DAY ONE PROJECT

Privacy Laws Should Help, Not Harm, Criminal-Justice Reform

Rebecca Wexler
John Villasenor

January 2021

Summary

American society urgently needs to address structural disparities in the criminal-justice system. One important disparity—which is both easily mitigated and generally unrecognized—is the asymmetry of information access granted to prosecutors and defendants. Prosecutors can easily access digital records that establish guilt. But defendants are far less empowered to access digital records that prove innocence.

Privacy laws are a key source of this disparity. The Stored Communications Act (SCA), for instance, permits law enforcement—but not defense investigators—to access certain evidence from Internet companies. Fortunately, there are two straightforward policy solutions to this problem. First, new federal privacy legislation should include language requiring symmetric information access for defendants. Second, the Department of Justice should adopt a new interpretation of the SCA to protect fairness in criminal proceedings.

Challenge and Opportunity

Current federal privacy laws, as well as many proposals for new privacy laws, tip the scales against criminal defendants. Privacy statutes often include exceptions that grant police and prosecutors access to evidence of guilt. But these same privacy laws frequently lack similar exceptions for defense investigators to access evidence of innocence. These "privacy asymmetries"[1] are almost certainly unintentional side effects of the legislative process—a process in which criminal-defense interests are often inadequately represented. Limited access to evidence for defense investigators increases the risk of wrongful convictions and unnecessarily threatens accuracy and fairness in criminal proceedings.

In addition, the Department of Justice (DOJ) currently interprets the Stored Communications Act—a key data-privacy law for the Internet—to bar defense counsel from subpoenaing technology companies for certain types of data, even when that data could exonerate the wrongfully accused, and even though police and prosecutors can access the same data when seeking to establish guilt. This interpretation is unnecessary and broadly harmful. Most major Internet companies are governed by the SCA, so this view of the law means that defendants cannot access social-media records, emails, and other digital data. Defense attorneys have argued for years, mostly without success, for a fairer application of the SCA. Recently heightened bipartisan recognition of the need for criminal-justice reform provides an opportunity to garner support for a better, more equitable privacy policy.

[1] For an in-depth analysis introducing and critiquing the phenomenon of "privacy asymmetries," see Wexler, R. (forthcoming 2021). Privacy Asymmetries: Access to Data in Criminal Defense Investigations. UCLA Law Review, 68(1). https://ssrn.com/abstract=3428607.

Plan of Action

A bipartisan, multi-stakeholder effort is needed to raise awareness in Congress about the importance of *symmetrical* exceptions in privacy statutes: that is, exceptions that apply equally to both law enforcement and criminal-defense counsel. Both President-Elect Biden and Vice President-Elect Harris are committed to reforming the criminal-justice system—a commitment shared by many members of Congress from both parties. Thus, both the executive branch and Congress are primed to solve the asymmetry problem now.

During the 116th Congress (2019–2020), multiple proposed federal privacy bills included provisions that exempt law-enforcement investigators, but not defense investigators, from privacy protections. An unintentional side effect of these bills would be to systematically advantage the search for evidence of guilt over that for evidence of innocence.

To avoid this outcome in the 117th Congress, the next administration should advocate for symmetrical exceptions in privacy laws that afford law enforcement and defense investigators comparable access to sensitive and crucial evidence. Ideally, this position would be supported by privacy-policy experts at the Federal Trade Commission (FTC), Department of Commerce (DOC), the Office of Management and Budget (OMB), the White House Office of Science and Technology Policy (OSTP), and the White House National Economic Council (NEC). Experts at federal agencies could propose draft statutory language adding a symmetrical savings clause to the end of each federal privacy bill, such as:

> *"Nothing in this Act shall be construed to prohibit a good-faith response to or compliance with otherwise valid warrants, subpoenas, or court orders, or to prohibit providing information as otherwise required by law."*[2]

Second, the next administration should work to raise awareness regarding the importance of revising interpretations of the SCA. Current DOJ practice is for U.S. attorneys to file amicus briefs in criminal cases supporting the view that "the SCA prohibits service providers from disclosing the contents of electronic communications in response to a defendant's trial subpoena."[3] But this is mistaken as a matter of binding Supreme Court doctrine as well as good policy.[4] This view erroneously reads silence in the SCA's text to create an expansive evidentiary privilege for the entire medium of the Internet. It violates courts' duties to construe privileges narrowly because they are "in derogation of the search for truth,"[5] and suppresses evidence from the truth-seeking

