proportionality inquiry on machine surveillance would regard national security as an adequate justification. This would include machine surveillance for the purposes listed in PPD-28: counterterrorism, counterespionage, antiproliferation of WMDs, cybersecurity, international crime, and sanctions evasion.[331] Moreover, a deferential proportionality standard would reject the equivalency thesis's conflation of a state's own nationals (or others within its borders) with persons abroad. Instead, a deferential reading of proportionality would credit a state's need to engage in surveillance abroad,[332] particularly given the

328. *Id.* at 690–91.

329. *Id.* at 691.

330. In citing *Zana*, this Article in no way suggests that the United States should second-guess the more robust protections built into the First Amendment. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 39 (2010) (holding that Congress could prohibit speech directed by or coordinated with foreign terrorist groups, but observing that the First Amendment protects speech involving domestic groups as well as speech that is independent of foreign terrorist organizations). The Article's sole point is to illustrate how the ECHR has applied a deferential proportionality standard.

331. *See* Kennedy v. United Kingdom, 52 Eur. H.R. Rep. para. 159 (2010) (accepting "national security" as an adequate justification for surveillance and noting that requiring more specific justification might impair states' efforts to safeguard national security). *But see* Frank La Rue (Special Rapporteur), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶¶ 53–54, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (cautioning about unduly broad use of national security as justification for surveillance); Emmerson, *supra* note 12, ¶¶ 11–13 (same).

332. *See* Weber v. Germany, 2006-XI Eur. Ct. H.R. para. 84.

difficulties of tracking overseas threats and the risk that terrorists will find safe havens in other countries. The ECHR case law also suggests that machine access to a substantial database of communications content may be appropriate as long as human access is restricted.[333] This principle would cover directed searches tailored to terrorism and autonomous searches based on data sets dealing with terrorism as long as those searches were properly validated.

However, a state could not engage in untrammeled bulk collection of content, even if human access were limited. Such untrammeled collection would be problematic under both the deontological and consequential branches of the first equivalency thesis. In a deontological sense, unfettered machine searches would undermine the perception of control that persons abroad have a right to expect. On a consequential level, unbridled access could cause harm given the amount of incorrect information in searched databases and human analysts' unawareness of or indifference to this problem.[334]

In an effort to accommodate LOAC, states would be allowed to use machine searches in other countries that are the site of an armed conflict involving the state conducting surveillance. That would authorize the United States to engage in bulk collection of content throughout Afghanistan. In countries without an armed conflict, a state would only be able to engage in more tailored bulk collection of content linked to a particular geographic area within that country where evidence indicated a substantial terrorist presence and where more targeted techniques indicated a spike in terrorist activity. In the Bahamas, for example, the United States could target drug or human traffickers, but it could not collect in bulk all other Bahamian communications content. Complying with this standard would represent a change from current reported U.S. policy. However, that change would be worthwhile in confirming the United States' devotion to constraints mandated by international human rights.

2. Reliability

A valid purpose for a search is of little help if the search is unreliable. Searches that are unreliable will yield too many false positives and thus intrude unduly on innocent individuals. Validation is necessary to avoid

333. *See id.* at para. 32 (noting that German authorities used keywords to search communications content).

334. *See* Latif v. Holder, 28 F. Supp. 3d 1134, 1152 (D. Or. 2014) (discussing "a 2009 report by the Department of Justice Office of the Inspector General that concluded that the TSDB contains many errors and that the TSC has failed to take adequate steps to remove or to modify records in a timely manner even when necessary").

this risk.[335] However, criteria for the reliability of machine searches should respect the transparency paradox, which holds that transparency in substantive explanations reduces the accuracy of the search.

