U.C.L.A. Law Review

Privacy Asymmetries: Access to Data in Criminal Defense Investigations

Rebecca Wexler

ABSTRACT

This Article introduces the phenomenon of "privacy asymmetries," which are privacy statutes that permit courts to order disclosures of sensitive information when requested by law enforcement but not when requested by criminal defense counsel. In the U.S. adversarial criminal legal system, defense counsel are the sole actors tasked with investigating evidence of innocence. Law enforcement has no constitutional, statutory, or formal ethical duty to seek out evidence of innocence. Therefore, statutes that selectively suppress defense investigations selectively suppress evidence of innocence. Privacy asymmetries form a recurring, albeit previously unrecognized, pattern in privacy statutes. They likely arise from legislative oversight and not reasoned deliberation. They risk unnecessary harms to criminal defendants and the truth-seeking process of the judiciary by advantaging the search for evidence of guilt over that for evidence of innocence. The number of these harms will only increase in the digital economy as private companies collect immense quantities of data about our heart beats, movements, communications, consumption, and more. Much of that data will be relevant to criminal investigations and available to the accused solely through the very defense subpoenas that privacy asymmetries block. Moreover, the introduction of artificial intelligence and machine learning tools into the criminal justice system will exacerbate the consequences of law enforcement's and defense counsel's disparate access to data. To avoid enacting privacy asymmetries by sheer accident, legislators drafting privacy statutes should include a default symmetrical savings provision for law enforcement and defense investigators alike.

AUTHOR

Assistant Professor of Law at the University of California, Berkeley, School of Law.

This Article benefited from workshops at Berkeley, Chicago, Duke, and UCLA Law Schools, as well as the Northeast Privacy Scholars Workshop. For thoughtful comments and conversations, thank you to Ian Ayres, William Baude, Kiel Brennan-Marquez, Lincoln Caplan, Catherine Crump, Jim Dempsey, Yan Fang, Catherine Fisk, Brandon Garrett, Jonah Gelbach, Albert Gidari, Megan Graham, Chris Hoofnagle, Aziz Huq, Edward Imwinkelried, Amy Kapczynski, Orin Kerr, Christopher Morten, Ngozi Okidegbe, David Oppenheimer, Anna Roberts, Andrea Roth, Paul Schwartz, Jeffrey Selbin, David Sklansky, Christopher Slobogin, Erik Stallman, Jennifer Urban, Pamela Samuelson, Molly Shaffer Van Houweling, John Villasenor, Ari Waldman, Charles Weisselberg, and my Berkeley

JWIG colleagues. Thank you Tyler Slay for faculty support; Chelsea Hanlock, Joon Hwang, Joseph Kroon, and Tyler Takemoto for research assistance; Dean Rowan for reference assistance; and Derek Robertson for additional editing. Emme Tyler and the editors of the *UCLA Law Review* provided excellent editorial work.

TABLE OF CONTENTS

INTRODUCTION

Based on evidence offered by a complaining witness, police in New York City arrested and jailed a man, John Doe, for allegedly violating a family court protective order.[1] The witness provided police with both screenshots of "harassing text messages and phone calls" and a threatening, whispered voicemail that she claimed John Doe sent to her.[2] Neither the police nor the prosecutor questioned the authenticity of this evidence. As such, the man might well have pled guilty while incarcerated or been convicted at trial. Instead, John Doe protested his innocence. He claimed he did not send the texts or leave the voicemail. Hence, his defense counsel[3] challenged the source of the evidence. Defense counsel managed to subpoena a private technology company, called SpoofCard, for records from the alleged victim's paid subscription account.[4] SpoofCard provides a commercial "spoofing" service that permits its users to send text messages and voicemails that appear to originate from someone else's phone number.[5] The company responded to the subpoena and disclosed records establishing that the alleged victim had disguised her own phone number and sent the texts and phone calls to herself, creating the impression that they originated from John Doe's number. She faked the voicemail, as well, using a feature called "voice changer" that altered her voice to sound like a man.[6] When defense counsel showed those records to the prosecutor, the prosecutor dropped the charges and released the man from jail.[7]

This case shows why criminal defense investigations matter. The exonerating evidence was revealed solely because defense counsel could subpoena SpoofCard for records from the alleged victim's account. The government's *Brady*[8] due process and statutory discovery disclosures would not have surfaced this critical evidence because a private company possessed the information, not the

1. Affirmation in Support of Motion for Issuance of Subpoena Duces Tecum at ¶¶ 3, 5, People v. [Redacted], No. [Redacted] (N.Y. Crim. Ct. [Date Redacted]) (on file with author).
2. *Id.*
3. Jerome Greco, Supervising Attorney, Digital Forensics Unit of the Legal Aid Society of New York City.
4. Judicial Subpoena Duces Tecum at ¶ 1, People v. [Redacted], No. [Redacted] (N.Y. Crim. Ct. [Date Redacted]) (on file with author).
5. SPOOFCARD, https://www.spoofcard.com [https://perma.cc/SC3X-VTWZ] (last visited Sept. 21, 2020).
6. SpoofCard User Reports I, II ([Date Redacted]) (on file with author).
7. Interview with Jerome Greco, Supervising Att'y, Digit. Forensics Unit of the Legal Aid Soc'y of N.Y.C, in New York, N.Y. (June 13, 2019).
8. Brady v. Maryland, 373 U.S. 83 (1963).

prosecution team. Subpoenaing the alleged victim herself would also almost certainly have been futile, given her efforts to falsify the records. In a case like this, subpoenas from the defense to private entities seeking records about someone other than the defendant can be the sole means by which that defendant can establish innocence. If something had barred defense counsel from serving that subpoena, John Doe might still be incarcerated today.

Unfortunately, whether due to legislative oversight or the under-representation of criminal defense interests in the political process, multiple privacy statutes do just that: bar defense counsel from subpoenaing private entities for entire categories of information. This threatens to keep exonerating evidence out of defendants' reach. In addition, these privacy statutes skew heavily in favor of law enforcement.[9] The statutes often contain express exceptions that permit police and prosecutors to access protected information but contain textual silence regarding access by criminal defense investigators. Courts have repeatedly interpreted that type of textual silence to categorically prohibit defense subpoenas,[10] which risks wrongful convictions in cases like that of John Doe.

This Article is the first to document this pattern of statutory imbalances across multiple information privacy laws. It introduces the phenomenon of "privacy asymmetries," which are privacy statutes that permit courts to order disclosures of sensitive information if requested by law enforcement but not if requested by the defense. Privacy asymmetries risk unnecessary harms to accuracy and fairness in criminal proceedings by putting entire categories of useful data within the reach of law enforcement investigating guilt but beyond the reach of defense counsel investigating innocence. As explained in Subpart I.A, criminal defense counsel are the sole actors in the U.S. criminal justice system who are tasked with investigating evidence of innocence. Therefore, selectively suppressing defense subpoenas means selectively suppressing evidence of innocence.

Identifying and addressing privacy asymmetries matters urgently now. Digital evidence is increasingly salient[11] in criminal investigations and increasingly possessed by private companies rather than by the government. For example, DNA and face print databases were once primarily if not exclusively possessed by

9. Throughout, I use the term "law enforcement" to refer to both police and prosecutors.

10. *See* Petition for Writ of Certiorari at App. F, Facebook, Inc. v. Superior Ct., 140 S. Ct. 2761 (2020) (No. 19-1006), 2020 WL 703528, at App. F (collecting cases).

11. *See* Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 2 (2004) (on salience, novelty, and technology law); Rebecca Crootof & BJ Ard, *Structuring Techlaw*, 34 HARV. J.L. & TECH. (forthcoming 2021) (on salience and legal analogic reasoning).

government agencies[12] but are now commonplace in the private sector.[13] Data stored by private service providers have proven relevant to both law enforcement[14] and criminal defense investigations. Amazon Echo recordings,[15] cellphone photograph metadata,[16] smart water meter data,[17] pacemaker data,[18] and Fitbit data,[19] to name just a few, have all been used in criminal cases, both to convict and to exonerate.

Private possession of increasing quantities of relevant, digital evidence raises the stakes of privacy asymmetries. As in John Doe's case, exculpatory evidence possessed by private entities falls beyond the scope of the prosecution's disclosure

12. *See, e.g.*, Brandon L. Garrett, *Big Data and Due Process*, 99 CORNELL L. REV. ONLINE (2014).
13. Private sector DNA databases, such as GEDmatch, 23andme, and Ancestry.com, are quickly developing into key resources to conduct genetic searches. *See* Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [https://perma.cc/QW6J-XNK3]. *But cf.* Andrea Roth, *"Spit and Acquit": Prosecutors as Surveillance Entrepreneurs*, 107 CALIF. L. REV. 405 (2019) (prosecutor-collected DNA databases). Regarding private sector face print databases, *see* Kashmir Hill, *Unmasking a Company That Wants to Unmask Us All*, N.Y. TIMES (Jan. 20, 2020) https://www.nytimes.com/2020/01/20/reader-center/insider-clearview-ai.html [https://perma.cc/8JJL-LA3N].
14. *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*,107 CALIF. L. REV. 1753, 1816 (2019) (describing how technology companies that provide life-logging services generate data that may be useful to law enforcement).
15. *See* Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence From Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo [https://perma.cc/F6W7-XW32]; *see also* Joseph Jerome, *Alexa, Is Law Enforcement Listening?*, CTR. FOR DEMOCRACY & TECH. (Jan. 4, 2017), https://cdt.org/insights/alexa-is-law-enforcement-listening [https://perma.cc/B3FC-9MCW].
16. *See* Thomas McMullan, *How an Apple Watch Could Decide a Murder Case*, MEDIUM (June 21, 2018), https://medium.com/s/story/how-an-apple-watch-could-decide-a-murder-case-94314c8d95a2 [https://perma.cc/6V2K-CM8J].
17. *See* Kathryn Gilker, *Bentonville Police Use Smart Water Meters as Evidence in Murder Investigation*, 5 NEWS ONLINE (Dec. 29, 2016, 8:46 AM) https://www.5newsonline.com/article/news/local/outreach/back-to-school/bentonville-police-use-smart-water-meters-as-evidence-in-murder-investigation/527-e74e0aa5-0e2a-4850-a524-d45d2f3fd048 [https://perma.cc/2YNH-5L59].
18. *See* Chris Matyszczyk, *Judge Rules Pacemaker Data Can Be Used Against Defendant*, CNET (July 12, 2017, 7:32 PM), https://www.cnet.com/news/judge-rules-pacemaker-data-can-be-used-against-defendant/?ftag=COS-05-10aaa0b&linkId=39705414 [https://perma.cc/B7ML-7ECK].
19. *See* Nicole Black, *Fitbit Evidence Provides Alibi for Victim's Boyfriend*, LEGALNEWS.COM (Nov. 1, 2018), http://legalnews.com/detroit/1466140 [https://perma.cc/6TWC-L2EL]; Andrew L. Smith, *Meet Your New Star Eyewitness*, CLM MAG., July 2017, at 26; Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J.: L. BLOG (Apr. 21, 2016, 1:53 PM), https://www.wsj.com/articles/BL-LB-53611 [https://perma.cc/UGA7-3NUY].

obligations. As a result, the sole means to surface such evidence may be defendants' independent subpoena powers, which privacy asymmetries quash. At the same time, the introduction of artificial intelligence and machine learning tools into the criminal justice system risks exacerbating the consequences of law enforcement's and criminal defense counsel's disparate access to data. Privacy asymmetries may selectively block defense counsel's ability to deploy and assess existing artificial intelligence and machine learning tools, and impede the development of other tools designed to serve the needs of defense investigators.

Meanwhile, private companies' collection of vast quantities of personal data[20] motivates the passage of new privacy statutes—in turn risking the proliferation of new privacy asymmetries and the further obstruction of defense investigations.[21] At least eight federal privacy bills proposed over the past two years contain privacy asymmetries that selectively disadvantage defense investigators, authorizing evidence gathering that might establish guilt but not that which might establish innocence.[22] In short, the data economy is fueling both the need for criminal

20. Third-party service providers possess data not merely about our emails, internet searches, and consumer purchases, but also about our heart beats, locations, fingerprints, sexual habits, the temperature in our homes, the visitors at our doors, the food in our refrigerators, our family members' genomes, and more. *See generally* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 76–86 (2019) (documenting commercial surveillance platforms and microtargeting advertisements); Danielle Keats Citron, *A New Compact for Sexual Privacy*, WM. & MARY L. REV. (forthcoming 2020); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 29–30 (2019) (describing range of data collected on service users online and offline). *See also* Ari Ezra Waldman, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 10 (2018) (advancing view of "privacy as a social norm based on trust").

21. *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1737–38 (2021).

22. The proposed Data Care Act, S. 3744, 115th Cong. §§ 3(b)(2)(B)(i), 3(b)(3)(A), 4(b)(7)(B) (2018); Data Broker Accountability and Transparency Act, H.R. 6548, 115th Cong. §§ 5(f)(2), 7(b)(4), 7(b)(6) (2018); Balancing the Rights of Web Surfers Equally and Responsibly Act, S. 1116, 116th Cong. §§ 3(a)–(b), 4(c)(4)(A) (2019); and American Data Dissemination Act, S. 142, 116th Cong. § 4(b)(1) (2019), would all impose more onerous burdens on defense investigators than on law enforcement to access the same information. The proposed COVID-19 Consumer Data Protection Act, S. 3663, 116th Cong. §§ 3(a), 3(i), 4(c)(4) (2020); Social Media Privacy Protection and Consumer Rights Act, S. 189, 116th Cong. §§ 3(b), 4(b)(6)(B) (2019); Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S. 2639, 115th Cong. § 2(b)(2)(B)(iii), (e)(3)(A), (e)(3)(C) (2018); and the Privacy Bill of Rights Act, S. 1214, 116th Cong. § 4(a)(1)(E), (a)(1)(E)(i) (2019), all contain notice requirements for disclosures that have exceptions for law enforcement but not for defense investigations. And the California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, entitles consumers to notice of disclosures, and excepts disclosures to "federal, state, or local authorities" or "law enforcement" but not to defense investigators. CAL. CIV. CODE § 1798.145(a)(2)–(3) (West 2020). Specifically, the CCPA preamble states that the law's

defense investigations and the proliferation of privacy asymmetries that undermine those very investigations.[23]

Despite this urgency, privacy asymmetries, as well as the broader relationship between privacy law and criminal defense investigations of which they are a part, have been largely overlooked in legal scholarship. Widespread, ongoing scholarly debates over appropriate privacy safeguards in criminal investigations have focused instead on disclosures of sensitive information to law enforcement.[24] Scholars have debated the effects of technological change on "the balance between privacy rights and law enforcement needs"[25] in Fourth Amendment doctrine;[26] privacy and government subpoena power;[27] transparency surrounding

purpose is to protect "[t]he right of Californians to know whether their personal information is . . . disclosed and to whom." California Consumer Privacy Act of 2018, ch. 55, § 2(i)(2), 2018 Cal. Legis. Serv. (West). Section 1798.100 requires that companies tell consumers about any new uses of personal information beyond the purposes for which the information was initially collected. CAL. CIV. CODE § 1798.100 (West 2020). Section 1798.110 requires that companies tell consumers, upon request by the consumer, about the "categories of third parties with whom the business shares personal information." *Id.* § 1798.110(a)(4). Section 1798.145 states that the disclosure requirements do *not* apply if the company is responding to a criminal "inquiry, investigation, subpoena, or summons by federal, state, or local authorities[,]" or is cooperating "with law enforcement agencies." *Id.* § 1798.145(a)(2)–(3).

23. *Cf.* Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563 (2019); David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 221 (2016) ("Whenever securing privacy on one margin compromises privacy on another margin, a privacy-privacy tradeoff arises.").

24. *See, e.g.*, Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1017 (1995) ("Privacy, at least as the word is used in criminal procedure, protects the interest in keeping information out of the government's hands . . . .").

25. *In re* Askin, 47 F.3d 100, 105–06 (4th Cir. 1995); *see id.* (collecting citations). *See also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

26. For illustrative examples, see Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 485 (2018) (addressing law enforcement's infrastructural capacity as enhanced by private sector surveillance); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205 (2015); and David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1070, 1074–75, 1113–14 (2014) (advocating a "zone of refuge" conception of privacy for Fourth Amendment doctrine, rather than a purely information-centered conception, and noting the particular dangers in permitting government officers and agencies to invade privacy "because of the tools of coercion and violence they can lawfully employ").

27. *See, e.g.*, Christopher Slobogin, *Policing, Databases, and Surveillance*, CRIMINOLOGY, CRIM. JUST. L. & SOC'Y, Dec. 2017, at 70, 72 (recommending that government access to Cloud databases be accompanied by a heightened regulatory regime contingent on the motivation for access); Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805 (2005) [hereinafter Slobogin, *Subpoenas and Privacy*] (tracing the history of government access to

government use of electronic surveillance;[28] statutory privacy protections from government investigations;[29] and law enforcement access to digital evidence possessed by third party service providers;[30] among many other related issues.[31] Especially pertinent here, Erin Murphy has documented in powerful detail how law enforcement interest groups influence legislatures to write exceptions in privacy statutes that permit law enforcement to continue accessing sensitive information.[32] As Murphy observes, the information thus exposed to law enforcement frequently concerns poor, minority, and overpoliced communities.[33] This Article seeks to build on Murphy's work by identifying a related phenomenon whereby criminal defense counsel fail to obtain similar exceptions to privacy statutes.

Defense investigations raise tensions between privacy and truth-seeking that are parallel to their law enforcement counterparts but have received comparatively

personal papers through subpoena and arguing for a more robust standard to protect private information).

28. *See, e.g.*, Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008); Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders*, 93 WASH. L. REV. 145 (2018).

29. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485 (2013).

30. *See, e.g.*, Hannah Bloch-Wehba, *Transparency After* Carpenter, 59 WASHBURN L.J. 23 (2020); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 866–72 (2016) (proposing a "digital curtilage" theory of Fourth Amendment protection for data associated with smart devices); Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 IDAHO L. REV. 661, 667–72 (2015); Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 285–86, 293–96 (2005) (arguing that then-existing privacy protections limiting law enforcement's use of grand jury subpoenas to collect digital evidence from third parties were too lax for the increased salience of that investigative mechanism).

31. Elizabeth Joh has argued persuasively that big data software companies wield "undue influence" over law enforcement and distort Fourth Amendment safeguards. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies in Policing*, 92 N.Y.U. L. REV. ONLINE 19, 38–44 (2017). On the relationship between private companies, the digital services economy, and law enforcement collection of digital evidence from private service providers, see also Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265 (2020); Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183 (2019); Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595 (2016); SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS (2015); Amanda Levendowski, *Trademarks as Surveillance Transparency*, 36 BERKELEY TECH. L.J. (forthcoming 2021); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018).

32. Murphy, *supra* note 29.

33. *Id.*

little attention.[34] To the extent that the literature has addressed defense investigations, it has tended to concentrate on defendants' access to evidence from the government. Scholars have, for instance, critiqued criminal defendants' lack of access to the fruits of government investigations, including government databases[35] and other evidence in the constructive possession of the prosecution.[36] This Article fills a gap in the literature by examining defendants' power—or lack thereof—to compel disclosures from nongovernmental sources.[37]

Part I describes the need for defense investigations in an adversarial system. It then explains and defends the numerous, reasonable baseline privacy safeguards that are already built into those investigations through the criminal subpoena and evidence rules. These rules would control defense subpoenas if privacy

34. Welcome exceptions to this trend to which this Article is especially indebted include Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014) (recognizing that digital evidence poses unique opportunities and challenges for defense representation), and Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569 (2007) (first identifying the Stored Communications Act's imbalanced treatment of law enforcement and defense investigations). *See also* Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. CRIM. L. & CRIMINOLOGY 237, 262 (2019) (describing how digital evidence in criminal cases is exacerbating power imbalances between prosecutors and defendants, in part due to issues with discovering evidence from third parties). Scholarship on the victims' rights movement and rape shield laws has also addressed similar tensions between privacy and truth-seeking. *See, e.g.*, Rosanna Cavallaro, *Rape Shield Evidence and the Hierarchy of Impeachment*, 56 AM. CRIM. L. REV. 295 (2019).

35. *See, e.g.*, Jason Kreag, *Letting Innocence Suffer: The Need for Defense Access to the Law Enforcement DNA Database*, 36 CARDOZO L. REV. 805 (2015) (DNA databases); Jonathan Abel, Brady*'s Blind Spot: Impeachment Evidence in Police Personnel Files and the Battle Splitting the Prosecution Team*, 67 STAN. L. REV. 743 (2015) (police impeachment evidence); Cynthia H. Conti-Cook, *Open Data Policing*, 106 GEO. L.J. ONLINE 1 (2017) (police impeachment evidence); Cynthia H. Conti-Cook, *Defending the Public: Police Accountability in the Courtroom*, 46 SETON HALL L. REV. 1063 (2016) (police impeachment evidence); Garrett, *supra* note 12 (discovery and *Brady* access to government data); Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205 (2015) (due process access to government data); Fairfield & Luna, *supra* note 34 (intelligence authorities' surveillance data); V. Noah Gimbel, Note, *Body Cameras and Criminal Discovery*, 104 GEO. L.J. 1581 (2016); Erin Murphy, *DNA in the Criminal Justice System: A Congressional Research Service Report* (*From the Future)*, 64 UCLA L. REV. DISCOURSE 340, 367 (2016) (raising "important questions surrounding privacy and the proper scope of government access to a person's genetic material"); Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803 (2010).

36. Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180 (2020); Barry Scheck, Preface, *The Integrity of Our Convictions: Holding Stakeholders Accountable in an Era of Criminal Justice Reform*, 48 GEO. L.J. ANN. REV. CRIM. PROC. iii (2019).

37. *Cf.* Jedediah Britton-Purdy, David Singh Grewal, Amy Kapczynski & K. Sabeel Rahman, *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784, 1807 (2020) (identifying and critiquing a "Twentieth-Century Synthesis" in legal scholarship that encased the private market from questions of public justice).

asymmetries were replaced with neutral and symmetrical exceptions for law enforcement and defense investigators alike. Part II documents the privacy asymmetries that layer on top of this baseline subpoena and evidence balancing regime. It shows that privacy asymmetries are a recurring, albeit previously overlooked, phenomenon. Further, they are distributed haphazardly throughout laws that regulate various domains of sensitive information, which suggests that they are unintentional side effects of the legislative process rather than deliberate policy choices. Part III makes the normative case for why privacy asymmetries are an unreasonable policy default and responds to likely counterarguments.

In 1967, Justice John Marshall Harlan II's concurrence in *Katz v. United States*[38] announced the "reasonable expectation of privacy" test for Fourth Amendment searches.[39] That same year, his concurrence in *Washington v. Texas*[40] explained that a Texas rule permitting prosecutors, but not the accused, to introduce codefendants' testimony was unconstitutional because Texas had failed to justify its "discrimination between the prosecution and the defense in the ability to call the same person as a witness."[41] Part IV takes up Justice Harlan's sentiment in the context of privacy law. It recommends that legislators seek to avoid enacting privacy asymmetries unintentionally by adding a default symmetrical savings provision to the end of each privacy statute. It then proposes a model default provision stating: "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."[42] Some lawmakers may wish to depart from this default to deliberately enact asymmetrical privacy safeguards that grant law enforcement more or better access to sensitive information than they afford to criminal defense investigators. In that case, those lawmakers should expressly abrogate defense subpoenas in statutory text and explain in the legislative record why their treatment of law enforcement and defense investigations differs.

38. 389 U.S. 347 (1967).
39. *Id.* at 360 (Harlan, J., concurring).
40. 388 U.S. 14 (1967).
41. *Id.* at 24 (Harlan, J., concurring); *see also* United States v. Burr, 25 F. Cas. 30, 33 (Marshall, Circuit Justice, C.C.D. Va. 1807) (No. 14,692D) ("[W]ith respect to the means of compelling the attendance of witnesses to be furnished by the court, the prosecution and defence [sic] are placed by the law on equal ground.").
42. *Infra* Part IV.

