Greetings,

I am excited to share this rough draft with you. The project is still very rough and has a long way to go in development. So I appreciate your patience with the current text, and deeply appreciate the opportunity to seek your feedback and critique.

If you are short for time, Part I would be good to skip. It provides background on what defense investigations are, and existing reasonable limits on those investigations from subpoena rules, evidence rules, and symmetrical privacy statutes, all of which together provide a baseline balancing regime to resolve conflicting interests in defense investigations and nonparty privacy. The asymmetrical privacy laws that are the focus of this project layer on top of that baseline, and my discussion of those privacy asymmetries begins in Part II.

Thank you!

Best,
Rebecca
Privacy Asymmetries: Access to Data in Criminal Investigations
Rebecca Wexler

Table of Contents

Introduction .................................................................................................................. 3

I. Balancing Defense Investigations and Nonparty Privacy .................. 9
   A. The Need for Defense Investigations in an Adversary System .... 9
   B. Reasonable Symmetrical Privacy-Protective Limits on Defense Investigations ................................................................. 12
      2. Privileges ............................................................................. 16
      3. Symmetrical Privacy Statutes ............................................. 19
   C. Sporadic Precedents Disfavoring Rules that Asymmetrically Disadvantage Defense Investigations ...................................................... 20
      1. Against-Penal-Interest Hearsay ................................... 20
      2. Right to Present a Defense ............................................. 23

II. Privacy Asymmetries ....................................................................................... 24
   A. Asymmetries Disadvantaging Defendants ....................... 25
      1. The Stored Communications Act................................... 25
      2. Video Rental Records .................................................. 28
      3. Educational Records .................................................. 29
      4. Tax Returns ........................................................................... 30
      5. Police Disciplinary Records ..................................... 30
   B. Asymmetries Disadvantaging Law Enforcement ................. 32
      1. Financial Records .......................................................... 32

III. Correcting for Irrational Privacy Asymmetries ............................... 32
   A. The Policy of Privacy Asymmetries ................................ 34
      1. Risks of Overbroad Collection, Retention, and Use ...... 34
      2. Risks of Abuse ................................................................. 35
      3. Case Study: The Stored Communications Act ............... 37
   B. The Limited Avenues for Constitutional Challenge ............. 41
      1. Positive Rights to Compel Pretrial Access to Evidence ...... 41
      2. Negative Rights Against Arbitrary and Disproportionate Exclusionary Rules ................................................................. 43
   C. An Interpretive Rule to Rebuttably Presume Symmetry ........ 45

Conclusion ........................................................................................................... 46

1 Acknowledgments forthcoming.
Introduction

In 2019, a man in New York City was jailed after a complaining witness produced screenshots of harassing text messages and phone calls, and audio of a whispering voicemail, that the man allegedly sent to her in violation of a family court protective order. Defense counsel subpoenaed SpoofCard, a commercial service that enables customers to disguise their phone numbers, for records pertaining to the complaining witness. SpoofCard produced records showing that the witness was a paid subscriber; that she used the service to send the texts and phone calls to herself, disguised as coming from the defendant’s number, and that she recorded some calls using the service: “voice changer: man.” In response to a subsequent court-ordered subpoena, SpoofCard produced audio of voicemails that the complaining witness sent to herself from the defendant’s number, which contained whispers modified by “voice changer: man.” Defense counsel showed these records to the prosecutor, who dropped the charges and released the man from jail. This case illustrates why defense counsel’s ability to conduct independent investigations matters. While due process requires prosecutors to disclose material exculpatory and impeachment evidence in their possession, law enforcement has no obligation to actively investigate exculpatory evidence that would support a defendant’s theory of the case. In the United States adversarial system, that duty to investigate is defense counsel’s alone.

This Article identifies a troubling and almost certainly unintentional pattern in consumer data privacy laws; many make exculpatory evidence selectively unavailable to the accused. These laws include carve outs for criminal investigations that give law enforcement more or better access to sensitive information than they give to criminal defense investigators. I call these disparities “privacy

---

2 People v. [Redacted], Affirmation in Support of Motion for Issuance of Subpoena Duces Tecum, at ¶¶ 3, 5 (N.Y. Ct’y [Redacted]) (on file with author).
3 Jerome Greco, Supervising Attorney, Digital Forensics Unit of the Legal Aid Society of New York City.
4 https://www.spoofcard.com/.
5 People v. [Redacted], Subpoena Duces Tecum, at ¶ 1 (N.Y. Ct’y [Redacted]) (on file with author).
7 People v. [Redacted], Judicial Subpoena Duces Tecum, at ¶ 1 (N.Y. Ct’y [Redacted]) (on file with author).
8 SpoofCard User Report II [Redacted] (on file with author).
9 Conversation between author and Jerome Greco.
12 See Erin Murphy, The Politics of Privacy in the Criminal Justice System.
asymmetries.” Privacy asymmetries skew investigations in favor of the prosecution by making substantial quantities of useful data available to law enforcement while placing critical information beyond reach of the defense.\textsuperscript{13} The legislative histories of these laws are generally silent as to defense investigations, suggesting that the laws’ asymmetrical treatment of law enforcement and defense investigators is the product of oversight, not reason.\textsuperscript{14} This Article argues that exceptions to privacy laws that enable police and prosecutors to access sensitive information should also apply to defense investigators, or in the alternative the government should have to justify why the treatment differs. To achieve this goal, the Article urges both legislatures and courts to adopt a “symmetry or justification” interpretive rule: privacy statutes with exceptions for law enforcement but silence as to defense investigations should create the rebuttable presumption of an implied, parallel exception for defense subpoenas.\textsuperscript{15} Defeating the presumption should require express justification for asymmetrical treatment, not merely justification for law enforcement access, or for defense restrictions, considered in isolation.

Privacy asymmetries are part of a broader trend whereby the government’s abilities to collect, store, and analyze data are far outpacing those of criminal defendants.\textsuperscript{16} Artificial intelligence and machine-learning technologies exacerbate these growing inequalities in investigative power,\textsuperscript{17} threatening principles of parity and reciprocity. Disparate access to relevant information impedes defense challenges to prosecution evidence, hinders the development of plausible defense-oriented technologies, and undermines the promise of adversarial process. Without correction, this trend will only worsen as access to data from private sector intermediaries is becoming more and more important to criminal cases.\textsuperscript{18} Private sector service providers currently collect data about our heartbeats, location information, personal associations, facial expressions, phone calls, emails, news and other media consumption, consumer purchases, health, exercise, genetics, and more. Much of this data can be relevant evidence to criminal investigations. Amazon Echo recordings,\textsuperscript{19} cellphone photograph

\textsuperscript{13} Wexler, How Data Privacy Laws Could Make the Criminal Justice System Even More Unfair, LA Times.

\textsuperscript{14} Cf. Marc J. Zwillinger & Christian S. Genetski, Criminal Discovery of Internet Communications Under the Stored Communications Act, 97 J. Crim. L & Criminology (2007).


\textsuperscript{17} Cf. Katyal & Stallman, Access to Data piece; Cuellar & Huq, Privacy’s Political Economy.

\textsuperscript{18} See, Jane Bambauer, Other People’s Papers, 94 Tex. L. Rev. 205 (2015).

\textsuperscript{19} See, Colin Dwyer, Arkansas Prosecutors Drop Murder Case that Hinged on Evidence from Amazon Echo, NPR, Nov. 29, 2017, at 5:42 p.m.; see also, https://cdt.org/insights/alexa-is-law-enforcement-listening/.
metadata,

see Tom McMullan, How an Apple Watch Could Decide a Murder Case, Medium (June 21, 2018).

smart water meter data, pacemaker data,

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/?flag=COS-05-10aa0b&linkId=39705414.

Fitbit data, have all been used in criminal cases, both to convict and to exonerate.

Police increasingly rely on private sector DNA databases, such as GEDmatch, 23andme, and Ancestry.com, to conduct genetic searches.

Meanwhile, artificial intelligence and machine-learning search tools, including 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. DNA searches rely on algorithmic tools to analyze crime scene samples and compare them to DNA databases, as well as to conduct “familial searching” to identify and rank possible matches to suspects’ genetic relatives. 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. Similar disparities plague access to training data. The Arnold Foundation has explained that data sharing agreements prevent it from disclosing the training data for its Public Safety Assessment tool, a risk assessment instrument currently in use in bail decisions across the country, despite the fact that the training data comprised judicial records to which First Amendment and common law rights of public access apply. Beyond capacity to use or assess artificial intelligence and machine-learning systems designed with prosecution interests in mind, disparate access to training data impedes the development of similar systems designed to serve defense interests. Privacy laws that shield police disciplinary records from disclosure to defendants and the

see Nicole Black, Fitbit Evidence Provides Alibi for Victim’s Boyfriend, LegalNews.com (Nov. 1, 2018); Andrew K. Smith, Meet Your new star Eyewitness, The CLM (July 28, 2017); Jacob Gershman, Prosecutors Say Fitbit Data Exposed Fibbing in Rape Case, Wall St. J. Law Blog, Apr. 21, 2016, at 1:53 p.m.


see, Andrew Ferguson, Digital Brady; Roth, New Work on AI?

see, Andrea Roth, Machine Testimony; Trial by Machine.


see, e.g., TrueAllele, STRMix, FST trade secret claims. See Kashmir Hill, NYT.

see Email from Arnold Foundation to David Murdter, Oct. 25, 2018 (on file with author).

see https://www.psapretrial.org/about.

The initial PSA was trained on 746,525 bail outcomes selected from an initial 1,515,051 drawn from multiple jurisdictions.
public, for instance, obstruct the development of risk assessment tools to flag police misconduct.

While existing privacy asymmetries do not yet apply to much of the data discussed in the preceding paragraphs, a new wave of state and federal data privacy bills risks imposing privacy asymmetries on new and broader categories of data. At least eight federal privacy bills introduced in 2019 contained privacy asymmetries. The proposed Data Care Act, Data Broker Accountability and Transparency Act, Balancing the Rights of Web Surfers Equally and Responsibly Act, and American Data Dissemination Act would all impose more onerous burdens on defense investigators than on law enforcement to access the same information. The proposed Consumer Data Protection Act, Social Media Privacy Protection and Consumer Rights Act, Balancing the Rights of Web Surfers Equally and Responsibly Act, and American Data Dissemination Act all contain notice requirements for disclosures that have exceptions for law enforcement but not for defense investigations. And the California Consumer Privacy Act, 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.

In 1967, the same year Justice Harlan’s concurrence in Katz v. United States announced the “reasonable expectation of privacy” test for Fourth Amendment searches, Harlan’s concurrence in Washington v. Texas explained that a Texas rule permitting prosecutors, but not the accused, to introduce
Privacy Asymmetries


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.”

This Article takes up Harlan’s sentiment in the context of privacy laws. Part I describes the need for defense investigations in an adversary system, and the numerous, reasonable, symmetrical limits on the defense investigative power that already balance defense investigations with nonparty privacy interests. Privacy asymmetries layer on top of this baseline balancing regime. Part II details the privacy asymmetries in multiple federal privacy statutes, almost all of which disadvantage defendants. Part III explains the limitations of constitutional challenges to privacy asymmetries under current doctrine, and proposes that legislatures and courts fill the constitutional void by adopting an interpretive rule to limit the risk that lawmakers will inadvertently proliferate privacy asymmetries.

Of course, numerous information, power, and resource asymmetries characterize the relationship between the government and the accused. The government alone bears the burden of proof, and has power to issue grand jury subpoenas and offer immunity in exchange for testimony. Defendants alone wield confrontation and speedy trial rights. Prosecutors alone enjoy immunity from suit. Defendants have sole rights to appeal convictions. Certain aspects of criminal defendants’ investigative power have expanded since the mid-Twentieth Century, such as the recognition of a constitutional right to a public defender, to expert witnesses, to the disclosure of exculpatory and impeachment evidence, and the enactment of statutory rights to subpoena power and discovery. Meanwhile, the government has demonstrated informal power to pressure technology companies to disclose information or otherwise assist in investigations, while anecdotal evidence shows the opposite for defense counsel: difficulty compelling technology companies to cooperate with investigations, even pursuant to court orders.