Since autonomous search strategies such as neural networks or support vector machines use hidden layers to boost accuracy,[336] requiring a substantive explanation would entail foregoing the accuracy that hidden layers produce. That is a bad bargain. Instead of requiring analysts to dumb down searches, human rights law should permit analysts to offer a methodological explanation of their chosen search strategy. In other words, officials can justify their search by explaining the technical basis for the search and the criteria analysts have employed to validate the search technique. One could argue that a substantive, verbal test is important for other reasons: it requires officials to explain and justify their decisions, permits easy review of search criteria, and offers guidance for the public. In the domestic realm, parting with these attributes would be unwise and illegal. However, pivoting to a methodological explanation for *overseas* collection does not clash with the U.S. Constitution or human rights norms. Indeed, by promoting more accurate searches, permitting methodological explanations ensures that searches will be less arbitrary. At least in the overseas realm, that trade-off is worthwhile.[337]

The methodology used in the search requires validation. A search should yield more true positives (needles spotted in the haystack) than alternative methods, while limiting the number of false positives (handfuls of hay). In the national security surveillance context, the stakes are higher: false negatives that should have been spotted are terrorists who can commit acts of violence, while false positives who were mistakenly tracked do not merely promote inefficiency but constitute intrusions on individual privacy. Statisticians have developed a wealth of indicia to assess the accuracy of a search.[338] Four of these are precision (the number of true positives among the number of predicted positives); recall (the number of true positives identified as such by the search compared with the number of actual positives, including those not

335. *See* Hu, *supra* note 143, at 808–16 (discussing the *Daubert* standard).

336. *See supra* Subsection I.C.2.a.ii.

337. Granting states the flexibility to use methodological, not substantive, explanations for overseas computer searches is consistent with what Professor Paul Berman has called global legal pluralism. For more detail on global legal pluralism, see generally PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM (2012) (examining the difficulties of a legal pluralistic world where multiple legal regimes imposed by state, sub-state, transnational, supranational, and non-state communities may regulate one person); Paul Schiff Berman, *Global Legal Pluralism*, 80 S. CAL. L. REV. 1155 (2007) (recognizing that the existence of multiple, overlapping legal regimes causes conflict but arguing that this conflict can be beneficial to produce alternative ideas and provide a forum for communication among multiple communities).

338. *See* FLACH, *supra* note 80, at 56; WITTEN, *supra* note 1, at 174–77 (discussing various methods used to evaluate false positive versus false negative trade-off).

identified); the false negative rate for positives (the number of false negatives as a proportion of the total number of actual positives); and the false positive rate for negatives (the "false alarm" rate—the number of false positives as a proportion of the total number of actual negatives). Statisticians can plot these criteria against each other for a more refined assessment.

To illustrate precision and recall, consider a stylized example. Suppose software engineers have developed a program for recognizing celebrities on the streets of New York. Analysts test the program on a day in which an inordinate number of celebrities are present, such as Saturday Night Live's fortieth-anniversary bash. A video of Fifth Avenue includes nine actual celebrities, such as Beyoncé, Jay Z, and Kim Kardashian, along with dozens of anonymous pedestrians. The program identifies seven celebrities. Four of the identifications are correct, but three of the persons labeled as celebrities are actually random passers-by. The program's precision is 4/7, while its recall is 4/9.

This example highlights a challenge noted previously for machine searches for terrorists, as opposed to celebrities: the availability of adequate data. The celebrities are already identified. There may be questions at the margins, such as people who used to be celebrities but are now forgotten, or people who may be celebrities tomorrow but are still part of the pack today. At the core, however, good data exists, based on web searches, social media mentions, and the like. On the other hand, ISIS recruits cannot necessarily be individually identified; if they could, counterterrorism would be easier than it is. Indeed, identifying previously unknown terrorists is a prime purpose of machine searches. That creates a problem, at least for the recall criterion, which requires knowledge of the number of actual positives in the relevant statistical universe.[339] So the lack of data, which is a problem for the efficacy of a national security machine search in the first instance is also a problem in assessing the efficacy of the search.

Analysts can work around this obstacle by comparing machine searches to each other and to other search methods, using measures such as the false negative rate for positives and the false positive rate for negatives (the "false alarm" rate). For example, analysts could calculate such rates for a search based only on human intelligence sources, such as informants. Analysts could do similar calculations for the results of directed searches that used identifiers such as phone numbers to trace the contacts of suspected terrorists. Finally, analysts could compare the results for autonomous searches using hidden layers in a neural network.

339. *See* WITTEN, *supra* note 1, at 175.

