68 STAN. L. REV. ONLINE 9
May 18, 2015

WIDENING THE APERTURE ON FOURTH AMENDMENT INTERESTS: A COMMENT ON ORIN KERR'S *THE FOURTH AMENDMENT AND THE GLOBAL INTERNET*

David G. Delaney*

INTRODUCTION

In *The Fourth Amendment and the Global Internet*, Orin Kerr highlights several important Fourth Amendment questions that few courts have addressed. But in "offer[ing] a general framework for applying the Fourth Amendment to a global computer network in a way that maintains the existing territorial conception of the Fourth Amendment,"[1] Kerr's article focuses too narrowly on the Internet, the *Verdugo-Urquidez* sufficient connection test, and the border search exception. Such issues must, as Kerr acknowledges, be considered in broader context.[2] This Comment proposes that courts maintain flexibility to conceive of a Fourth Amendment that does not depend exclusively on territory to fulfill its twin aims of ordering government and enabling redress of liberty infringements. It also encourages federal and state courts and legislatures to regulate searches, seizures, and surveillance through simple rules that can easily adapt to the contours of a rapidly evolving cyber landscape and new government activity in cyberspace.

I. CYBERSPACE CONVERGENCE

It is important to state the challenges of framing legal and policy issues in this area. Kerr focuses on the global Internet. But the real focus is cyberspace, which may be understood as the broader integrated networked realm created by the convergence of analog and digital networks that support Internet and other

* Visiting Assistant Professor, Indiana University Maurer School of Law, and Deputy Director, Indiana University Center for Applied Cybersecurity Research. I am grateful to Ivan K. Fong, Jennifer Daskal, Craig Jackson, and Drew T. Simshaw for their feedback on an earlier draft, and also to Muge Fazlioglu for her invaluable research assistance.

1. Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 291 (2015).

2. *See id.* at 291 n.25.

communications. Nations may define the term differently, but national and international interests extend to cyberspace, not just the Internet.[3] Federal and subfederal governments increasingly rely upon cyberspace to perform public functions, from waging war to maintaining accurate records. And nearly all government activity in cyberspace is imbued with both foreign and domestic attributes. Convergence thus melds a significant range of individual and government information and activities into a single environment—a circumstance that defies easy analogy to the physical world.

Because cyberspace brings global threats equally into federal, subfederal, and private sector spheres of interest, public and private roles and responsibilities are in flux. When discussing the Fourth Amendment across these communities and the different fields of expertise within them, it is essential to consider how terminology and factual variety affect outcomes. Consider a scenario that Kerr offers to propose a general good faith rule: "investigators conduct broad monitoring" of "Internet traffic targeting U.S. government computers" that "originates from a proxy server routing anonymized Internet traffic from elsewhere in the world," and "the monitoring that occurred would not satisfy Fourth Amendment standards based on later-discovered facts."[4] This most plainly reads as a law enforcement scenario, but it is presented broadly enough to encompass monitoring by other parts of government for other purposes. Courts and legislatures must understand those different circumstances in greater detail to prescribe suitable rules for law enforcement, intelligence, administrative, or other officials.

Kerr's specific proposal is that courts borrow from apparent authority doctrine and find no Fourth Amendment violation if an officer operates under a reasonable good faith belief that the target lacked Fourth Amendment rights under *Verdugo-Urquidez*, even when the target is later determined to be a citizen located in the United States.[5] Applying the rule in a law enforcement setting, the search would be constitutionally reasonable, the officer would not be personally liable, and evidence could be admitted at trial. But there is insufficient detail in the scenario to analogize to apparent authority doctrine or to accept such outcomes outright.