[2] For more on this proposal, see Wexler, R. (forthcoming 2021). Privacy Asymmetries.
[3] See: District of Columbia Court of Appeals. (2019). No. 18-CO-958: Facebook, Inc., Appellant v. Daron Wint., Appellee, and United States, Intervenor, Br. for the United States (Oct. 2, 2018), at *6.
[4] For a detailed presentation of these law and policy arguments, see Wexler, R. (forthcoming 2021). Privacy as Privilege: The Stored Communications Act and Internet Evidence. Harvard Law Review, (134). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3673403.
[5] Supreme Court of the United States (2020). No. 19-635: Donald J. Trump, Petitioner, v. Cyrus R. Vance, Jr., In His Official Capacity as District Attorney of the County of New York, et al., at *3. https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/19-635.html.

process of the courts without regard to the sensitivity of its contents or the relationship between communicants.[6]

Not all law-enforcement agencies have taken this view. The San Diego District Attorney's office recently filed an amicus brief in the California Supreme Court advocating on behalf of the rights of criminal defendants to subpoena relevant evidence without being blocked by the SCA.[7] U.S. attorneys should also file amicus briefs urging courts to construe the silence in the SCA's statutory text as insufficient to block valid defense subpoenas, and require litigants with legitimate privacy interests in subpoenaed communications to present those interests to the courts on a case-by-case basis.[8] The DOJ Chief Privacy and Civil Liberties Officer (CPCLO) and the DOJ Computer Crime and Intellectual Property Section (CCIPS) should work with other DOJ offices to spearhead the change by issuing a General Counsel memo advising U.S. attorneys nationwide of the updated uniform policy for federal prosecutors.

Conclusion

Privacy laws that unintentionally preference law-enforcement investigations of guilt over defense investigations of innocence risk undermining the truth-seeking function of the courts. These harms are unnecessary because baseline criminal-procedure rules already protect legitimate privacy interests. It is no longer acceptable to ignore disparities that privacy laws impose on criminal defendants. A balanced and sustainable information privacy policy must do better.

[6] Wexler, R. (2021). Privacy as Privilege.
[7] Supreme Court of California (2018). S245203: Facebook, Inc., Petitioner, v. The Superior Court of San Diego County, Respondent; Lance Touchstone, Real Party in Interest; Summer Stephan, as District Attorney, etc. Intervener. https://law.justia.com/cases/california/supreme-court/2020/s245203.html.
[8] Wexler, R. (2021). Privacy as Privilege.

DAY ONE PROJECT

Frequently Asked Questions

1. Why did this problem with privacy laws arise in the first place?

Legislators have long been aware of the need to avoid drafting privacy laws that would unduly impede criminal prosecutions. As a result, privacy laws often include specific carve-outs to give law enforcement—under proper legal authority—access to data that can establish guilt. However, there has been little to no awareness of the importance of providing defendants with similar access to data establishing innocence. The result is a collection of privacy laws that provide better access to evidence for law enforcement than they do for defense investigators.

2. Will the actions proposed in this memo increase or reduce law-enforcement access to private data?

No. They will not affect law enforcement's access to data in any way.

3. This memo proposes giving defendants in criminal cases greater access to data. Will your proposal require companies to give similar data to litigants in civil cases?

No. Policymakers concerned about how the SCA applies in civil cases can amend the SCA to expressly block civil subpoenas. Policymakers enacting new federal legislation can expressly limit exceptions granted to law enforcement and criminal defense counsel.

4. Will the actions proposed in this memo impose undue administrative burdens on technology companies?

No. Courts already require technology companies to disclose data similar to the data discussed in this memo. Adding a requirement that technology companies respond to all valid, judicially ordered criminal-defense subpoenas would not substantively increase administrative burden. It is also worth noting that cellular-communications providers, banks, and hospitals all have to comply with criminal-defense subpoenas because privacy laws for these sectors already include balanced exceptions for disclosure pursuant to valid legal process. If these institutions can manage symmetrical data requests, so can technology companies.

About the Authors

Rebecca Wexler is an assistant professor of law at the University of California, Berkeley. She is also a co-director of the Berkeley Center for Law & Technology and a nonresident fellow at the Brookings Institution.

John Villasenor is a professor of electrical engineering, law, public policy, and management at the University of California, Los Angeles. He is also director of the UCLA Institute for Technology, Law, and Policy and a nonresident senior fellow at the Brookings Institution.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.