False positives are likely to occur in human intelligence and in both types of machine searches. The human intelligence search relies on informants, who often have agendas of their own that can compromise accuracy.[340] For their part, directed searches include all contacts of suspected terrorists and sometimes (as in the Patriot Act domestic metadata program) include more "hops" (the contacts of the terrorists' contacts, once or twice removed).[341] False positives are certain here: suspected terrorists may talk to lawyers, journalists, and dry-cleaners, as well as other terrorists, and the terrorists' contacts (and the contacts of their contacts) may talk to even more innocent parties. Because of the difficulty of getting data to fuel autonomous searches, false positives are certain here as well. Nevertheless, an autonomous search might result in fewer false positives than other approaches.

Settling on one formula for validation would undermine the deference owed to the state conducting surveillance. Nevertheless, a couple of observations are in order. As a general matter, each search in the order listed (human, directed, and autonomous) should have a successively higher cumulative recall rate. In other words, a directed search should uncover actual positives missed by human intelligence, and an autonomous search should reveal actual positives missed in the sum of the first two searches. At the same time, the false positive rate for negatives (the "false alarm" rate: false positives as a proportion of total actual negatives) should remain within two standard deviations of the previous search for each successive search. Again, this approach is not the only appropriate validation strategy, but it suggests an overall approach that would comply with human rights norms.

3. Review

Another cornerstone in the human rights architecture of surveillance is review by an independent body. Review includes several elements, including independence, notice to those potentially affected by surveillance, rules regarding retention of irrelevant information, and redress for those whose information was collected or retained arbitrarily. This Article addresses each in turn.

a. Independence

The biggest post-Snowden development in human rights law regarding surveillance has been the CJEU's insistence on independent

340. *See* Ellen Yaroshefsky, *Cooperation with Federal Prosecutors: Experiences of Truth Telling and Embellishment*, 68 FORDHAM L. REV. 917, 937 n.89 (1999) ("Most prosecutors distinguish informants from cooperators and believe that informants have even greater incentives to lie than cooperators because, not only are they 'working off' cases, but their entire livelihood is dependent on the Drug Enforcement Administration (DEA).").

341. *See* Kris, *supra* note 51, at 219 (explaining "hops").

review of data retention and access in *Schrems* and *Digital Rights Ireland*.[342] The CJEU did not specifically address national security surveillance, ruling only that the comprehensive EU data retention regime violated fundamental rights.[343] However, in its ruling, the court highlighted the importance of independent review.[344] Indeed, the CJEU found that "automatic processing" of data created an additional risk of abuse in the absence of independently enforced safeguards on access to the information retained.[345] This emphasis on independent scrutiny has featured prominently in European human rights cases. In *Kennedy v. United Kingdom*,[346] the ECHR noted that the United Kingdom had established an Investigatory Powers Tribunal (IPT), which the ruling party protects from interference.[347] In *Weber v. Germany*, the ECHR noted that Germany relies on an independent agency, the G10, to review surveillance.[348]

The United States provides for independent judicial review of most domestic law enforcement searches and has done so since the Constitution's enactment, but that framework has two gaps, one serious and one bridgeable. The bridgeable gap is the absence of prior review

342. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-22 ("The establishment in Member States of independent supervisory authorities is . . . an essential component of the protection of individuals with regard to the processing of personal data." (internal citations omitted)); Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Comm'r, 2014 E.C.R para. 62 (disapproving of Directive 2006/24 because "access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body").

343. *See* Joined Cases C-293/12 & C-594/12, *Digital Rights Ireland*, 2014 E.C.R. at para. 34.

344. *See id.* at 62 (stressing the need to provide for "prior review" by a court or an "independent administrative body").