An effective good faith rule for criminal investigators should include significant consideration of technical issues and monitoring methods. Regardless whether a reviewing court borrows from apparent authority doctrine or otherwise conducts a fact-specific reasonableness inquiry, key technical issues like the use of anonymizing software and proxy servers must be understood in context. These technologies, which may be hallmarks of some criminal activity, also provide a means to conduct lawful, constitutionally protected activity in

3. *See Cyber Definitions*, NATO COOPERATIVE CYBER DEF. CENTRE OF EXCELLENCE, https://ccdcoe.org/cyber-definitions.html (last visited Apr. 6, 2015) (compiling various cyber definitions as used in NATO and other nations' strategy and policy documents).

4. Kerr, *supra* note 1, at 308.

5. *Id.* at 308-10.

cyberspace. The reasonableness of an officer's belief may also be a function of where and how the monitoring is conducted—on the proxy server itself, on government computers, on privately owned networks, inside the United States, outside the United States, as an independent action based on a personal interpretation of *Verdugo-Urquidez*, or pursuant to government policy and legal guidance for monitoring large volumes of Internet traffic.

Good faith rules may also be appropriate for government communities conducting broad monitoring in cyberspace to protect government computers or information. Federal and state agencies perform administrative monitoring to maintain secure government networks and information.[6] The National Security Agency and Department of Defense conduct information assurance monitoring to protect sensitive and classified information. They also ensure that integrated domestic and foreign communication networks can be sustained, defended, and used to project force.[7] Law enforcement and intelligence officers conduct broad monitoring under the Foreign Intelligence Surveillance Act.[8] While there will be some common aspects of monitoring across these communities, these activities involve different legal authorities, objectives, methods, degrees of intrusiveness, procedural checks, legislative oversight, judicial review, transparency, and public engagement. Courts and legislatures should therefore be prepared to tailor good faith rules according to the administrative, law enforcement, foreign intelligence, military, or other monitoring activity being performed.

II. LOOKING BACK TO LOOK AHEAD

Although the Fourth Amendment operates most frequently and directly on those in the criminal justice field—through prohibitions like per se warrant requirements and the exclusionary rule—it also unquestionably regulates all elements of federal and state government.[9] Analogies involving law enforcement

---

6. The activity in federal agencies extends from the Federal Information Security Modernization Act § 202, 44 U.S.C. § 3554(a) (2013) ("The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency . . . .").

7. *See, e.g.*, 10 U.S.C. § 2224 (2013); GEORGE H.W. BUSH, NATIONAL SECURITY DIRECTIVE 42: NATIONAL POLICY FOR THE SECURITY OF NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS 2 (1990), *available at* https://www.hsdl.org/?view&did=458706.

8. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-1885c).

9. *E.g.*, New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) ("It may well be true that the evil toward which the Fourth Amendment was primarily directed was the resurrection of the pre-Revolutionary practice of using general warrants or 'writs of assistance' to authorize searches for contraband by officers of the Crown. But this Court has never limited the Amendment's prohibition on unreasonable searches and seizures to operations conducted by the police." (citations omitted)).

officials carry great weight when federal and subfederal governments attempt to discern the Fourth Amendment's meaning in other settings—like administrative and national security monitoring—involving cyberspace. But it is not obvious that they should. To help all parts of government preserve Fourth Amendment values in their emerging cyberspace functions, courts and legislatures should address non-law-enforcement scenarios more directly to establish suitable search-and-seizure frameworks that match society's dependence on cyberspace.

In the field of administrative monitoring, governments may look for guidance in cases involving "special needs, beyond the normal need for law enforcement"[10] because the function is performed for information security purposes. However, the special needs cases speak to only a small fraction of ways that government actors are able to search or seize data for non-law-enforcement purposes in cyberspace. Governments should also look to administrative search cases like *Camara v. Municipal Court of San Francisco*, in which the Supreme Court found the warrant process essential to protect citizens against arbitrary administrative inspections to enforce fire, health, housing, and other municipal codes.[11] It is unlikely, however, that preconvergence cases can be extended directly to postconvergence fact patterns.