I. CRIMINAL DEFENSE INVESTIGATIONS AND PRIVACY SAFEGUARDS

Before detailing the phenomenon of privacy asymmetries, it is helpful to explain the context in which they operate. Defense investigations, like their law enforcement counterparts, can risk excessive invasions of privacy. For instance, defense subpoenas can implicate sensitive information about an alleged victim's health records, or a witness's interpersonal communications. As a result, the criminal subpoena and evidence rules have developed built-in safeguards to balance defense investigative needs with conflicting privacy interests. This Part presents and defends those baseline privacy protections. To foreground the tradeoffs that the existing protections address, it begins by explaining why defense investigations matter so much in an adversarial justice system. Next, it describes the baseline balancing regime built into the subpoena and evidence rules. Finally, it argues that judicial discretion is a key characteristic that helps to make these safeguards reasonable.

A. The Need for Defense Investigations

In the U.S. adversarial criminal justice system, defense counsel are the sole actors tasked with finding evidence of innocence. Law enforcement has no affirmative duty to investigate exculpatory evidence.[43] This point is worth emphasizing. At no point, from pretrial investigations through to conviction, does law enforcement have any constitutional, legal, or formal ethical obligation to affirmatively investigate evidence of innocence or to seek out any evidence in the possession of a third party that would support a defendant's theory of the case.[44]

43. *See* People v. Hayes, 950 N.E.2d 118, 123 (N.Y. 2011) ("[W]e . . . decline to impose an affirmative obligation upon the police to obtain exculpatory information for criminal defendants . . . ."). And balance of powers concerns may hinder courts from ordering unwilling law enforcement agents to wield their search and seizure powers on behalf of the defense. *See* Zwillinger & Genetski, *supra* note 34, at 596. *But cf.* Carter v. United States, 684 A.2d 331 (D.C. 1996) (government might be required to grant selective immunity to assist defense investigations); United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (declining to adopt the *Carter* framework).

44. Two limited exceptions prove the rule. Postconviction, after the core adversarial stage of a case is over, if a prosecutor "knows of new, credible and material evidence" of innocence, then that knowledge triggers an ethical obligation under the Model Rules of Professional Conduct to investigate whether the defendant was wrongfully convicted. MODEL RULES OF PRO. CONDUCT r. 3.8(g)(2)(ii) (AM. BAR. ASS'N 2020). CRIM. JUST. STANDARDS FOR THE PROSECUTION FUNCTION r. 3-5.4(g) (AM. BAR ASS'N 2017) (and state analogues) also imposes an obligation that "[a] prosecutor should not avoid pursuit of information or evidence because the prosecutor believes it will damage the prosecution's case or aid the accused." Thank you to Ngozi Okidegbe for pointing me to this rule.

Of course, *Brady v. Maryland*[45] and its progeny require prosecutors to disclose material, exculpatory evidence that is in their constructive possession.[46] And statutory discovery rules require prosecutors to disclose certain material information over which they have possession, custody, or control.[47] But disclosure requirements are not investigative duties. *Brady* and statutory discovery procedures apply solely to evidence that the prosecution happens to obtain. When instead a third party possesses crucial exculpatory evidence, that evidence is beyond the reach of these disclosure procedures.

Therefore, rather than rely exclusively on *Brady* and statutory discovery disclosures, defense counsel must conduct independent investigations on behalf of their clients. As the Hawai'i Supreme Court has explained, defense investigations designed:

> to make best use of cross-examination and impeachment of witnesses at trial; . . . to understand the account of [the] client; . . . to [find evidence] not shown in the discovery that "may be significant to the defense"; and . . . to coherently present the case to a jury. . . are inherent to providing effective assistance of counsel and apply in nearly all criminal cases.[48]

Similarly, the American Bar Association's black letter law criminal justice standards require defense counsel to investigate "inconsistencies, potential avenues of impeachment of prosecution witnesses, and other possible suspects and alternative theories that the evidence may raise."[49]

There are myriad reasons that defense counsel might pursue information in fulfilling their investigative mandate. Defense counsel might seek to obtain impeachment information about nonparties,[50] including police witnesses,[51] other prosecution witnesses, the defendant's own witnesses, and complaining witnesses.

45. 373 U.S. 83 (1963).
46. *See* Kyles v. Whitley, 514 U.S. 419, 437 (1995); Giglio v. United States, 405 U.S. 150 (1972).
47. *See, e.g.*, FED. R. CRIM. P. 16; ROBERT M. CARY, CRAIG D. SINGER & SIMON A. LATCOVICH, FEDERAL CRIMINAL DISCOVERY 2 (2011).
48. State v. Tetu, 386 P.3d 844, 861–62 (Haw. 2016); *see also* Eleanor Swift, *Narrative Theory, FRE 803(3), and Criminal Defendants' Post-Crime State of Mind Hearsay*, 38 SETON HALL L. REV. 975, 983–86, 1007 (2008) (explaining "narrative theory" of jury decisionmaking and advocating for admissibility of defendants' state of mind hearsay to present a coherent story).
49. CRIM. JUST. STANDARDS FOR THE DEFENSE FUNCTION r. 4-4.1(c) (AM. BAR ASS'N 2017).
50. I use the term "nonparty" to refer to individuals other than the government or the accused, and "third party" to refer to entities such as communications service providers who may be subpoenaed for information about their users.
51. *See* People v. Rouse, 140 N.E.3d 957, 959 (N.Y. 2019) (concluding that the trial court "committed reversible error in refusing to allow defendant to cross-examine" police officer witnesses concerning evidence of prior "office dishonesty").

If a defendant argues third party guilt, claiming that a different individual committed the alleged crime, defense investigators might seek information about that alternate third-party suspect. Defense counsel might investigate a client's codefendants to show that the client played a relatively small role in a criminal enterprise or was threatened into participating, or to identify other mitigating circumstances. Defense counsel might also investigate to corroborate an alibi or to seek information about locations associated with the case, such as to examine the alleged crime scene for lines of sight in order to challenge the reliability of an eyewitness. Each of these types of inquiry are legitimate and can be essential to effective defense representation. Pursuing them is why defendants have Sixth Amendment and due process rights to investigative powers,[52] as well as statutory subpoena rights.[53]

B. Reasonable Privacy Safeguards in Subpoena and Evidence Rules

As essential as defense investigations are, they, like their law enforcement counterparts, can risk excessive invasions of privacy. To address this risk, the legal process requirements for defense counsel to exercise investigative power incorporate multiple safeguards and oversight mechanisms that balance defendants' investigative needs with conflicting privacy interests. These status quo privacy safeguards would apply to defense investigations if privacy asymmetries were eliminated and legislators instead adopted the default symmetrical savings provision recommended in Part IV. As detailed below, these baseline privacy safeguards have at least two key characteristics that help make them reasonable. First, they are rarely if ever absolute; they incorporate judicial discretion to override privacy protections on a case-by-case basis in circumstances that would otherwise create injustice. Second, the level of judicial discretion varies inversely with the breadth of the privacy protection.

More specifically, under the baseline subpoena and evidence rules, privacy interests do not by default defeat a litigant's right to compel the production of relevant evidence.[54] In John Henry Wigmore's words, "[n]o pledge of

52. *See generally* Peter Westen, *Confrontation and Compulsory Process: A Unified Theory of Evidence for Criminal Cases*, 91 HARV. L. REV. 567, 574–89 (1978).

53. *See* FED. R. CRIM. P. 17. Defendants may also rely on open records laws and other avenues for obtaining information that are available to the public generally.

54. *See, e.g.*, 3 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 2211, at 2998 (1904) ("The mere fact that a document concerns the private affairs of the witness . . . does not create a privilege . . . . [A]ny and every document may be called for, however personal and private its contents may be."); United States v. Tilden, 28 F.

privacy . . . can avail against demand for the truth in a court of justice."[55] Nonetheless, the subpoena and evidence rules do strictly limit the exercise of defense investigative powers. Those limits apply in stacking tiers, like a pyramid. The initial, bottom layer of privacy safeguards broadly protects any type of private information while incorporating high levels of judicial discretion to override the protection and compel disclosure as needed. The middle layer more narrowly applies to particular categories of especially sensitive information and imposes heightened privacy safeguards that incorporate less judicial discretion to override on a case by case basis. At the very top layer are evidentiary privileges. Privileges apply to exceedingly narrow categories of information and offer extremely strong privacy protections that incorporate the least amount of judicial discretion to override.

Beginning at the bottom layer, which applies to the broadest amount of information and incorporates the most judicial discretion, subpoena rules protect privacy through mandatory judicial oversight, high threshold burdens to enforce, and substantial judicial discretion to quash. Crucially, defense counsel cannot compel nonparties to produce documents without judicial oversight[56] because subpoenas are a process of the courts, not of the litigants before them.[57] Even when statutes authorize attorneys to issue subpoenas on behalf of the court, the subpoenaed documents remain under the court's control.[58] Defense counsel must also satisfy challenging threshold burdens to enforce subpoenas—burdens that can be difficult or even impossible to satisfy for evidence that defense investigators have not yet seen.[59] Defense counsel must establish that they are using the

Cas. 174, 177–78 (S.D.N.Y. 1879) ("[P]arties litigant have the right to have private writings which are competent for proof in their causes produced in evidence; and to this imperative demand of justice, all scruples as to the confidential character of the writings as private property, except in certain well-ascertained exceptions growing out of professional employment, must yield from considerations of public policy.").

55. *See also* 4 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 2286, at 3186 (1905).

56. To be sure, defense attorneys can and do send cover letters requesting that subpoena recipients voluntarily share documents earlier, or send courtesy copies to defense counsel. Businesses might, for instance, willingly share copies of surveillance tapes with defense investigators on request. But these types of cover letters are not subpoenas and have no binding legal authority.

57. *See, e.g.*, People v. Natal, 553 N.E.2d 239, 241–42 (N.Y. 1990) (finding it is error for an attorney subpoena to make documents returnable directly to the attorney, circumventing the court).

58. *Id.*

59. State analogues are similarly challenging. The New York Court of Appeals, for example, requires "a good faith factual predicate sufficient . . . to draw an inference that specifically identified materials are reasonably likely to contain information that has the potential to be both relevant and exculpatory." People v. Kozlowski, 898 N.E.2d 891, 902 (N.Y. 2008).

subpoena to access evidence that they already know is likely to be relevant and not using the subpoena to discover new evidence.[60] For instance, pretrial, federal defendants must show a "good faith" likelihood that the documents sought are "relevant" and "admissible," and must identify the documents with enough "specificity" to allay concerns of a "fishing expedition."[61] Even if defendants satisfy these burdens, judges retain broad discretion to quash subpoenas if compliance would be "unreasonable or oppressive."[62] Privacy intrusions are a basis for quashal,[63] as is the availability of information from alternate, less privacy-intrusive means.[64]

Meanwhile, evidence rules protect privacy at this vast bottom layer through trial judges' discretion to limit the introduction of evidence on collateral issues,[65] and to restrict the scope of witness examination and cross-examination,[66] as well as through judges' general authority to manage their courtrooms and the presentation of evidence. For instance, the Federal Rules of Evidence instruct judges to make "procedures effective for determining the truth[,]" and to "protect witnesses from harassment or undue embarrassment."[67] Following that

60. *See In re* Terry D., 619 N.E.2d 389, 390 (N.Y. 1993).

61. United States v. Nixon, 418 U.S. 683, 699–700 (1974). Most federal circuits apply the *Nixon* standard broadly, although its scope is subject to some debate. *See* Douglas E. Roberts, *SCOTUS Asked to Determine Third Party Subpoena Standard in Criminal Cases*, LEXOLOGY (Nov. 1, 2016), https://www.lexology.com/library/detail.aspx?g=71c862a2-4bc0-4eba-80b6-a47d96659803 [https://perma.cc/8C5P-7UQK]; Benjamin E. Rosenberg & Robert W. Topp, *The By-Ways and Contours of Federal Rule of Criminal Procedure 17(C): A Guide Through Uncharted Territory*, 45 CRIM. L. BULL. 195 (2009).

62. FED. R. CRIM. P. 17(c)(1)–(2); *cf.* WIGMORE, *supra* note 54, § 2211, at 2998 (noting a judge's discretion to quash subpoenas where "the document's utilty in evidence would not be commensurate with the detriment to the witness").

63. *See, e.g.*, CAL. CIV. PROC. CODE § 1987.1(a) (West 2013) ("[T]he court may make any other order as may be appropriate to protect the person from unreasonable or oppressive demands, including unreasonable violations of the right of privacy of the person.").

64. *See, e.g.*, Facebook, Inc. v. Superior Court, 417 P.3d 725, 755 (Cal. 2018) ("[A]ny third party or entity—including a social media provider—may defend against a criminal subpoena by establishing that, for example, the proponents can obtain the same information by other means, or that the burden on the third party is not justified under the circumstances.").

65. *See, e.g.*, People v. Gissendanner, 399 N.E.2d 924, 927 (N.Y. 1979) (explaining the "traditional evidentiary rule" that the availability of proof of collateral issues "rests largely on the exercise of a sound discretion by the trial court").

66. *See* 2 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 944, at 1081, § 1006, at 1168 (1904) ("[I]n extracting evidence by cross-examination the *largest possible scope* shall be given . . . ; the scope in a given instance being left chiefly to the *discretion of the trial Court*.").

67. FED. R. EVID. 611(a)(1), (a)(3). *But see* David S. Schwartz & Chelsey B. Metcalf, *Disfavored Treatment of Third-Party Guilt Evidence*, 2016 WIS. L. REV. 337, 395 (arguing that "evidence codes provide virtually no grounds for a court to limit evidence in order to protect reputational rights, especially of non-witnesses" and that Federal Rule of Evidence (FRE) 611 merely

instruction necessarily involves an ad hoc balancing of competing interests according to the "particular circumstances" of a case.[68] The rules of evidence are also incorporated into, and narrow, the subpoena power; the requirement that subpoenaed information must be "admissible" means that subpoenas cannot reach information that the evidence rules clearly exclude from admissibility at trial, such as information protected by rape shield laws.[69]

The middle layer protections are content-specific and incorporate less judicial discretion. For instance, the subpoena rules include a special requirement to notify alleged victims about subpoenas that seek private information about them from nonparty intermediaries,[70] such as their "medical or school records"[71] obtained from a hospital or educational institution. That rule is designed to recognize victims' rights to "privacy."[72] Yet, even in this especially sensitive scenario, the rule includes judicial discretion. Judges may override the notice requirement on an ex parte basis[73] if, for example, providing such notice could put evidence at risk of being "lost or destroyed" or unfairly prejudice the defendant.[74] Indeed, as with law enforcement, when defense counsel investigate dangerous or untrustworthy individuals who might threaten or intimidate witnesses or spoliate evidence, defense counsel may apply to the court for a

restricts the mode of cross-examination, not the admission of reputation-damaging evidence). Hurdles to the admissibility of evidence of third-party guilt have also sometimes been justified as protections for third-party reputational interests, although David Schwartz and Chelsey Metcalf have shown the weakness of this rationale. *Id.* at 351, 394–96 (identifying forty-five states and ten federal circuits that impose such hurdles); *see also* 1 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 139 (1904) (commission of crime by a third person).

68. FED. R. EVID. 611 advisory committee's note to Subdivision (a) (1972).

69. Criminal subpoenas are thus far narrower than their civil counterparts, which reach any information likely to lead to the discovery of admissible evidence. *See also* Meg Garvin, Alison Wilkinson & Sarah LeClair, *Protecting Victims' Privacy: Moving to Quash Pretrial Subpoenas Duces Tecum for Non-Privileged Information in Criminal Cases*, NAT'L CRIME VICTIM L. INST.: VIOLENCE AGAINST WOMEN BULL. 1 (Sept. 2014), https://law.lclark.edu/live/files/18060-quashing-pretrial-subpeonasbulletinpdf [https://perma.cc/FQ8K-46D8].

70. FED. R. CRIM. P. 17(c)(3).

71. FED. R. CRIM. P. 17(c)(3) advisory committee's note to 2008 amendment.

72. *Id.* (quoting Crime Victims' Rights Act, 18 U.S.C. § 3771(a)(8)).

73. *Id.* (leaving to judge's discretion whether to decide issue of exceptional circumstances ex parte).

74. *Id.* Note that courts generally retain discretion to issue ex parte subpoenas under seal to prevent premature and prejudicial disclosures of defense strategy to the government. *See, e.g.*, Defendant Arturo Lopez's Unopposed Motion to Compel Compliance With Subpoena Duces Tecum for Sprint/Nextel at 1 n.1, United States v. Lopez, No. H-05-446 (S.D. Tex. Apr. 24, 2006), 2006 WL 5002747 (subpoena for defendant's own historical cell-site location information [CSLI] issued under seal to preserve confidentiality of an alibi defense from premature exposure to the prosecution).

nondisclosure order prohibiting a third party served with a subpoena from notifying the target of the investigation.[75]

Top layer privacy protections—evidentiary privileges—are extraordinarily strong, highly content-specific, and incorporate the least amount of judicial discretion to override. Privileges are exclusionary rules of evidence that shield very particular information from adjudication, not because the information lacks relevance[76] or reliability,[77] but rather, to serve social policies that are extrinsic to the truth-seeking process of the courts, including privacy.[78] Illustrating the strength of privileges, privileged communications are protected even after they are lawfully seized by the government, such as through an authorized wiretap[79] or warranted search of an electronic device.[80] Even privileges, though, incorporate some safety-valve judicial discretion to override the privilege protections in extreme

75. In *People v. Touchstone*, for example, the trial court issued such an order accompanying a defense subpoena to Facebook, stating: "The Court further orders that Facebook, Inc., the District Attorney, and law enforcement NOT disclose this Order directing preservation, as such notification may lead to tampering with or destruction of evidence." Order for Preservation of Stored Account Content, People v. Touchstone, No. SCD268262 (Cal. Sup. Ct. Mar. 16, 2017) (on file with author). *See also* Facebook, Inc. v. Pepe, 241 A.3d 248 (D.C. 2020) (evaluating a defense-initiated nondisclosure order to Facebook accompanying a subpoena for First Amendment strict scrutiny compliance).

76. *Cf.* FED. R. EVID. 402 (excluding irrelevant evidence).

77. *Cf.* FED. R. EVID. 803 (hearsay exclusions).

78. *See* Edward J. Imwinkelried, *The Alienability of Evidentiary Privileges: Of Property and Evidence, Burden and Benefit, Hearsay and Privilege*, 80 ST. JOHN'S L. REV. 497, 508 (2006) (positing that "the protection of privacy is the *raison d'etre* for granting privilege protection").

79. *See* 18 U.S.C. § 2517(4) ("No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.").

80. At least twenty state bar associations have found that attorney-client privilege is not waived by storing information in the cloud with sufficient confidentiality protections, such as passwords. *See* Mark C. Palmer, *Can Lawyers Ethically Store and Transmit Client Info in the Cloud?*, ATT'Y AT WORK (July 16, 2018), https://www.attorneyatwork.com/client-information-cloud-ethics [https://perma.cc/95KF-LQH7].

The government may engage in ex post minimization procedures such as using a "taint team" to purge privileged content prior to delivering the materials to the prosecution team. *See* Eric D. McArthur, Comment, *The Search and Seizure of Privileged Attorney-Client Communications*, 72 U. CHI. L. REV. 729, 740–44, 751 (2005). To be sure, some scholars believe that privileges are not absolute, and can always be defeated with a sufficient showing of necessity. *See* Edward J. Imwinkelried, *Questioning the Behavioral Assumption Underlying Wigmorean Absolutism in the Law of Evidentiary Privileges*, 65 U. PITT. L. REV. 145, 162–67 (2004). For example, in *Nixon*, a demonstration that subpoenaed information was "essential to the justice of" a pending criminal case defeated the President's claim to a generalized, nonmilitary, nondiplomatic confidential communications privilege, despite the constitutional basis of that privilege. *See* United States v. Nixon, 418 U.S. 683, 713–14 (1974). Nonetheless, defeating a privilege requires a significantly more onerous showing of need than would otherwise be required for legal process, whether a subpoena or a warrant.

circumstances. For instance, multiple statutory privileges contain express exceptions for circumstances in which applying them would "deprive the People or the defendant of a fair trial."[81] And even those privileges that are facially absolute and constitutionally grounded, such as the attorney-client privilege, are sometimes pierced by defendants' competing constitutional interests in accessing evidence of innocence.[82]

In sum, subpoena and evidence rules have built-in privacy safeguards in the form of mandatory judicial oversight, high threshold burdens, judicial discretion to quash, and—for particularly sensitive information—notice and privilege. These safeguards range from broad baseline protections that apply to private information generally and incorporate substantial judicial discretion to override, to narrow heightened protections that apply to very specific private information and incorporate less judicial discretion to override. The closest that the rules come to absolute privacy protections are privileges. Yet, even at that top layer, the rules often contain some safety-valve judicial override options for edge cases in which abiding by the safeguards would risk extreme harm. These override options inject critical nuance into the privacy protections. As will be explored in Part III, *infra*, privacy asymmetries generally lack these reasonable characteristics of judicial discretion, and of discretion that is inversely correlated with the breadth of privacy protection. Before delving into that absence, though, Part II introduces the phenomenon of privacy asymmetries.

II. THE RECURRING AND HAPHAZARD PHENOMENON OF PRIVACY ASYMMETRIES

A diverse set of information privacy statutes shield specific categories of sensitive data stored with service providers, including internet communications, financial transactions, health records, and more. These statutes often protect privacy by restricting the circumstances in which service providers, such as online video streaming sites, banks, and hospitals, may disclose information about the people who use their services. Many of the statutes include express textual exceptions that authorize disclosures to law enforcement but remain silent regarding disclosures to criminal defense investigators. Courts have repeatedly

81. CAL. EVID. CODE § 1062 (West 2021).

82. *See* Morales v. Portuondo, 154 F. Supp. 2d 706, 729–31 (S.D.N.Y. 2001) (habeas proceeding overriding attorney-client privilege to introduce evidence of innocence). Of course, defendants' constitutional rights could also defeat statutory privacy asymmetries on an as-applied constitutional challenge.

construed that pattern of statutory text to permit law enforcement access while categorically barring criminal defense subpoenas.[83] Therefore, in current practice,[84] these facial textual disparities, or "privacy asymmetries," permit judges to order disclosures of sensitive information when requested by prosecutors but not when requested by criminal defense counsel.[85]

Privacy asymmetries come in two types: "access asymmetries" and "notice asymmetries." Access asymmetries block defense investigators' access to certain information, or to a key source for the information, while permitting access to law enforcement. Notice asymmetries selectively block defense investigators' capacity to engage in confidential investigations, whether by preventing them from delaying an otherwise-required notice to the target of an investigation or by preventing them from obtaining a court order that prohibits a third-party recipient of a subpoena from informing the target about the receipt of legal process. Notice asymmetries sometimes create access asymmetries. This happens when notifying the target of an investigation would create such serious risks, like the destruction of evidence or threats to life or physical safety, that requiring notice effectively precludes access altogether. And access asymmetries sometimes create notice asymmetries. This happens when a statute bars access to the sole confidential source for information, leaving defense counsel with no alternative but to seek information directly from the target of their investigation and thereby notify them in the process.

This Part presents examples of privacy asymmetries drawn from across the patchwork of federal statutes that make up U.S. information privacy law.[86] It examines statutes that protect various domains of sensitive information, ranging from the contents of messages stored by social media companies, to health and substance abuse treatment records possessed by medical service providers, to

83. *See generally* Facebook, Inc. v. Pepe, 241 A.3d 248, 258 n.34 (D.C. 2020) (collecting cases).

84. In *Privacy as Privilege*, I argue that courts should construe this pattern of statutory text differently to yield to otherwise valid criminal defense subpoenas. If courts were to adopt that recommended construction, many privacy asymmetries would be eliminated. Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021).

85. Note that this definition of privacy asymmetries focuses on facial textual disparities in privacy statutes. Privacy asymmetries sometimes operate alongside other constitutional and statutory disparities between the government's and criminal defendants' access to, and requirements to obtain, different forms of compulsory legal process, such as warrants, administrative subpoenas, grand jury subpoenas, and trial subpoenas. This Article takes no position on the symmetries or asymmetries of these other criminal procedure and evidence rules.

86. *See, e.g.*, Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RSRV. L. REV. 297, 308–09 (2003) (describing "a panoply of federal, state, and regulatory guidelines" that protect information privacy in the United States).

information obtained through criminal trespass or wiretapping. In each information domain, it details statutes with and without privacy asymmetries. To avoid a laundry list of statutory interpretation, the discussion below offers a high-level summary of each example followed by two tables that synthesize the distribution of privacy asymmetries within and across information domains. The Appendix provides a more detailed analysis of each statute, including relevant text, legislative history, judicial interpretations, and significance to criminal defense investigations.