50 See, Old Chief.
51 US Const. Amend. VI.
53 Gideon.
55 Brady, Giglio, Ruiz.
56 See, e.g., Jencks Act; New York’s new discovery laws.
57 See, e.g., Crompton contempt judgement.
This Article takes as given that many such asymmetries exist, and seeks to evaluate the wisdom of adding more through the specific mechanism of privacy statutes that block defense subpoena power. For purposes of this Article, then, I advance no particular position as to status quo asymmetries arising from sources other than privacy legislation. Perhaps, as argued by Akhil Amar, the Sixth Amendment requires “parity of subpoena-like compulsion power,” even though “compulsion parity does not entirely even the scales between prosecution and defendant.” 58 Or perhaps, analogizing to Orin Kerr’s “equilibrium-adjustment” theory of the Fourth Amendment, 59 constitutional asymmetries between government powers and defense rights strike a baseline “equilibrium” that courts 60 and legislators 61 should seek to maintain in the face of technological and societal change. Or perhaps, following David Sklansky, criminal procedure should case its reliance on “anti-inquisitorialism,” which could blunt the stakes of enduring asymmetries between the government and defendants. 62 This Article’s more targeted aim is to identify and assess asymmetries in privacy statutes that extend the consequences of other constitutional, statutory, and practical constraints.

More broadly, this Article aims to spotlight criminal defense investigations as a foil for ongoing scholarly debates over law enforcement investigations and privacy. Defense investigations raise similar tensions between truth-seeking and privacy as their law enforcement counterparts, but in a parallel universe where the Fourth Amendment does not apply. Yet, scholarship on privacy and criminal investigations has primarily focused on law enforcement. 63 Scholars have debated the effect of technological change on “the balance between privacy rights and law enforcement needs” 64 in Fourth Amendment doctrine 65; privacy and

64 See Askin, 47 F 3d at 105–06 (collecting citations).
government subpoena power; transparency surrounding government use of electronic surveillance; and statutory privacy protections from government investigations; among many other issues. To the extent that the literature has addressed defendants’ investigative power, it has concentrated on defense access to information from the government. Scholars have, for instance, critiqued criminal defendants’ lack of access to the fruits of government investigations, including government databases, and other evidence in the constructive possession of the prosecution. Defense investigations have received substantially less scholarly attention, despite their potential to cross-fertilize critical thinking about trade-offs between truth-seeking and privacy.

I. Balancing Defense Investigations and Nonparty Privacy

A. The Need for Defense Investigations in an Adversary System

Criminal defense attorneys must conduct independent investigations into the facts of each case; they may not rely solely on discovery materials provided by the government. As the Hawai‘i Supreme Court explained in 2016, defense investigations designed “to make best use of cross-examination and impeachment of witnesses at trial; to understand the account of [their] 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.”

66 Christopher Slobogin, Policing Databases and Surveillance at 209; Christopher Slobogin, Privacy and Subpoenas.


69 See, e.g., Fairfield & Luna, Digital Innocence, Cornell L. Rev (intelligence authorities’ surveillance data); Kreag, Letting Innocence Suffer (DNA databases); Abel, Brady’s Blind Spot (police impeachment evidence); Conti-Cook, Open Data Policing (police impeachment evidence); Conti-Cook, Defending the Public (police impeachment evidence); Garrett, Big Data and Due Process (discovery and Brady access to government data); Bambauer, Other People’s Papers (due process access to government data); Noah Gimbel, Body Cameras and Criminal Discovery, Geo. L. J. (2016); other access to body cam footage paper; Erin Murphy, DNA in the Criminal Justice System: A Congressional Research Service Report, 64 UCLA L. Rev. Discourse, 340 (2016) (“government access to a person’s genetic material”).

70 Andrew Ferguson, Big Data Prosecution and Brady, 67 UCLA L. Rev. __ (2020); Barry Scheck, Preface – The Integrity of our Convictions – Holding Stakeholders Accountable in an Era of Criminal Justice Reform, Georgetown Annual Review of Criminal Procedure (2020).

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.”

Pursuant to this investigative mandate, defense counsel may seek to obtain information about nonparties, including police witnesses, other prosecution witnesses, the defendants’ own witnesses, and victims, as well as seeking information about locations associated with a crime or alibi. If a defendant argues ‘third party guilt,’ claiming that a different individual committed the crime and law enforcement has arrested the wrong person, defense investigators may seek information about that alternate third-party suspect. Similarly, defense counsel may investigate a client’s co-defendants, for instance, to show that the client played a relatively small role in a criminal enterprise, was threatened into participating, or other mitigating circumstances. Defense counsel may investigate to corroborate an alibi, or examine the crime scene for lines of sight in order to challenge the reliability of an eye witness. These types of evidence may not be in the possession of the prosecution, so defense counsel may not rely exclusively on the government’s *Brady* and statutory discovery disclosures. Instead, defense investigations rely on defendants’ Sixth Amendment and due process rights, as well as their statutory subpoena powers.

With proper legal process and judicial oversight, defense counsel is authorized to obtain even private information protected by the Fourth Amendment from unreasonable government searches and seizures. For instance, most state supreme courts that have considered the issue have recognized a criminal defendant’s entitlement in certain circumstances to a court order compelling access to inspect a nonparty’s private home, as have most intermediate appellate courts.

73 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.
74 See, People v. Rouse, No. 93 (NY, Nov. 25, 2019).
Privacy Asymmetries

__ Privacy Asymmetries __

U.C.L.A.

L.

R
ev.

( ___ forthcoming ___ 2020 ___)

courts. 78 New York State’s recently enacted discovery statute makes express the right of criminal defendants to a court order granting defense counsel “access to inspect” a home “that relates to the subject matter of the case.” 79 ADD MORE STUFF ABOUT THE HOME!!

Similarly, defendants can subpoena third-party intermediaries for sensitive information about nonparty witnesses or other individuals. For instance, Carpenter v. United States’s holding that the Fourth Amendment protects historical cell site location records does not alter defendants’ longstanding capacity to subpoena telecommunications service providers for nonparties’ cell site location information. 80 Defense counsel regularly subpoena communications, financial, and medical service providers, and others for private information about nonparties. And, as with law enforcement, when defendants investigate dangerous or untrustworthy individuals who might threaten or intimidate witnesses or spoliate evidence, defense counsel may apply to the court for a nondisclosure order prohibiting a third party served with a subpoena from notifying the target of the investigation. 82

Given these powers, defense investigations, like law enforcement investigations, risk excess invasions of privacy. The National Crime Victim Law Institute asserts that, in “criminal cases, especially those involving rape or sexual assault, defendants routinely attack victims’ privacy by seeking personal records, such as counseling, mental health, medical, employment, educational, and child protective services records.” 83 Beyond the possibility that otherwise legitimate defense subpoenas could be overbroad or unduly burdensome, there is a risk that rogue defense counsel — like rogue prosecutors — could abuse their investigative power to harass or intimidate potential witnesses, including victims, police officers, and others. 85 As a result, the legal process requirements for defense investigations may need to be strengthened.


79 NY S1716 § 245.30(2).


83 Discovery Versus Production: There is a Difference, NCVLI News, Spring/Summer 2006.


counsel to exercise investigative power must include safeguards and oversight mechanisms. Access-to-premises orders for inspection of private homes, for instance, generally require criminal defendants to meet a threshold showing of relevance, materiality, or even necessity, following which the court will balance the competing interests in access versus privacy before determining whether to issue the order. The following Part details some existing reasonable safeguards and oversight mechanisms to balance defense investigative interests with nonparty privacy. Notably, these safeguards apply symmetrically to law enforcement and defense investigations alike.

B. Reasonable Symmetrical Privacy-Protective Limits on Defense Investigations

As the prior Part explained, defense counsel must conduct independent investigations, rather than rely solely on information disclosures from the government. In the U.S. adversarial system, defense counsel alone has responsibility to affirmatively seek out exculpatory evidence. Like law enforcement investigations, defense investigations can conflict with nonparty privacy interests. Accordingly, subpoena and evidence rules incorporate baseline privacy safeguards to balance the competing interests. Initial layers of privacy protection in both the subpoena and evidence rules apply generally to any type of private information. These layers incorporate substantial judicial discretion through standards (such as the “unreasonable or oppressive” basis for quashing subpoenas), and through inherent authority (such as judges’ power to restrict evidence on collateral issues). The rules also include heightened protections for specific types of private information, such as personal or confidential information about victims and privileged information. Those protections permit less judicial discretion but still safety-valve judicial overrides for extreme circumstances. Hence, judges may override the requirement to notify victims about subpoenas that seek private information about them if providing such notice would risk witness tampering, destruction of evidence, or threats to a person’s life or physical safety. And some statutory privileges contain express exceptions for circumstances in which applying them would “deprive the People or the defendant of a fair trial.”

From initial discretionary layers of privacy protection to the zenith of privilege, the privacy safeguards built into subpoena and evidence rules generally apply symmetrically to law enforcement and defense investigations alike. The Part then describes symmetrical privacy statutes that layer further categorical protections on top of the subpoena-evidence baseline, yet still manage to treat law enforcement and defense investigations alike.

1. Balancing Tests in Subpoena and Evidence Rules

This Part explains how subpoena and evidence rules combine to balance defense investigations with nonparty privacy.

Two overarching characteristics of the subpoena-evidence baseline balance are especially pertinent here. First, the privacy protections built into subpoena and evidence rules incorporate substantial judicial discretion to balance the competing interests on a case-by-case basis, albeit with varying weights on the scale in different circumstances. Even in cases involving highly sensitive information, such as personal and confidential information about victims, subpoena and evidence privacy protections generally contain safety valve judicial override options for edge cases in which abiding by the safeguards could risk witness tampering, destruction of evidence, threats to physical safety, or other extreme harms. Second, the privacy safeguards in subpoena and evidence rules generally apply symmetrically to law enforcement and defense investigations alike. Of course, it may be possible to improve the precise calibration of privacy protections that current subpoena and evidence rules afford. But legislators seeking to modify that calibration through privacy statutes should be informed of and by the preexisting evidence baseline privacy protections that subpoena and evidence rulemakers have already created. At minimum, subpoena and evidence rules provide alternate, more nuanced, models for balancing truth-seeking versus privacy that can enrich the development of privacy law and policy.

The default rule for subpoenas at both common law and today is that privacy interests do not generally defeat a litigant’s right to compel the production of relevant evidence.87 In Wigmore’s words, “[n]o pledge of privacy . . . can avail against the demand for truth in a court of justice.”88 Contemporary rules, however, impose substantial limits on defense investigative power. This Subpart describes privacy safeguards built into subpoena rules. Subpoena rules protect privacy through mandatory judicial oversight, high threshold burdens, broad judicial discretion to quash, and — when the risk of privacy invasion is especially concerning — notice requirements.

To start, defense counsel cannot compel nonparties to produce documents without judicial oversight. To obtain a court-ordered subpoena, defense counsel generally must petition the court and file a sworn declaration. For attorney subpoenas, defense counsel may serve the subpoena directly but may generally command only that documents be produced to the court, not to counsel. Some jurisdictions permit defense counsel to serve attorney subpoenas at any point pretrial, but require counsel to petition the court and make a showing for release of the documents. Other jurisdictions restrict attorney subpoenas to evidentiary hearings, including preliminary hearings, suppression hearings, or trial itself.