It would seem uncontroversial to propose that *Camara* should apply to government inspectors when entering a "connected" or "smart" home to acquire code-related digital information directly from electronic devices and communications networks. Present or future governmental interests in acquiring, analyzing, and retaining such data introduce a range of informational privacy concerns that have arisen since *Camara*. This drives a need for new probable cause requirements or warrant procedures to address government actions in the home as well as future use of data acquired there. Of equal or greater interest are the Fourth Amendment considerations arising from government use of cyberspace to acquire the same information from in-home devices remotely, from cables carrying the information outside the home, from third-party companies delivering services to residents, from regulators or other government entities possessing the data, or from data aggregators.[12] By addressing such issues, courts and legislatures expand the body of law that informs and guides the many administrative entities interacting with personal information in cyberspace.

In the national security arena a good starting point to consider the suitability of current search-and-seizure law is the Supreme Court's 1972 decision in *United States v. United States District Court* (*Keith*).[13] The Court held that do-

10. *Id.* at 351 (Blackmun, J., concurring).

11. 387 U.S. 523, 531, 540 (1967).

12. For an expansive treatment of ways that data in cyberspace challenge existing domestic and international legal frameworks, see Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. (forthcoming 2015-16).

13. 407 U.S. 297 (1972).

mestic security surveillance conducted solely within the discretion of the executive is inconsistent with Fourth Amendment freedoms, including individual privacy and free expression.[14] The *Keith* Court also observed that the stringent review standards suitable in domestic criminal law settings may not be suitable for "domestic security surveillance" or "activities of foreign powers or their agents."[15] Because convergence blurs (if not eliminates) lines between foreign and domestic threats and security measures, Congress and the courts should be open to reconsidering these principles. Reasonableness determinations regarding government searches and seizures in the foreign security realm derive almost exclusively from executive and judicial processes established by the Foreign Intelligence Surveillance Act.[16] But the secrecy that the President and Congress attach to surveillance programs and judicial review by the Foreign Intelligence Surveillance Court all but precludes court challenges of the sort that enabled the *Keith* Court's clear statement on broad Fourth Amendment principles.[17] To enable meaningful application of the Fourth Amendment in the digital age, the branches must independently and collectively endeavor to minimize secrecy, enable broad discussion and review of government activity in cyberspace, and articulate clear rules to guide public officials.

III. SEEKING TERRA FIRMA IN CYBERSPACE

If history is any guide, the century-long trend in which courts have found greater Bill of Rights protections for citizens and aliens is important to consider.[18] The king's soldiers carrying out general warrants are the historical antecedents to contemporary government entities performing public functions through intrusive means. As government increasingly deploys law enforcement, military, intelligence, and other officials globally to perform physical and virtu-

14. *Id*. at 314-20.

15. *Id*. at 321-22.

16. Exceptions include *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 159 (2d Cir. 2008) (holding that the search of a U.S. citizen's home and surveillance of his cell phone and landline during a terrorism investigation in Kenya must comply with the Fourth Amendment's reasonableness requirement).

17. In the wake of Edward Snowden's disclosures of classified national security cyberspace programs, Article III courts have begun to hear a variety of Fourth Amendment challenges in foreign security cases. *See, e.g.*, United States v. Daoud, 755 F.3d 479, 480-81 (7th Cir. 2014); United States v. Qazi, No. 12-60298, 2015 WL 728386, at *1 (S.D. Fla. Feb. 19, 2015); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *10 (D. Or. June 24, 2014); ACLU v. Clapper, 959 F. Supp. 2d 724, 735 (S.D.N.Y. 2013); Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D.D.C. 2013); Defendant's Motion to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act & Motion for Discovery at 2-3, United States v. Muhtorov, No. 12-cr-00033-JLK-1 (D. Colo. Jan. 1, 2014), ECF No. 520.

18. For a historical overview of territoriality in American law and a discussion of Bill of Rights protections for citizens and aliens, see KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 241-43 (2009).

al searches and seizures, it is appropriate to ask why Fourth Amendment protections should not also extend globally, first to U.S. citizens and then to others in appropriate circumstances.