Taken together, the examples described below show that privacy asymmetries appear repeatedly in information privacy statutes; they are a recurring, albeit previously overlooked, phenomenon. These examples also show that privacy asymmetries are distributed haphazardly amidst facially symmetrical privacy statutes. This is so both within and across information domains. This haphazard distribution indicates that privacy asymmetries do not reflect consistent policy choices about how to treat different categories of sensitive information and suggests, instead, that they are legislative accidents.

Two inconsistencies are particularly striking and consequential. There are privacy asymmetries for electronic communications possessed by private internet companies but not for physical letters possessed by private mail carriers. And there are privacy asymmetries for unauthorized access to computer networks but not for physical trespass onto private property. These inconsistencies matter because they undermine a likely defense of privacy asymmetries: that the asymmetries simply mirror, in the digital world, longstanding disparities between law enforcement and defense investigations in the physical world.[87] As discussed in greater detail in Subpart III.C.1, *infra*, the inconsistencies between the privacy asymmetries for private electronic communications services and computer systems, and the facially symmetrical statutes that govern access to private paper mail services and physical trespass, rebut this line of argument.

87. Commentators have repeatedly analogized federal statutory prohibitions on unauthorized access to computer systems to statutes that criminalize physical trespass. *See, e.g.*, Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1498 (2016) (arguing that "'authorization' under the [Computer Fraud and Abuse Act] CFAA has the same meaning as authorization under criminal physical trespass laws"). *But see* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 542 (2003) (critiquing "blind application" of a physical space metaphor to cyberspace law). For a full discussion of the role of this analogy in defending privacy asymmetries, see *infra* Subpart III.C.1.

A. Communications Contents

Statutes within the communications contents information domain protect privacy in the contents of written and oral messages that are sent through intermediary service providers. Examples include letters, emails, social media messages, and telephone conversations sent through services such as the postal mail, Gmail, Facebook, or Verizon. Messages transmitted over these communications networks can raise substantial privacy concerns because of the risk that the network service providers might access, use, or reveal the contents of the messages without authorization.[88] Various federal statutes have addressed this risk in part by limiting when communications service providers may disclose the contents of messages that they possess.[89] Some of these statutes contain privacy asymmetries, while others have facially symmetrical exceptions that treat law enforcement and defense investigators alike.

Starting with the asymmetrical statutes, the Postal Accountability and Enhancement Act generally prohibits U.S. postal employees from opening sealed letters that are possessed by the U.S. postal service; the Act contains an express exception permitting law enforcement officers to compel access to sealed letter contents, but the statutory text is silent on defense access.[90] Similarly, the Stored Communications Act generally prohibits private technology companies, such as Google and Facebook, from disclosing the contents of stored electronic messages; the Act contains an express exception permitting law enforcement officers to compel such disclosures, but the statutory text is silent on defense access.[91] Construing that statutory silence to selectively bar defense subpoenas risks creating both access and notice asymmetries by foreclosing the sole means for defendants to compel discrete disclosures without alerting the target of an investigation.

In contrast, no similar asymmetry applies to the closely analogous scenario of letters possessed by private mail service providers, such as FedEx or UPS.[92] Nor are there privacy asymmetries in the federal statutes that protect privacy in the

88. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 523–48 (2006) (discussing privacy harms from improper "information dissemination" as distinct from harms of improper information collection and processing).

89. In other words, this domain includes statutes that regulate service providers' disclosures of message contents that they already possess, such as messages possessed as a result of previously authorized wiretapping, but does not include statutes that regulate the initial collection of message contents, such as by engaging in wiretapping.

90. 39 U.S.C. § 404(c).

91. 18 U.S.C. 2702.

92. *See infra* Appendix.

contents of previously intercepted and stored wire communications. The Wiretap Act generally prohibits service providers from disclosing the contents of wire conversations,[93] but the Act contains a facially symmetrical express exception that authorizes disclosures in courtroom testimony of the contents of communications that were previously intercepted with authorization.[94] The historical predecessor to this portion of the Wiretap Act was also symmetrical. The relevant portion of that law—the Communications Act of 1934—generally prohibited service providers from disclosing the contents of wire conversations, but the Act included a facially symmetrical express exception permitting the providers to disclose any known communications contents in response to court-ordered subpoenas or "other lawful authority."[95] Note that the laws that govern disclosures of previously intercepted wiretap materials are distinct from laws that control real time intercepts of communications in transit. This Subpart discusses the former. Subpart II.D, *infra*, discusses the latter.

The privacy asymmetries in the Postal Accountability and Enhancement Act, and in the Stored Communications Act, thus do not reflect a consistent policy choice across the broader domain of communications contents transmitted through intermediary service providers.

B. Noncontent Digital Services Records

Beyond the contents of messages, other statutes protect privacy in sensitive noncontent information that digital service providers possess about their users. Sensitive noncontent information can be generated through the use of a wide variety of digital services. Illustrative examples include users' heartbeats, location data, website login times, biometric information, personal and professional associations, and patterns of reading, viewing, and purchasing, all of which may be tracked and stored by companies such as Fitbit, Netflix, Google, and Amazon. As with message contents, service providers' possession of sensitive noncontent information can raise substantial privacy concerns due to the risk that the providers might access, use, or reveal the information improperly.[96] Various federal statutes mitigate these risks by regulating when digital service providers

93. 18 U.S.C. § 2511(3)(a).
94. *See infra* Appendix.
95. Communications Act of 1934, Pub. L. No. 73-416, ch. 652, § 605, 48 Stat. 1064, 1103–04 (codified as amended in scattered sections of 47 U.S.C.).
96. *See, e.g.*, Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 586 (2003) (discussing privacy harms from resale of noncontent data about internet users' "intellectual preferences").

may disclose noncontent records about their users. Once again, some of these statutes contain privacy asymmetries and others do not.

Beginning again with the asymmetries, the Video Privacy Protection Act generally prohibits video rental service providers, including online streaming services such as Hulu and iTunes, from disclosing personally identifiable information about their users; the statutory text contains an express exception permitting law enforcement officers to compel access to this information with prior notice to the user, but the text remains silent on defense access.[97] The Act thus creates an access asymmetry but not a notice asymmetry. The Stored Communications Act's provisions concerning noncontent information are also symmetrical as to notice, but they contain an atypical access asymmetry that facially disadvantages law enforcement.[98] Specifically, the Act imposes special requirements for law enforcement to compel disclosures of noncontent information, not including notice to the user,[99] while expressly permitting unrestricted disclosures to nongovernmental persons.[100]

Meanwhile, federal statutes that protect privacy in noncontent records pertaining to children's online behavior and to cable subscriber records are facially symmetrical.[101] The Children's Online Privacy Protection Act generally prohibits covered online service providers from disclosing information about child users without parental consent,[102] but the text contains a facially symmetrical exception for disclosures made "to respond to judicial process."[103] Similarly, the Cable Communications Policy Act generally prohibits cable operators from disclosing personally identifiable information about their subscribers,[104] but the text contains express exceptions that permit either law enforcement or defense counsel to obtain court-ordered disclosures with prior notice to the subscriber.[105]

Privacy asymmetries are thus inconsistent across the broader domain of sensitive noncontent information possessed by digital service providers.

97. 18 U.S.C. § 2710(b)(2)–(3).
98. In practice, law enforcement investigators are likely still advantaged over defense investigators because the baseline standards for defendants to obtain subpoenas are more onerous than the requirements that the Stored Communications Act imposes on law enforcement. For details, *see infra* Appendix.
99. 18 U.S.C. 2703(c)(1)–(3).
100. 18 U.S.C. 2702(c)(6).
101. *See infra* Appendix.
102. 15 U.S.C. 6502(b)(1)(A)(ii).
103. 15 U.S.C. 6502(b)(2)(E)(iii).
104. Cable Communications Policy Act, 47 U.S.C. § 551(c)(1) (2012).
105. 47 U.S.C. § 551(c)(2)(B), (h).

C. Financial, Educational, and Health Records

A third cluster of statutes protect privacy in information concerning specific, sensitive subject matter that various service providers possess about the people who use their services. For instance, a bank, school, or hospital may possess information about a customer's financial information, a student's disciplinary history, or a patient's health status. As with the statutes discussed above, service provider possession of this type of information raises privacy concerns due to the risks that the service providers might improperly access, use or disseminate the information.[106] Topical privacy statutes mitigate those risks by regulating when service providers that possess covered information may disclose it. Once again, some of these statutes contain privacy asymmetries while others do not.

Indeed, the distribution of asymmetries does not even reflect a consistent policy choice about financial documents alone. A variety of overlapping federal laws regulate disclosures of financial records in criminal investigations.[107] These laws contain at least one privacy asymmetry disadvantaging defendants, one facially symmetrical statute, and one notice asymmetry that, again atypically, disadvantages law enforcement. More specifically, Section 6103 of the Tax Code generally bars the IRS from disclosing federal tax returns; the Act contains express exceptions for disclosures to federal law enforcement, but the statutory text is silent on defense access.[108] In contrast, the pre-1977 version of Section 6103 contained a symmetrical express exception for all court-ordered disclosures.[109] Today, the Gramm-Leach-Bliley Act gives financial services customers certain rights to notice of disclosures, but it contains a facially symmetrical express exception for disclosures made "to respond to judicial process."[110] And the Right to Financial Privacy Act is asymmetrical disadvantaging law enforcement because it imposes a default notice requirement on federal law enforcement investigators

106. *See generally* Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1228 (2017) (discussing legal obligations on fiduciaries "to protect their client's privacy" by restricting their disclosure of information about their clients); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1209–10 (2016) (same).

107. Cohen, *supra* note 96. *See also* Mohammed Shahabuddin, *Post-colonial Boundaries, International Law, and the Making of the Rohingya Crisis in Myanmar*, 9 ASIAN J. OF INT'L L. 347 (2019).

108. 26 U.S.C. § 6103(i)(1)(A), 6103(i)(2)–(7).

109. *See* McSurely v. McAdams, 502 F. Supp. 52, 55 & n.6 (D.D.C. 1980).

110. 15 U.S.C. § 6802(a), (e)(5), (8).

seeking customer records from financial services providers but no such requirement on defense investigators.[111]

Examining privacy protections for educational and health records adds no readily discernable logic to the distribution of privacy asymmetries. With respect to educational records, the Family Educational Rights and Privacy Act creates a notice asymmetry without an access asymmetry. The Act and related regulations authorize schools to disclose students' disciplinary records pursuant to "any lawfully issued subpoena,"[112] but they require predisclosure notice to both students and their parents.[113] The regulations then establish procedures for law enforcement to circumvent the notice requirement,[114] but they remain silent as to defense investigators.[115]

In terms of health information, federal regulations that protect privacy in substance abuse treatment records asymmetrically disadvantage defendants, while a key federal statute that protects privacy in general medical records is facially symmetrical. Specifically, federal regulations impose a general confidentiality requirement on federally-assisted providers of substance abuse treatment[116] that expressly bars compliance with unexempted subpoenas.[117] The regulations then expressly exempt disclosures to law enforcement,[118] prosecutors,[119] and civil litigants,[120] sometimes with and sometimes without required notice,[121] but they are silent as to criminal defense investigators. In contrast, the Health Insurance Portability and Accountability Act and related

111. 12 U.S.C. §§ 3404(c), 3405(2), 3406(c), 3407(2), 3408(4), 3412(b). The practical consequence of this asymmetry is lessened because law enforcement can obtain court orders to delay notice, potentially indefinitely. *See* 12 U.S.C. § 3409(a)(3)(A)–(E), (b)(1)–(2).
112. 20 U.S.C. § 1232g(b)(2)(B).
113. 34 C.F.R. § 99.31(a)(9)(i)–(ii) (2020); *see* Reeg v. Fetzer, 78 F.R.D. 34, 36–37 (W.D. Okla. 1976) (holding that the Family Educational Rights and Privacy Act [FERPA] imposes a notice obligation but does not create an evidentiary privilege).
114. 34 C.F.R. § 99.31(a)(9)(ii)(B) (2020).
115. *Id.* § 99.31(a)(9)(ii)(A)–(C).
116. *See* 42 C.F.R. § 2.13(a) (providing that patient records "may be disclosed or used only as permitted by the regulations in this part and may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any federal, state, or local authority").
117. *See* 42 C.F.R. § 2.13(b) ("The restrictions on disclosure . . . apply whether or not . . . the person seeking the information . . . has obtained a subpoena. . . . "); 42 C.F.R. § 2.20 ("[N]o state law may either authorize or compel any disclosure prohibited by the regulations in this part.").
118. *See* 42 C.F.R. § 2.65.
119. *See* 42 C.F.R. § 2.65.
120. *See* 42 C.F.R. § 2.64.
121. *Compare* 42 C.F.R. § 2.65(b) *and* § 2.66(b).

regulations[122] impose a default notice requirement on disclosures of medical and mental-health records pursuant to an attorney-signed subpoena.[123] But the regulations contain facially symmetrical express exceptions that permit either law enforcement or defense investigators to circumvent the notice requirement with judicial approval.[124] In other words, the general medical records privacy statute and regulations provide for symmetrical access without notice.

Taken together, privacy asymmetries are distributed irregularly in topical privacy statutes that protect financial, educational, and health records.

D. Criminal Intercepts and Unauthorized Access

The statutes discussed in the prior three Subparts rely on civil liability to protect individuals from the risk that a service provider might reveal sensitive information about them without authorization. But there can also be privacy risks from another source, namely that an eavesdropper might break into a network or storage facility.[125] Multiple statutes address this latter concern by criminalizing the interception of sensitive information while the information is in transit between the sender and intended recipient, or by criminalizing unauthorized access to computer networks where sensitive data may be stored. Like the civil statutes discussed above, these criminal statutes also often contain investigative exceptions.

Incorporating investigative exceptions into statutes that prohibit intercepts or unauthorized access poses distinct privacy risks. Investigators engaged in real time intercepts cannot know in advance precisely what information they will encounter and when. Meanwhile, investigators engaged in unauthorized access may encounter substantial quantities of irrelevant information while pursuing particular documents or records. Intercepts and unauthorized access thus create peculiar risks of overcollection. One might, therefore, imagine that the distribution of privacy asymmetries within criminal statutes for intercepts and

122. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, & 42 U.S.C.); *see also* 45 C.F.R. §§ 160, 162, 164 (2020) (promulgating regulations from the Department of Health and Human Services guiding operation of HIPAA).

123. *See* 45 C.F.R. § 164.512(e)(1)(vi).

124. *See id.* § 164.512(e)(1)(i)–(vi), (f)(1)(ii).

125. *See generally* PRINCIPLES OF THE L. DATA PRIVACY § 11 (AM. L. INST. 2020) (observing that "security is a key element of data privacy"); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018) (discussing privacy harms from data breaches); Solove, *supra* note 88, at 549–53 (discussing privacy harms from intrusions).

unauthorized access would be more consistent than their distribution in civil privacy statutes.

As it turns out, they are not. Just like their civil counterparts, some of the criminal statutes contain privacy asymmetries while others are facially symmetrical. First, consider the asymmetries. The Wiretap Act generally criminalizes real time intercepts of wire, oral, and electronic communications[126]; the Stored Communications Act generally criminalizes unauthorized access to stored electronic communications[127]; and the Computer Fraud and Abuse Act generally criminalizes unauthorized access to protected computer systems.[128] All three statutes contain access asymmetries that disadvantage the defense. All three have the same textual structure—a broad criminal prohibition followed by express enumerated exceptions for law enforcement investigations and silence as to defense investigations.[129] The access asymmetries in all three statutes can also create notice asymmetries because they risk barring the sole source for discrete collection of relevant evidence.

In contrast, other criminal laws that prohibit unauthorized access are facially symmetrical. Especially significant, most physical trespass statutes broadly prohibit unauthorized entry onto private property, but they include express exceptions for entry done "lawfully," with "legal cause," or with a "claim of right." Those exceptions are facially symmetrical because they apply without regard to the identity of the person doing the entering.[130] In practice, both law enforcement and nongovernmental litigants can obtain court-ordered entry onto private property.[131] This includes criminal defense counsel.[132]

126. 18 U.S.C. § 2511(1)(a), (4)(a).
127. 18 U.S.C. § 2701(a)–(b).
128. 18 U.S.C. § 1030(a)(2)(C). The definition of a "protected computer" is vast, including any computer "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).
129. *See* 18 U.S.C. §§ 2511(2)(a)(ii)(B), 2516, 2518 (Title III exceptions); 18 U.S.C. § 2701(c)(3) (Stored Communications Act [SCA] exceptions referencing sections 2703, 2704, and 2518, all of which apply exclusively to law enforcement or government entities); 18 U.S.C. § 1030(f) (CFAA provision providing that "[t]his section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency.").
130. *See infra* Appendix. *See also* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1149 (2016) (noting textual ambiguity in the definition of the phrase "unlawfully," but not addressing whether court-ordered entry qualifies).
131. *See* FED. R. CIV. P. 45 & advisory committee's note to 1991 amendment (observing that "[p]ractice in some states has long authorized [the] use of a subpoena for this purpose").
132. For an in-depth discussion of defense counsel's access to court orders that compel entry onto private property, see *infra* Subpart III.C.1.

Meanwhile, federal laws that criminalize the interception of and tampering with U.S. postal mail are also facially symmetrical. These laws contain no express exceptions; they are facially silent as to both law enforcement and defense investigators.[133] While published judicial opinions construing these statutes in the context of criminal defense investigations are rare to nonexistent, there are some indications that courts may read the statutes to yield to otherwise valid legal process served by nongovernmental litigants, including criminal defendants.[134]

The historical predecessor to today's criminal wiretap law was also symmetrical. The relevant portion of that law—the Communications Act of 1934[135]—contained a general prohibition on intercepting and divulging communications, without express exceptions for either law enforcement or defense investigators.[136] The U.S. Supreme Court construed that symmetrical statutory silence to exclude all wiretap materials from admissibility into evidence.[137] The Act was thus unusual in that it achieved symmetrical treatment of law enforcement and defense investigators by ratcheting down access for both.

In sum, privacy asymmetries are distributed haphazardly across statutes that criminalize real time intercepts of and unauthorized access to sensitive information. Despite the peculiar risks of overcollection that attend intercepts and unauthorized access, some of the privacy statutes that regulate these investigative techniques contain privacy asymmetries while others do not.

E. Synthesizing the Information Domains

The preceding Subparts have shown that privacy asymmetries occur repeatedly in different types of privacy statutes that govern disparate domains of sensitive information. At the same time, not all privacy statutes contain privacy asymmetries; many treat law enforcement and defense investigations symmetrically. Tables 1 and 2 synthesize the examples described above and visualize their distribution across information domains. A more detailed analysis of each statute is provided in the Appendix.

133. *E.g.*, 18 U.S.C. § 1703(b) (imposing criminal sanctions for "[w]hoever, without authority, opens, or destroys" mail not addressed to them); *id.* § 1708 (imposing criminal sanctions on "[w]hoever steals [or] takes . . . out of any mail, post office, or station thereof, letter box, mail receptacle, or any mail route or other authorized depository for mail matter"); *id.* § 1700 (imposing same for desertion of mail); *id.* § 1701 (imposing same for obstruction of mail).
134. *See infra* Appendix.
135. Pub. L. No. 73-416, ch. 652, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).
136. *See id.* at 1104.
137. *See* Nardone v. United States (*Nardone I*), 302 U.S. 379, 382–84 (1937); Nardone v. United States (*Nardone II*), 308 U.S. 338 (1939).

Table 1: Civil Statutes Regulating Service Provider Disclosures

Domain	Law	Access Symmetry	Notice Symmetry	Access Asymmetry	Notice Asymmetry
Communications Contents	USPS Postal Mail (PAEA)			X	X
	Authorized Wiretap Materials—Historical (1934 Communications Act)	X	X		
	Authorized Wiretap Materials—Today (Wiretap Act)	X	X		
	Stored Electronic Communications (SCA)			X	X
Noncontent Digital Services Records	Video Rental Records (VPPA)		X	X	
	Child Privacy Online (COPPA)	X	X		
	Cable Subscriber Records (Cable Communications Policy Act)	X	X		
	Stored Electronic Communications (SCA)		X	X*	
Financial Records	Tax Filings with the IRS—Historical (Tax Code)	X	X		
	Tax Filings with the IRS—Today (Tax Code)			X	X
	Financial Services (RFPA)	X			X*
	Financial Services (GLBA)	X	X		

Domain	Law	Access Symmetry	Notice Symmetry	Access Asymmetry	Notice Asymmetry
Educational Records	Discipline of Students (FERPA)	X			X
Health Records	General Medical (HIPAA)	X	X		
	Substance Abuse (42 C.F.R. § 2.65)			X	X

** Facial asymmetry disadvantaging law enforcement.*

Table 2: Criminal Statutes Prohibiting Intercepts and Unauthorized Access

Domain	Law	Access Symmetry	Notice Symmetry	Access Asymmetry	Notice Asymmetry
Criminal Intercepts & Unauthorized Access	Trespass	X	X		
	USPS Postal Mail	X	X		
	Wiretapping—Historical	X**	X**		
	Wiretapping—Today (Wiretap Act)			X	X
	Stored Electronic Communications(SCA)			X	X
	Protected Computers (CFAA)			X	X

*** Symmetrical exclusion of all wiretapped evidence.*

Some key descriptive observations are worth highlighting before proceeding to the normative claims that build on them in the following Part. Privacy asymmetries occur repeatedly throughout information privacy statutes. They are distributed haphazardly amongst facially symmetrical statutes with no readily discernible pattern. As such, privacy asymmetries appear not to reflect any consistent policy choices about how to balance fairness and accuracy in criminal investigations with conflicting privacy interests. Perhaps the most surprising inconsistency is the presence of privacy asymmetries in statutes that govern private electronic communications services and unauthorized access to computer systems versus the absence of privacy asymmetries in statutes that

govern private paper mail services and physical trespass onto private property. Part III considers the policy consequences of these observations.

III. UNREASONABLE PRIVACY ASYMMETRIES

Privacy asymmetries are an unreasonable policy default. This Part begins by arguing that privacy asymmetries currently proliferate throughout information privacy law as unintentional side effects of the legislative process, not through reasoned deliberation. Next, it contends that privacy asymmetries impose substantial harm on both individual criminal defendants and the adversarial system of criminal adjudication as a whole. Privacy asymmetries selectively and unqualifiedly suppress evidence of innocence from the truth-seeking process of the courts. They do so without the reasonable, discretionary judicial balancing that characterizes privacy protections in the rules of evidence and procedure. These harms will only escalate as the introduction of artificial intelligence and machine learning algorithms into criminal proceedings raises the stakes of disparities between who has access to data and who does not. Finally, the discussion responds to likely counterarguments. It initially rebuts a possible defense of privacy asymmetries as analogous to home searches and seizures. It then considers and ultimately rejects the view that privacy asymmetries might be justified based on their purported benefits for protecting information privacy, limiting abuse of legal process, aiding law enforcement, or reducing administrative burdens on subpoena recipients.

A. Proliferation by Oversight Not Reasoned Deliberation

Privacy asymmetries are legislative accidents.[138] While it is difficult if not impossible to determine legislative intent with certainty, many privacy asymmetries share characteristics indicating that Congress enacted them unintentionally.

To start, privacy asymmetries generally arise from statutory texts and legislative histories that are silent as to criminal defense investigations. For instance, as explained in the preceding Part and with further detail in the Appendix, the Postal Accountability and Enhancement Act, the Stored Communications Act, the Video Privacy and Protection Act, Section 6103 of the Tax Code, the Right to Financial Privacy Act, the Family Educational Rights and

138. *But cf.* Ion Meyn, *Constructing Separate and Unequal Courtrooms*, 63 ARIZ. L. REV. 1 (2021) (detailing how criminal procedure rules have been employed to ensure the criminal law's objective to maintain racial hierarchy).