345. *See id.* at paras. 54–55. Other cases in European national courts have followed the CJEU's lead. *See* Davis v. Home Sec'y, No. CO/3365/2014, [2015] EWHC (Admin) 2092 [para. 91(c)] (Royal Ct. of Justice London Div. 2015); *see also* Case C-362/14, *Schrems*, 2015 E.C.R. at I-32 (citing *DRI* in observing that EU–U.S. Safe Harbor regime, which allows corporations on both sides of the Atlantic to self-certify that they are observing privacy rules, is problematic in light of revelations about U.S. surveillance); *cf. id.* at I-28 (finding a lack of authority to invalidate the Safe Harbor program and referring the matter to CJEU); Nikolaj Nielsen, *French Court Backs Mass Surveillance*, EUROBSERVER (July 24, 2015, 9:26 AM), https://euobserver.com/justice/129760 (reporting on the French decision); Sam Schechner & Matthew Dalton, *French Constituonal Court Approves New Powers for Intelligence Services*, WALL STREET J. (July 24, 2015, 5:40 AM), http://www.wsj.com/articles/french-constitutional-court-approves-new-powers-for-intelligence-services-1437730809 (discussing France's constitutional court decision that allows intelligence services broad powers to spy).

346. 52 Eur. H.R. Rep. 4 (2010).

347. *Id.* at para. 232. A UK bill pending as of January 6, 2016, added a layer of judicial review. *See* Shaheed Fatima, *The "Snooper's Charter" and Judicial Oversight*, JUST SECURITY (Dec. 21, 2015, 9:40 AM), https://www.justsecurity.org/28443/snoopers-charter-judicial-oversight/.

348. Weber v. Germany, 2006-XI Eur. Ct. H.R. para. 25. The G10 has a mixed membership, including a former judge and members of Parliament. *Id.*

under Section 702, which concerns targeted surveillance. The FISC reviews certifications from the Executive Branch under Section 702 but does not approve particular selectors in advance of their use.[349] On balance, this is not a fatal flaw from a human rights perspective. A number of ECHR cases have upheld surveillance regimes that did not include prior review,[350] and the need for speed in exigent national security contexts[351] surely demonstrates the undue burden that prior review would cause.

The other more serious gap concerns U.S. bulk collection under EO 12,333.[352] The FISC does not review this collection, which Congress has consigned solely to the Executive Branch subject to a presidential finding.[353] An interagency body reviews collection under EO 12,333, but that does not provide the independence that human rights precedents require. The State Department ombudsperson created under the new U.S.–EU Privacy Shield agreement[354] may fall short in independence, because that individual serves at the pleasure of the President. To fill this gap, either Congress should empower the FISC to engage in this review, aided by a public advocate who would push back against the Executive Branch's arguments,[355] or the President or Congress should set up an independent board to perform the task, with the board's members removable by the President only "for cause."[356] Without this

349. 50 U.S.C. § 1801a(e)(2) (2012).

350. *E.g.*, *Kennedy*, 52 Eur. H.R. Rep. paras. 79–80 (upholding a regime in which a cabinet ministry issues warrants for its own investigations).

351. U.S. courts have recognized this issue in crafting a foreign intelligence exception to the warrant requirement. *See, e.g.*, United States v. Duka, 671 F.3d 329, 341 (3rd Cir. 2011); United States v. Truong, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Mohamud, No. 3:10–CR–00475–KI–1, 2014 WL 2866749, at *15 (D. Or. June 24, 2014); *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *cf.* THE FEDERALIST NO. 70 (Alexander Hamilton), at 424 (Clinton Rossiter ed. 1961) (celebrating the Executive's virtue of "dispatch").

352. *See supra* note 33 and accompanying text.

353. *See supra* note 45.

354. *See supra* notes 299–302 and accompanying text.

355. *See* Lederman & Vladeck, *supra* note 16.

356. *Cf.* Free Enter. Fund v. Pub. Co. Accounting Oversight Bd., 561 U.S. 477, 483–84 (2010) (invalidating removal restrictions on members of the Public Company Accounting Oversight Board within the Securities and Exchange Commission). This level of independence might well be consistent with the ECHR case law, which has approved Germany's reliance on the G10; the G10 is not fully independent of politics, because it includes members of Germany's parliament. *See* Weber v. Germany, 2006-XI Eur. Ct. H.R. para. 25. Departmental inspectors general (IGs) can provide another kind of independent check, although IGs' role entails assessment of programs, not review of particular decisions. Because IGs issue reports to Congress, they have a constituency in another branch of government that insulates them in part from executive branch pressure. *Cf.* Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. 3, 88 (2014) (noting the importance of IGs in assessment of FBI's role in

comprehensive commitment to independent scrutiny, U.S. overseas surveillance will suffer from a significant vulnerability under human rights norms.