Throughout the twentieth century, as the United States acquired territory and projected force for national and global security, U.S. courts began to find constitutional protections that were unimagined in the previous century. In the context of jury trials for crimes committed in the Philippines, Justice Harlan's dissent in *Dorr v. United States* embodies the importance of conceiving of a Bill of Rights that protects individuals anywhere:

> In my opinion, guaranties for the protection of life, liberty and property, as embodied in the Constitution, are for the benefit of all, of whatever race or nativity, in the States composing the Union, or in any territory, however acquired, over the inhabitants of which the Government of the United States may exercise the powers conferred upon it by the Constitution.[19]

Since *Reid v. Covert*,[20] this philosophy has operated to extend Bill of Rights protections to U.S. citizens abroad. The *Reid* Court found Fifth and Sixth Amendment protections for the civilian spouses of service-members on trial for murder in England and Japan under the Uniform Code of Military Justice.[21] Regarding *Dorr* and the earlier *Insular Cases*, the Court exhorted, "neither the cases nor their reasoning should be given any further expansion."[22]

While the Fifth and Sixth Amendments operate very differently from the Fourth Amendment to preserve liberty interests, Justice Harlan's philosophy resonates in instances where U.S. citizens' Fourth Amendment interests are implicated outside the United States. As Kerr notes, courts are only beginning to inquire into Fourth Amendment protections when government agents encounter citizens abroad, as well as information about those citizens that is in cyberspace.[23] Given the opportunity for more instances of federal and state cyberspace activity to be discussed publicly, debated by local governments and legislatures, studied by scholars,[24] and reviewed by courts, it is likely that those democratic processes will yield greater digital-age search-and-seizure protections than currently exist.

Until Fourth Amendment protections for citizens are more clearly defined and routinely accepted abroad and in cyberspace, it may seem daunting to envision search-and-seizure protections for aliens under *Verdugo-Urquidez* or oth-

---

19. 195 U.S. 138, 154 (1904) (Harlan, J., dissenting).

20. 354 U.S. 1 (1957).

21. *Id.* at 5-6.

22. *Id.* at 14.

23. Kerr, *supra* note 1, at 286 n.1 (citing courts that have found Fourth Amendment protections for e-mails and the content of computers connected to a university network).

24. For a discussion of a technology-centered approach to digital-age privacy, see David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013).

erwise.[25] But the analysis begins with circumstances, as in *Verdugo-Urquidez*, where the government subjects an alien to criminal process in the United States. As the *Verdugo-Urquidez* Court recognized, aliens generally enjoy the same rights as citizens inside the United States.[26] The question becomes whether convergence and other changes of circumstance prompt government entities to approach governments' extraterritorial or cyberspace activities differently.

In a contemporary case presenting an extraterritorial or cyberspace search involving an alien, courts applying *Verdugo-Urquidez* should consider the scale and intrusiveness of the government's activity. Convergence has certainly prompted new relationships between government and citizen since the case was decided twenty-five years ago. It is also likely that government's law enforcement, intelligence, or other interests effected through cyberspace bear little resemblance to the one-time Drug Enforcement Administration search of the defendant's residence in Mexico. This is enough for courts to distinguish *Verdugo-Urquidez* factually. Such comparison of pre- and postconvergence circumstances is demonstrated most clearly by Judge Leon's memorandum opinion in *Klayman v. Obama* ordering an injunction of NSA surveillance under the Foreign Intelligence Surveillance Act.[27] Judge Leon addresses the pen register metadata case of *Smith v. Maryland*,[28] finding that "the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[29]

Courts might also respond to the evolving digital-age landscape by revisiting the dissenting Brennan-Marshall view of the sufficient connection test:

> The "sufficient connection" is supplied not by Verdugo-Urquidez, but by the Government. Respondent is entitled to the protections of the Fourth Amendment because our Government, by investigating him and attempting to hold him accountable under United States criminal laws, has treated him as a member of our community for purposes of enforcing our laws. He has become, quite literally, one of the governed.[30]

From this perspective, the importance of extending Fourth Amendment protections to individuals affected by government cyberspace policies increases as intrusive activity and prosecutions increase. Whether the Fourth Amendment is

---

25. *See, e.g.*, Douglas I. Koff, *Post*-Verdugo-Urquidez*: The Sufficient Connection Test—Substantially Ambiguous, Substantially Unworkable*, 25 COLUM. HUM. RTS. L. REV. 435, 484-90 (1994) (asserting that the sufficient connection test is unworkable and proposing instead that the Fourth Amendment should extend to everyone, except nonresident enemy aliens searched incident to a military confrontation).

26. United States v. Verdugo-Urquidez, 494 U.S. 259, 270-71 (1990).

27. 957 F. Supp. 2d 1, 30-31 (D.D.C. 2013).

28. 442 U.S. 735 (1979).

29. *Klayman*, 957 F. Supp. 2d at 30-37.

30. *Verdugo-Urquidez*, 494 U.S. at 283-84 (Brennan, J., dissenting).

ultimately satisfied for aliens by a warrant-like process, a different type of judicial process, administrative procedures, or as-yet-undeveloped international standards would remain an open question of implementation.[31]

CONCLUSION

Cyberspace enables nation-states, organized criminal groups, and politically motivated actors to affect global U.S. interests differently than in the physical world alone. Federal and state governments' adaptation to threats in this converged world may be envisioned along a spectrum. On one end, the President and Congress structure and authorize government to act based on the foreign nature of many cyberspace threats or the potential for sudden, catastrophic consequences. Coordination with international bodies, nongovernmental organizations, private companies, and subfederal governments centers on military defense needs. Regardless how likely those catastrophic outcomes are, the President's national security role is emphasized and central to the growth and application of military, intelligence, and related law enforcement capabilities to the law's fullest extent.

On the other end of the spectrum, the federal executive and legislative branches focus on technical, social, and other dimensions of cyberspace threats and interests. They structure and authorize government to act in concert with other communities poised to identify, calculate, prioritize, and mitigate risks. In a converged world, this includes significant interaction with international bodies, nongovernmental organizations, private companies, and subfederal governments. Coordination is slower and more difficult on this end, and the federal government's presumed security role may change from service provider to enabler.

Courts deciding Fourth Amendment cases along this spectrum will confront myriad old and new circumstances. Their Fourth Amendment calculations require reframing and recalibrating in the digital age, given the factual variety and rate of change that a technology-dependent world presents. Indeed, the Supreme Court has demonstrated that straight-line application of physical-world Fourth Amendment holdings should not be presumed when nodes of cyberspace introduce seemingly slight variations to common fact patterns, at least in the criminal law setting. One example is *United States v. Jones*, in which a plurality of the Court expressed concern about informational privacy interests affected by surveillance enabled by a wireless global positioning system.[32] Another is *Riley v. California* in which the Court gave equal Fourth Amendment

31. For a thorough discussion of *Verdugo-Urquidez* and suggestions on the role of international law shaping U.S. searches and seizures, see Eric Bentley, Jr., *Toward an International Fourth Amendment: Rethinking Searches and Seizures Abroad After* Verdugo-Urquidez, 27 VAND. J. TRANSNAT'L L. 329, 370-99 (1994).

32. 132 S. Ct. 945, 948-50 (2012).

protection to flip phones and smart phones found on an arrestee.[33] The Court's Occam's Razor-like approach in *Reid* and *Riley* is particularly instructive for legislatures and courts contemplating digital age search-and-seizure issues—simple rules with few exceptions can be particularly powerful and give the Fourth Amendment great vitality.

33. 134 S. Ct. 2473, 2495 (2014).