Privacy Act, the Wiretap Act, and the Computer Fraud and Abuse Act all contain privacy asymmetries disadvantaging defendants that arise from similar textual structures. These statutes first provide a broad confidentiality protection against disclosures of sensitive information; they then enumerate express exceptions for law enforcement investigations but remain silent as to defense investigations.[139] Meanwhile, nothing in the legislative records of these statutes indicates that Congress ever considered how they would affect the criminally accused, much less intended them to selectively suppress access to evidence of innocence.[140]

Of course, different canons of statutory interpretation will counsel courts to draw different inferences from these silences in statutory text and legislative history,[141] and to place more or less weight on the legislative record in discerning legislative purpose.[142] Nevertheless, the silences make it more likely that privacy asymmetries result from oversight than it would be if the texts expressly abrogated defense investigations while expressly authorizing their law enforcement counterparts, or if the legislative records revealed congressional debates about both types of investigations.

Moreover, disparities between law enforcement's and the criminal defense bar's relative influence over the legislative process present a likely mechanism for how privacy asymmetries could proliferate through legislative accident. Law enforcement interest groups wield well-documented political power.[143] They

139. *See infra* Appendix.

140. *See infra* Appendix.

141. For instance, the narrow construction rule for statutory privileges presumes that Congress does not intend to bar compulsory legal process unless a statute, strictly construed, requires that result. *See* St. Regis Paper Co. v. United States, 368 US. 208, 218 (1961). Hence, when Congress enacted privacy statutes that enumerate express exceptions for law enforcement investigations but remain silent on criminal defense subpoenas, it must not have intended to create privacy asymmetries obstructing criminal defense investigations. *See generally* Wexler, *supra* note 84. In contrast, the *expressio unius est exclusio alterius* canon of interpretation presumes that Congress intends to omit unmentioned items in an enumerated list. *See* Facebook, Inc. v. Wint, 199 A.3d 625, 632–33 (D.C. 2019); *but see* William N. Eskridge, Jr., *Dynamic Statutory Interpretation*, 135 U. PA. L. REV. 1479, 1490 & n.41 (1987) (describing expressio unius as a "highly unreliable maxim of statutory construction"). Applying that logic to the same statutory texts leads to the opposite conclusion that Congress did intend to create privacy asymmetries. *See* Facebook, Inc. v. Wint, 199 A.3d at 632–33.

142. *See* Abbe R. Gluck, *The States as Laboratories of Statutory Interpretation: Methodological Consensus and the New Modified Textualism*, 119 YALE L.J. 1750, 1762–64 (2010) (describing debate between textualists and purposivists).

143. *See generally* Catherine L. Fisk & L. Song Richardson, *Police Unions*, 85 GEO. WASH. L. REV. 712, 734–36 (2017) (discussing the post–Civil Rights Movement rise of police unions); Kevin M. Keenan & Samuel Walker, *An Impediment to Police Accountability? An Analysis of Statutory Law Enforcement Officers' Bills of Rights*, 14 B.U. PUB. INT. L.J. 185, 196 (2005) (police union influence over the criminal justice system). *See also* Katherine J. Bies, Note, *Let the*

engage in regular lobbying in state and local politics[144] and the U.S. Congress.[145] In contrast, organizations that provide indigent criminal defense services and receive federal funding from the Legal Services Corporation are prohibited from lobbying.[146] And, while defense-focused NGOs and interest groups do lobby, their contributions pale in comparison to those of law enforcement.[147] Further, public choice theorists[148] have identified multiple structural impediments to the adequate representation of criminal defendants' interests in the legislative process.[149] For instance, it is difficult to ascertain and hence to mobilize future

Sunshine In: Illuminating the Powerful Role Police Unions Play in Shielding Officer Misconduct, 28 STAN. L. & POL'Y REV. 109, 123 (2017) (police union mobilization to influence legislation).

144. *See* Samuel Walker, *The Neglect of Police Unions: Exploring One of the Most Important Areas of American Policing*, 9 POLICE PRAC. & RSCH. 95, 107 (2008) (police union focus on influencing local and state politics); Noam Scheiber, Farah Stockman & J. David Goodman, *How Police Unions Became Such Powerful Opponents to Reform Efforts*, N.Y. TIMES (June 20, 2020), https://www.nytimes.com/2020/06/06/us/police-unions-minneapolis-kroll.html [https://perma.cc/8CBH-26KK] (over $1 million dollars in New York State and New York City elections since 2014).

145. For instance, law enforcement interest groups have contributed more than $1.1 million to U.S. congressional campaigns since 1994, and individuals self-identifying as law enforcement personnel have contributed another $9 million to congressional campaigns since 1990. Grace Haley & Ian Karbal, *Amid Calls for Police Reform, New Dataset Shows Where Police Money Has Flowed in Congress*, OPEN SECRETS (June 5, 2020, 4:43 PM), https://www.opensecrets.org/news/2020/06/police-reform-new-dataset-shows-where-police-money-has-flowed-in-congress [https://perma.cc/5GG9-645B].

146. 42 U.S.C. § 2996e(c)(2); *see also* Liza Q. Wirtz, *The Ethical Bar and the LSC: Wrestling With Restrictions on Federally Funded Legal Services*, 59 VAND. L. REV. 971, 973 (2006).

147. In 2018, for instance, the Innocence Project contributed $254,258, *see Client Profile: Innocence Project*, OPEN SECRETS, https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2018&id=D000052172 [https://perma.cc/MZ3N-Y97Z], and the National Association of Criminal Defense Lawyers (NACDL) contributed $60,000, *see Client Profile: Natl Assn of Criminal Defense Lawyers*, OPEN SECRETS, https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2018&id=D000054408 [https://perma.cc/WS7Z-QU2W], in lobbying funds. For more general commentary on the limited lobbying funds available to criminal defendants and to the organizations that advocate for them, see W.C. Bunting, *The Regulation of Sentencing Decisions: Why Information Disclosure Is Not Sufficient, and What to Do About It*, 70 N.Y.U. ANN. SURV. AM. L. 41, 49 (2014).

148. While the public choice hypothesis may not apply neatly to all types of criminal and criminal procedure laws, the theory aligns with the dynamics surrounding statutes that grant law enforcement investigative power. *See* Ronald F. Wright, *Parity of Resources for Defense Counsel and the Reach of Public Choice Theory*, 90 IOWA L. REV. 219, 257–58 (2004). Statutes empowering law enforcement investigations provide generalized public benefits that are made visible and promoted by organized law enforcement groups, while the financial costs to taxpayers are diffuse, and the "privacy and autonomy" costs fall disproportionately on poorer, politically less influential groups. *See id.*

149. *See generally id.* ("Prosecutors, as local elected officials with effective political operations of their own, have ready access to the media and communicate often with large groups of voters. . . . So far, our analysis leads to the same predictions to be found elsewhere in criminal justice scholarship: criminal suspects and defendants are likely to lose in the legislature, and

criminal defendants.[150] Legislators may also view criminal defendants as a weak political constituency and thus ignore bills that serve their interests.[151]

Regarding privacy legislation in particular, Erin Murphy has documented the successful efforts of law enforcement interest groups to gain exceptions to privacy statutes that permit police and prosecutors to continue accessing protected information.[152] Murphy points out that legislators may feel compelled to concede to law enforcement demands for such exceptions in order to get consumer privacy laws enacted.[153] She also shows that law enforcement groups have been especially successful at gaining exceptions to privacy statutes that govern sensitive information about poor, minority, and heavily-policed communities.[154] She argues that this result may be due to the fact that NGOs and other interest groups that represent these communities tend to focus on other urgent issues, such as welfare reform, antidiscrimination, and the death penalty,[155] while privacy-focused advocacy organizations generally emphasize the privacy interests of higher socioeconomic groups.[156]

The dynamics that Murphy observes support a related possibility; not only are the privacy interests of poor, minority, and heavily-policed communities underrepresented in the legislative process surrounding privacy bills, but so are the access interests of criminal defendants, who come overwhelmingly from these

criminal prosecutors are likely to win."); *see also* William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 780, 783–84 (2006).

150. For example, William Stuntz has argued that legislators will predictably push to expand the substantive criminal code because they can tout the general public benefits of increased criminalization while resting assured that those most likely to bear the costs—the future accused—are difficult to ascertain, poorly organized, and unlikely to mount a vigorous opposition. William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505 (2001).

151. Wright, *supra* note 148, at 254. *See also* JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW 135 (1980) ("[T]hose with most of the votes are in a position to vote themselves advantages at the expense of the others, or otherwise to refuse to take their interests into account.").

152. Murphy, *supra* note 29, at 504 (describing extensive law enforcement comments on proposed privacy bills).

153. *Id.* at 504 (describing the threat that "resistance by law enforcement may hinder or even prevent the passage of a generally applicable statute").

154. *Id.* at 508–14. Relatedly, Khiara Bridges has argued more broadly that "wealth is a condition for privacy rights and that, lacking wealth, poor mothers do not have any privacy rights." KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 10, 12, 14 (2017) (documenting that "the legal and social condition of poor mothers is one that is devoid of privacy," and advocating "to bring this group within the class of persons to whom privacy rights are ascribed").

155. Murphy, *supra* note 29, at 505.

156. *Id.* at 505–06.

same communities.[157] As a result, legislators considering new privacy bills might be alert to law enforcement's investigative needs but not to the parallel investigative needs of criminal defense counsel. They might be unaware that law enforcement has no duty to investigate evidence of innocence.[158] Hence, they might not know that enacting privacy asymmetries systematically skews the adversarial process of truth-seeking in adjudication towards findings of guilt rather than of innocence.

These factors combined strongly suggest that privacy asymmetries proliferate through legislative oversight not reasoned deliberation.

B. Harms to the Accused and to the Adversary System

Privacy asymmetries impose substantial harms on individual criminal defendants and on the adversary system as a whole. Privacy asymmetries selectively block defense counsel's access to relevant, material evidence.[159] Given that defense counsel alone has a duty to investigate evidence of innocence, laws that make such evidence selectively unavailable to the defense also selectively suppress evidence of innocence. The result threatens accuracy, fairness, and the ideal of neutral truth-seeking in the adversary system.[160]

Privacy asymmetries layer on top of, and distort, the careful balanced privacy protections built into the subpoena and evidence rules. Recall that the baseline privacy safeguards in the subpoena and evidence rules share two key characteristics that help to make them reasonable.[161] First, they incorporate judicial discretion to balance the competing interests and override the privacy protection if barring defense counsel's access to evidence would risk extreme

157. A report published by the U.S. Bureau of Justice Statistics in November, 2020, estimated that 66 to 80 percent of felony defendants are indigent. U.S. BUREAU OF JUST. STAT., DEFENSE COUNSEL IN CRIMINAL CASES 1 (2020), https://www.bjs.gov/content/pub/pdf/dccc.pdf [https://perma.cc/L68W-EPKT]. *See also* THE SENT'G PROJECT, REPORT OF THE SENTENCING PROJECT TO THE UNITED NATIONS SPECIAL RAPPORTEUR ON CONTEMPORARY FORMS OF RACISM, RACIAL DISCRIMINATION, XENOPHOBIA, AND RELATED INTOLERANCE (2018), https://www.sentencingproject.org/publications/un-report-on-racial-disparities [https://perma.cc/ZM9S-LQ8V].

158. *See supra* Subpart I.A.

159. Of course, transparent access to evidence, without more, will often be insufficient to protect defense rights. *See* Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLA. L. REV. 181, 194–96 (2017) (discussing how "too much information" can actually undermine accountability efforts).

160. *See* Jocelyn Simonson, *The Place of "the People" in Criminal Procedure*, 119 COLUM. L. REV. 249, 294–95 (2019) (emphasizing that "the people" have an interest "on both sides of the 'v'" in criminal procedure).

161. *See supra* Subpart I.B.

harm. Second, the level of judicial discretion correlates inversely with the breadth of the privacy safeguard. Judges have greater discretion to override rules that shield vast swaths of information from disclosure, and only for narrower categories of information is that discretion is tempered.

Privacy asymmetries lack both characteristics. They impose facially absolute bars on criminal defense subpoenas, with no judicial discretion to override the privacy protection on a case-by-case basis. And they apply these discretionless bars to vast swaths of information.[162] For instance, the privacy asymmetries in the Postal Accountability and Enhancement Act, and in the Stored Communications Act, apply to all communications contents transmitted through, respectively, first class U.S. postal mail or an electronic communications service provider, without regard to the sensitivity of the subject matter discussed in the communications, to the relationship between the communicants, or to the communicants' expectations of confidentiality.[163] The statutes thus suppress more and less sensitive information alike.[164] The privacy asymmetry in the Video Privacy Protection Act applies to a comparatively narrow category of information, namely video rental records, but again imposes a facially categorical bar on defense subpoenas with no opportunity for discretionary judicial balancing.[165] The same is true for the privacy asymmetries in Section 6103 of the Tax Code,[166] the Family Educational Rights and Privacy Act,[167] and federal regulations protecting privacy in substance abuse records.[168] In each of these instances, the lack of judicial discretion means that privacy asymmetries risk suppressing relevant information

162. Of course, as with evidentiary privileges, defendants' constitutional rights to compulsory process and to present a defense may sometimes defeat even facially absolute statutory barriers. Nevertheless, the burdens for defendants to successfully mount a right-to-present-a-defense challenge to defeat statutory barriers to subpoenas on an as-applied basis are extremely high, and often unattainable even where the evidence at issue is relevant and exculpatory. *See generally* Holmes v. South Carolina, 547 U.S. 319, 319–20 (2006) ("This right is abridged by evidence rules that infring[e] upon a weighty interest of the accused and are arbitrary or disproportionate to the purposes they are designed to serve." (internal citations and quotation marks omitted). As a result, this Article focuses on the harms that privacy asymmetries impose by suppressing relevant, exculpatory evidence from the truth-seeking process of courts that would likely not be attainable through a right-to-present-a-defense challenge.

163. 39 U.S.C. § 404(c); 18 U.S.C. § 2702(a). *Cf.* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136–38 (2004) (proposing that privacy protections should maintain the "contextual integrity" of "information[] norms" surrounding disclosures made in particular contexts).

164. 39 U.S.C. § 404(c); 18 U.S.C. § 2702(b).

165. 18 U.S.C. § 2710(b).

166. 26 U.S.C. § 6103(a).

167. 34 C.F.R. § 99.31(a)(9)(ii) (2020).

168. 42 C.F.R. § 2.13(b).

from the truth-seeking process of the courts even when that information has significant evidentiary value and implicates minimal privacy interests.

In addition, artificial intelligence and machine learning technologies risk exacerbating the harms from privacy asymmetries for at least three reasons: deployment, assessment, and development. First, these technologies expand the capacity to search and analyze data, which raises the stakes of disparities between those with access to data and those without. If privatized possession of data coupled with privacy asymmetries selectively block defendants' access to evidence of innocence, that process also selectively blocks defendants' capacity to deploy new technologies to facilitate defense investigations. For instance, computer vision, natural language processing, and face recognition systems can help law enforcement parse digital evidence data dumps from cloud accounts and forensic device extractions.[169] DNA searches rely on algorithmic tools to analyze crime scene samples and compare them to DNA databases,[170] as well as to conduct "familial searching" to identify and rank possible matches to suspects' genetic relatives.[171] If law enforcement can access data possessed by private companies but defense investigators cannot, then law enforcement but not defendants will benefit from deploying new algorithmic artificial intelligence and machine learning tools to search and analyze that data.[172]

Privatized possession of data combined with privacy asymmetries might also constrain defendants' capacity to assess algorithmic tools that are used by law enforcement. These developments block defense access to data used to train the machine learning models that are central to new search and predictive technologies. To illustrate, the Arnold Foundation has explained that data sharing agreements prevent it from disclosing the training data for its Public Safety

169. *See* Ferguson, *supra* note 36.

170. *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972 (2017); Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245 (2016).

171. *See* SARA DEBUS-SHERILL & MICHAEL B. FIELD, UNDERSTANDING FAMILIAL DNA SEARCHING: POLICIES, PROCEDURES, AND POTENTIAL IMPACT (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251043.pdf [https://perma.cc/G4NZ-WQBE]; Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291 (2010); *cf.* Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy and the State of Machine Learning*, N.Y.U. ANN. SURV. AM. L. (forthcoming 2019) (manuscript at 9) (on file with author) (predicting that machine learning tools will eventually "be able to reveal not just identity but also a range of preferences and behavioral traits" from DNA samples).

172. *Cf.* David Freeman Engstrom & Jonah B. Gelbach, *Legal Tech, Civil Procedure, and the Future of Adversarialism*, 169 U. PA. L. REV. (forthcoming 2020) (manuscript at 13), ("[L]egal tech tools vary in their data inputs and, in particular, whether those inputs are widely available at little or no cost, or instead are proprietary and thus held only by certain actors within the system.").

Assessment tool,[173] a risk assessment instrument currently in use in bail decisions across the country,[174] despite the fact that the training data comprised judicial records to which First Amendment and common law rights of public access may apply.[175] Limited access to training data can inhibit defense expert witnesses from thoroughly evaluating predictive models that are built from that data, including for example by scrutinizing the training data for biases that might be replicated in the model.[176] Notably, like the data to which these tools are applied, the tools themselves are sometimes made selectively available to law enforcement and shielded from scrutiny by defendants.[177]

Finally, blocking defense access to training data may impede the development of similar artificial intelligence and machine learning systems designed to serve defense interests.[178] In a related pattern of design bias, Andrew Ferguson has shown that big data systems built to aid prosecutors in identifying and tracking crime, which prosecutors may deploy to evaluate evidence that is in their possession and thus subject to *Brady*, have not been designed to identify the exculpatory and impeaching evidence that the *Brady* doctrine requires prosecutors to disclose to defendants.[179] Analogously, privacy asymmetries could mean that no tools are developed to assist defense investigations. For example, while there are many risk assessment instruments to predict defendants' likelihood of failing to appear for a court date or re-arrest,[180] far fewer if any risk

173. *See* E-mail from Arnold Found. to David Murdter (Oct. 25, 2018) (on file with author).
174. *See About the Public Safety Assessment*, ADVANCING PRETRIAL POL'Y & RSCH., https://advancingpretrial.org/psa/psa-sites [https://perma.cc/3C4S-G7LA].
175. The initial Public Safety Assessment was trained on 746,525 bail outcomes selected from an initial 1.5 million drawn from multiple jurisdictions. ARNOLD FOUND., DEVELOPING A NATIONAL MODEL FOR PRETRIAL RISK ASSESSMENT 3 (2013) [https://perma.cc/4W8Z-C2CW].
176. *See generally* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS MACHINE LEARNING RSCH. 77 (2018) (showing that skewed facial data sets led to face recognition software that is more reliable for white males than black females and using access to the initial training data sets to explain the cause of these disparities).
177. For instance, Greyshift refuses to sell digital device extraction tools to defense counsel. *See* Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone*, N. Y. TIMES (Nov. 22, 2019) https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html [https://perma.cc/LZL9-L6L7] ("Though public defenders aren't their typical customers, most forensics companies are willing to sell to them. Not Grayshift[,]" the company behind GrayKey, a digital device extraction tool exclusively available to law enforcement) .
178. Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1195, 1244 (2019).
179. Ferguson, *supra* note 36.
180. *See* John Logan Koepke & David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform*, 93 WASH. L. REV. 1725, 1748 (2018) ("Cities and counties across the country

assessment instruments are available to defense investigators to predict police officers' likelihood of committing perjury or excessive use of force.

In sum, privacy asymmetries impose substantial harms on individual criminal defendants and on the truth-seeking process of the judiciary. The following Subpart contends that these harms are not outweighed by countervailing policy benefits.

C. Responding to Policy Counterarguments

This Subpart considers the best available justifications for privacy asymmetries along four dimensions: analogizing to searches and seizures of evidence inside private homes; safeguarding against excessive invasions of privacy and abuse of legal process; serving legitimate law enforcement interests; and reducing administrative burdens on subpoena recipients. The following discussion concludes that none of these justifications withstand rigorous scrutiny. It may be that no amount of countervailing benefits along any of these dimensions could normatively outweigh the unfairness of legislators enacting statutes that selectively suppress evidence of innocence. Regardless, even adopting a cost-benefit analysis for the sake of argument does not justify privacy asymmetries. On the contrary, these statutes' asymmetrical treatment of law enforcement versus defense investigations selectively suppresses evidence of innocence with little to no benefit for privacy, security, or efficiency.

1. The Fourth Amendment and Evidence in the Home

Before turning to plausible policy benefits from privacy asymmetries, it is helpful to correct a common misimpression about privacy protections for the home. Some argue that privacy asymmetries should be unconcerning because they reflect other well-established disparities between law enforcement's search and seizure power and criminal defense counsel's subpoena power. More specifically, commentators sometimes defend privacy asymmetries by arguing that they mimic disparities in law enforcement's and defense counsel's relative power to access evidence inside private homes. For instance, the U.S. Attorney's Office for the District of Columbia recently argued that it is fine for the Stored Communications Act to selectively bar defense subpoenas because "criminal unlawful entry and burglary statutes prohibit a defendant from entering a

have experimented with pretrial risk assessment—some develop their own tools, while others implement or purchase another tool.").

witness's home to gather evidence absent consent."[181] This argument proceeds from a flawed premise about the relationship between the Fourth Amendment and criminal defense investigations. The fact that the Fourth Amendment requires the government to obtain a warrant before searching or seizing certain categories of information does not generally bar courts from issuing other forms of compulsory legal process for that same information when requested by criminal defense counsel.[182]

It is true, of course, that law enforcement has search and seizure power if authorized by a valid warrant, and defense counsel generally does not.[183] And, of course, warrants can authorize law enforcement to conduct nonconsensual searches of the home that, without the warrant, would violate generally applicable laws such as criminal trespass laws.[184] But it is also true that court orders can authorize defense investigators to do the same: conduct nonconsensual searches of the home that, without the court order, would violate those same, generally applicable laws.[185] Most state supreme courts that have considered the issue have recognized criminal defendants' entitlement to court orders compelling such access in certain circumstances.[186] Most intermediate appellate courts have

181. Brief for United States at 35, 35 & n.22, Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019). *But cf.* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (analogizing issue concerning "authorization" under the SCA to trespass, but appearing to presume that a valid subpoena would defeat the SCA confidentiality bar just as court-ordered entry can defeat common law trespass).

182. Courts often assert, without substantial analysis, that the Fourth Amendment does not bind nongovernmental litigants. To be sure, the U.S. Supreme Court has squarely held that the Fourth Amendment does not constrain private searches. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984); Burdeau v. McDowell, 256 U.S. 465, 467 (1921). Still, it is not immediately apparent why the Fourth Amendment would not apply to nongovernmental litigants who exercise compulsory legal process powers. Indeed, it seems likely that the Fourth Amendment might apply in some such circumstances, as when criminal defendants request that a judge issue a bench warrant to compel the production of witnesses. This is not the only area of criminal procedure where the logical boundary between governmental and nongovernmental action is ambiguous. *Cf.* David. A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1270 (1999) ("The Supreme Court's state action jurisprudence fails to provide firm reasons for distinguishing private police either from public police or from the public at large."). Regardless, since criminal defendants rarely get warrants and primarily exercise subpoena power, the Fourth Amendment is not a prominent presence in defense investigations.

183. *See* FED. R. CRIM. P. 41(b). There are some exceptions, such as defense counsel's ability to request a bench warrant to compel the production of witnesses in their favor.

184. *See* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1824–25 (2016).

185. Of course, even if there was an asymmetry in access to evidence inside the home, one asymmetry does not justify another. (Thank you to Anna Roberts for emphasizing this point.).

186. *See* State v. Tetu, 386 P.3d 844, 862 (Haw. 2016); State in Int. of A.B., 99 A.3d 782, 785 (N.J. 2014); State v. Muscari, 807 A.2d 407, 417–18 (Vt. 2002); State v. Brown, 293 S.E.2d 569, 578–

reached the same conclusion.[187] And some states have even codified criminal defendants' entitlement to court orders that grant compelled access to "premises relevant to the subject matter of the case."[188]

It should not be surprising that defense investigators have this power; even nongovernmental civil litigants can obtain a court order to compel entry into private homes.[189] Indeed, the Federal Rules of Civil Procedure on their face grant

79 (N.C. 1982). The Colorado Supreme Court has taken the self-proclaimed outlier position that courts have no inherent authority over criminal discovery, and on that basis—not on the basis of the privacy interests of nonparties—has declined to find that criminal defendants have a right to court-ordered access to a nonparty's home. *See* People in Int. of E.G., 368 P.3d 946, 949–50 (Colo. 2016). *But see id.* at 954–58 (Gabriel, J., concurring in judgment only) (disagreeing); People v. Chavez, 368 P.3d 943, 944–45 (Colo. 2016); *see also* State *ex rel.* Beach v. Norblad, 781 P.2d 349, 350 (Or. 1989) (en banc) (including a short, almost entirely unreasoned, opinion denying trial court's authority to order access to premises); NAT'L CRIME VICTIM L. INST., DEFENSE ACCESS TO VICTIMS' HOMES 3 (2006), https://law.lclark.edu/live/files/21753-defense-access-to-victims-homespdf [https://perma.cc/4XW5-RS62] ("In sum, with two exceptions—Oregon and Minnesota—the courts that have addressed this issue have all developed a balancing test between the defendant's interests in preparing for trial and the homeowner's privacy interests, and then applied the test to the facts before them, with differing results.").