Defendants must also satisfy challenging threshold burdens to obtain subpoenas that can be difficult or even impossible to satisfy for evidence that

87 See, e.g., Wigmore, p. 2998, § 2211 (1904); United States v. Tilden, 28 F. Cas. 174, 177-78 (S.D.N.Y. 1879).
88 See also, Wigmore, p. 3186, §2286 (1904).
defense investigators have not yet seen. Defendants must show in advance that the subpoenas seek documents that are reasonably likely to be relevant and exculpatory. They may not use subpoenas “for the purpose of discovery or to ascertain the existence of evidence.” For pretrial subpoenas, defendants must overcome further “hurdles,” including showing “good faith,” showing a sufficient likelihood that the documents sought are “relevant” and “admissible,” and identifying the documents with enough “specificity” to allay concerns of “a general fishing expedition.” The requirement that information must be “admissible” means that subpoenas cannot be used to obtain hearsay information or information that would be protected by rape shield laws.

Next, even if defense counsel satisfies the initial burdens to obtain a subpoena, trial courts retain broad discretion to quash otherwise valid subpoenas if compliance would be “unreasonable or oppressive.” Privacy intrusions are a basis for quashal, as is the availability of information from other, less privacy-intrusive means. And when subpoenas are served on third-party intermediaries, such as communications, financial, or medical service providers, the individual who is the subject of the investigation generally has standing to move to quash before the documents may be compelled. Even if a court ultimately denies quashal, it may minimize the privacy intrusion by ordering sensitive information disclosed under a protective order that restricts access to attorneys’ eyes only, preventing exposure to the defendant and others. Such orders are enforceable through civil and criminal contempt judgments as well as bar disciplinary proceedings.

Evidence rules also regulate defense investigations. Exclusionary rules of evidence limit defense subpoena power because, as explained supra, criminal subpoenas may seek only admissible evidence. As with subpoenas, privacy interests do not generally defeat a litigant’s right to introduce relevant evidence.

89 Pennsylvania v. Ritchie, 480 U.S. at 43.
91 418 U.S. at 700.
92 Nixon, 418 U.S. at 699-700 (citing United States v. Iozia, 13 F.R.D. 335, 338 (S.D.N.Y. 1952)).
95 See Wright & Miller; Trump v. Vance, No. 19-3204 (2d Cir., Nov. 4, 2019) (Mazars tax returns).
97 See, e.g., Facebook, Inc. v. Superior Court, 4 Cal. 5th 1245, 1290 (2018).
100 See, e.g., Trump v. Vance, No. 19-3204 (2d Cir., Nov. 4, 2019) (Mazars tax returns).
However, like subpoena rules, evidence rules contain safeguards against excessive privacy intrusions. An initial layer of privacy protection comes from trial judges’ discretion to limit the introduction of evidence on collateral issues, and to restrict the scope of witness examination and cross-examination. The Federal Rules of Evidence reaffirm judges’ inherent authority to control their courtrooms, and instruct courts to wield that authority both to make “procedures effective for determining the truth,” and to “protect witnesses from harassment or undue embarrassment.” That assessment necessarily involves an ad hoc balancing of competing interests according to the “particular circumstances” of a case. Like the privacy safeguards in subpoena rules, this initial layer of privacy protection in evidence law applies to all types of private information, regardless of subject matter, communicants, or medium; incorporates substantial judicial discretion; and applies symmetrically to prosecutors and defendants.

Perhaps no scenario presents more difficult tensions between defense investigations and nonparty privacy than when defendants subpoena third parties for sensitive information about victims. As the advisory committee notes to the federal rules of criminal procedure appropriately emphasize, “victims have a right to respect for their ‘dignity and privacy.’” Accordingly, the subpoena rules impose special notice requirements to protect victim privacy in this scenario. The rules do not generally require defense counsel subpoenaing third parties to notify the subjects of their investigations, so the subject’s opportunity to move to quash may depend on the third party providing notice voluntarily or by contractual or fiduciary duty (or on a privacy law that separately compels notice). The exception is that before defendants may subpoena a third party for “personal or confidential information about a victim,” such as “medical or school records,” the court must give “notice to the victim so that the victim can move to quash.”

Yet even in this especially difficult scenario of defense investigations that implicate victim privacy, subpoena rules include a safety valve judicial override option. In “exceptional circumstances,” a judge may override the requirement to notify a victim, and may do so on an ex parte basis. Non-exhaustive examples

of such “exceptional circumstances” include situations where providing notice could put evidence at risk of being “lost or destroyed,” or “where the defense would be unfairly prejudiced by premature disclosure of a sensitive defense strategy.”\footnote{Fed. R. Crim. P 17(c)(3) Adv. Comm. Note. See, e.g., Defendant Arturo Lopez’s Unopposed Motion to Compel Compliance with Subpoena Duces Tecum for Sprint/Nextel at n.1, United States v. Lopez, No. H-05-446 (S.D. Tex. Apr. 25, 2006), 2006 WL 5002747.} That safety valve injects critical nuance into the privacy safeguards that would otherwise strip judges of discretion to fashion appropriate orders in extreme circumstances.

In sum, subpoena and evidence rules have built-in privacy safeguards in the form of mandatory judicial oversight, high threshold burdens, broad judicial discretion to quash, and, for particularly sensitive information, notice. Apart from special notice requirements specifically for investigations into victims, these safeguards are general and expansive. They apply to all types of private information, regardless of its particular subject matter, regardless of to whom it was communicated, and regardless of the medium in which it is stored. The safeguards are also characterized by substantial judicial discretion. Even the categorical notice requirement for victims includes a safety valve exception for judicial overrides. Finally, while this Subpart has focused on defense investigations, the privacy safeguards in subpoena rules apply symmetrically to subpoenas served by either prosecutors or defendants.\footnote{Christopher Slobogin has pointed out that grand jury and administrative subpoenas, which are available solely to government investigators, are “extremely easy to enforce.” Slobogin, Subpoenas and Privacy, at 806. Different standards apply to prosecutors’ post-indictment subpoenas, which are subject to the same requirements as defense subpoenas. See Fed. R. Crim. P. 17. Most federal circuits apply the Nixon safeguards for pretrial subpoenas to both the prosecution and defense. https://www.lexology.com/library/detail.aspx?g=71c862a2-4bc0-4eba-80b6-a47d96659803.}

2. Privileges

Beyond the broad, content-neutral, and highly discretionary privacy safeguards built into the subpoena and evidence rules, evidentiary privileges create narrow, content-specific, and extraordinarily strong privacy protections. Privileges are exclusionary rules of evidence that shield information from truth-seeking in adjudication, not because it lacks relevance\footnote{Cf. FRE 402 (excluding irrelevant evidence).} or reliability,\footnote{Cf. FRE 803 (hearsay exclusions).} but in order to serve social policies that are extrinsic to the truth-seeking process, including privacy.\footnote{See, Imwinkelried, Alienability of Privileges 508.} Privileges have vast procedural scope and power. Whereas most evidence rules apply solely to trial, privileges apply to every stage of a case, from
grand jury investigations to pre-trial discovery and subpoenas,\(^{116}\) to trial and post-conviction proceedings.\(^{117}\) Any individual who holds a privilege, even non-parties, can intervene to assert it at any time.\(^{118}\) Privileges even defeat warrants; privileged communications are protected even after they are lawfully seized by the government, such as in an authorized wiretap\(^{119}\) or warranted search of an electronic device.\(^{120}\) Privileges thus block not merely the admissibility of relevant evidence in court, but also litigants’ mere knowledge that the evidence exists.\(^{121}\) They even bind judges determining preliminary questions concerning the admissibility of other evidence.\(^{122}\)

Put differently, privilege protections for privacy are more powerful than any from contract, fiduciary duty, or tort liability; they are more powerful than the Fourth Amendment. Indeed, the mainstream position in privilege law, advanced by Wigmore\(^ {123}\) and repeatedly endorsed by the Supreme Court,\(^ {124}\) lower courts, and prominent judges and commentators,\(^ {125}\) is that the longstanding common law privileges, such as the attorney-client privilege, offer absolute protection that cannot be overcome by any showing of need for the information.\(^ {126}\) Edward Imwinkelried has challenged that paradigm both descriptively and normatively, arguing that criminal defendants’ Sixth Amendment rights\(^ {127}\) do and should qualify even purportedly absolute privileges when defendants show sufficient need for

---

\(^{116}\) See FRCP 17; *Bowman Dairy*, *Iozia*. See also, Imwinkelried, *Blurring Confidentiality versus Privacy* *7*.

\(^{117}\) FRE 1101. Privileges also shield information from distribution to foreign tribunals. 28 USC 1782.


\(^{119}\) 18 USC 2517(4).

\(^{120}\) See, *Eric D. MacArthur*, *The Search and Seizure of Privileged Attorney-Client Communications*, *U. Chi. L. Rev.* __, 740-44 (comment). To be sure, some scholars believe that privileges are not absolute, and can always be defeated with a sufficient showing of necessity. See Imwinkelried, *Questioning Wigmorean Absolutism*, at *162-67. See *Nixon*, 418 U.S. at 713-14.


\(^{122}\) FRE 104(a).

\(^{123}\) Wigmore


\(^{126}\) Imwinkelried, *Questioning Wigmorean Absolutism*, at *147-48. See also Imwinkelried, *Dangerous Trend*, at *8*.

\(^{127}\) Imwinkelried, *Questioning Wigmorean Absolutism*, at *162-67.*
privileged information.\textsuperscript{128} And more recent statutory privileges do not enjoy the same status; some contain express qualifications, such as balancing tests to weigh the interests of the privilege holder against the party seeking to access information,\textsuperscript{129} or exceptions if application of the privilege would “conceal a fraud, work an injustice, or deprive the People or the defendant of a fair trial.”\textsuperscript{130} Regardless of whether privileges are absolute or qualified,\textsuperscript{131} they mark a clear legal zenith of privacy protection in evidence law. And, once again, privileges are symmetrical, barring evidence from the government and defendants alike.\textsuperscript{132}

Evidentiary privileges’ remarkable timing and strength impose well-recognized costs.\textsuperscript{133} In Geoffrey Hazard, Jr.’s compelling description, recognizing a “privilege will express a value choice between protection of privacy and discovery of truth and the choice of either involves the acceptance of an evil — betrayal of confidence or suppression of truth.”\textsuperscript{134} The Supreme Court has repeatedly recognized that “privileges impede the search for the truth,”\textsuperscript{135} and mandated that “these exceptions to the demand for every man’s evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth.”\textsuperscript{136} At least in individual cases, privileges are anti-accuracy, anti-transparency, and often harmful to individual litigants.\textsuperscript{137} Both lawyers and priests, for instance, have maintained the secrecy of privileged communications for decades, despite knowing that confidential information in their possession could exonerate wrongfully convicted, innocent people serving lengthy or life sentences or even facing execution.\textsuperscript{138} Parties denied access to privileged evidence may be ignorant of its existence and lack sufficient information to even attempt proof by alternate means.