b. Notice

Notice is important to review, since potentially aggrieved parties need notice to seek recourse from an independent body. The international law principle of legality also enshrines notice in a broader sense, requiring that members of a polity know before the fact of actions governments may take that adversely affect their interests.[357] Moreover, in human rights law, notice and legality require some degree of formality in the enactment of policy. Policy should be written, not made on the fly through furtive official conversations. Nonetheless, a state need not provide every subject of an investigation with notice that she is under surveillance, since such broad notice would provide suspects with a road map of law enforcement efforts.[358] Snowden's revelations, by pushing states toward greater transparency, have moved the dial toward compliance with the notice prong of human rights law.

In Britain, the IPT found that Britain had violated provisions of the European Convention on Human Rights prior to the Snowden disclosures.[359] However, in the wake of Snowden's disclosures, the IPT concluded that Britain's surveillance framework passed muster.[360] While recent statutory changes that broadened surveillance powers may change

---

domestic intelligence-gathering); Margo Schlanger, *Offices of Goodness: Influence Without Authority in Federal Agencies*, 36 CARDOZO L. REV. 53, 94–95 (2014) (suggesting that privacy and civil liberties officers within executive departments can provide different perspective that influences policy); DeLong, *supra* note 182, at 86–88 (discussing importance of internalizing compliance within intelligence agencies dealing with large-scale data analysis).

357. This principle is clearest when the government seeks to criminalize conduct. Since fundamental fairness requires that individuals have an opportunity to conform their conduct to law, both the principle of legality and the U.S. Constitution's Ex Post Facto Clause, U.S. CONST. art. I, § 8, cl. 10, bar punishment for conduct that *preceded* enactment of a statutory prohibition. As the text explains, once the state meets this requirement, it need not provide specific notice to each individual who may be subject to surveillance for violating a duly enacted law.

358. *Weber*, 2006-XI Eur. Ct. H.R. at 135 (observing that "notification might reveal the working methods and fields of operation of the Intelligence Service" and that "the very absence of knowledge of surveillance . . . ensures the efficacy" of the surveillance effort); *see also* Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751, 776 (2003) (observing that under European law secrecy is appropriate if "interests of the State justified secrecy"); *but see* Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 STAN. J. INT'L L. 69 (2015) (warning that secrecy can insulate government overreaching from effective review).

359. *See* Liberty & Others v. Sec'y of State for Foreign and Commonwealth Affairs, [2015] UKIPTrib 13 77-H para. 23, http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf.

360. *Id.* at paras. 22–23.

that assessment, as a British court recently held,[361] at least Britain's new law was the product of open debate.

In the United States, official public documents outlining implementation of PPD-28 provide notice of machine access overseas.[362] The PPD-28 documents articulate—in a fashion that is unprecedented in its candor regarding intelligence collection—that the United States engages in bulk collection, as well as scanning, of transnational material.[363] The U.S. documents' discussion of "SIGINT [signals intelligence] data that is temporarily acquired to facilitate targeted collection"[364] signals to any reasonably attentive reader that the United States is using machines to scan international communications. The PPD-28 documents also reveal the purposes served by U.S. bulk collection abroad, such as counterterrorism, counterespionage, antiproliferation, and transnational crime.[365] With some fairly modest steps, the United States has leapt to the head of the class on notice. More is unnecessary, particularly given legitimate concerns about tipping off terrorists.

c. Recourse

Notice to an individual subject of inappropriate surveillance is part of the recourse that human rights law requires for victims of government overreaching.[366] Recourse, which should entail an independent decision maker,[367] is especially important for machine access because of the risk that mining multiple databases will compound input errors (as the saying goes, "Garbage in, garbage out").[368] That has happened in the case of no-fly lists,[369] and it is a risk in other contexts as well.