Note that, as with other "middle-layer" privacy protections in the subpoena and evidence rules, access-to-premises orders for inspection of private homes incorporate some balancing; they generally require criminal defendants to meet a threshold showing beyond mere relevance, following which the court will balance the competing interests in access versus privacy before determining whether to issue the order. *See, e.g.*, *Muscari*, 807 A.2d at 417–18 (noting defendant's threshold burden to show relevance and materiality); Howard v. State, 156 A.3d 981, 999 (Md. Ct. Spec. App. 2017) (explaining that the "court must balance [the defendant's] need against the privacy interests of the third party" before issuing access-to-premises order).

187. *See, e.g.*, State v. Lee, No. 27-CR-16-18160, 2018 WL 1145724 (Minn. Ct. App. Mar. 5, 2018); Welch v. Superior Court, No. E050535, 2011 WL 95607 (Cal. Ct. App. Jan. 11, 2011); State v. Gonsalves, 661 So. 2d 1281 (Fla. Dist. Ct. App. 1995); Henshaw v. Commonwealth, 451 S.E.2d 415 (Va. Ct. App. 1994).

188. New York State's recently enacted discovery statute makes this right express, entitling defendants in certain circumstances to "a court order to access a crime scene or other premises relevant to the subject matter of the case, requiring that counsel for the defendant be granted reasonable access to inspect, photograph, or measure such crime scene or premises." N.Y. CRIM. PROC. LAW § 245.30(2) (McKinney 2020). Courts must balance the privacy interests and perceived hardship of ordering access against its probative value. *See* KRYSTAL RODRIGUEZ, CTR. FOR CT. INNOVATION, DISCOVERY REFORM IN NEW YORK: MAJOR LEGISLATIVE PROVISIONS (2019), https://www.courtinnovation.org/sites/default/files/media/document/2019/Discovery-NYS_Full.pdf [https://perma.cc/QSS7-GGN7].

189. For cases in which private civil litigants obtained court orders to inspect the private property of a nonparty, see Johnson v. Air Liquide Large Industries, No. 2:18-CV-259-WCB, 2019 WL 4394854 (E.D. Tex. Sept. 13, 2019); Toussie v. Allstate Insurance Co., No. 14 CV 2705 (FB) (CLP), 2017 WL 4773374 (E.D.N.Y. Oct. 20, 2017); Liberty Mutual Insurance Co. v. Kohler Co., No. CV 08-867 (SJF) (AKT), 2010 WL 1930270 (E.D.N.Y. May 11, 2010); and JB *ex rel.* Palmer v. Asarco Inc., No. 03-CV-498, 2005 WL 8174815 (N.D. Okla. Jan. 10, 2005).

civil litigants express authority to command nonparties to "permit the inspection of premises."[190] And the vast majority of state criminal trespass laws contain express statutory language limiting their prohibitions to acts of entering or remaining on private property "unlawfully," "without legal cause," "without claim of right," or similar.[191] Court-ordered entry thus falls entirely beyond the scope of these criminal trespass laws, regardless of what type of litigant requests the court order. The upshot is that, while law enforcement and defense counsel sometimes have access to different forms of legal process, both entities may use their respective forms of process to compel entry into private homes.

Nor is this reality limited to evidence inside private homes. For another example in which nongovernmental litigants may obtain subpoenas or court orders to compel access to Fourth Amendment–protected information, consider cell-site location information (CSLI) and bailees. In *Carpenter v. United States*, the Supreme Court held that the Fourth Amendment requires a warrant before the government may obtain long-term cell site location records.[192] But criminal defense counsel and private civil litigants regularly subpoena telecommunications service providers for the CSLI of other people such as codefendants, witness, and other nonparties.[193] There is no readily discernable indication in current case law

190. FED. R. CIV. P. 45(a)(1)(A)(iii); *see also* FED. R. CIV. P. 45(c)(2)(B); FED. R. CIV. P. 45(d)(2).
191. *See infra* Appendix.
192. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
193. For examples of criminal defendants subpoenaing CSLI, see *Oudin v. Warden, Cal. State Prison*, No. EDCV 16-774 AG(JC), 2018 WL 7204073 (C.D. Cal. Sept. 4, 2018) *report and recommendation adopted*, 2018 WL 6931288 (C.D. Cal. Dec. 29, 2018); United States v. Martin (Briddy), No. 3:07-CR-51 (E.D. Tenn. Dec. 23, 2008) (rejecting government's argument that Fed. R. Crim. P. 17 and 18 U.S.C. § 2703 did not entitle defendant to subpoena nonparty's CSLI because obtaining CSLI requires a showing of probable cause and a warrant (Dkt. 414, at *2), holding the subpoena valid (Dkt. 433-1, at *9–10)); United States v. Lopez, No. H-05-446, 2006 WL 5002747 (S.D. Tex. Apr. 24, 2006) (note that in *Lopez* the defendant was subpoenaing his own CSLI).

For discussion of private civil litigants' power to subpoena nonparties' CSLI, see Henderson-Burkhalter v. Nat'l Union Fire Ins. Co., No. CV 18-0928, 2019 WL 8889978, at *2 (E.D. La. Jan. 18. 2019) (denying nonparty's motion to quash subpoena seeking the nonparty's cell phone records and finding the records relevant, the subpoena proper, and the Fourth Amendment inapplicable); Sundaram v. Genworth Life Ins. Co., No. CV 16-06218 TJH (AFMx), 2018 WL 5227385, at *1 (C.D. Cal. Apr. 24, 2018) (acknowledging that the SCA does not impede private litigants' subpoenas for nonparties' CSLI, though denying the motion to compel in this case due to procedural errors); and *In re* Estate of Angstadt, No. 1355 EDA 2013, 2014 WL 10919557, at *6 (Pa. Super. Ct. June 4, 2014) (noting that two litigants presented CSLI belonging to seven different cell phones not their own, but not discussing the discovery or subpoena process).

that *Carpenter* affects nongovernmental litigants' ongoing ability to compel access to this evidence, and at least one federal court has ruled explicitly that it does not.[194]

Put succinctly, neither the fact that the government may and generally must obtain a warrant to access Fourth Amendment-protected information, nor the fact that generally applicable laws shield information from nonlitigants, automatically places that information beyond reach of criminal defense investigators. Law enforcement may have stronger forms of compulsory process, such as warrants and grand jury subpoenas, that enable more invasive means to obtain information, such as by use of force, with different threshold burdens and procedures for judicial oversight. But exclusive access to those means for obtaining information does not equal exclusive access to particular sources or categories of information. Privacy asymmetries are something different. With that common misconception out of the way, the following discussion anticipates and responds to likely arguments about plausible policy benefits from privacy asymmetries.

2. Privacy and Abuse, Law Enforcement Interests, and Administrative Burdens

The three most likely policy defenses of privacy asymmetries are protecting privacy and limiting abuse, furthering law enforcement interests, and alleviating administrative burdens on subpoena recipients. On close scrutiny, none of these potential benefits justify asymmetrically obstructing criminal defense investigations.

First, some may suspect that privacy asymmetries are necessary to protect against excessive invasions of privacy or other abuses of legal process, such as to harass or to intimidate. Yet, eliminating privacy asymmetries would not eliminate safeguards for privacy and against abuse. On the contrary, privacy laws with neutral, symmetrical exceptions for law enforcement and defense investigators alike would default to the baseline privacy safeguards built into the subpoena and evidence rules.[195] That baseline subpoena and evidence balancing regime already protects extraordinarily sensitive information that is regularly implicated in criminal cases, ranging from an individual's detailed location information, to a rape survivor's mental health records, to the compelled testimony of a parent against their child. And it does so without the categorical,

194. *See Henderson-Burkhalter*, 2019 WL 8889978, at *2 (characterizing counsel's citation to *Carpenter* as "frivolous" in a civil proceeding between private litigants because "[t]he Fourth Amendment proscribes only governmental action").

195. *See supra* Subpart I.B.

discretionless bars on defense access to evidence that privacy asymmetries produce. It is thus unclear why video rental records or social media posts should receive greater protections through privacy asymmetries.

Moreover, the risk of privacy invasions and abuse of process does little to justify the asymmetric treatment of law enforcement and defense investigators because compulsory legal process entails some risks when wielded by either. For instance, victims' rights advocates have emphasized that "[i]n nearly every criminal case, counsel for the parties (both the defendant and the state) seek some amount of victim information pretrial[,]" which victims may "prefer to keep private."[196] And, unfortunately, there are egregious examples of abuse of process by both law enforcement and defense counsel.[197]

In the absence of strong empirical evidence, then, it is difficult to ascertain whether such risks are greater for one type of investigation than the other. On the one hand, factors indicating heightened risks from law enforcement include

196. Garvin, Wilkinson & LeClair, *supra* note, at 69 ("For example, the parties may seek the victim's diary, Facebook account information, email, cell phone records, computer hard drives, or Google searches . . . ."). The National Crime Victim Law Institute has also published model legal arguments to protect victim privacy by moving to quash criminal subpoenas, including subpoenas "from defendants to victims . . . [and] from defendants to third parties who hold victims' records, as well as requests from the state to victims and third parties who hold victims' records." *Id.* at 4 n.1; s*ee also* Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054 (2017) (discussing law enforcement mistreatment of African American and poor victims and their families); ROXANNA ALTHOLZ, LIVING WITH IMPUNITY: UNSOLVED MURDERS IN OAKLAND AND THE HUMAN RIGHTS IMPACT ON VICTIMS' FAMILY MEMBERS (2020) (presenting research on law enforcement mistreatment of victims and families).

197. In one recent incident, a police sergeant allegedly filed fraudulent warrants to seize entire Google accounts belonging to a juvenile defendant's lawyers, family, and teacher, "for the sole purpose of intimidating and silencing" them. Notice of Motion and Motion to Unseal Affidavits and Disclose Warrants at 2, *In re* Application of Scott Budnick to Unseal Search Warrants and Supporting Documents, (Cal. Super. Ct. Nov. 22, 2019) (on file with author). In an older, especially disturbing case, a sheriff allegedly called a press conference to release "'extremely humiliating details'" about a rape in order to retaliate against the rape survivor for criticizing the sheriff's failure to investigate the crime. Bloch v. Ribar, 156 F.3d 673, 676 (6th Cir. 1998); *see also* Rosenfeld v. Lenich, No. 17-CV-7299 (NGG) (PK), 2019 WL 418861, at *1 (E.D.N.Y. Feb. 1, 2019) (alleging that former assistant district attorney used public "resources to unlawfully intercept, record, and review electronic communicatios [sic]"). Meanwhile, commentators have alleged that defense counsel in rape and sex assault cases "routinely attack victims' privacy by seeking personal records," NAT'L CRIME VICTIM L. INST., DISCOVERY VERSUS PRODUCTION: THERE IS A DIFFERENCE 1 (2006), https://law.lclark.edu/live/files/21768-discovery-versus-productionthere-is-a [https://perma.cc/M3KX-RRKS], and specifically by seeking alleged victims' psychotherapy records "to take advantage of the myth that women who make rape reports are unstable and mentally ill." Anne W. Robinson, *Evidentiary Privileges and the Exclusionary Rule: Dual Justifications for an Absolute Rape Victim Counselor Privilege*, 31 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 331, 332 (2005).

stronger compulsory process powers;[198] the ex parte nature of warrants; that it is more difficult for courts to impose ex post minimization requirements on law enforcement searches and seizures to mitigate harms from overbroad collection, retention, and use of sensitive information[199] than it is to impose protective orders on defense subpoenas to mitigate those same harms;[200] that at least in some circumstances, law enforcement might face less opposition to overreach;[201] and that law enforcement enjoys unique qualified immunity for investigative functions and absolute immunity for prosecutorial functions, which reduce deterrents against misconduct.[202] On the other hand, risks from defense investigations may be heightened by defense counsel's ethical obligations to zealously advocate for their clients as compared to prosecutors' more nebulous ethical duties to serve the tribunal and the public;[203] the lower barrier to entry whereby any member of the bar may serve as defense counsel while prosecutors undergo vetting through election or appointment; and that defense clients and pro se defendants may be more likely to be personally acquainted with the subjects of their investigations than are law enforcement officers, and thus more likely to have improper motives for serving subpoenas. Alternately, perhaps the risks from both

198. Baude & Stern, *supra* note 184, at 1845 ("The basic premise of our constitutional order is that government presents special dangers because it wields special powers . . . ."); *see also* Sklansky, *supra* note 182, at 1271 (noting that public and private police pose different risks).

199. *See* United States v. Ganias, 824 F.3d 199, 200 (2d Cir. 2016) (en banc) (avoiding question of whether law enforcement's retention and overbroad search of mirrors of defendant's hard drives violated the Fourth Amendment by finding that the agents relied in good faith on search warrants and the reliance was objectively reasonable); Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras)*, 18 J. CONST. L. 933 (2016) (considering ex post constraints on bulk government capture); Bihter Ozedirne, *Fourth Amendment Particularity in the Cloud*, 33 BERKELEY TECH. L.J. 1223 (2018) (identifying risks of overcollection of cloud data); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1, 8–9 (2015).

200. *See* Zaal v. State, 602 A.2d 1247, 1264 (Md. 1992) (holding that a protective order may be sufficient to protect allegedly abused child's school records and that judicial review "should not only be aimed at discovering evidence directly admissible but also that which is usable for impeachment purposes, or that which would lead to such evidence.").

201. *See, e.g.*, United States v. Noriega, 764 F. Supp. 1480, 1493 (S.D. Fla. 1991) ("[I]t is wishful thinking to expect that prison officials will either oppose a government-requested subpoena which implicates an incarcerated defendant's interests or else enable the defendant to file his own motion to quash by notifying him that such subpoenas have been issued. If anything, the coinciding interests of prosecutors and prison authorities in law enforcement renders these subpoenas mere formalities and all but guarantees that prosecutorial overreaching such as that present here will go unchecked . . . .").

202. *Cf.* David Alan Sklansky, *The Problems With Prosecutors*, 1 ANN. REV. CRIMINOLOGY 451, 459 (2018) (discussing weak enforcement of checks on prosecutorial power).

203. *See* Eric S. Fish, *Against Adversary Prosecution*, 103 IOWA L. REV. 1419 (2018).

types of investigations are roughly equivalent since both law enforcement and defense counsel operate in diverse institutional structures nationwide, with varying scale, resources, and oversight mechanisms; both are officers of the court subject to civil and criminal contempt sanctions and bar disciplinary proceedings; and like prosecutors, many defense counsel are public employees.[204] Risks of privacy invasions and abuse of process thus do not clearly justify the asymmetrical treatment of law enforcement and defense investigations.

Second, some may assume that privacy asymmetries serve legitimate law enforcement interests. Indeed, at least some prosecutors appear to favor them. The U.S. Attorney's office for the District of Columbia, for instance, recently argued that it would be "illogical" to require the government to use a warrant to obtain contents of messages from electronic communications service providers while permitting defense investigators to obtain the same with a subpoena.[205] But, as discussed above, the fact that the government must obtain a warrant before searching and seizing certain types of information says little about whether criminal defense counsel may compel access to the same information pursuant to a court order.[206]

More generally, it is unclear why law enforcement should have any legitimate interest in impeding otherwise valid criminal defense subpoenas. These subpoenas satisfy the privacy-protective requirements built into the subpoena and evidence rules, which are arguably more onerous than the showing of probable cause and particularity required to obtain a warrant. The subpoenas are subject to judicial oversight; are not issued ex parte; must be served in good faith; are not being used as a discovery device or fishing expedition; do not seek privileged material or evidence on collateral issues; satisfy special notice requirements if they seek sensitive information about an alleged victim from a third party; if served pretrial, they seek relevant, admissible evidence identified with specificity; and, if opposed, they have been found by a judge to be neither unreasonable nor oppressive.[207] Selectively suppressing defense subpoenas that satisfy all of these requirements does not aid law enforcement. On the contrary,

204. *But cf.* Polk County v. Dodson, 454 U.S. 312, 324–25 (1981) (holding that public defenders are sometimes private actors). For a powerful critique of current criminal procedure's presumed dichotomy between "the People" and criminal defense advocates, *see* Simonson, *supra* note 160, at 286–97.

205. Brief for United States at 25–26, Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019) 10.2.18 at 26 (citing Carpenter v. United States, 138 S. Ct. 2206 (2018) and Riley v. California, 573 U.S. 373 (2014)).

206. *See supra* Subpart III.C.1.

207. *See supra* Subpart I.B.

it impedes the disclosure and admission of relevant evidence to further judicial truth-seeking process,[208] and thus arguably clashes with prosecutors' ethical duties to pursue justice and serve the public.[209] Perhaps for these reasons, the San Diego District Attorney recently urged the California Supreme Court to rule that the Stored Communications Act does not apply to Facebook and thus does not block defense subpoenas seeking the contents of other users' private Facebook communications.[210]

Third, some may contend that privacy asymmetries are necessary to alleviate significant administrative burdens on certain subpoena recipients. But the haphazard distribution of privacy asymmetries across information domains challenges this view. It is unclear why video streaming services should be gifted an immunity from the burdens of subpoena compliance that telephone companies, banks, and hospitals successfully manage. Similarly, it is unclear why electronic communications service providers should be free to disregard criminal defense subpoenas seeking communications contents when they successfully comply with criminal defense subpoenas seeking noncontent information, and when private paper mail service providers bear the full burden of complying with criminal defense subpenas to supply relevant evidence to the courts.

Synthesizing these points, privacy asymmetries impose harms that are not outweighed by countervailing policy benefits. Contrary to common assumption, privacy asymmetries cannot be justified by analogy to physical evidence inside private homes because courts can order access to that physical evidence on request by either law enforcement or defense counsel. Meanwhile, the three most likely policy defenses of privacy asymmetries—safeguarding against excessive invasions of privacy and abuse of legal process; serving legitimate law enforcement interests; and reducing administrative burdens on subpoena recipients—fail to withstand close scrutiny. More should be required to justify selectively suppressing evidence of innocence in criminal cases.

IV. PROPOSING A DEFAULT SYMMETRICAL SAVINGS PROVISION

This Part recommends a strategy to check the accidental proliferation of unreasoned and unreasonable privacy asymmetries. Legislators who wish to avoid

208. *See generally* Ben Grunwald, *The Fragile Promise of Open-File Discovery*, 49 CONN. L. REV. 771, 778–88 (2017) (describing current, comparatively lenient statutory discovery regimes and efforts to make them more so through open file discovery).

209. *See* Fish, *supra* note 203.

210. Brief for San Diego County District Attorney at 23, Facebook, Inc. v. Superior Ct., 408 P.3d 406 (Cal. 2018), 2018 WL 4035631, at *23.

enacting privacy asymmetries unintentionally should add a default symmetrical savings provision to the end of each privacy statute. A model provision might state: "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." The phrase "otherwise valid warrants, subpoenas, or court orders" is a key component of this model text. It ensures that the savings provision would maintain the status quo investigative powers of both law enforcement and defense counsel without expanding or reducing either one. Hence, if the Fourth Amendment independently requires law enforcement to obtain a warrant with a showing of probable cause and particularity before searching or seizing certain information, then the savings provision would be consistent with that requirement. Similarly, if the subpoena rules independently require defense counsel to show relevance, admissibility, and specificity before compelling disclosures of certain information, then the savings provision would maintain those safeguards. What the savings provision would do is prevent courts from reading a privacy statute that contains an express exception for law enforcement investigations but remains silent as to defense subpoenas as a categorical and discretionless bar on defense counsel's access to court-ordered compulsory legal process.[211]

Notably, because a default symmetrical savings provision in privacy statutes would neither expand nor reduce the status quo investigative powers of either law enforcement or defense counsel, it also would not alter the status quo symmetries and asymmetries that the underlying criminal procedure rules impose. Thus, for instance, law enforcement officers would maintain their exclusive access to pre-indictment grand jury and administrative subpoenas,[212] their general monopoly on use of force and coercive searches and seizures,[213] and their power to offer witnesses immunity in exchange for testimony.[214] Meanwhile, criminal defendants would maintain their unique constitutional rights to the disclosure of

211. Of course, legislators could also achieve symmetry by ratcheting down law enforcement's investigative power to match that of defense investigators. The Communications Act of 1934 provides an historical precedent that did ratchet down in just this manner. *See infra* Appendix.

212. *See* Slobogin, *Subpoenas and Privacy*, *supra* note 27, at 806 (explaining administrative subpoenas can be "extremely easy to enforce"); *see also* Darryl K. Brown, *How to Make Criminal Trials Disappear Without Pretrial Discovery*, 55 AM. CRIM. L. REV. 155, 168 (2018).

213. *See* Baude & Stern, *supra* note 184, at 1848 ("The government's operational *monopoly* on the legitimate use of force arises precisely because the government is not constrained by laws that govern everyone else."); Sklansky, *supra* note 182, at 1187 (identifying "legal distinctions between the powers of public and private police").

214. Brown, *supra* note 212, at 168.

exculpatory and impeachment evidence from the prosecution;[215] to confront the witnesses against them;[216] and to be protected from conviction at trial unless the government proves guilt beyond a reasonable doubt.[217] And prosecutors' and defense counsel's post-indictment subpoena powers would remain, as they currently are, largely identical.[218] A default savings provision in privacy statutes would preserve this existing parity in post-indictment subpoena power, along with the other symmetries and asymmetries in the underlying procedural rules.

The same is true for the underlying symmetries and asymmetries in the federal rules of evidence. As explained in Subpart I.B, evidence rules can govern investigations as well as the admissibility of evidence at trial because, for instance, Rule 17 subpoenas must seek solely admissible evidence.[219] And, like the criminal procedure rules, the underlying evidence rules contain both symmetries and asymmetries. Privileges, for example, are largely if not entirely facially symmetrical.[220] The attorney-client privilege can block the prosecution's access to a defendant's communications, or block defense access to a cooperating witness's communications. Nonparties may assert privileges against either the prosecution

215. *See* Giglio v. United States, 405 U.S. 150 (1972); Brady v. Maryland, 373 U.S. 83 (1963); United States v. Ruiz, 536 U.S. 622 (2002); Jencks Act, 18 U.S.C. § 3500.

216. U.S. CONST. amend. VI.

217. *See In re* Winship, 397 U.S. 358 (1970).

218. *See* FED. R. CRIM. P. 17. Prosecutors' grand jury subpoena powers expire once charges are filed, leaving both prosecutors and defense investigators to rely, post-indictment, on subpoenas governed by Federal Rule of Criminal Procedure 17. Brown, *supra* note 212, at 168. The sole distinction that Rule 17 makes between the parties advances parity by establishing that, for indigent defendants, "witness fees will be paid in the same manner as those paid for witnesses the government subpoenas." FED. R. CRIM. P. 17(b). Some argue that pretrial subpoenas should be easier for defense counsel to obtain because certain heightened burdens imposed by *United States v. Nixon*, 418 U.S. 683 (1974), should apply solely to the prosecution, but most federal circuits currently apply the *Nixon* safeguards to both prosecutors and defendants. *See* Roberts, *supra* note 61.

219. For instance, evidentiary exclusionary rules can block subpoena power because *Nixon* and Rule 17 restrict criminal subpoenas to admissible evidence.

220. The advisory committee notes to the federal rules of evidence promote symmetry by stating that privilege law shall develop "a uniform standard applicable both in civil and criminal cases." Fed. R. Evid. 501 advisory committee's note to 1974 enactment (emphasis added).