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{128} See also, Peter Westen, The Compulsory Process Clause, 73 Mich. L. Rev. 71, 161 (1974).
\item \textsuperscript{129} Bridgestone v. Firestone (trade secret privilege).
\item \textsuperscript{130} Cal Evid. Code § 1062(a) (trade secret privilege). Other legislated exclusionary rules expressly — though redundantly — exempt “evidence whose exclusion would violate the defendant’s constitutional rights.” FRE 412(b)(1)(C).
\item \textsuperscript{132} See Scallen, Relational and Informational Privileges, at 567.
\item \textsuperscript{133} See, Melanie B. Leslie, The Costs of Confidentiality and the Purpose of Privilege, 2000 Wis. L. Rev. 31 (2000).
\item \textsuperscript{134} Geoffrey C. Hazard, Jr., An Historical Perspective on the Attorney-Client Privilege, 66 Cal. L. Rev. 1061, 1085 (1978).
\item \textsuperscript{135} Pierce County v. Guillen, 537 U.S. 129, 144 (2003).
\item \textsuperscript{136} United States v. Nixon, 418 U.S. 683, 710 (1974).
\item \textsuperscript{137} See, Stein, Implications for Evidence Theory, \textemdash, n.47.
\end{enumerate}
\end{footnotesize}
Two key limits bound the timing, power, and cost of privileges. First, most privileges are content specific, meaning they apply solely to certain, carefully conscribed categories of information. Some such categories are topical, as in the trade secrets privilege.139 The majority are relational; they shield communications between parties in certain special relationships. For instance, the spousal communications privilege covers confidential communications “made in reliance upon the marital relationship.”140 Other privileges mix topical and relational limits, such as the attorney-client privilege for communications “made for the purpose of obtaining legal advice or services.”141

Second, most privileges are symmetrical; they impose facially parallel constraints on prosecutors and defendants. The attorney-client privilege could block the government’s access to a defendants’ communications with his or her counsel, or block a defendant’s access to the communications of a cooperating government witness. The spousal privilege could block the government from compelling a defendant’s spouse to testify as to the defendant’s guilt, or block a defendant from compelling a third party’s spouse to testify that the third party committed the crime. Nonparties may assert Fifth Amendment privileges to block subpoenas by either the government or criminal defendants. Even the controversial general federal privilege against disclosure in state criminal proceedings would, presumably, block both subpoenas from state prosecutors and subpoenas from state criminal defendants.142

Wigmore’s classic test for justifiable privileges requires that privileged information must have originated in a confidence; that confidentiality must be essential to the relationship in which the information was communicated; that the relationship must be one that society ought to foster; and that the harm to the relationship from compelled disclosure in court would exceed the benefit to the case.143 This remains the primary test that state and federal courts rely on to determine the appropriate limits of privilege recognition, and the test is also cited in the Advisory Committee notes for the Federal Rules of Evidence.144 Nothing in Wigmore’s criteria discriminates based on the identity of the party seeking information.

3. Symmetrical Privacy Statutes

Not all privacy laws contain privacy asymmetries. This Subpart describes that are facially symmetrical, or neutral as to the identity of the seeking party. These statutes provide alternate models for safeguarding privacy in investigations, and suggest that inadvertent privacy asymmetries in other statutes may be

139 See, Paul F. Rothstein, Federal Testimonial Privileges § 9:1 (2d ed.).
140 See, Paul F. Rothstein, Federal Testimonial Privileges § 4:12 (2d ed.).
141 Paul F. Rothstein, Federal Testimonial Privileges § 2:10 (2d ed.).
142 Cf., The Right to Inter-Sovereign Disclosure in Criminal Cases, at 1437-40.
143 Wigmore § 2285, 527-28.
144 Imwinkelried, at § 3.2.3.
irrational and unnecessary. [TBD – Privacy statutes that grant symmetrical access include those for call detail records, cable records, medical and psychiatric records, and substance abuse records. The original 1934 federal wiretap law created a symmetrical absolute bar on wiretapping by either law enforcement or private persons.]

C. Sporadic Precedent Disfavoring Rules that Asymmetrically Disadvantage Defense Investigations

1. Against-Penal-Interest Hearsay

Other evidentiary exclusionary rules beyond privilege also have doctrinal and rulemaking precedent that expressly seeks to promote symmetrical treatment of government and defense evidence. The evolution of FRE 804(b)(3) demonstrates this value.145 FRE 804(b)(3) creates an exception to admit hearsay statements that are against the declarant’s penal interest.146 Defendants rely on the exception to introduce nonparties’ self-incriminating statements that inculpate the declarant to the exclusion of the defendant.147 Prosecutors rely on the same exception to introduce nonparties’ self-incriminating statements that inculpate the declarant along with the defendant.148 Both types of hearsay present risks of unreliability. On the one hand, friends or family of the defendant might fabricate a self-inculpating statement that shifts blame away from the defendant if, for instance, they are already serving a long sentence so have little to lose,149 or otherwise faced a low risk of prosecution.150 On the other hand, an accomplice’s confession might cast false aspersions on the defendant in order to make him or herself appear less blameworthy in comparison.151 Yet, when first enacted, FRE 804(b)(3) required that against-penal-interest statements had to be accompanied by corroborating evidence if proffered by the defense, but not if proffered by the government.152

As Peter Tague describes in a detailed examination of the initial enactment of the rule,153 the drafters “did not detect the disparity” between the rule’s

145 Thank you to Ed Imwinkelried for pointing me to FRE 804(3)(b)’s original asymmetry, and to Peter Tague’s, Daniel Capra’s, and Liesa Richter’s work on this issue.
146 FRE 804(b)(3)(B).
147 Capra, Amending the Hearsay Exception, at 2424-25.
148 Capra, Amending the Hearsay Exception, at 2424-25.
149 Tague, Perils, at 869.
150 See, Deborah Jones Merritt, Social Media, the Sixth Amendment, and Restyling: Recent Developments in the Federal Law of Evidence, 28 Touro L. Rev. 27, 37 (2012).
152 See, Capra & Richter, Poetry in Motion, at n.170.
treatment of defense and prosecution evidence. Daniel Capra, Reporter to the Advisor Committee, and Liesa Richter, an advisor to the Committee, later recalled that “[t]here was no rational reason for this evidentiary disparity. It arose as a result of a misconception in Congress and a miscommunication with the original Advisory Committee.” According to Tague, the Advisory Committee, the Department of Justice, and Congress engaged in protracted debate over whether courts should condition defendants’ ability to admit against-penal-interest hearsay statements on corroborating evidence. Initial debate over the defense-only corroboration requirement was based in part on ignorance of the concerns motivating prior drafting changes. Subsequent inquiry into the asymmetry was abandoned based on an erroneous assumption that then-controlling Confrontation Clause jurisprudence would necessarily bar the government from admitting any against-penal-interest hearsay statements at all. Neither Congress nor the Advisory or Standing Committees gave any “reason for imposing the corroboration requirement solely on the defendant.”

Despite FRE 804(b)(3)’s silence on the issue, at least seven federal circuits read in a parallel corroboration burden on government-proffered penal interest statements. The Fifth Circuit reasoned that, “by transplanting the language governing exculpatory statements onto the analysis for admitting inculpatory hearsay, a unitary standard is derived which offers the most workable basis for applying Rule 804(b)(3).” The Supreme Court considered (though declined to resolve) whether imposing a corroboration requirement on the defense necessitated imposing a parallel requirement on the government. Capra and Richter explain that, “[i]n light of the blatant double standard, many courts had refused to tolerate the inexplicable comparative disadvantage to the criminal defendant. These courts required the government to establish corroborating circumstances as well, even though the plain language of the Rule did not.” Deborah Merritt has characterized these courts’ opinions as “finding the one-way corroboration

156 Tague, Perils, at 866-878.
157 Tague, Perils, at 886-87.
159 Tague, Perils, at 990 & n.717.
160 See United States v. Shukri, 207 F.3d 412, 416 (7th Cir. 2000); United States v. Barone, 114 F.3d 1284, 1300 & n.10 (1st Cir. 1997); United States v. Garcia, 897 F.2d 1413, 1420 (7th Cir. 1990).
161 United States v. Alvarez, 584 F.2d 694, 701 (5th Cir. 1978).
163 Capra & Richter, Poetry in Motion, at 1911.
requirement unfair, inconsistent with other rules, and possibly unconstitutional.”

Reacting to these doctrinal interpretations of the rule, the Advisory Committee began proposing a series of amendments to extend the corroboration requirement to the government with the express purpose of advancing symmetry. According to Capra, “the primary stated purpose of [a 2001] proposal was to provide for symmetry and fairness in criminal cases.” The Department of Justice initially objected, not to the goal of symmetry but to the method of achieving it, arguing that the government already faced other admissibility burdens not matched by the defense, so extending the corroboration requirement would disadvantage the government and create an asymmetry in the other direction. In 2002, the Advisory Committee proposed an amendment that, according to Capra, was again “intended to provide symmetry and unitary treatment,” but that responded to DOJ concerns by applying slightly different language to the government to mirror the requirements already imposed by the Confrontation Clause jurisprudence of the time. However, between 2004 and 2007, the Court eliminated those Confrontation Clause requirements. As a result, circa 2005, the Advisory Committee began considering a “return to the original, symmetry-based proposal that would have extended the ‘corroborating circumstances’ requirement” to the government. Once the constitutional doctrine settled in 2007, removing the Confrontation Clause concerns, the Committee again expressed symmetry-based as well as reliability-based considerations for amending the penal interest exception. This time, DOJ supported extending the corroboration requirement to the government. In 2010, the rule was finally amended to make the corroboration requirement expressly symmetrical in criminal cases. The Advisory Committee note explains, “[a] unitary approach to declarations against penal interest assures both the prosecution and the accused that the Rule will not be abused and that only reliable hearsay statements will be

164 Merritt, Social Media, at 38.
165 Capra, Amending, at 2429.
167 Capra, Amending, at 2428-31.
168 Capra, Amending, at 2433-39. See also, Ohio v. Roberts at 66.
170 Capra, Amending the Hearsay Exception, at 2446-47.
172 Comm. Minute Notes April at 22-23.
175 FRE 804(b)(3)(B).
admitted under the exception.”176 In Capra and Richter’s words, “the 2010 amendment to Rule 804(b)(3) . . . leveled the playing field[].”177

2. Right to Present a Defense

Two key right-to-present-a-defense cases concern asymmetrical exclusions of defense versus prosecution evidence. Washington v. Texas178 struck down a Texas rule permitting codefendants to testify for the prosecution but not for the defense.179 The rule was an asymmetrical variation on common law rules of evidence that had disqualified “interested” witnesses — including parties in civil and criminal matters and codefendants indicted together — in order to reduce temptations to perjury.180 Texas similarly sought to justify its rule as reducing perjury, but the Court found no “rational”181 basis to conclude that codefendants were more likely to perjure themselves when testifying for the defense than for the prosecution, and thus concluded that the rule was unconstitutionally “arbitrary.”182 Writing in concurrence, Justice Harlan emphasized that Texas had failed to justify its “discrimination between the prosecution and the defense in the ability to call the same person as a witness.”183 And in 2006, the Court reaffirmed Washington’s reasoning; Holmes v. South Carolina184 restated the Washington Court’s finding that the asymmetrical rule against defense testimony from convicted codefendants did not “‘rationally set[]’ apart a group of persons who are particularly likely to commit perjury’ since the rule allowed an alleged participant to testify if he or she . . . was called by the prosecution.”185 Holmes in turn struck down a rule that conditioned a defendant’s ability to admit evidence of third party guilt on an evaluation of the strength or weakness of the prosecution’s forensic evidence.186 The Court explained that evaluating the strength of one party’s evidence in a vacuum gave no logical insight into the strength of the other party’s counterevidence.187

Prior commentators188 have drawn on these cases to posit that asymmetrical treatment of prosecution and defense evidence might be unconstitutional, at least

177. Capra & Richter, Poetry in Motion, at 1911.
180. Id. at 19–21.
181. Id. at 22.
182. Id. at 22.
183. Id. at 24 (Harlan, J., concurring).
186. 547 U.S. at 321.
188. 96 Geo. L.J. 273.
where it disadvantages defendants. Writing in 1981, Tague argued that the initial asymmetrical “corroboration requirement of rule 804(b)(3) [was] unconstitutional because it impose[d] a higher burden on the defendant.” 189 Tague floated an equal protection challenge to this asymmetry based on Washington v. Texas, 190 and proposed that courts should both impose a corroboration requirement on the government and also admit defense evidence of “a related statement” in a multi-defendant case. 191 He concluded that “such a judicial interpretation of the rule probably is justified” based on the oversight and misunderstanding that characterized its legislative history. 192 And Amar has advanced a theory that asymmetrical privacy-based privileges are unconstitutional violations of the “compulsion parity” principle, at least where they disadvantage defendants. 193 More recently, Martin Hewett proposed a broad nondiscrimination reading of both Washington v. Texas and Holmes v. South Carolina to suggest that asymmetrical treatment of government versus defense evidence indicates unconstitutional arbitrariness. 194 Put differently, Holmes reinforces Washington’s finding of irrationality based on asymmetry, and treats that finding of irrationality as unconstitutional arbitrariness.