The United States needs to improve its avenues for recourse. Currently, recourse in the national security surveillance space is exceedingly limited.[370] No independent agency exists to field complaints, and standing doctrine restricts remedies in federal courts.[371] The Judicial

---

361. *See* Davis v. Home Sec'y, No. CO/3365/2014, [2015] EWHC (Admin) 2092 [para. 91] (Royal Ct. of Justice London Div. 2015).

362. *See* PPD-28 Supplemental Procedures, *supra* note 27, at 7 n.1 (defining bulk collection).

363. *Id.* at 7–8.

364. *Id.* at 7 n.2.

365. *Id.* at 7–8; *see also* 50 U.S.C. § 1801(e)(2)(B) (2012) (permitting limited collection of foreign intelligence information related to "foreign affairs" of United States); *supra* notes 283–93 and accompanying text (discussing "foreign affairs" prong of Section 702).

366. *See* Kennedy v. United Kingdom, 52 Eur. H.R. Rep. paras. 79–80 (2010).

367. *See id.* at para. 127.

368. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., *supra* note 5, at 76, 274–75.

369. *See, e.g.*, Latif v. Holder, 28 F. Supp. 3d 1134, 1141–42 (D. Or. 2014).

370. *See* Margulies, *supra* note 8, at 2163.

371. *See* Clapper v. Amnesty, Int'l USA, 133 S. Ct. 1138, 1149–50 (2013) (narrowly construing the standing requirement for recourse in federal courts); *cf.* Obama v. Klayman, 800

Redress Act enhances recourse.[372] This legislation extends protections in the U.S. Privacy Act to non-U.S. persons outside the United States who are nationals of states that agree to share information with the United States for law enforcement purposes and provide "appropriate privacy protections" for such information.[373] The Privacy Act furnishes a mechanism for individuals to gain access to government data or records about them and seek judicial remedies for denying individuals such access or engaging in improper collection, storage, or use of such data.[374] However, like the Privacy Act, the Judicial Redress Act exempts data collected, acquired, or stored for law enforcement[375] or national security[376] purposes.[377] These categorical exemptions undermine the Judicial Redress Act's utility as an avenue for recourse.[378] While the ombudsperson established by the new Privacy Shield agreement may aid in promoting recourse, the CJEU has in a prior case viewed an ombudsperson as an inadequate cure for procedural deficits.[379]

Recognition of this weakness can readily coexist with the understanding that law enforcement and national security necessarily impose some limits on recourse. Law enforcement and national security needs will shape the contours of government agencies' responses to queries from individuals. In Britain, for example, the IPT provides recourse, while ensuring that its decisions do not allow terrorists to "game plan" attempts to elude surveillance. When the IPT rejects a complaint, it informs the complainant with characteristic British concision that "no determination has been made in his favour."[380] That sparse pronouncement is sufficient under human rights law.[381] A similar finding in a U.S. tribunal would not jeopardize the U.S. intelligence apparatus.

F.3d 559, 561–62, (D.C. Cir. 2015) (vacating the preliminary injunction and remanding for further proceedings on the ground that the plaintiffs had not demonstrated a likelihood of success on standing to challenge government surveillance policies, since the plaintiffs had not shown a sufficiently high probability that they had been subject to surveillance).

372. Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (codified at 5 U.S.C. 552a note).

373. *Id.* § 2(d).

374. *See* 5 U.S.C. § 552a(d)–(g) (2012).

375. *See id.* § 552a(k)(2).

376. *See id.* § 552(b)(1).

377. *See* H.R. 1428, § 2(a)(1) (incorporating by reference exemptions in the Privacy Act).

378. If the Judicial Redress Act does not provide adequate recourse, then European data commissioners and the European Court of Justice may not approve revisions to regimes such as "Safe Harbor," which permitted companies on both sides of the Atlantic to share customer data to facilitate commercial transactions.

379. *See* Joined Cases C-584/10, C-593/10 & C-595/10, *Kadi v. European Commission* (European Court of Justice 18 July 2013) (holding that ombudsperson was not sufficient to cure procedural flaws in regime for blocking assets of suspected terrorist financiers).