For another example of a rule that is facially symmetrical but substantively asymmetrical, some jurisdictions impose heightened burdens to introduce evidence of third-party guilt. Those rules asymmetrically disadvantage defendants because defendants are more likely to try to introduce such evidence. It is possible to characterize these rules as privacy-protective because they effectively shield third-party reputational interests. But privacy is not their underlying rationale. As David Schwartz and Chelsey Metcalf have argued persuasively, protecting third-party reputational interests is neither the primary motivation nor a sufficient justification for these rules. Schwartz & Metcalf, *supra* note 67, at 351, 394–96. See also 1 Wigmore, *supra* note 67, § 139.

or against the defense, including spousal, clergy, and the Fifth Amendment privilege against self-incrimination.[221] And common law doctrines encourage symmetrical application of privilege rules on a case-by-case basis by preventing a party from selectively claiming privilege for unfavorable evidence while waiving it for the opposite.[222] Meanwhile, Federal Rules of Evidence 404(a) exemplifies an asymmetrical evidence rule; it creates special admissibility options for character propensity evidence that differ for prosecutors versus criminal defendants.[223] A default symmetrical savings provision in privacy statutes would neither add to nor subtract from the underlying symmetries and asymmetries in the evidence rules.

Adopting a default symmetrical savings provision for privacy statutes would also encourage lawmakers who do intend to enact privacy asymmetries to do so expressly in the statutory text and to justify in the legislative record why their treatment of law enforcement versus defense investigations differs. Express privacy asymmetries would not merely include express exceptions for law enforcement investigators but also express abrogations of defense subpoena power. The privacy asymmetry in federal regulations protecting substance abuse records provides a rough model. Those regulations state that the pertinent "restrictions on disclosure . . . apply whether or not . . . the person seeking the information . . . has obtained a subpoena."[224] Beyond quelling doubt about congressional intent, incorporating express explanations for the asymmetries in

221. Even the controversial general federal privilege against disclosure in state criminal proceedings could, presumably, be asserted against either state prosecutors or state defendants. *Cf.* Anna VanCleave, *The Right to Inter-Sovereign Disclosure in Criminal Cases*, 2013 WIS. L. REV. 1407, 1437–40.

Of course, facial symmetry does not guarantee substantive symmetry. Defendants' assertions of Fifth Amendment privilege might impose greater costs on prosecutors than witnesses' assertions of the same impose on defendants (although the government's unique power to grant selective immunity to witnesses gives it a countervailing advantage in avoiding costs of the privilege when asserted by anyone other than the defendant). Similarly, as I have argued elsewhere, if "the government's incentives to seek out certain types of information are systematically lower [or higher] than those of criminal defendants[,]" then a facially symmetrical privilege for that type of information does not impose a balanced restraint. Rebecca Wexler, *supra* note 31, at 1428.

222. *See, e.g.*, 36 TEX. JUR. 3D *Evidence* § 502 (2021) (describing the "offensive use doctrine").

223. Note that the Federal Rules of Evidence (FRE) 404(a) asymmetry is not particularly strong since the rule permits the prosecution to introduce comparable evidence once a defendant elects to do so. FED. R. EVID. 404(a)(1)–(2). Meanwhile, FRE 404(b) generally favors the prosecution by admitting what would otherwise be prohibited evidence of the defendant's character (although the rule is facially symmetrical and defendants do sometimes introduce 404(b) evidence, referred to as "reverse 404(b)"). FED. R. EVID. 404(b).

224. 42 C.F.R. § 2.13(b) (2019).

the legislative record would, ideally, enhance the quality of legislative reasoning, facilitate judicial analysis, and improve democratic accountability.[225]

Put succinctly, adopting the model savings provision text recommended above would preserve the status quo criminal procedure and evidence rules, including the numerous, reasonable privacy safeguards that are already built into those rules. At the same time, it would help lawmakers to avoid unintentionally distorting those rules via privacy legislation that selectively suppresses evidence of innocence.

CONCLUSION

Justice Harlan's concurrence in *Washington v. Texas*[226] insisted that, if the government enacts a procedural rule permitting prosecutors but not criminal defense counsel "to call the same person as a witness," then the government should at a minimum put forward some "justification for this type of discrimination between the prosecution and the defense."[227] This Article has taken up Justice Harlan's sentiment in the context of privacy law. It has identified a pattern of "privacy asymmetries," or privacy statutes that permit courts to order disclosures of sensitive information if requested by law enforcement but not if requested by criminal defense counsel. It has argued that privacy asymmetries are products of legislative oversight not reasoned deliberation, and that they risk substantial and unnecessary harms to criminal defendants and the adversary process by selectively suppressing evidence of innocence with no clear countervailing policy benefits. The multiple, symmetrical privacy statutes that exist alongside privacy asymmetries, as well as the numerous, reasonable privacy safeguards built into the criminal procedure and evidence rules, model a better path. At a minimum, laws that selectively advantage the search for evidence of guilt over that for evidence of innocence should not proliferate by sheer accident.

In arguing against privacy asymmetries, this Article has taken no position on the symmetry or asymmetry of criminal procedure and evidence rules as a whole. Legal scholars have offered thoughtful commentary on possible policy benefits from symmetrical and asymmetrical rules in different circumstances.[228] On the

225. *See* Katherine J. Strandburg, *Rulemaking and Inscrutable Automated Decision Tools*, 119 COLUM. L. REV. 1851, 1867–71 (2019) (presenting arguments that compelling decisionmakers to explain their reasoning can improve the quality of rulemaking).

226. 388 U.S. 14 (1967).

227. *Id.* at 24 (Harlan, J., concurring).

228. *See, e.g.*, Kiel Brennan-Marquez, Darryl K. Brown & Stephen E. Henderson, *The Trial Lottery*, WAKE FOREST L. REV. *supra* note 145, at 16–19, 46–47 & n.130 (extolling virtues of increased

one hand, symmetry in legislation might help to show that special interests have not unduly compromised the legislative process,[229] or to facilitate "interest convergence" between more and less powerful groups.[230] And symmetry specifically in criminal procedure and evidence rules might protect fairness in the adversary system,[231] and prevent government self-dealing in the rules of proof.[232] On the other hand, symmetry might also mask or falsely legitimize preexisting inequalities.[233] Perhaps, then, criminal procedure should ease its reliance on "anti-inquisitorialism,"[234] which could blunt the stakes of enduring asymmetries

symmetry in plea bargaining achieved through a "trial lottery," while recognizing that the need to accommodate the "totality of interests" might push against a "fairness as equivalence" norm).

229. William N. Eskridge, Jr., *Politics Without Romance: Implications of Public Choice Theory for Statutory Interpretation*, 74 VA. L. REV. 275, 323 (1988).

230. Derrick Bell, Brown v. Board of Education*: Reliving and Learning From Our Racial History*, 66 U. PITT. L. REV. 21, 22 (2004). *See also* Michelle A. Travis, *Lashing Back at the ADA Backlash: How the Americans With Disabilities Act Benefits Americans Without Disabilities*, 76 TENN. L. REV. 311, 332 (2009).

231. Edward J. Imwinkelried, *Should Rape Shield Laws Bar Proof That the Alleged Victim Has Made Similar, False Rape Accusations in the Past?: Fair Symmetry With Rape Sword Laws*, 47 U. PAC. L. REV. 709, 738 (2019).

232. Akhil Reed Amar, Foreword, *Sixth Amendment First Principles*, 84 GEO. L.J. 641 (1996) [hereinafter Amar, *Sixth Amendment First Principles*]; *see also* AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 116–17 (1998) (arguing that a "symmetry principle" was "at work" in the original Fifth and Sixth Amendments). Meanwhile, Paul Ohm has identified a different yet related check on government power from symmetry in what he terms "parallel-effect statutes," or statutes that tie the scope of generally applicable criminal prohibitions on eavesdropping or wiretapping to the scope of law enforcement's warrantless surveillance powers. Rather than balance the adjudicative powers of defendants and prosecutors, "parallel-effect statutes" balance law enforcement's power to charge conduct as criminal against law enforcement's power to investigate criminal conduct. Paul K. Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1603 (2004) ("If law enforcement agents seek to 'push the envelope' in their interpretation of the statute to justify their investigative techniques, they will be forced to live with the same interpretations when they pursue" defendants).

233. Barbara Flagg & Katherine Goldwasser, *Fighting for Truth, Justice, and the Asymmetrical Way*, 76 WASH. U. L.Q. 105, 110 (1998). *See also* Christopher Slobogin, *The Right to Voice Reprised*, 40 SETON HALL L. REV. 1647, 1659–60 (2010) (discussing *Holmes v. South Carolina* and the right to present a defense in the context of asymmetrical hearsay rules advantaging the defense); Alice Ristroph, *Respect and Resistance in Punishment Theory*, 97 CALIF. L. REV. 601 (2009) (arguing a Hobbesian theory that criminal defendants should be entitled to resist punishment and that this entitlement might sometimes justify asymmetrical evidentiary rules in their favor). Anna Roberts has argued persuasively against a trend toward symmetry in the allocation of peremptory strikes and questioned trends toward symmetry elsewhere in the criminal system, emphasizing that asymmetry can often better protect fairness against the backdrop of prosecutors' and defendants' very different roles. Anna Roberts, *Asymmetry as Fairness: Reversing a Peremptory Trend*, 92 WASH. U. L. REV. 1503, 1549–50 (2015).

234. Easing "anti-inquisitorialism" could also produce the opposite result. *See* David Alan Sklansky, *Anti-Inquisitorialism*, 122 HARV. L. REV. 1634, 1668, 1688 (2009) (noting the Court's

between the government and the accused.[235] Alternately, perhaps constitutional asymmetries between government powers and criminal defense rights strike a baseline "equilibrium"[236] that courts[237] and legislators[238] should seek to maintain in the face of technological and societal change. Or, perhaps subpoena powers should be symmetrical even while other procedural rules are not.[239] These issues are ripe for further research.

To date, longstanding debates in legal scholarship have focused on tensions between privacy and law enforcement investigations. Criminal defense investigations present similar issues to their law enforcement counterparts that would benefit from similar future scholarly attention.

rejection of the view that adversarialism requires presence of counsel during interrogations and observing that the fact that most defense attorneys are "chronically and drastically underfunded" could be viewed as either reason to retreat from anti-inquisitorial rhetoric or a "departure[] from the 'adversary ideal'").

235. Changing legislation is hardly the only possible solution to privacy asymmetries. Christopher Slobogin has proposed replacing the adversarial system of evidence gathering and production with a hybrid scheme in which the judge would be in charge of producing evidence during the adjudication stage, calling witnesses and serving as another questioner alongside the lawyers. Christopher Slobogin, *Lessons From Inquisitorialism*, 87 S. CAL. L. REV. 699, 715–23 (2014). Slobogin's "judge as truth-finder" proposal, and other efforts to increase inquisitorialism in criminal proceedings, would significantly mitigate the harms of privacy asymmetries. *Id.* at 723.

236. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011); *see also* Geoffrey R. Stone, *The Scope of the Fourth Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers*, 1976 AM. BAR FOUND. RSCH. J. 1993, 1216 (1976).

237. *Cf.* Orin S. Kerr, *Defending Equilibrium-Adjustment*, 125 HARV. L. REV. F. 84, 87–89 (2012) (applying the theory of "equilibrium-adjustment" to *United States v. Jones*). *But see* David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 236–41 (2015) (raising the difficulty of measuring how much privacy existed at any given historical point in time in order to try to maintain that quantity at equilibrium).

238. *Cf.* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004). *But see* Murphy, *supra* note 29, at 534–37 (identifying weakness in the institutional competence of legislatures to set privacy policy).

239. Amar, *Sixth Amendment First Principles*, *supra* note 232, at 702.

APPENDIX: STATUTES WITH AND WITHOUT PRIVACY ASYMMETRIES

A. Civil Statutes Regulating Service Provider Disclosures

1. Communications Contents

U.S. Postal Mail:

The Postal Accountability and Enhancement Act generally bars employees of the U.S. postal service from opening sealed letters.[240] The statutory text enumerates three express exceptions, which state that sealed letters may be opened pursuant to search warrants; to facilitate delivery; or with authorization from the addressee.[241] The text is silent as to court orders and subpoenas.[242] If courts read the textual silence as barring these forms of compulsory legal process, then the statute creates a privacy asymmetry disadvantaging defense investigators. Law enforcement officers can obtain a search warrant to compel U.S. postal service employees to disclose the contents of a sealed letter,[243] but defense investigators cannot use their compulsory process powers to do the same.

Note that this reading of the statutory text would create an access asymmetry for mail possessed by the U.S. postal service that does not exist for mail possessed by private mail service providers. There appear to be no statutory restrictions on compulsory legal process to compel disclosures of mail possessed by private service providers. The government may use a standard subpoena to obtain possession of unopened letters from a private mail service provider (although the Fourth Amendment may require a warrant before the government may open the letters thus obtained).[244] And there appear to be no statutory barriers to courts issuing similar subpoenas when requested by defense counsel.

Reviewing the Postal Accountability and Enhancement Act's congressional record, reports, and various hearings from 1995 through the eventual passage of the bill in 2006, reveals no indication that Congress ever considered the Act's effect

240. The Postal Accountability and Enhancement Act mandates that "[n]o letter [mailed first class and sealed against inspection] shall be opened except under authority of a search warrant authorized by law, or by an officer or employee of the Postal Service for the sole purpose of determining an address at which the letter can be delivered, or pursuant to the authorization of the addressee." 39 U.S.C. § 404(c).

241. *Id.*

242. *Id.* For a detailed discussion of the prohibition and its limits, see Anuj C. Desai, *Can the President Read Your Mail? A Legal Analysis*, 59 CATH. U. L. REV. 315 (2010).

243. *See* FED. R. CRIM. P. 41(b).

244. *See* United States v. Barr, 605 F. Supp. 114 (S.D.N.Y. 1985).

on criminal defendants' subpoena power or investigations.[245] Congress did discuss subpoena power, but solely in the context of administrative subpoenas,[246] law enforcement investigations,[247] and agency adjudications.[248]

Authorized Wiretap Materials (Historical and Today):

The historical predecessor to today's federal law regulating disclosures by wire, oral, and electronic communications service providers was symmetrical. The Communications Act of 1934[249] generally prohibited service provider

245. This review consisted of searching the legislative history complied for the Postal Accountability and Enhancement Act for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.

246. In oversight and bill hearings from 1995 and 1996, members of the Subcommittee on the Postal Service discussed whether the Postal Rate Commission should have the authority to subpoena documents from the Postal Service, and the scope of such authority. *General Oversight of the U.S. Postal Service: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 104th Cong. 89–90, 208, 327, 552, 583, 586, 622, 624, 632, 642–44 (1995); *General Oversight of the U.S. Postal Service: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 104th Cong. 82, 99, 112, 132, 148–49 (1996); *H.R. 3717, the Postal Reform Act of 1996: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 104th Cong. 50, 63, 73, 77, 106, 117, 138, 183, 292, 376, 384, 458, 462–63, 476–77, 479, 486, 502–03, 525, 617, 648, 684–85, 689, 695, 720, 777, 796, 903, 930, 978, 1014 (1996); *General Oversight of the U.S. Postal Service: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 105th Cong. 195 (1998); *H.R. 22, the Postal Modernization Act of 1999: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform*, 106th Cong. 304, 306, 353, 358–60, 414–15, 435, 479, 485 (1999).

247. In 1996 and 1997 oversight hearings, members of Congress and law enforcement witnesses discussed postal inspectors and the Office of the Inspector General's existing authority to "serve warrants and subpoenas" and contrasted this power with the inability of the Postal Service to issue investigative subpoenas. *General Oversight of the U.S. Postal Service: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 104th Cong. 189, 208, 213 (1996); *H.R. 3717, the Postal Reform Act of 1996: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 104th Cong. 304 (1996); *Oversight of the U.S. Postal Service: Inspector General of the U.S. Postal Service, Governors of U.S. Postal Service: Hearing Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 105th Cong. 12–13, 18–19 (1997); *General Oversight of the U.S. Postal Service: Hearings Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform & Oversight*, 105th Cong. 26, 33, 35, 101, 133 (1998); *The U.S. Postal Service and Postal Inspection Service: Market Competition and Law Enforcement in Conflict?: Hearing Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform*, 106th Cong. 56 n.27, 73, 141 (2000).

248. In a 2000 hearing, Congressional members heard testimony about the limited rights of defendants in agency adjudications before the Postal Service, including their general lack of any subpoena power. *The U.S. Postal Service and Postal Inspection Service: Market Competition and Law Enforcement in Conflict?: Hearing Before the Subcomm. on the Postal Serv. of the H. Comm. on Gov't Reform*, 106th Cong. 46 (2000).

249. Communications Act of 1934, Pub. L. No. 73-416, ch. 652, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

disclosures, but it contained an express exception in the statutory text that authorized either law enforcement or defense investigators to subpoena service providers for the contents of communications sent over their networks.[250] In construing this statute, the U.S. Supreme Court acknowledged that messages "known to employees of the carrier. . . . may be divulged in answer to a lawful subpoena."[251] Therefore, to the extent that service providers stored copies of the contents of messages transmitted over their networks, the service providers could be served with a subpoena and compelled to disclose the message contents in court.[252]

Today, federal law generally prohibits the providers of wire and electronic communications services from divulging the contents of their users' communications.[253] The statutory text of the Wiretap Act expressly exempts disclosures to law enforcement under certain circumstances,[254] but lacks any express exception specifically for disclosures to criminal defense investigators. Therefore, at first glance, the text appears to create a privacy asymmetry. Nevertheless, I classify the wiretap law's service providers regulations as symmetrical because the statutory text includes an express exemption authorizing "[a]ny person" to disclose the contents of authorized wiretap materials in courtroom testimony.[255] That exemption could, and I submit should, be construed neutrally to permit either law enforcement or defense investigators to subpoena service providers for the contents of certain communications (specifically, communications that the providers previously intercepted incident to performing their service).

The argument for a symmetrical reading proceeds as follows. The statute provides that any person testifying in court may disclose the contents of authorized intercepts.[256] The statute also authorizes service providers to intercept

250. The provision of the 1934 Act that regulated service provider disclosures stated: "No person receiving or assisting in receiving, or transmitting, or assisting in transmitting [wire or radio communications] shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof. . . ." *Id.* at 1103. The Act then enumerated a series of exceptions for permissible disclosures, including "in response to a subpena [sic] issued by a court of competent jurisdiction, or on demand of other lawful authority." *Id.* at 1104.

251. *Nardone I*, 302 U.S. 379, 381 (1937).

252. Telegraph service providers did routinely store message contents, though telephone and radio communications service providers may not have. *See* T.M. Cooley, *Inviolability of Telegraphic Correspondence*, 27 AM. L. REG. 65, 66 (1879).

253. 18 U.S.C. § 2511(3)(a).

254. *See id.* §§ 2511(2)(a)(ii)(B), 2511(3)(b)(i), 2516, 2518.

255. *Id.* § 2517(3).

256. *Id.*

communications incident to performing their service.[257] Therefore, service providers testifying in court may disclose the contents of communications that they intercepted incident to performing their service.[258] Either law enforcement or defense counsel should be able to compel such testimony from service providers using a subpoena ad testificandum. And, by extension, either law enforcement or defense counsel should also be able to compel the service providers to disclose the intercepted communications directly, pretrial, using a subpoena duces tecum.[259] This textual reading of the testimonial exception might also entitle criminal defendants to subpoena law enforcement for previously authorized wiretap materials.

While I have been unable to locate any case law addressing this textual argument directly, current doctrine contains some reasons to think it might succeed and some reasons to think it might not.[260] The federal courts have weighed in on the related issue of whether the "any person" testimonial exception permits civil litigants to subpoena law enforcement for pretrial disclosure of authorized wiretap materials.[261] The Ninth and Fifth Circuits have construed the statute to permit civil litigants to do this, although in both cases the litigant seeking disclosure was another government entity, namely the IRS.[262] The Eighth Circuit

257. *Id.* § 2511(2)(a)(i), (h).

258. There is also another statutory route to reach the same conclusion: Section 2511 expressly permits service providers to disclose contents "as otherwise authorized in section . . . 2517[,]" 18 U.S.C. § 2511(3)(b)(i), and Section 2517 in turn authorizes disclosure of lawful intercepts by any person testifying in court, *id.* § 2517(3).

259. SEC v. Rajaratnam, 622 F.3d 159, 175 (2d Cir. 2010) ("Surely, prior to testimonial disclosure, a district court may order that wiretap materials be disclosed to the attorney who will examine or cross-examine the witness, thereby allowing counsel to prepare for trial.").

260. In civil cases where one litigant already has possession of wiretap materials, courts have required a follow-on disclosure to the other litigant in order to avoid an "informational imbalance." *E.g.*, *id.*; *In re* Packaged Ice Antitrust Litig., No. 08-md-01952, 2011 WL 1790189, at *10 (E.D. Mich. May 10, 2011); *see also* Rosenfeld v. Lenich, No. 17-CV-7299(NGG)(PK), 2019 WL 418861, at *4 (E.D.N.Y. Feb. 1, 2019) (denying plaintiff's motion for one-sided disclosure of wiretap materials from law enforcement but indicating willingness to order parallel disclosure to both parties at the damages stage).

261. *See generally* Lori K. Odierna, Note, In re Motion to Unseal Electronic Surveillance Evidence*: Third Party Access to Government-Acquired Wiretap Evidence*, 17 W. NEW ENG. L. REV. 371, 381–98 (1995) (discussing the progression of federal case law and concluding that "[n]o court has read § 2517(3) to authorize disclosure of wiretap materials to the general public or to private litigants prior to the materials' use in a criminal trial or during the discovery phase of a private litigant's civil action.").

262. *See* Spatafore v. United States, 752 F.2d 415, 417 (9th Cir. 1985) (holding that the "any person" testimonial exception permitted the Federal Bureau of Investigation [FBI], pretrial, to disclose authorized wiretap materials to the Internal Revenue Service [IRS] for use in civil litigation); Fleming v. United States, 547 F.2d 872, 875 (5th Cir. 1977) (stating the same in dicta).

held explicitly that the testimonial exception is not available to nongovernmental civil litigants (without commenting on whether it might be available to criminal defendants).[263] Meanwhile, the Second Circuit has acknowledged that a plain text reading of the testimonial exception could support permitting any litigant to subpoena law enforcement for authorized wiretap materials, but ultimately declined to construe the statute in that manner on the basis of Title III's legislative history.[264]

Stored Electronic Communications:

After electronic communications have been transmitted over the internet, the contents of those communications are sometimes stored by service providers, such as Facebook, Twitter, and Google. The Stored Communications Act (SCA)[265] regulates service provider disclosures of those communications contents. Section 2702 generally prohibits electronic communications service providers from disclosing the contents of stored communications.[266] The statute then expressly exempts certain disclosures, including to law enforcement;[267] incident to performing the communications service;[268] and with consent of the sender or intended recipient.[269] The text is silent on disclosures pursuant to criminal defense subpoenas.[270] As a result, federal appellate and state supreme court case law since 2006 has held that Section 2702 prohibits service providers from complying with criminal defendants' subpoenas for stored communications contents.[271]

As for a notice asymmetry, the SCA authorizes law enforcement to indefinitely delay notice to the subject of an investigation[272] if notice would risk

263. *See In re* Motion to Unseal Elec. Surveillance Evidence, 990 F.2d 1015, 1019–20 (8th Cir. 1993) (en banc).
264. NBC v. U.S. Dep't of Just., 735 F.2d 51, 53 (2d Cir. 1984) ("NBC's argument based upon the language of § 2517(3) has a surface plausibility, but only if one concentrates on the language alone and ignores the rest of Title III and the legislative struggle leading to its enactment.").
265. 18 U.S.C. §§ 2701–2712.
266. *Id.* § 2702(a).
267. *Id.* §§ 2702(b)(7), 2703.
268. *Id.* § 2702(b)(5).
269. *Id.* § 2702(b)(3).
270. *See id.* § 2702(b).
271. *See* Petition for Writ of Certiorari at *11–*14, Facebook, Inc. v. Superior Ct., 140 S. Ct. 2761 (2020) (No. 19-1006), 2020 WL 703528 (discussing Facebook v. Wint, 199 A.3d 625 (D.C. 2019); State v. Bray, 422 P.3d 250 (Or. 2018); United States v. Pierce, 785 F.3d 832 (2d Cir. 2015)).
272. Law enforcement may delay notice for unlimited, successive, ninety-day periods. 18 U.S.C. § 2705(a)(4).