II. Privacy Asymmetries

A diverse set of federal and state privacy statutes protect special categories of sensitive information, such as mental health records, financial documents, and police disciplinary records. These laws sometimes limit disclosures of sensitive information in criminal investigations. And, as this Part identifies, many facially discriminate between law enforcement and defense investigations.

Privacy asymmetries layer on top of the baseline subpoena and evidence rules that are themselves designed to balance nonparty privacy with the truth-seeking interests served by criminal defense investigations. At times, privacy laws duplicate protections already built into this subpoena-evidence balancing regime. For instance, both the Stored Communications Act (“SCA”) and privilege law bars defendants from subpoenaing service providers for a nonparty’s attorney-client communications. 195 At other times, privacy laws alter the default subpoena-evidence balancing regime, such as when a defendant subpoenas a service provider for a victim’s “personal or confidential” communications; federal

---

189 Tague, Perils, at 995.
190 Tague, Perils, at 989, 992, 996.
191 Tague, Perils, at 996.
192 Tague, Perils, at 996-97.
rules permit such subpoenas with certain safeguards, whereas the SCA content-disclosure bar precludes them altogether.

Privacy asymmetries come in two types. “Access asymmetries” block defendants’ access to certain information, or to the sole available source for the information, while permitting access to law enforcement. “Notice asymmetries” require defendants, but not law enforcement, to notify the subject of an investigation before subpoenining information about that individual from a third party. Notice asymmetries sometimes create access asymmetries, as when notifying the subject of an investigation would risk threats to life or physical safety, so requiring notice effectively precludes access altogether. And access asymmetries sometimes create notice asymmetries, as when the sole means for confidential access is barred.

A. Asymmetries Disadvantaging Defendants

This Subpart presents examples of privacy statutes with facial asymmetries that afford law enforcement more or better access to sensitive information than they afford defense investigators. As with the SCA, the legislative histories as well as the statutory texts of most of these laws expressly carve out law enforcement investigations but are silent as to defense investigations. Erin Murphy has documented that police consistently gain exceptions to privacy laws to enable law enforcement to access to sensitive information about poor, minority, and heavily policed communities, while sensitive information about more advantaged communities remains relatively protected from law enforcement scrutiny. This Part seeks to build on Murphy’s work by identifying a related phenomenon whereby criminal defendants predictably fail to obtain parallel exceptions.

1. The Stored Communications Act

The SCA restricts when Internet communications service providers, such as Facebook and Twitter, can disclose the contents of their users’ private communications. The statute’s restrictions except various types of disclosures, including for certain business purposes, those made with the “lawful consent” of one of the intended participants of a communication, and disclosures compelled by

---

196 Fed. R. Crim. P. 17(c).
197 Erin Murphy, The Politics of Privacy in the Criminal Justice System, at 535.
198 It is hardly surprising to observe that the legislative process can overlook the interests of disadvantaged groups, including criminal defendants. See, e.g., Khiara M. Bridges, The Poverty of Privacy Rights 10, 14 (2017); John Hart Ely, Democracy and Distrust 135 (1980). But see, Natasha Duarte, Congress is Writing a Privacy Law: It Must Address Civil Rights, CDT Blog, May 7, 2019.
199 18 USC § 2702(a).
200 18 USC 2702(a)(4)-(5).
201 18 USC 2702(a)(3).
law enforcement. The statute also authorizes law enforcement to indefinitely delay a default requirement to notify the account holders whose communications are disclosed, and to gag service providers from giving such notice voluntarily. Specifically, law enforcement may repeatedly delay notice and obtain gag orders if a “supervisory” government official repeatedly certifies that “there is reason to believe” notice “may” risk “endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.”

In contrast, the SCA contains no express authorization for criminal defendants to subpoena the same service providers for the same information. Like the statutory text, the SCA’s legislative history is silent as to defense investigations, suggesting the asymmetrical treatment of law enforcement and defendants was unintentional, or at least unreasoned.

Major technology companies have adopted a strictly literal reading of the SCA statutory text and concluded that federal law bars them from complying with criminal defendants’ otherwise valid subpoenas for the contents of communications. This interpretation is often credited to *O’Grady v. Superior Court*, a 2006 California appellate case in which Apple sought to subpoena an email service provider for a journalist’s communications with an anonymous source who had allegedly leaked Apple’s trade secrets. Apple argued that the court should read an implicit exception for civil subpoenas into the statute because nothing in the legislative history of the SCA supports the conclusion that Congress intended to preempt civil subpoena power. The court disagreed, holding instead that “there is no pertinent ambiguity in the language of the statute. It clearly prohibits any disclosure of stored email other than as authorized by enumerated exceptions.” The court reasoned that the silence of the legislative history “suggests an intent to protect the privacy of stored electronic communications except where legitimate law enforcement needs justify its

---

202 18 U.S.C. 2702(a)(2), 2703(b)(1)(B)(i)-(ii), 2703(d). On its face, the plain text of the law permits law enforcement to use court orders to compel the disclosure of these communication contents, although the Fourth Amendment likely also requires a warrant. See, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
204 18 USC § 2705(b)(1)-(5).
205 18 U.S.C. § 2705(a)(1)-(2); § 2705(b).
207 See Zwillinger.
209 139 Cal. App. 4th 1423.
210 *O’Grady*, 139 Cal. App. 4th at 1433.
211 *O’Grady*, 139 Cal. App. 4th at 1443.
infringement.”

To date, every appellate court to have considered this issue, both state and federal, has agreed with O’Grady. Further, courts across the nation have extended O’Grady’s reading of the statutory text to bar not merely private civil litigants’ but also criminal defendants’ subpoenas, at least pretrial subpoenas. In 2017, for instance, a California appeals court held that interpreting the SCA to bar a criminal defendant’s subpoena to Facebook did not violate due process, despite the fact that similar legal process is “routinely used as a sword by the prosecution and government.” In 2018, the California Supreme Court held that criminal defendants’ pretrial subpoenas are unenforceable under the SCA “with respect to communications . . . configured by the registered user to be restricted.” In 2019, the District of Columbia Court of Appeals reversed a contempt judgment against Facebook for refusing to comply with a criminal defendant’s subpoena, holding that the SCA’s enumerated exceptions “comprehensively address the circumstances in which providers may disclose covered communications [and] . . . do not include complying with criminal defendants’ subpoenas.” The Second Circuit Court of Appeals, the Oregon State Supreme Court, the Tennessee Court of Criminal Appeals, and federal district courts in the Western District of New York, and the Eastern District of Virginia, have all ruled similarly. Meanwhile, technology companies have maintained an uncompromising position in criminal cases, arguing that the statute bars any and all compliance with defense subpoenas for communications contents, even when faced with defendants’ countervailing federal constitutional rights.

Note that the content-disclosure bar is not the only SCA asymmetry. For non-content information (other than basic subscriber records), the SCA asymmetrically disadvantages defendants because it authorizes law enforcement to compel disclosures with a 2703(d) order, which requires a less onerous showing than the Rule 17 and Nixon requirements that defense counsel must satisfy to obtain the same information using a subpoena. Symmetrical construction of the SCA would thus grant defense access to non-content records (other than basic

---

212 O’Grady, 139 Cal. App. 4th at 1444.
213 Add CITES.
215 Facebook v. S.C. (Hunter).
216 Facebook, Inc. v. Wint, 199 A.3d 625, 628 (D.C. 2019).
217 United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015).
subscriber information\(^{223}\)) on a 2703(d) showing. The SCA also contains a largely theoretical asymmetry disadvantaging law enforcement; it technically authorizes service providers to voluntarily disclose non-content information to defendants but not to law enforcement, without any legal process. While service providers are exceedingly unlikely to make such voluntary disclosures in practice, this possibility does create another technical asymmetry.

2. Video Rental Records

The Video Privacy Protection Act (“VPPA”)\(^{224}\) protects privacy in, as the name suggests, records of video rentals. In a similar asymmetry to the SCA, the Act authorizes law enforcement to collect information about an individual’s video rentals,\(^{225}\) albeit with required prior notice to the individual,\(^{226}\) but altogether bars criminal defendants from subpoenaing the same information.\(^{227}\) 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.\(^{228}\) Like the SCA, the VPPA blanket-prohibits video rental service providers, including online video streaming services,\(^{229}\) from disclosing personally identifiable information about their users,\(^{230}\) and then enumerates certain exceptions,\(^{231}\) including disclosures made with the “informed, written consent” of the users.\(^{232}\) One express exception authorizes law enforcement access pursuant to a warrant, grand jury subpoena, or court order supported by probable cause.\(^{233}\) 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.\(^{234}\) But the statutory text is

\(^{223}\) The SCA rule for compelled access to basic subscriber information is already symmetrical; it requires that both law enforcement and defense investigators obtain a subpoena.


\(^{225}\) 18 USC § 2710(b)(2)(C).

\(^{226}\) 18 USC § 2710(b)(3).


\(^{229}\) See, e.g., Motion to Compel Defendant’s Consent to Plaintiff’s Third-Party Subpoenas, 2019 WL 4386148 (M.D. Fla., Jan. 10, 2019) (applying VPPA to iTunes); In re Hulu Privacy Litigation, No. C 11–03764 LB, 2012 WL 3282960, slip op. (N.D. Cal.) (applying VPPA to Hulu).

\(^{230}\) 18 USC 2710(b)(1).

\(^{231}\) 18 USC 2710(b)(2).

\(^{232}\) 18 USC 2710(b)(2)(B).

\(^{233}\) 18 USC 2710(b)(2)(C); 2710(b)(3). See generally, Rebecca E. Harch, 148 Amjur. Trials 305 (Oct. 2019 update).

\(^{234}\) 18 USC 2710(b)(2)(F)(i)-(ii).
silent as to criminal defense subpoenas. Unlike the SCA, the legislative history contains one mention of defense investigations; testimony before the House and Senate Judiciary Committees informed Congress of an instance where a “subpoena served by the attorney of one defendant in a criminal prosecution . . . sought the video records of his client’s co-defendants.” But the legislative history contains no other indication that Congress contemplated defense investigations, whereas there were extensive discussions of law enforcement access.

3. Educational Records

The Family Educational Rights and Privacy Act (“FERPA”) requires educational institutions receiving federal funds to protect the confidentiality of students’ educational records. 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. Records concerning a student’s cognitive, mental, or emotional disabilities, might be relevant to impeach credibility. Records concerning a student’s classroom, classmate, and teacher assignments might be relevant to show acquaintance or relationships.