380. Kennedy v. United Kingdom, 52 Eur. H.R. Rep. para. 79 (2010).

381. *See id.*

Of course, a finding for a complainant might reveal that, on occasion, U.S. intelligence agencies make mistakes. However, freely acknowledging missteps might actually bolster the United States' standing around the globe. Thanks to the PPD-28 process initiated by President Obama, transparency has reinvigorated the United States' stance on intelligence collection overseas. Independent recourse would be consistent with this salutary trend.

CONCLUSION

Anger was a common reaction in the United States and abroad to Edward Snowden's disclosures. Some indignation against government is healthy in a democracy. However, indignation can polarize positions and obscure nuance that makes debate productive. In analyzing machine surveillance, this Article has endeavored to redress the balance.

Two camps have battled over the scope of state machine surveillance abroad. The state-centric camp argues that human rights agreements such as the ICCPR do not even apply and that machine access is inherently unintrusive. Surveillance critics respond with the three-pronged equivalency thesis: machine and human access are equivalent invasions of privacy, a state's technological *capabilities* drive surveillance practice, and legal protections must be equivalent for both a state's nationals and non-nationals overseas. Each approach is flawed.

The state-centric camp is wrong about the applicability of human rights agreements, which have extra-territorial effect. It is also in part wrong about machine access, which can wreak both deontological and consequential harm. However, the equivalency thesis also misses the mark. While machine access can be problematic, safeguards can ease the problem and ensure that law governs a state's capabilities. Moreover, international law, including Security Council resolutions combating ISIS and Al Qaeda, permits surveillance abroad that will prevent terrorist groups from gaining safe havens, even when that surveillance is more intrusive than domestic surveillance efforts.

Machine searches are a powerful tool, but surveillance critics are right that they are not a panacea. Safeguards are needed to channel their benefits and reduce the risk of abuse abroad. Because of the need to accommodate Security Council resolutions, LOAC, and privacy–privacy trade-offs, along with the margin of appreciation that courts have usually accorded states and the ICCPR's loose arbitrariness standard, a deferential proportionality test should govern the search for safeguards. This standard, as applied to machine searches abroad, has three pillars: purpose, reliability, and review.

The purpose of surveillance must be exigent, such as national security, although human rights decisions demonstrate that states need not cite more specific purposes that would tip off terrorists. Nevertheless, a

national security purpose creates some clear baselines. For example, while a state can engage in bulk collection of content in another country involved in an armed conflict with the collecting state, bulk collection of *all* of a country's communications content is inappropriate outside the sphere of armed conflict. In other words, the United States should permit jet ski enthusiasts in the Bahamas to arrange their transportation without a machine listening to the call, unless U.S. law enforcement has evidence that the jet skis will be used for terrorism or the transport of drugs to another country.

Each state should validate machine searches. Validation can replace the substantive verbal explanation that the transparency paradox precludes. In addition, validation should involve commonly accepted metrics, such as precision and recall. Machine searches should demonstrate their worth in finding false negatives without excessive false positives. If machines cannot meet this standard, older methods, such as human informants, should be used.

Review should be independent, as the CJEU stressed in *Schrems*. In the United States, courts issue domestic warrants, ensure that domestic metadata collected under the Patriot Act and queried by analysts has reasonable and articulable links to terrorism, and review targeted collection under FISA's Section 702. The FISC should have a public advocate who pushes back against government surveillance requests. Moreover, an independent board or agency should review bulk collection under EO 12,333. In addition, an independent agency should review complaints from individuals who assert that the government wrongfully collected or retained their personal information. Machines are not good at detecting flawed inputs, and humans are sometimes too enchanted with their own machine creations to do the follow-up required to ensure accuracy. Recourse is a necessary backstop.

The safeguards suggested in this Article may not satisfy the state-centric camp or the champions of the equivalency thesis. For the state-centric camp, anything less than untrammeled discretion is a disappointment. The equivalency theorists, for their part, may wish for more onerous restrictions on machine surveillance. The model suggested here does not opt for either of these polar positions. However, it will impose accountability on machine surveillance abroad, while enabling innovation and protecting the public. That combination of virtues is an improvement over either rage or complacency.