"endangering the life or physical safety of an individual[,]" "flight from prosecution[,]" or "intimidation of potential witnesses[,]"[273] or if notice would risk "destruction of or tampering with evidence" or "unduly delaying a trial."[274] Defense investigations can face similar risks because they often investigate the same persons, facts, and locations as law enforcement; indeed they investigate the same charges for the same crimes. But, because current readings of the SCA categorically bar defense subpoenas to service providers seeking contents of communications, the statute effectively channels these subpoenas directly to account holders without providing an option for defendants to delay notice to those account holders.[275]

The legislative history of the Electronic Communications Privacy Act of 1986, of which the Stored Communications Act is a subpart,[276] demonstrates that Congress focused on government and law enforcement access to electronic communications contents, and discussed criminal defense investigations only through generalized statements or in passing. The congressional record and reports[277] on the bill and oversight hearings[278] describe law enforcement's use of warrants, court orders, administrative subpoenas and grand jury subpoenas to obtain communications contents. A 1985 hearing includes comments from two witnesses about whether the SCA would bar disclosure to nongovernmental

273. *Id.* § 2705(a)(1)–(2), (b).

274. *Id.* § 2705(a)(2). A recent DOJ memorandum emphasizes that prosecutors may apply to courts for SCA nondisclosure orders if there is the "potential for related accounts or data to be destroyed or otherwise made inaccessible to investigators." Memorandum from Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Just., to all U.S. Att'ys 2 (Oct. 19, 2017), https://assets.documentcloud.org/documents/4116081/Policy-Regarding-Applications-for-Protective.pdf [https://perma.cc/9FFD-FFQS].

275. *See* Zwillinger & Genetski, *supra* note 34, at 591 n.104 (discussing the SCA's notice asymmetry).

276. This review consisted of searching the legislative history complied for the Electronic Communications Privacy Act of 1986 for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.

277. S.. REP. NO. 99-541 (1986); H.R. REP. NO. 99-647 (1986);132 CONG. REC. 27553 (1986); 132 CONG. REC. 27457 (1986) (not mentioning nongovernmental entities' access to contents, whether criminal defendants or civil litigants).

278. *See, e.g.*, *The Matter of Wiretapping, Electronic Eavesdropping, and Other Surveillance: Hearings Before the Subcomm. on Cts., C.L., & the Admin. of Just. of the H. Comm. on the Judiciary*, 94th Cong. (1975) (discussing law enforcement and grand jury subpoenas with no mention of criminal defense subpoenas); *S. 1667 A Bill to Amend Title 18, United States Code, With Respect to the Interception of Certain Communications, Other Forms of Surveillance, and for Other Purposes: Hearing Before the Subcomm. on Pats., Copyrights and Trademarks of the S. Comm. on the Judiciary*, 99th Cong. (1985) [hereinafter *Hearings on S. 1667*] (discussing civil and grand jury subpoenas with no mention of criminal defense subpoenas).

entities who possessed a valid subpoena for the materials.[279] A witness in a 1983 hearing described a defendant facing an obscenity charge who subpoenaed lists of the names of TV viewers who watched the same adult movies he had screened in his theater.[280] These two references to nongovernmental subpoenas and one case example of a defense subpoena are the sole plausible references to criminal defense investigations in the legislative history. All of these comments were raised by witnesses and did not become part of the bill's congressional record.

2. Noncontent Records From Digital Service Providers

Video Rental Records:

The Video Privacy Protection Act of 1988 (VPPA)[281] protects privacy in, as the name suggests, records of video rentals. Video rental records can provide relevant evidence in criminal cases, for instance to corroborate an alleged child sexual assault victim's statement that the defendant showed her a pornographic video.[282] The Act expressly authorizes law enforcement to collect information about an individual's video rentals from rental service providers,[283] albeit with required prior notice to the individual,[284] but remains silent on criminal defense subpoenas for the same information.[285] Specifically, the VPPA blanket-prohibits video rental service providers, including online video streaming services,[286] from disclosing personally identifiable information about their users,[287] and then

279. *Hearings on S. 1667*, *supra* note 278, at 99 (statement of Philip M. Walker on behalf of the Electronic Mail Association commenting that "the law is, at best, unclear"); at 102, 105 (statement of P. Michael Nugent, Government Affairs Counsel for Electronic Data Systems, mentioning ambiguity in the bill concerning disclosure of contents "to both governmental and non-governmental parties in both criminal and civil litigation").

280. *1984: Civil Liberties and the National Security State: Hearings Before the Subcomm. on Cts., C.L., & the Admin. of Just. of the H. Comm. on the Judiciary*, 98th Cong. 289 (1984) (statement of Richard M. Neustadt & M. Anne Swanson).

281. 18 U.S.C. § 2710.

282. State v. Walker, No. 28647-5-II, 2004 WL 52413, at *2 (Wash. Ct. App. Jan. 13, 2004); *see also* Daniel v. Cantrell, 375 F.3d 377, 379 (6th Cir. 2004).

283. 18 U.S.C. § 2710(b)(2)(C).

284. *Id.* § 2710(b)(3).

285. Criminal defendants may obtain the records solely with consent of the customer, *id.* § 2710(b)(2)(B), while civil litigants may compel disclosure using a subpoena, *id.* § 2710(b)(2)(F).

286. *See, e.g.*, Motion to Compel Defendant's Consent to Plaintiffs' Third-Party Subpoenas, Lasswell Found. for Learning & Laughter v. Schwartz, No. 8:17-cv-00046-JDW-TBW, 2019 WL 4386148 (M.D. Fla. Jan. 10, 2019) (arguing that the Video Privacy Protection Act [VPPA] applies to iTunes); *In re* Hulu Priv. Litig., No. C 11-03764 LB, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012) (applying VPPA to Hulu).

287. 18 U.S.C. § 2710(b)(1).

enumerates certain exceptions,[288] including disclosures made with the "informed, written consent" of the users.[289] One express exception authorizes law enforcement access pursuant to a warrant, grand jury subpoena, or court order supported by probable cause.[290] The VPPA also expressly authorizes civil litigants to compel disclosure with a subpoena, provided they give the subscriber notice and an opportunity to be heard in opposition.[291] But the statutory text is silent as to criminal defense subpoenas.[292]

Defense investigations are also almost entirely absent from the VPPA's legislative history. Congressional consideration of the VPPA involved extensive discussion of law enforcement use of, or failure to use, subpoenas to obtain video and library patrons' records, but only one mention of a criminal defense investigation.[293] That sole mention occurred during testimony before the House and Senate Judiciary Committees in which a video store chain owner informed Congress of one instance in which a "subpoena served by the attorney of one defendant in a criminal prosecution . . . sought the video records of his client's co-defendants."[294] In this same hearing, members of Congress debated whether the bill should include "civil discovery" for the records, and whether the records could ever be of use in a civil case or criminal prosecution.[295] Meanwhile, other hearings discussed law enforcement access.[296] Thus, while Congress was made aware of

288. *Id.* § 2710(b)(2).
289. *Id.* § 2710(b)(2)(B).
290. *Id.* § 2710(b)(2)(C), (b)(3). *See generally* 148 AM. JUR. *Trials* § 18 (2021) (describing case law applying the VPPA's law enforcement disclosure exception and sanctioning law enforcement who obtain protected materials in violation of the VPPA).
291. 18 U.S.C. § 2710(b)(2)(F)(i)–(ii).
292. *See id.* § 2710(b)(2)(A)–(F).
293. Reviewing the legislative history consisted of searching the legislative history complied for the Video Privacy Act of 1988 for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.
294. *Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 & S. 2361 Before the Subcomm. on Cts., C.L., & the Admin. of Just. of the H. Comm. on the Judiciary and the Subcomm. on Tech. & the L. of the S. Comm. on the Judiciary*, 100th Cong. 85 (1989) [hereinafter *Video and Library Privacy Protection Act Hearing*](statement of Vans Stevenson, Director of Public Relations, Erol's Inc.).
295. *Id.* at 124–25.
296. For instance, the hearing emphasized the restrictions placed on law enforcement to obtain confidential information from libraries and retail stores. *Id.* at 24 ("The Government has to fulfill a detailed subpoena requirement before it can get access to library records."). And oversight hearings in the U.S. House of Representatives and U.S. Senate discussed controversies generated by federal law enforcement making informal requests of librarians and video store clerks for reading and watching histories of patrons. *FBI Counterintelligence Visits to Libraries: Hearings Before the H. Subcomm. on Civ. & Const. Rts. of the Comm. on the*

defense investigations, the concerns raised about the scope of disclosure by members of Congress mentioned only civil discovery and law enforcement access.

Children Privacy Online:

The Children's Online Privacy Protection Act of 1998 (COPPA)[297] protects privacy in information that websites knowingly collect from children. It requires websites to provide notice of, and obtain parental consent for, their collection, use, and disclosure practices.[298] It includes a special exception for disclosures to law enforcement, and also includes a neutral, symmetrical exception for disclosures made "to respond to judicial process."[299] COPPA was passed as part of the Omnibus Consolidated Emergency Supplemental Appropriations Act of 1999 and therefore has a limited legislative history.[300] Congress held two hearings related to the bill, one on internet privacy before the House Telecommunications Subcommittee before the bill was introduced,[301] and one in the Senate on the bill.[302] Neither hearing mentioned criminal defense investigations specifically.[303]

Cable Subscriber Records:

The Cable Communications Policy Act of 1984[304] also contains a neutral symmetrical exception. It prohibits cable operators from disclosing a subscriber's personally identifiable information (for example, name, address, phone number) to either a private party or the government except pursuant to a court order that provides the subscriber with notice and an opportunity to object.[305] The legislative history for the Cable Communications Policy Act of 1984 contains a brief mention

Judiciary, 100th Cong. at 15, 32, 36, 37, 62, 67, 86, 103, 340, 348, 363 (1988); *Video and Library Privacy Protection Act Hearing*, *supra* note 294, at 35, 77.

297. 15 U.S.C. §§ 6501–6506.
298. *Id.* § 6502(b)(1)(A).
299. *Id.* § 6502(b)(2)(E)(iii)–(iv).
300. This search of the legislative history was conducted by searching for the terms "subpoena", "criminal", and "defendant" in the ProQuest Legislative Insight database for the Omnibus Consolidated Emergency Supplemental Appropriations Act, 1999.
301. *Consumer Privacy on the World Wide Web: Hearing Before the Subcomm. on Telecomm., Trade, & Consumer Prot. of the H. Comm. on Com.,* 105th Cong. (1998) [hereinafter *Consumer Privacy Hearing*].
302. *S. 2326, Children's Online Privacy Protection Act of 1998: Hearing Before the Subcomm. on Communications of the S. Comm. on Com., Sci., & Transp.,* 105th Cong. (1998) [hereinafter *Hearing on S. 2326*].
303. *Consumer Privacy Hearing*, *supra* note 301; *Hearing on S. 2326*, *supra* note 302.
304. Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified in scattered sections of 47 U.S.C.).
305. 47 U.S.C. § 551(c)(1)–(2)(B), (h).

of the Spectrum Commission's administrative subpoena power,[306] and no mention of criminal defense investigations or judicial subpoenas.[307]

Stored Electronic Communications Noncontent Information:

The section of the SCA that regulates disclosures of noncontent information, such as IP logs and contact lists, contains a facial asymmetry disadvantaging law enforcement; it requires law enforcement to use specific forms of legal process to compel disclosures of noncontent records from service providers, without restricting defense investigators' use of legal process to compel disclosures of the same information.[308] Note that if one looks beyond the four corners of the statutory text to consider the baseline burdens that defense investigators must satisfy to obtain a subpoena in the first place, defendants may still be disadvantaged. This is because, read in context, the SCA authorizes noncontent disclosures to law enforcement pursuant to certain forms of legal process that are arguably less onerous than the baseline subpoena burdens.[309] Specifically, the SCA authorizes law enforcement to compel disclosures of noncontent information (other than basic subscriber records)[310] merely by showing "reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation[,]"[311] whereas federal defendants seeking the same records with a pretrial subpoena must satisfy the *Nixon* hurdles[312] by showing not merely

306. In a 1979 oversight hearing, an industry witness complained that the Spectrum Commission's subpoena power was too broad, and asked Congress to limit the subpoena power to prevent the Commission from divulging trade secrets. *Amendments to the Communications Act of 1934: Hearings Before the Subcomm. on Commc'ns of the S. Comm. on Com., Sci., & Transp.*, 96th Cong. 2781 (1979).

307. This conclusion is based on a review that consisted of searching the legislative history compiled for The Cable Communications Policy Act of 1984 for the terms "defendant", "criminal", and "subpoena" in the ProQuest Legislative Insight database.

308. *See* 18 U.S.C. § 2702(c). *See* Fairfield & Luna, *supra* note 34, at 1064 ("Disclosure of non-content data to nongovernmental entities is not barred by the SCA, and, in fact, it is the one category of data that is easier to obtain by private parties than it is by government entities."); Zwillinger & Genetski, *supra* note 34, at 590 ("[I]n the context of non-content information held by ISPs, the roles are reversed, with the government facing greater, though not insurmountable, challenges, and criminal defendants facing no legal hurdle at all.").

309. *See* Zwillinger & Genetski, *supra* note 34, at 591 & n.104 (recognizing that in general, "criminal defendant[s] seeking non-content information about an ISP subscriber must serve a subpoena on the ISP[,]" and that this practical reality advantages the government).

310. The SCA rule for compelled access to basic subscriber information is facially symmetrical; it requires that both law enforcement and defense investigators obtain a subpoena, so both law enforcement and defense investigators must operate under the Rule 17 and *Nixon* subpoena standards.

311. 18 U.S.C. § 2703(c)–(d).

312. *See supra* Subpart I.B.

relevance but also specificity and admissibility.[313] As described above, the SCA's legislative history is almost entirely silent on criminal defense investigations.

3. Financial, Educational, and Health Records

Tax Filings with the IRS (Historical and Today):

Federal law protecting privacy in tax information was historically facially symmetrical, but it is no longer. Section 6103 of the Tax Code imposes confidentiality restrictions on the Internal Revenue Service (IRS) that limit it from disclosing federal tax returns.[314] Prior to 1977, Section 6103 contained an express exception permitting disclosures pursuant to court orders, without expressly limiting the court orders to those obtained by government entities.[315] The Tax Reform Act of 1976 eliminated that language and replaced it with enumerated exceptions for law enforcement investigations that did not account for defense subpoenas. As a result, today's version of the federal tax privacy law asymmetrically disadvantages defendants. Currently, the Act expressly exempts court-ordered disclosures to "officers and employees of any Federal agency" engaged in criminal investigations.[316] The Act also expressly excepts disclosures in criminal judicial proceedings "pertaining to tax administration," including pursuant to the government's Jencks Act and statutory criminal discovery disclosure obligations.[317] Yet Section 6103 is silent as to disclosures pursuant to subpoenas in judicial proceedings other than those pertaining to tax

313. *See* 18 U.S.C. § 2702(c)(6) (placing no restrictions on the disclosure of noncontent records "to any person other than a governmental entity[,]" thus defaulting in the context of criminal defense investigations to defendants' subpoena powers); United States v. Nixon, 418 U.S. 683, 699–700 (1974). To be sure, the SCA technically authorizes service providers to voluntarily disclose noncontent information to defendants, but not to law enforcement, without any legal process. Nevertheless, most service providers are unlikely to make such voluntary disclosures in practice, so this technical asymmetry is largely theoretical.

314. Note that nonparty tax returns are not privileged from subpoenas served on persons or entities other than the IRS. *See, e.g.*, Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2035–36 (2020) (holding that Congress could issue a subpoena for the President's personal tax returns subject to certain limits specific to the respective roles of the executive and the legislature); Trump v. Vance, 140 S. Ct. 2412, 2420–21, 2429 (2020) (holding that accounting firm must comply with state grand jury subpoena for President and his organization's tax returns).

315. *See* McSurely v. McAdams, 502 F. Supp. 52, 55 & n.6 (D.D.C. 1980).

316. 26 U.S.C. § 6103(i)(1)(A); *see also id.* § 6103(i)(2)–(7) (detailing other permissible disclosures to law enforcement and intelligence agencies).

317. *See id.* § 6103(h)(4)(A)–(D).

administration, and courts have expressed divergent views on whether this silence precludes IRS compliance with such subpoenas.[318]

The legislative history of the Tax Reform Act of 1976 focuses in large part on the IRS's own authority to compel tax records and financial documents from third parties. For instance, Senate hearings from 1975 outlined the IRS's power to subpoena records from "banks, insurance companies, stock brokers, customers, accountants, etc."[319] Nothing in the record indicates that Congress considered criminal defense investigative powers.[320]

Financial Services (Gramm-Leach-Bliley Act):

More general privacy protections regulating private sector financial information are symmetrical. The Gramm-Leach-Bliley Act[321] protects privacy in customer records and information held by certain types of financial institutions, including banks and investment advisors. The law gives consumers rights to notice when institutions share nonpublic information about them (such as names, addresses, social security numbers, and bank or credit card account histories) with third parties,[322] and also gives consumers limited rights to opt out of some of those

318. *Compare McSurely*, 502 F. Supp. at 52 (holding that Section 6103 of the Tax Code did not bar disclosure of IRS records pursuant to a subpoena issued by plaintiffs in a civil suit), *with* United States v. Recognition Equipment Inc., 720 F. Supp. 13, 14 (D.D.C. 1989) (holding that Section 6103 barred a criminal defendant's motion for disclosure of nonparty's tax records), *and* Dowd v. Calabrese, 101 F.R.D. 427 (D.D.C. 1984) (holding that Section 6103 barred disclosure of tax records held by the IRS).

319. *Federal Tax Return Privacy: Hearings Before the Subcomm. on Admin. of the Internal Revenue Code of the S. Comm. on Finance,* 94th Cong. 67 (1975). The hearing record also reveals unease with the U.S. Department of Justice's ability to avoid "the statutory restrictions" on law enforcement through the use of grand jury subpoenas or through informal demands made on tax preparers. *Id.* at 69, 277. House hearings from 1975 expressed concern with agents who "have a working relationship with a given bank and its employees" that enable them to go "in without benefit of any subpoena and ask[] to look at records." *Proposals for Administrative Changes in Internal Revenue Service Procedures: Hearings Before the Subcomm. on Oversight of the H. Comm. on Ways & Means*, 94th Cong. 354 (1975). The record includes a substantial number of news clippings reviewing the Supreme Court's decision in *United States v. Bisceglia*, 420 U.S. 141 (1975) upholding the IRS's John Doe subpoena directed to a bank. *Tax Reform (Administration and Public Witnesses): Public Hearings Before the H. Comm. on Ways and Means*, 94th Congress 385–477 (1975). These clippings generally frame the case as one in which the Court increased the IRS's power to subpoena records, and highlight banks' unease with complying with subpoenas for unspecified customers and without giving customers notice. *Id.* at 445, 446, 477.

320. This conclusion is based on a search of the terms "defendant", "criminal", and "subpoena" in the ProQuest Legislative Insight database for the Tax Reform Act of 1976.

321. 15 U.S.C. §§ 6801–6810.

322. *Id.* § 6802(a).

disclosures.[323] While the law does contain some exceptions for disclosures made specifically to law enforcement,[324] it also contains a general exception for disclosures made "to respond to judicial process."[325] The judicial process exception is not facially limited by the identity of the party seeking information.

Reviewing the record, reports, and hearings associated with the Gramm-Leach-Bliley Act[326] shows that Congress was concerned about ensuring bank compliance with agency and law enforcement subpoenas.[327] For instance, several hearings concerned what law enforcement and members of Congress found to be excessive limitations on law enforcement access to bank records due to the Right to Financial Privacy Act. In these hearings spanning from 1987 to 1998, witnesses and members of Congress recommended that banks be permitted, or required, to respond to law enforcement requests for information without a valid subpoena and without notice to the affected customer.[328]

None of these materials mentions criminal defense subpoenas or investigations directly. The closest the record comes is one 1998 hearing, which included reference to laws in eleven states that, in turn, made financial information confidential except when the institution has "been served with a valid legal subpoena" or where the customer consents.[329] This generalized statement could include criminal defense subpoenas, but there is no indication that Congress considered the criminal defense context when passing the Gramm-Leach-Bliley Act.

323. *Id.* § 6802(b); *see also The Gramm-Leach-Bliley Act*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/glba [https://perma.cc/4BKJ-YVB9].
324. 15 U.S.C. § 6802(e)(5), (8).
325. *Id.* § 6802(e)(8).
326. This review consisted of searching the legislative history complied for the Gramm-Leach-Bliley Act of 1984 for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.
327. Several hearings and a report focused on agency subpoenas and bank compliance. COMM. ON BANKING, HOUS., & URB. AFFS., COMPREHENSIVE DEPOSIT INS. REFORM & TAXPAYER PROT. ACT OF 1991, S. REP. NO. 102-167, at 121 (1991).
328. *Reform of the Nation's Banking and Financial Systems: Hearings Before the Subcomm. on Fin. Insts. Supervision, Regul. & Ins. of the H. Comm. on Banking, Fin. & Urb. Affs.*, 100th Cong. 320 (1988); *Financial Privacy: Hearings Before the Subcomm. on Fin. Insts. & Consumer Credit of the H. Comm. on Banking & Fin. Svcs.*, 106th Cong. 455 (1999).
329. *H.R. 4321—Financial Information Privacy Act: Hearing Before the H. Comm. on Banking & Fin. Svcs.*, 105th Cong. 68 (1998) (discussing Alaska, Connecticut, Florida, Illinois, Louisiana, Maine, Maryland, Massachusetts, North Dakota, Tennessee, and Vermont).

Financial Services (Right to Financial Privacy Act):

The Right to Financial Privacy Act (RFPA)[330] requires that federal law enforcement investigators[331] seeking customer financial records from a financial services intermediary, such as a bank, must provide the customer with written notice[332] and an opportunity to object to the disclosure.[333] Law enforcement may obtain a court order to indefinitely delay notice,[334] and gag the financial service provider if notice would risk "endangering life or physical safety of any person[,]" "flight from prosecution[,]" "destruction of or tampering with evidence[,]" "intimidation of potential witnesses[,]" or "otherwise seriously jeopardizing an investigation . . . or unduly delaying a trial."[335] The Act imposes no requirements whatsoever on criminal defense subpoenas.[336] Thus, like the SCA's noncontent provisions, it facially asymmetrically disadvantages law enforcement.[337]

The legislative history of the RFPA shows that Congress was concerned with law enforcement subpoenas to third parties in the wake of *United States v. Miller*.[338] Despite extensive discussions and documents presenting legal analysis of grand jury, administrative, and judicial subpoena law generally, there is no direct

330. 12 U.S.C. §§ 3401–3423.

331. The law regulates financial institutions' voluntary and compelled disclosure of customer records to "any agency or department of the United States." *Id.* § 3401(3).

332. *Id.* §§ 3404(c), 3405(2), 3406(c), 3407(2), 3408(4), 3412(b).

333. BD. OF GOVERNORS OF THE FED. RSRV., RIGHT TO FINANCIAL PRIVACY ACT 1 (2017), https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf [https://perma.cc/Y9UY-AAPW].

334. 12 U.S.C. § 3409(b)(1)–(2).

335. *Id.* § 3409(a)(3)(A)–(E); *see also The Right to Financial Privacy Act*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/rfpa [https://perma.cc/7B6K-EADF].

336. Note that there is a litigation exception for post-indictment government investigations, mitigating any asymmetry between government and defense investigative power. Also untouched are grand jury subpoenas, *see* 12 U.S.C. § 3413(i), and subpoenas by federal authorities in civil, criminal, or administrative disputes in which the government and the customer are parties, *see id.* § 3413(e)–(f).

Similarly, the California Right to Financial Privacy Act provides that state or local authorities seeking to subpoena records from a financial institution generally must give the customer ten days advanced notice and an opportunity to move to quash the subpoena, but imposes no parallel requirement on defense subpoenas. *See* CAL. GOV'T CODE §§ 7474(a)(3), 7476(a)(2) (West 2021).

337. The Bank Secrecy Act, which is not a privacy law and thus not examined here, may offset any disadvantages to law enforcement from other financial privacy laws by requiring financial institutions to affirmatively report suspicious activities and transactions to law enforcement. *See* 12 U.S.C. §§ 1951–1959; 31 U.S.C. §§ 5311–5330.