The Act and related regulations authorize both law enforcement and criminal defendants to access educational records via a general exception for “any lawfully issued subpoena,” while requiring educational institutions to notify students and parents prior to complying with legal process. Yet the FERPA regulations currently permit only law enforcement to circumvent the notice requirement, and to gag educational institution from voluntarily providing notice, without a parallel option for defense investigators. 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. 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

235 See 18 USC 2710(b)(2)((A)-(F).
243 34 CFR 99.31(a)(9)(i)-(ii).
244 34 CFR 99.31(a)(9)(ii)(B).
246 34 CFR 99.31(a)(9).
law enforcement purpose.”247 The legislative and regulatory histories contain no indication that defense investigations were discussed or considered.248

4. Tax Returns

Section 6103 of the Tax Code imposes confidentiality restrictions on IRS disclosures of federal tax returns and return information.249 The Act expressly exempts court-ordered disclosures to “officers and employees of any Federal agency” engaged in criminal investigations.250 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.251 However, Section 6103 is silent as to disclosures pursuant to subpoenas in judicial proceedings other than those pertaining to tax administration, and courts have expressed divergent views on whether this silence precludes IRS compliance with such subpoenas.252

This was not always so. Prior to 1977, Section 6103 contained an express exception permitting disclosures pursuant to “court orders.”253 But the Tax Reform Act of 1976 eliminated that language and replaced it with detailed enumerated exceptions for law enforcement investigations that did not account for defense subpoenas.254

5. Police Disciplinary Records

Some state laws make it harder for defense counsel to access the disciplinary records of police officer witnesses than it is for law enforcement to do the same.255 (Prosecutors can also face obstacles, albeit lesser ones, to accessing police disciplinary records.256) New York’s Civil Rights Law Section 50-a makes

249 See, e.g., Trump v. Mazars; Vance v. Trump.
250 6103(i)(1). See also, 6102(i)(2)–(7).
251 6103(h)(4)(A)–(D).
254 To Do: Further research legislative history of this change.
256 See, Mike Hayes & Kendall Taggart, The District Attorney Says The NYPD Isn’t Telling Prosecutors Which Cops Have A History Of Lying, BUZZFEED NEWS (Jun. 2, 2018),
police disciplinary records by default “confidential and not subject to inspection or review.” It excepts government investigators, but not defense investigators, from this confidentiality shield. Note that the law does not entirely bar defense access; it prevents defendants from acquiring the records via public records requests, but permits disclosures to defendants pursuant to “lawful court order,” so long as a judge first holds a hearing, and conducts in camera review to assess relevance and materiality. The New York Court of Appeals has, however, construed 50-a to impose special heightened ex ante burdens on defense subpoenas, making this avenue for access uniquely difficult and sometimes unattainable.

Particularly significant for purposes of this Article, 50-a was enacted with the express intent to regulate defense investigations, and its legislative history and subsequent judicial evaluations contain substantial discussion of the drafters’ rationales for limiting defense access. As the New York Court of Appeals has explained, 50-a “was designed to limit access to said personnel records by criminal defense counsel, who used the contents of the records, including unsubstantiated and irrelevant complaints against officers, to embarrass officers during cross-examination.” The explicit assertion of a justification for limiting defense access has, in turn, enabled doctrinal, scholarly, and popular democratic debate over the scope and wisdom of that rationale. Judge Weinstein in the Eastern District of New York refused to read 50-a as an evidentiary privilege that could block subpoenas by federal civil rights plaintiffs, explaining that the “sole function of section 50-a is . . . to protect irrelevant materials from disclosure: to prevent fishing expeditions, not to safeguard privacy itself.” More recently, as


259 50-a(1).

260 50-a(2).

261 50-a(3).


privacy rhetoric has gained societal influence, scholars and practitioners have debated attempts to re-characterize 50-a as a privacy law.\textsuperscript{265}

B. Asymmetries Disadvantaging Law Enforcement

1. Financial Records

A variety of overlapping federal laws regulate disclosures of financial records in criminal investigations.\textsuperscript{266} The Right to Financial Privacy Act ("RFPA")\textsuperscript{267} requires that federal law enforcement investigators\textsuperscript{268} seeking customer financial records from a financial services intermediary, such as a bank, must provide the customer with written notice\textsuperscript{269} and an opportunity to object to the disclosure.\textsuperscript{270} Law enforcement may obtain a court order to indefinitely delay notice,\textsuperscript{271} 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.”\textsuperscript{272} The Act imposes no requirements whatsoever on criminal defense subpoenas.\textsuperscript{273}

III. Correcting for Irrational Privacy Asymmetries

On July 26, 2019, a San Francisco Superior Court judge held Facebook and Twitter in contempt for, in the judge’s words, “misusing their immense resources to manipulate the judicial system in a manner that deprives two indigent young men facing life sentences of their constitutional right to defend themselves at


\textsuperscript{266} The Bank Secrecy Act, which is not a privacy law and thus not examined here, offsets 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 USCA 1951-59; 31 USCA 5311-30; https://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html.

\textsuperscript{267} 12 USC 3401-23.

\textsuperscript{268} 12 USC § 3401-03.

\textsuperscript{269} 12 USC §§ 3404(c), 3405(2), 3406(c), 3407(2), 3408(4), 3412(b).


\textsuperscript{271} 12 USC 3409(b)(1)-(2).

\textsuperscript{272} 12 USC 3409(a)(3)(A)-(E); see also, https://epic.org/privacy/rfpa/.

\textsuperscript{273} 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 USC § 3413(i), and subpoenas by federal authorities in a civil, criminal, or administrative disputes in which the government and the customer are parties, see 12 USC § 3413(e)-(f).
trial.”274 One of those young men, Derrick Hunter, was ultimately acquitted. But not before he was forced to undergo trial for a gang-related homicide without potentially crucial evidence to cross-examine a key witness against him.275 Hunter and his co-defendant had subpoenaed Facebook and Twitter for the private messages of a central prosecution witness: the woman arrested driving the getaway car, who had also been threatened with prosecution and had a Fifth Amendment privilege not to produce the messages herself. The judge ordered the companies to comply with the defendants’ trial subpoena,276 ruling that the defendants’ due process and Sixth Amendment rights entitled them to in camera review of the messages,277 that no viable alternative existed for them to obtain the information,278 that production would not be unduly burdensome for Facebook and Twitter,279 and that the companies would be immune from civil liability for complying with the court’s order.280 Yet, even after the appeals court and the California Supreme Court both denied the companies’ motion to stay the order, Facebook and Twitter still refused to disclose the messages.281 The companies explained that they took “a stand” against the court’s order because they believed it violated a federal privacy law from 1986 called the Stored Communications Act (“SCA”).282 As described supra, that law would not have stopped police or prosecutors from obtaining the messages,283 but — in the companies’ view — it bars defense counsel from doing the same.

The fact that many reasonable, privacy-protective limits on criminal investigations apply symmetrically to law enforcement and defense investigations alike, as detailed in Part I, suggests that privacy asymmetries in the SCA and other laws described in Part II may be irrational. Repeat silence as to defense investigations in the legislative histories of asymmetrical privacy laws bolsters this suggestion of irrationality. This Part begins by assessing two plausible policy arguments that might initially appear to justify privacy asymmetries

275 Lee Sullivan was convicted. Derrick Hunter was acquitted. See email to author from Bicca Barlow (Jan. 10, 2020, 1:50 p.m.).
276 Prior litigation in the same case concerned the defendants’ pretrial subpoena.
277 Ma 1 Order, at 40-41.
278 May 1 Order, at 22.
279 May 1 Order, at 41-42.
280 May 1 Order, at 19-20.
281 People v. Sullivan and Hunter, No. 13035657 & 13035658, Order and Judgment of Contempt ¶¶ 1, 6-13 (Cal. Sup. Ct. S.F. Ct’y, July 26, 2019) (Crompton, J.) (“July 26 Order”). To be sure, subpoenas are often ignored absent enforcement actions. See, e.g., Donny O’Sullivan & Paula Newton, Facebook’s Zuckerberg Ignores Subpoena from Canadian Parliament, CNN Business, May 27, 2019. But it is unusual to refuse to comply with a subpoena after being denied a stay by the California Supreme Court.
282 Kashmir Hill, Imagine Being on Trial.
283 See 18 USC 2702(c)(1) & 2703. Compare, Warshak.
disadvantag...ing defendants: disparate legal constraints on overbroad collection, retention, and use of sensitive information by law enforcement versus defense investigators; and disparate risks of abuse from rogue investigators. It concludes that, at least in the absence of strong empirical evidence to the contrary, these policy concerns cannot rationally justify privacy asymmetries.

A. The Policy of Privacy Asymmetries

1. Risks of Overbroad Collection, Retention, and Use

Courts and commentators have long expressed concern over the possibility that law enforcement might over-seize digital data using warrants that fail to adequately comply with the Fourth Amendment’s particularity requirement, indefinitely retain the nonresponsive seized data, and then search it repeatedly for purposes remote from those initially proffered to obtain the warrant. These concerns have evolved in part from practical challenges surrounding the search and seizure of electronic from personal computers, hard drives, and other digital storage devices. Practical limits on law enforcement’s capacity to sift through irrelevant data on devices while conducting physical searches in often dangerous locations initially motivated the creation of a “two-step” search process, which authorizes law enforcement to seize entire hard drives, and then search the devices for responsive data at a later time in a safe location. This ex ante relaxation of the Fourth Amendment’s particularity requirement in turn created uncertainty over the scope and propriety of courts imposing remedial ex post use restrictions on seized data, such as requiring predetermined search terms or imposing time limits on retention.\(^{284}\) While the practical limits that initially motivated this two-step search process do not apply to the collection of cloud data from Internet service providers, many courts have nonetheless uncritically extended a relaxed Fourth Amendment particularity requirement to cloud accounts, authorizing controversial, broad warrants to seize entire social media accounts from inception to the present, often without any ex post minimization requirements.

This backdrop of concern about law enforcement’s over-seizure of digital data could provoke analogous anxiety over defense investigators engaging in overbroad collection, retention, and use of digital data. But, while such concerns may at first appear superficially compelling, a deeper examination of the issue shows that such concerns cannot justify asymmetrical treatment disadvantaging defendants. This is because the legal constraints on defendants’ subpoena power are already more robust than those the Fourth Amendment imposes on law enforcement.

To start, warrants are far broader than criminal subpoenas. Whereas warrants reach any information that is likely related to a crime,\(^ {285}\) pretrial criminal subpoenas reach solely *admissible* evidence. That means warrants permit seizures

\(^{284}\) See Gancias; Stephen Henderson, *Fourth Amendment Time Machines* (considering ex post constraints on bulk government capture).

\(^{285}\) See Kiel Brennan-Marquez, *Plausible Cause*. 
of hearsay materials and information protected by rape shield laws; subpoenas do not. And enforcing a subpoena against countervailing privacy interests generally requires showing “necessity,” well beyond any constraint on ex parte warrants, which do not even enable pre-disclosure adversarial process. Warrants have a “particularity” requirement; subpoenas have a “specificity” requirement. Warrant execution traditionally entails intrusions that risk exposure of irrelevant private material. Subpoenas protect against such risks by requiring the party served to locate and produce responsive records.

Next, ex post minimization requirements are more readily available for subpoenas than for warrants. While the propriety of courts imposing post-collection retention and use restrictions on Fourth Amendment seizures of electronic data remains doctrinally unsettled, judges routinely issue protective orders to limit defense counsel’s retention and use of sensitive information returned on a subpoena. Some protective orders restrict information to “attorney’s eyes only,” preventing counsel from divulging the information to anyone, even their client. Protective orders can authorize data to be used solely for purposes of representing one client in one matter, and require counsel to return or destroy data after that purpose has expired.

In sum, then, the risk of overbroad collection, retention, and use of sensitive data cannot rationally justify privacy asymmetries that disadvantage defendants because existing legal safeguards against this conduct are already more robust for defense subpoenas than for law enforcement searches and seizures.

2. Risks of Abuse

Of course, legal constraints on the proper scope of data collection, retention, and use do not obviate the risk of rogue investigators abusing their compulsory process powers. But merely identifying that a risk of abuse exists cannot rationally justify asymmetrical treatment of law enforcement and defense investigations because compulsory process entails risks of abuse whether exercised by law enforcement or defense counsel.

Victims’ rights advocates have emphasized the risk of excessive invasions of privacy from both law enforcement and defense counsel. In a particularly egregious example of the former, a rape victim alleged that a sheriff called a press conference and publicly released “highly personal and extremely humiliating details” about her rape in order to retaliate against her for criticizing his failure to investigate the crime. NCVLI observes that, “[i]n nearly ever 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. For example, the parties may seek the victim’s diary, Facebook account information,

287 Bloch v. Ribar, 156 F.3d 673, 676, 687 (6th Cir. 1998).
Privacy Asymmetries

Accordingly, NCVLI has 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.”

Similarly, the Crime Victim Rights Act of 2008 modified the federal rules of criminal procedure to require notice to victims when either prosecutors or defendants subpoena third parties for “personal or confidential information” about victims.

A recent case illustrates the risk of abuse in law enforcement investigations of digital data. After a juvenile defendant who participated in the killing of a police officer negotiated a plea deal that allowed him to avoid transfer to adult court, the sergeant who had investigated the homicide opened investigations into the defendant’s two lawyers, members of the defendant’s family, and a Hollywood producer who taught the defendant creative writing in Juvenile Hall and had advocated on his behalf. The sergeant obtained delayed-notice warrants for the targets’ cloud accounts, authorizing him to seize for instance, “all records associated with” the Hollywood producer’s google account, including “calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations . . . all user created documents stored by Google . . . [the message content or body of] all email messages . . . whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder . . . all images, graphic files, video files, and other media files . . . all location data,” and more, from the “inception of the account to the date th[e] warrant [wa]s signed.”

Defense counsel and the producer have alleged that the sergeant used fraudulent affidavits to obtain these warrants “for the sole purpose of intimidating and silencing” them.

There is also legitimate concern that rogue defense counsel might serve subpoenas with a bad faith intent to harass, intimidate, threaten, or silence victims

---

292 Budnick, Notice of Motion at *3 (on file with author).
293 See Alene Tchekmedyian, ‘Hangover’ Producer Helped a Teen Convicted in Killing: Now he’s Under Investigation, LA Times (Dec. 15, 2019).
294 Budnick, In re Application to Unseal, Ex. A (on file with author).
295 Budnick, In re Application to Unseal, Ex. A (on file with author).
296 Budnick, In re Application to Unseal, Notice of Motion at *3 (Nov. 22, 2019) (on file with author).
and other potential witnesses, rather than to obtain legitimate relevant evidence for their client’s defense. Commentators have explained, for instance, that defense counsel may seek access to victim’s psychotherapy records in order to “use the fact that a victim has received counseling to take advantage of the myth that women who make rape reports are unstable and mentally ill.”

Given that both law enforcement and defense investigations present risks of abuse, it could be rational to asymmetrically disadvantage defendants if the institutional safeguards against such abuse were clearly more robust for law enforcement. But that is not the case. Both prosecutors and defense counsel are officers of the court subject to civil and criminal contempt sanctions and bar disciplinary proceedings. Both serve the public interest in accurate and fair criminal proceedings. Like prosecutors, many defense counsel are public employees. Both operate across the country in institutional structures of widely varying scale, resources, and oversight mechanisms. Indeed, at least one key difference suggests that risks of prosecutorial misconduct may be greater: unlike prosecutors, defense counsel enjoy no immunity from civil liability, either absolute or qualified.

If strong empirical evidence were to show a greater comparative risk of abuse from defense counsel’s exercise of compulsory process than from law enforcement’s exercise of the same, that difference might justify asymmetrical treatment in privacy laws. Without such evidence, however, merely identifying that risks of abuse exist cannot justify privacy asymmetries.

3. Case Study: The Stored Communications Act

That neither the risk of overbroad collection nor the risk of abuse can justify privacy asymmetries, at least without strong empirical evidence to the contrary, undermines any attempt to rationalize the SCA’s block on defense subpoenas for stored communications contents. Additional scrutiny undermines the possibility of a rationale further still.

From a privacy-maximizing perspective, the SCA block on defense subpoenas makes little sense. While immunizing technology companies from defense subpoenas may gift those companies a special freedom from the burdens of compliance with legal process, it provides minimal privacy protection because in the


vast majority of cases defendants can still subpoena account holders directly. The account holders may, in turn, either provide “lawful consent”\(^\text{299}\) for service provider disclosure or obtain their own records to produce in response to the subpoena. This means that a rogue defense counsel seeking to harass and intimidate victims, police witnesses, or others, could still subpoena those individuals directly, or subpoena their social media communications from their friends, family members, and associates. Put differently, the SCA does not shield victims, witnesses, or even particular categories of highly sensitive information; it shields technology companies.

To be sure, channeling defense subpoenas to account holders has some privacy benefits because it effectively compels notice to the account holder. (The SCA content-disclosure bar thus creates both an access asymmetry and a notice asymmetry.) While imperfect as a privacy safeguard – notice to account holders neither guarantees notice to other individuals whose communications are revealed in the account\(^\text{300}\) nor enables access to courts – notice facilitates pre-disclosure motions to quash.\(^\text{301}\) The better means for ensuring notice, though, would be to legally require notice. Indeed, many communications service providers already have voluntary, contractual, and perhaps fiduciary obligations,\(^\text{302}\) to notify account holders about service of legal process.\(^\text{303}\) Those obligations could be formalized in law or regulations.\(^\text{304}\)

Legally-required notice would be preferable to the SCA bar on defense subpoenas because there are circumstances in which defendants cannot subpoena users or account holders directly. Such subpoenas are unavailable when, for example, the user refuses consent\(^\text{305}\); is difficult to locate or contact (consider itinerant or homeless users, and incarcerated users with restricted access to computers and limited, potentially very slow, alternate means for communication); has a Fifth Amendment, reporter’s, or other privilege against production\(^\text{306}\); or when notifying the user about the investigation could lead to the destruction of or tampering with evidence, to flight, to witness intimidation, or

\(^{299}\) 18 USC 2702(a)(3).

\(^{300}\) Cf., Title III; Fed. R. Crim. P. 17(c).

\(^{301}\) See Kashmir Hill, (quoting Albert Gidari).

\(^{302}\) See Balkin, Blog Post; Balkin, Information Fiduciaries; Balkin & Zittrain, Atlantic article. But cf. Khan & Pozen.


\(^{304}\) See Deirdre Mulligan, Privacy Smart Grid, at 25 & n.91.


\(^{306}\) See Zwillinger at 592.
to a threat to life or safety. Just like law enforcement investigations, defense investigations can involve dangerous individuals. In one recent case, the SCA barred a homicide defendant’s subpoena for records concerning an individual in witness protection whom the defendant alleged to be the true perpetrator of the homicide. In another, a defendant charged with shooting at an SUV claimed self-defense; an individual associated with the SUV had previously been caught on surveillance video shooting at the defendant, but the SCA barred the defendant from subpoenaing Instagram for messages to show that that individual had allegedly used an Instagram account to harass, threaten, and stalk the defendant for months, keeping him “in constant fear for his life.”

As these cases illustrate, the same circumstances that may sometimes justify law enforcement obtaining records directly from service providers, while indefinitely delaying notice to affected users, can also arise in defense investigations. Yet in these types of circumstances, the SCA expressly recognizes and protects the interests of law enforcement but not defendants. The SCA authorizes law enforcement to indefinitely delay notice to the subject of an investigation if notice would risk “endangering the life or physical safety of an individual; flight from prosecution” or “intimidation of potential witnesses.” And this is so not only due to danger. The SCA also authorizes law enforcement to delay notice if notice would “risk destruction of or tampering with evidence … or unduly delaying a trial.” A recent DOJ memorandum emphasizes that prosecutors may apply to courts for SCA nondisclosure orders if there is “potential for related accounts or data to be destroyed or otherwise made inaccessible to investigators.” Similar circumstances may arise in defense investigations. But construing the SCA to require that defense subpoenas must go directly to account holders effectively mandates notice without a safety valve judicial override. Thus in People v. Touchstone, currently pending before the California Supreme Court, the SCA barred a defense subpoena to Facebook notwithstanding the trial judge’s

---

307 When Acquittal is a Tweet Away, at 2-3.
308 People v. Brian Baldino, No. SCD258141, Defendant’s Opposition to Facebook, Inc.’s Motion to Quash, July 15, 2016 (on file with author).
309 People v. [Redacted], No. 18012547, Subpoena to Facebook, [Check date], 2018 (on file with author); Opp. to Motion to Quash, Nov. 13, 2018, at *1 & n.1, *4-6, *8 (on file with author).
310 Cf. 18 U.S.C. §§ 2705(a)(4); 2705(b).
312 18 U.S.C. § 2705(a)(1)-(2); § 2705(b).
313 18 USC 2705.
315 See, [Redacted] (Instagram case).
finding that “notification may lead to tampering with or destruction of evidence.”

Thus, there are circumstances in which the SCA content-disclosure bar can entirely block criminal defendants’ access to relevant, material, exculpatory evidence. The frequency of these circumstances is difficult to measure, but almost certainly more expansive than case law reveals. Only a small percentage of subpoena denials reach the trial courts, much less appellate review. This is in part because letter traffic and ‘meet and confer’ negotiations over initial denials of defense subpoenas consume time and resources before either party will move to compel or quash. Defendants often take a plea before these negotiations can be resolved. Defense attorneys have reported receiving overbroad default denials from service providers via form letters that improperly cite the SCA content-disclosure bar even when subpoenas seek basic subscriber information, which the SCA unambiguously permits. Difficulty obtaining records can create chilling effects that deter counsel from seeking such subpoenas at all.

Unlike the SCA’s content disclosure bar, legally-required notice would protect privacy while still enabling defendants to subpoena service providers in circumstances when seeking records from account holders would risk destruction or tampering with evidence, or prejudicial delay. And legally-required notice could also be subject to a safety valve judicial override on a case by case basis if the account holder cannot be located or if notice might pose a danger to the defendant or other witnesses. Indeed numerous other privacy laws have precisely those types of judicial overrides — for both law enforcement and defense investigations — for circumstances in which notice would be infeasible or unwise.

In sum, the SCA’s immunization of technology companies from defense subpoenas does little to protect privacy, and the minimal privacy protections that it does afford are both under- and harmfully over-inclusive. It is difficult to conceive of a logically defensible reason to deny defense investigators the more nuanced delayed-notice options that the SCA affords to law enforcement. This is not to say that no conceivable purpose could rationally justify any privacy asymmetry. Perhaps the prosecution’s burden of proof for criminal convictions justifies granting prosecutors more investigative power than defendants. Perhaps the fact that police have duties to further general community safety and prevent

---

317 To be sure, Speedy Trial Rights are the defendant’s alone . . .
318 See Meghan Cassidy, S.F. Chronicle (forthcoming).
319 Hanni Fakhouri telephone interview, Jan. 30, 2019, 7:00 PM.
320 Hanni Fakhouri telephone interview, Jan. 30, 2019, 7:00 PM.
321 See HIPAA; Fed. R. Crim. P. 17(c).
322 For detailed discussion of notice requirements in other privacy laws, see infra, nn____.
323 Cf. Old Chief; but cf. Bruton.
crimes, as well as to collect evidence for trial, could justify bifurcated asymmetrical treatment of pre-indictment law enforcement investigative power, with symmetrical treatment for post-indictment investigations. But the very real risk of legislatures inadvertently proliferating unreasoned, irrational, and harmful privacy asymmetries requires some check.

B. The Limited Avenues for Constitutional Challenge

Because defendants’ positive rights to compel access to evidence do not reach full strength until trial, opportunities for as-applied challenges to privacy asymmetries based on defendants’ strongest positive countervailing constitutional rights are rare. Nonetheless, this Subpart explains the best arguments in support and the limitations of pretrial challenges to privacy asymmetries based on defendants’ constitutional rights to compel access to evidence. It then considers possible facial challenges based on defendants’ negative rights against privacy asymmetries that block defense access to evidence, which would apply consistently at all stages of a case from pre-trial to post-conviction proceedings. Current right-to-present-a-defense doctrine contains some basis for this negative right. While that basis is limited and on a trajectory to become more so, bringing challenges based on the doctrine could nonetheless help to correct irrational privacy asymmetries by forcing the government to justify statutory silence that results in the denial of defense investigative power.