338. *See* 425 U.S. 435 (1976); *Right to Financial Privacy Act: Hearings Before the Subcomm. on Fin. Insts. of the S. Comm. on Banking, Hous., & Urb. Affs.*, 94th Cong. 2, 20, 163–64, 168 (1976) [hereinafter *Right to Financial Privacy Act Hearings*]; *The Safe Banking Act of 1977: Hearings Before the Subcomm. on Fin. Insts. Supervision, Regul. & Ins. of the H. Comm. on Banking, Fin. & Urb. Affs.*, 95th Cong. 1515, 1620 (1977) [hereinafter *Safe Banking Act Hearings*].

mention of criminal defense investigations or subpoenas in the record, reports, or hearings. The record does reflect a general discussion of the existing law for judicial subpoenas, and highlights the courts' "inherent power to issue such a subpoena where there is an action pending before it" subject to procedural and constitutional limitations.[339] Yet, while judicial subpoena law certainly includes criminal defense investigations, congressional hearings discussed judicial subpoenas primarily in the law enforcement context.[340] One member of Congress stated that "financial records should be safeguarded from disclosure to government or private interests" without notice and valid legal process.[341] And another hearing recognized that records may be subpoenaed in divorce proceedings.[342] Despite these mentions of nongovernmental interests, criminal defense investigations are not specifically referenced.

Educational Records:

The Family Educational Rights and Privacy Act of 1974 (FERPA)[343] requires educational institutions that receive federal funds to protect the confidentiality of students' educational records.[344] Students' educational records can be relevant to criminal investigations. For example, a student's school disciplinary records might be relevant to a defendant arguing self-defense on an assault charge.[345] Records concerning a student's cognitive, mental, or emotional disabilities, might be relevant to impeach credibility.[346] Records concerning a student's classroom, classmate, and teacher assignments might be relevant to show acquaintance or relationships.[347] The Act and related regulations authorize both law enforcement and criminal defendants to access educational records via a general exception for

339. *Right to Financial Privacy Act Hearings*, *supra* note 338, at 75–79.
340. For example, witnesses described invalid subpoenas issued to banks by U.S. Attorneys and the cost of compliance. *Right to Financial Privacy Act Hearings*, *supra* note 338, at 35. *See also Safe Banking Act Hearings*, *supra* note 338, at 23 ("Other than obtaining a search warrant (Section 1107), the last access method is for the *agency* to secure a judicial subpoena under Section 1108") (emphasis added).
341. *Right to Financial Privacy Act Hearings*, *supra* note 338, at 33.
342. *Safe Banking Act Hearings*, *supra* note 338 at 2113.
343. 20 U.S.C. § 1232g; *see also* 34 C.F.R. § 99 (2020) (providing guidance on the operation of the Family Education Rights and Privacy Act from the Department of Education).
344. John E. Theuman, Annotation, *Validity, Construction, and Application of Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C.A. § 1232g)*, 112 A.L.R. Fed. 1 (1993).
345. *See* State v. Birdsall, 568 P.2d 1094, 1096 (Ariz. Ct. App. 1977).
346. *See* Zaal v. State, 602 A.2d 1247, 1261–62 (Md. 1992).
347. *See id.* at 1261.

"any lawfully issued subpoena,"[348] while requiring educational institutions to notify students and parents prior to complying with legal process.[349]

Yet the FERPA regulations currently contain express exceptions solely for law enforcement to circumvent the notice requirement and gag educational institutions from voluntarily providing notice,[350] with no parallel option for defense investigators.[351] This was not always the case. The statutory text is silent as to notice, and the initial 1981 version of the regulations promulgated thereunder required notice for all disclosures pursuant to legal process, without exception.[352] A 1994 amendment eliminated the notice requirement for grand jury subpoenas, and created a discretionary exception to the requirement for "any other subpoena issued for a law enforcement purpose."[353] The legislative and regulatory histories contain no indication that defense investigations were discussed or considered.[354]

There is limited legislative history on the intended scope of FERPA because it was enacted as an amendment to the Elementary and Secondary Education Act of 1965 without separate committee consideration.[355] Searching the legislative history of the Elementary and Secondary Education Act of 1965 reveals not one reference to subpoenas or legal process, let alone criminal defense subpoenas.[356] Congress appears not to have considered legal process when passing FERPA.

General Medical Records:

Health privacy laws model symmetrical, neutral exceptions that treat law enforcement and defense investigations alike, from access through to notice requirements. This is so despite the fact that health data is arguably some of the most sensitive information that third parties can possess about individuals. A key example is the Health Insurance Portability and Accountability Act of 1996

348. 20 U.S.C. § 1232g(b)(2)(B).
349. 34 C.F.R. § 99.31(a)(9)(i)–(ii) (2020); *see* Reeg v. Fetzer, 78 F.R.D. 34, 36–37 (W.D. Okla. 1976) (holding that FERPA imposes a notice obligation but does not create privilege).
350. 34 C.F.R. § 99.31(a)(9)(ii)(B) (2020).
351. *Id.* § 99.31(a)(9)(ii)(A)–(C).
352. 34 C.F.R. § 99.31(a)(9) (1981).
353. *Legislative History of Major FERPA Provisions*, U.S. DEP'T EDUC. (Feb. 11, 2004), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html [https://perma.cc/AN4R-GY3H].
354. *See, e.g.*, Family Educational Rights and Privacy, 61 Fed. Reg. 59,292 (Nov. 21, 1996); Family Educational Rights and Privacy, 65 Fed. Reg. 41,852 (July 6, 2000).
355. *Family and Educational Rights and Privacy Act*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/student/ferpa/#history [https://perma.cc/F79J-CA8E].
356. This review consisted of searching the legislative history complied for the Family Educational Rights and Privacy Act for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.

(HIPAA),[357] which imposes a default notice requirement on disclosures of medical and mental-health records pursuant to an attorney-signed subpoena.[358] Under HIPAA, however, either government or defense investigators can circumvent the notice requirement if they secure a qualifying protective order[359] or obtain a warrant or a court-ordered subpoena.[360]

Substance Abuse Treatment Records:

Regulations governing federally-assisted substance abuse treatment providers[361] impose a general confidentiality requirement for patient records.[362] The regulations contain express exceptions authorizing law enforcement or prosecutors to compel disclosures,[363] and require prior notice in some circumstances[364] but not in others.[365] The regulations also contain express exceptions authorizing court-ordered disclosures for noncriminal purposes.[366] There are no express exceptions permitting any form of compelled disclosure by criminal defendants, and the regulations expressly preclude any disclosures that are not expressly authorized, even if made pursuant to a judicially so-ordered subpoena.[367]

357. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, & 42 U.S.C.); *see also* 45 C.F.R. §§ 160, 162, 164 (2020) (promulgating regulations from the Department of Health and Human Services guiding operation of HIPAA).
358. *See* 45 C.F.R. § 164.512(e)(1)(vi).
359. *See id.* § 164.512(e)(1)(ii)–(vi). A protective order qualifies if it both prohibits the use of the records "for any purpose other than the litigation or proceeding for which such information was requested," and also requires that the records be returned or destroyed at the end of the proceeding. *Id.* § 164.512(e)(1)(v)(A)–(B).
360. *Id.* § 164.512(e)(1)(i), (f)(1)(ii). Additional procedures authorize limited disclosures to facilitate law enforcement investigations, outside the context of a judicial proceeding. *See id.* § 164.512(f)(2)–(6).
361. *See* 42 C.F.R. § 2.11 (defining covered programs).
362. *See* 42 C.F.R. § 2.13(a) (providing that patient records "may be disclosed or used only as permitted by the regulations in this part and may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any federal, state, or local authority").
363. *See* 42 C.F.R. § 2.65.
364. *See* 42 C.F.R. § 2.65(b).
365. *See* 42 C.F.R. § 2.66(b).
366. *See* 42 C.F.R. § 2.64.
367. *See* 42 C.F.R. § 2.13(b) ("The restrictions on disclosure . . . apply whether or not . . . the person seeking the information . . . has obtained a subpoena . . . ."); 42 C.F.R. § 2.20 ("[N]o state law may either authorize or compel any disclosure prohibited by the regulations in this part.").

B. Criminal Statutes That Prohibit Intercepts and Unauthorized Access

Trespass:

State criminal statutes prohibiting trespass are nearly uniformly symmetrical as to law enforcement and defense investigations. The majority of states define criminal trespass as entering or remaining on private property "unlawfully," "without legal cause," "without claim of right," or similar.[368] Use of words such as "unlawfully" in the statutory text leaves open the possibility that court-ordered entry would fall beyond the scope of the criminal prohibition, regardless of the identity of the litigant who obtains the court order.[369] Criminal trespass laws in a minority of states lack terminology such as "unlawful" or "unlawfully," but most of these state statutes are also silent as to both law enforcement and defense investigators.[370] As a result, the laws remain symmetrical, perhaps enabling access

368. For criminal trespass statutes that are contain symmetrical exceptions authorizing lawful access, see Alabama, ALA. CODE § 13A-7-4 (2021); Alaska, ALASKA STAT. § 11.46.320 (2021); Arizona, ARIZ. REV. STAT. ANN. § 13-1502 (2021); Arkansas, ARK. CODE ANN. § 5-39-203 (2021); Colorado, COLO. REV. STAT. § 18-4-502 (2020); Connecticut, CONN. GEN. STAT. ANN. § 53a-108 (West 2020); Delaware, DEL. CODE ANN. tit. 11, § 821 (2021); Florida, FLA. STAT. ANN. § 82.01 (West 2020); Georgia, GA. CODE ANN. § 16-7-21 (2020); Hawaii, HAW. REV. STAT. ANN. § 708-815 (LexisNexis 2020); Idaho, IDAHO CODE § 18-7008 (2021); Illinois, 720 ILL. COMP. STAT. ANN. 5 / 21-3 (West 2020); Kansas, KAN. STAT. ANN. § 21-5808 (West 2021); Kentucky, KY. REV. STAT. ANN. § 511.080 (West 2020); Louisiana, LA. STAT. ANN. § 14:63 (2020); Maine, ME. REV. STAT. ANN. tit. 17-A, § 402 (West 2019); Michigan, MICH. COMP. LAWS ANN. § 750.552 (West 2021); Minnesota, MINN. STAT. § 609.605 (2020) (defining trespass as entering "without claim of right"); Mississippi, MISS. CODE ANN. § 97-17-97 (2021); Missouri, MO. ANN. STAT. § 569.140 (West 2020); Montana, MONT. CODE ANN. § 45-6-203 (2021); Nebraska, NEB. REV. STAT. ANN. § 28-521 (LexisNexis 2020); New Hampshire, N.H. REV. STAT. ANN. § 635:2 (LexisNexis 2021); New Jersey, N.J. STAT. ANN. § 2C:18-3 (West 2021); New York, N.Y. PENAL LAW § 140.10 (McKinney 2021); North Carolina, N.C. GEN. STAT. § 14-159.12 (2021); North Dakota, N.D. CENT. CODE § 12.1-22-03 (2019); Ohio, OHIO REV. CODE ANN. § 2911.21 (LexisNexis 2020); Oregon, OR. REV. STAT. ANN. § 164.255 (West 2020); Pennsylvania, 18 PA. STAT. AND CONS. STAT. ANN. § 3503 (West 2020); Rhode Island, 11 R.I. GEN. LAWS § 11-44-26 (2020) (defining trespass as entry with "no legitimate purpose"); South Carolina, S.C. CODE ANN. § 16-11-620 (2020) (defining trespass as entry "without legal cause"); South Dakota, S.D. CODIFIED LAWS § 22-35-6 (2021) (defining trespass as entry that is "not privileged"); Utah, UTAH CODE ANN. § 76-6-206 (LexisNexis 2021); Vermont, VT. STAT. ANN. tit. 13, § 3705 (2021); Virginia, VA. CODE ANN. § 18.2-119 (2021); Washington, WASH. REV. CODE ANN. § 9A.52.080 (West 2021); West Virginia, W. VA. CODE ANN. § 61-3B-3 (LexisNexis 2021); Wyoming, WYO. STAT. ANN § 6-3-303 (2021).

369. Thank you to Joon Hwang for conducting a fifty-state survey of state penal codes criminalizing trespass, and for identifying that the vast majority use words such as "unlawfully" in their statutory text.

370. For criminal trespass statutes that are symmetrical, but lack words like "lawfully," see Iowa, IOWA CODE § 716.7 (2021); Maryland, MD. CODE ANN., CRIM. LAW § 6-403 (LexisNexis 2021); Massachusetts, MASS. GEN. LAWS ANN. ch. 266, § 120 (West 2021); Nevada, NEV. REV. STAT. ANN.

to both law enforcement and defense investigators via implied exceptions for court-ordered entry. California, Indiana, Oklahoma, and Texas are exceptions. In these states, the criminal trespass and loitering provisions do not use words such as "unlawfully," but they do expressly and selectively exempt law enforcement from their provisions without a parallel express exception for defense investigators.[371] These appear to be the only four states in which criminal trespass laws contain privacy asymmetries.

U.S. Postal Mail:

Various provisions of the generally applicable U.S. criminal code sanction "[w]hoever" steals, takes, or opens mail not directed to them.[372] For instance, 18 U.S.C. Section 1702 imposes criminal sanctions on "[w]hoever takes any letter . . . before it has been delivered to the person to whom it was directed, with design to obstruct the correspondence, or to pry into the business or secrets of another."[373] The statutory language is symmetrical in that it contains no express exceptions for either defense investigators or law enforcement. Courts could conceivably construe the statutory silence to exclude all evidence intercepted from the postal mail, whether intercepted by law enforcement or by nongovernmental litigants.[374]

Instead, courts routinely issue warrants authorizing law enforcement to search and seize mail in transit.[375] There is some indication that courts may also

§ 207.200 (LexisNexis 2020); New Mexico, N.M. STAT. ANN. § 30-14-1 (West 2021); Tennessee, TENN. CODE ANN. § 39-14-405 (2021); Wisconsin, WIS. STAT. § 943.14 (2021).

371. For criminal trespass statutes that are asymmetrical, with an express exemption for law enforcement but not defense investigators, see California, CAL. PENAL CODE § 602.5 (West 2021); Indiana, IND. CODE ANN. § 35-43-2-2 (West 2021); Oklahoma, OKLA. STAT. ANN. tit. 21, § 1835.2 (2021); Texas, TEX. PENAL CODE ANN. § 30.05 (West 2019).

372. *E.g.*, 18 U.S.C. § 1703(b) (imposing criminal sanctions for "[w]hoever, without authority, opens, or destroys" mail not addressed to them); *id.* § 1708 (imposing criminal sanctions on "[w]hoever steals [or] takes . . . out of any mail, post office, or station thereof, letter box, mail receptacle, or any mail route or other authorized depository for mail matter"); *id.* § 1700 (imposing same for desertion of mail); *id.* § 1701 (imposing same for obstruction of mail).

373. *Id.* § 1702.

374. *Cf. Nardone I*, 302 U.S. 379, 382–84 (1937) (construing section 605 of the Federal Communications Act to bar any litigant, including federal law enforcement, from admitting wiretapped messages because of the general statutory language directing that "no person" could disclose the messages); *Nardone II*, 308 U.S. 338, 340–41 (1939) (extending *Nardone I*'s holding to bar anyone, including law enforcement from derivatively using wiretapped messages).

375. *See, e.g.*, U.S. POSTAL INSPECTION SERV., A LAW ENFORCEMENT GUIDE TO THE U.S. POSTAL INSPECTION SERVICE 31 (2006), https://www.hsdl.org/?view&did=34409 [https://perma.cc/5DWR-F3K6]

authorize nongovernmental litigants to intercept postal mail. Specifically, the Bankruptcy Code authorizes trustees to intercept, redirect, and open mail addressed to the debtor, without running afoul of the criminal prohibitions on mail tampering, as long as the debtor is provided with prior notice and an opportunity to object in court.[376] If a debtor does object, the court may order that the mail be redirected to a neutral third party.[377]

While I have been unable to locate an example of a court authorizing defense investigators to conduct a USPS intercept, this may be due to an under-documentation of defense subpoena practice in criminal trial courts. It may also be due to the practical rarity of defense counsel having advanced notice of facts sufficient to establish relevance, specificity, and admissibility of postal mail in transit, and thereby to make the threshold showing necessary to obtain a subpoena. I have also not found any court orders rejecting defendants' entitlement to a postal intercept order, were they to meet their subpoena burden.

Wiretapping (Historical and Today):

Historically, under Section 605 of the Communications Act of 1934,[378] neither law enforcement nor defense counsel could introduce evidence from real time intercepts.[379] Current law, however, contains a privacy asymmetry. Today, Title III of the Omnibus Crime Control and Safe Street Acts of 1968[380] protects

376. *See In re* Benny, 29 B.R. 754, 767, 770 (Bankr. N.D. Cal. 1983) (reasoning that the Fourth Amendment is "not clearly applicable to such a situation," and holding that a trustee commencing a mail redirection must "provide notice and an opportunity for the debtor to ventilate his objections and to seek a protective order limiting the scope of the redirection"); *see also* 5A ALEXA ASHWORTH ET. AL., FEDERAL PROCEDURE, LAWYER'S EDITION § 9:967, Westlaw (database updated Mar. 2021); 11A COLLIER ON BANKRUPTCY § 5.002[4] (14th ed. 1978), *quoted in In re* Crabtree, 37 B.R. 426, 428 (Bankr. E.D. Tenn. 1984) ("The receiver must at once secure the bankrupt's mail, either by directing the postal authorities to make delivery to the receiver himself or to a new post office box opened by the receiver.").

377. *E.g.*, *In re* Coats, 53 B.R. 64, 66 (Bankr. N.D. Tex. 1985); *Crabtree*, 37 B.R. at 429.

378. Pub. L. No. 73-416, ch. 652, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

379. Section 605 of the Act stated, in pertinent part: "[N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . . ." *Id.* at 1104. The Supreme Court read "no person" to encompass federal law enforcement as well as everyone else, and then construed the phrase "intercept . . . and divulge" to create an evidentiary privilege. *See Nardone I*, 302 U.S. at 379; *Nardone II*, 308 U.S. at 340–41. At the time there was a void in Fourth Amendment regulation of wiretapping as a result of the Court's decision in *Olmstead v. United States*, 277 U.S. 438 (1928), *overruled by Katz v. United States*, 389 U.S. 347 (1967), so the Court's reading of Section 605 was purely statutory.

380. Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (codified as amended in scattered sections of 18 U.S.C. §§ 2510–2520).

wire, oral, and electronic communications from real time intercepts. Title III generally criminalizes unauthorized intercepts, or wiretaps.[381] The statutory text contains an express exception permitting law enforcement to conduct wiretaps, but the text remains silent as to defense investigators. Section 2511(1) states: "Except as otherwise specifically provided in this chapter *any person* who intentionally intercepts . . . any wire, oral, or electronic communication" is subject to criminal penalty.[382] Section 2511(2) then enumerates a series of express exemptions for permissible intercepts, including: by or for law enforcement pursuant to certain forms of legal process;[383] by service providers incident to performing the communications service;[384] and with the consent of a party to the communication.[385] There is no express exemption for intercepts made pursuant to criminal defendants' compulsory process powers.[386] The Supreme Court has construed the list of exemptions as exhaustive, parroting the plain text of the statute by asserting: "Except as expressly authorized in Title III . . . all interceptions of wire and oral communications are flatly prohibited."[387] Thus, the current wiretap law introduces a privacy asymmetry into the criminal code.

While the Omnibus Crime Control and Safe Streets Act of 1968 contained a variety of legislative proposals beyond the wiretapping statutes in Title III, reviewing the entire legislative history[388] reveals no indication that Congress ever considered the Act's impact on criminal defense investigations. Instead, discussions of legal process and access to evidence focused on law enforcement. For instance, in multiple hearings, Congress received testimony explaining how the law differed for law enforcement's use of search warrants versus subpoenas, and the Fourth and Fifth Amendment requirements for each.[389] There was also limited discussion of public resistance to law enforcement's overuse of subpoenas.[390]

381. *See* 18 U.S.C. §§ 2510–2520.
382. *Id.* § 2511(1)(a), (4)(a) (emphasis added).
383. *Id.* §§ 2511(2)(a)(ii)(B), 2516, 2518.
384. *Id.* § 2511(2)(a)(i), (h)(ii).
385. *Id.* § 2511(2)(c), (d).
386. *See id.* § 2511(2)(a)–(j).
387. Gelbard v. United States, 408 U.S. 41, 46 (1972).
388. This review consisted of searching the legislative history complied for the Omnibus Crime Control and Safe Streets Act of 1968 for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.
389. *See, e.g.*, *Anti-Crime Program: Hearings Before Subcomm. No. 5 of the H. Comm. on the Judiciary*, 90th Cong. 1134–35, 1228, 1241 (1967) (discussing *Hale v. Henkel*, 201 U.S. 43 (1906) and *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920)).
390. *Federal Firearms Act: Hearings Before the Subcomm. to Investigate Juv. Delinq. of the S. Comm. on the Judiciary*, 90th Cong. 1168 (1967).

Stored Electronic Communications:

The SCA[391] generally criminalizes unauthorized access to stored electronic communications, stating: "Except as provided in subsection (c) of this section whoever intentionally accesses [stored electronic communications] without authorization" is subject to criminal penalty.[392] Subsection (c) then lists three express exceptions: access by service providers;[393] access by parties to the communication;[394] and access by law enforcement.[395] The criminal prohibition asserts on its face that it applies "except as provided" elsewhere in the statute, meaning the list of exemptions is exhaustive.[396] There are no express exceptions for criminal defense investigators to gain access pursuant to a court order or subpoena. Thus, the SCA's criminal provisions replicate the privacy asymmetry in the criminal wiretap law for real time intercepts.[397]

Protected Computers:

Yet another privacy asymmetry for stored electronic communications appears in the Computer Fraud and Abuse Act (CFAA)[398] which—while not specific to communications—protects them along with other information stored on computers. The CFAA criminalizes unauthorized access to computer systems (or hacking) to obtain "information from any protected computer."[399] The statute expressly exempts law enforcement,[400] but contains no facial exception for defense investigators or others acting pursuant to a court order. Because courts have repeatedly construed this structure of statutory text as a categorical bar on defense investigative power, I classify the CFAA as an asymmetrical statute.

391. 18 U.S.C. §§ 2701–2712.
392. *Id.* § 2701(a)–(b).
393. *Id.* § 2701(c)(1).
394. *Id.* § 2701(c)(2).
395. *See id.* § 2701(c)(3) (referencing sections 2703, 2704, and 2518, all of which apply exclusively to law enforcement or government entities).
396. *Id.* § 2701(a). *Cf.* Gelbard v. United States, 408 U.S. 41, 46 (1972) (setting precedent that statutes with a general prohibition followed by enumerated exceptions render the exceptions exhaustive, through interpretation of Title III).
397. For a discussion of the legislative record of the SCA, see *supra* notes 286–90 and accompanying text.
398. 18 U.S.C. § 1030.
399. *Id.* § 1030(a)(2)(C). The definition of a "protected computer" is vast, including any computer "used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).
400. *Id.* § 1030(f) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency . . . .").

Yet, there is a possibility that courts could construe the statute symmetrically. The CFAA lacks any language similar to Title III's assertion that wiretapping is prohibited "[e]xcept as otherwise specifically provided in this chapter[,]"[401] which is the language that the Supreme Court parroted when holding that the enumerated exemptions to Title III's criminal prohibition are exhaustive.[402] Perhaps, then, the CFAA should be construed in the same way as the criminal mail tampering statute and unlawful entry and burglary statutes. In that case, the prohibition would yield to compulsory legal process, whether exercised by law enforcement or by criminal defendants.

The legislative history of the CFAA reveals only one reference to compulsory process.[403] In hearings held in 1983 and 1984, an Assistant State Attorney for Florida urged Congress to pass federal computer crime legislation because uniform laws and state statutes "do not create interstate subpoenas capable of compelling attendance of critical witnesses."[404] This testimony focused on evidence for criminal prosecutions. There was no mention in this hearing, or in the congressional record, reports, or other hearings, of criminal defense investigative powers.

401. *Id.* § 2511(1).
402. *See* Gelbard v. United States, 408 U.S. 41, 46 (1972).
403. This review consisted of searching the legislative history complied for the Computer Fraud and Abuse Act for the terms "defendant", "criminal", and "subpoena" in ProQuest Legislative Insight database.
404. *Counterfeit Access Device and Computer Fraud and Abuse Act: Hearings Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 98th Cong. 237 (1984).