1. Positive Rights to Compel Pretrial Access to Evidence

Any positive constitutional rights that defendants have to compel access to relevant evidence would most likely overcome conflicting statutory privacy safeguards. But at least under current doctrine, those positive rights are thin, especially pretrial. The Court has repeatedly announced that defendants have no general constitutional right to pretrial discovery from the government. It is unclear to what extent if any Confrontation rights apply pretrial. And the Court has rarely weighed in on the scope of Compulsory Process rights, pretrial or otherwise.

Brady is one exception that entitles defendants to pretrial disclosure of exculpatory material evidence in the constructive possession of the prosecution, regardless of legislated privacy safeguards. Hence, in Pennsylvania v. Ritchie, 480 U.S. 39, 52 (1987) (plurality op.).

See e.g., Pennsylvania v. Ritchie, 480 U.S. 39, 52 (1987) (plurality op.).


See Ritchie (plurality op.); People v. Hammond (Cal. XXXX).

the Court required in camera review of a state agency’s records of child abuse investigations, despite statutory confidentiality protections for the records. A plurality of the Court based the holding on due process, suggesting it was required to effect Brady disclosures. And in Association for L.A. Deputy Sheriffs v. Superior Court, the California Supreme Court permitted the L.A. County Sheriff’s Department to inform prosecutors of the names and identifying numbers of police officers who “may” have Brady materials in their personnel files, despite statutory confidentiality protections for the files, in order to enable prosecutors to comply with Brady. But Brady neither requires disclosure of material exculpatory evidence beyond the possession of the prosecution, nor requires disclosures of potential Brady material to defendants to determine what qualifies as material and exculpatory. While the due process principles motivating Brady, which concern government misconduct that suppresses exculpatory evidence, could theoretically extend to statutes that make exculpatory evidence selectively unavailable, this would stretch the doctrine well beyond its current limited application to the prosecution team.

Another exception is the due process requirement that, if lawmakers enact pretrial discovery statutes requiring disclosures from the defense, those statutes must require reciprocal disclosures from the government. Hence, in Wardius v. Oregon, the Court struck down a statute that required defendants to give pretrial notice of an alibi defense while imposing no reciprocal discovery obligations on prosecutors. Wardius also states in dicta that due process regulates “the balance of forces between the accused and his accuser.” That principle could, again theoretically, extend from statutes governing discovery between the parties to statutes governing investigations of nonparties. Briefs and scholarship that rely on Wardius in the context of investigative statutes could, I submit, strengthen existing articulations of their claim by arguing that notice asymmetries effectively compel nonreciprocal disclosures between the parties because they enable law enforcement, but not defendants, to conduct investigations confidentially. But even that strengthened argument offers little. The Court has not revisited or even discussed the Wardius holding in depth since issuing it in 1973, so the doctrine is unlikely to be expanded from discovery to investigations.

329 The plurality opinion left open the possibility that the Compulsory Process Clause would have required the same result, which could extend Ritchie to defendants’ independent investigative powers, including investigations of nonparties.
330 See L.A. Sheriffs.
332 412 U.S. at 475.
333 412 U.S. at 474.
334 See, Colin Fieman & Alan Zarky, Acquittal is a Tweet Away, at 6.
335 SCOTUS has cited the opinion a mere fourteen times.
Privacy Asymmetries

2. Negative Rights Against Arbitrary and Disproportionate Exclusionary Rules

As the prior Subpart showed, given the relative weakness of defendants’ pretrial constitutional rights combined with the rarity of trials, opportunities to challenge privacy asymmetries based on defendants’ positive rights to investigative power are limited. This Subpart considers a plausible alternative basis for constitutional challenges: defendants’ negative rights against arbitrary and disproportionate exclusions of defense evidence.

Cases establishing a constitutional right to present a defense have primarily addressed circumstances in which exclusionary rules of evidence block defendants’ ability at trial to introduce evidence that they already possess, not their ability pretrial to compel access to evidence during investigations. Thus, the positive entitlements that these cases establish apply solely to evidence already in hand. But exclusionary rules of evidence apply broadly to block both admissibility and investigations. This is so for privileges because they expressly apply to all stages of proceedings, from grand jury to pretrial to post-conviction, and because they block everything from subpoenas to warrants to cross-examination. This is also so for other evidentiary exclusionary rules because, at least in current statutory configuration, defendants’ subpoena power applies solely to evidence that is likely to be admissible. As a result, to the extent that right-to-present-a-defense doctrine establishes negative rights against particular types of exclusionary rules, those negative rights should apply to both admissibility and the defense investigative function.

Current doctrine provides some support for recognizing a negative constitutional right against privacy statutes that asymmetrically block disclosures of relevant evidence to the defense. Start with Pennsylvania v. Ritchie, in which the Court enforced a defendant’s pretrial subpoena seeking evidence from state records of a child abuse investigation, despite a statute that made those records confidential. As described supra, the most likely reading of the Ritchie plurality opinion is that it recognizes defendants’ entitlement to Brady disclosures, and perhaps to Compulsory Process disclosures. But Ritchie can also be read as recognizing a negative right against the confidentiality statute at issue in the case. That statute was asymmetrical: it included express exceptions for disclosures to “law-enforcement and judicial personnel,” but not for compliance with defense

337 FRE 1101.
338 Nixon.
340 See supra at __ & n. __.
subpoenas. The Court read in an implicit exception for defense-initiated in camera review, restoring some level of symmetry.

More directly, right-to-present-a-defense case law has expressly articulated a negative constitutional right against certain exclusionary rules of evidence. State and local rule makers have “broad latitude” to exclude relevant defense evidence from criminal trials. Indeed, most rules of evidence do just that: exclude relevant evidence (from both the prosecution and defense) because, for instance, the evidence is unduly prejudicial, cumulative, or privileged. But that “broad latitude” is limited by a constitutional prohibition on “evidence rules that infringe upon a weighty interest of the accused and are arbitrary or disproportionate to the purposes they are designed to serve.”

Earlier generations of this prohibition emphasized the negative right against “arbitrary or disproportionate” rules at least as much as the positive “weighty interest of the accused.” Accordingly, Chambers v. Mississippi struck down a (symmetrical) rule barring parties’ impeachment of their own witnesses where “the State had not even attempted to ‘defend’ or ‘explain [the] underlying rationale’” of the rule. And Rock v. Arkansas struck down a (symmetrical) rule excluding hypnotically refreshed testimony because “restrictions of a defendant’s right to testify may not be arbitrary or disproportionate to the purposes they are designed to serve.” Rock instructed courts to evaluate unconstitutional arbitrariness and disproportionality by assessing “whether the interests served by a rule justify the limitation imposed on the defendant’s constitutional right to testify,” effectively an evenly weighted balancing of the competing interests. Under that balancing test, an exclusionary rule that served de minimis societal interests could presumably fail to justify even a slight limitation on defense testimony.

Over time, however, the doctrine has thinned the definition of unconstitutional arbitrariness and disproportionality. The Court’s most recent formulation in Holmes v. South Carolina defines unconstitutionally “arbitrary” rules as “rules that exclude[] important defense evidence but that do not serve any legitimate interests,” and that also infringe a “weighty interest” of the accused.

---

343 See, FRE 403.
344 See, e.g., Crane v. Kentucky, 476 U.S. at 689-90.
345 CITE examples.
349 Id. at 56.
350 Id. at 325 (emphasis added).
351 Holmes, 547 U.S. at 324, 326.
(Logically, this must mean an interest other than freedom from arbitrary or disproportionate exclusions, without more.) Under *Holmes*, then, even a rule that excludes “important” defense evidence is not arbitrary if it serves any legitimate interest, and even one that does not so serve may yet be constitutional if it infringes less than a “weighty interest.”

In sum, right-to-present-a-defense doctrine would have to revert towards its prior form before it would provide a reliable foundation to strike down privacy asymmetries. But even in its current embodiment, bringing a *Holmes* challenge to privacy asymmetries would force the government to provide “clear evidence” that blocking relevant defense evidence through asymmetrical privacy laws serves some legitimate government interest. This requirement would be distinct from pure rational basis review because the government could likely satisfy the later merely by providing justification for law enforcement exceptions to privacy statutes, without addressing statutory silence as to defense investigations. In addition, defendants could leverage both the asymmetrical treatment of law enforcement versus defense investigations, and the existence of many other functional symmetrical privacy statutes, as evidence of unconstitutional arbitrariness and disproportionality in blocking defense investigations. Finally, even if a relatively sparse explanation from the government would satisfy courts conducting a *Holmes* inquiry, any requirement for justification would reduce the risk of purely inadvertent proliferation of privacy asymmetries and — as illustrated by the judicial opinions narrowly construing New York Civil Rights Law §50-a and the mounting democratic campaign to repeal that statute — facilitate judicial nuanced judicial application of the statute, and democratic accountability.

C. An Interpretive Rule to Rebuttably Presume Symmetry

Given the limited avenues for constitutional challenges to privacy asymmetries, this Subpart urges legislatures and courts both to adopt an interpretive rule to fill the constitutional void and reduce the risk that lawmakers will proliferate unreasoned and irrational privacy asymmetries by sheer accident of the legislative process. Privacy statutes with express exceptions for law enforcement investigations, but silence as to defense investigations, should create a rebuttable presumption of parallel implied exceptions for defendants. Legislators could avoid the presumption by drafting statutory text that expressly restricts defense subpoenas. And the government in litigation could defeat the presumption by

---


justifying the asymmetry. Whereas the government could satisfy rational basis review by justifying law enforcement exceptions in isolation, and could satisfy the Holmes test by justifying prohibitions on defense investigations in isolation, the interpretive rule would require an express justification for asymmetrical treatment. These justifications would in turn facilitate nuanced judicial reasoning and democratic debate over privacy asymmetries.

This proposed interpretive rule would run counter to the standard expressio unius principle of statutory construction whereby a list of express exceptions in a statutory text are presumed to indicate that Congress purposely excluded other, unmentioned potential exceptions. But there are at least two reasons why expressio unius should not control courts’ interpretations of privacy asymmetries. First, Congress presumably cares about accuracy and fairness in criminal proceedings, about the judiciary’s inherent authority to exercise compulsory process for the production of relevant evidence in judicial proceedings, and about the statutory authority that Congress gave to defense investigators to do the same via subpoena statutes. So we should presume that Congress did not intend to abrogate either the judiciary’s inherent, or defendants’ statutory, compulsory process powers unless it does so expressly. Second, the Court has never clarified the scope of defendants’ pre-trial Sixth Amendment rights to Compulsory Process. Founding era authority suggests that these rights should extend broadly, even pre-indictment to the accused target of grand jury investigations. More recently, the Court conceded that it “has had little occasion to discuss the contours of the Compulsory Process Clause,” and that it has not yet decided “whether and how the guarantees of the Compulsory Process Clause differ from those of the Fourteenth Amendment.” Constitutional avoidance thus counsels against construing privacy statutes to block defendants’ independent investigative powers, a result my proposed interpretive rule would enable.

Conclusion

A new wave of data privacy and consumer protection laws are poised to enact privacy asymmetries for an array of new categories of data. This Article has identified privacy asymmetries as an issue and proposed a response: courts should construe exceptions to privacy laws that enable law enforcement to access sensitive to imply parallel exceptions for defense investigators, or require the government to justify asymmetrical treatment.

358 Ritchie, 480 US at 55-56.