Life, Liberty, and Data Privacy: The Global CLOUD, the Criminally Accused, and Executive Versus Judicial Compulsory Process Powers

Rebecca Wexler*

U.S. policymakers' responses to a wave of global data privacy laws are creating a deep structural unfairness in the criminal legal system. In an era of cloud computing, when data about communications and activities occurring anywhere in the world can be stored on servers located anywhere else, access to such data can make the difference between convictions and acquittals. At the same time, new global data privacy laws risk cutting off cross-border access to digital evidence in criminal investigations. Recognizing the threat to law enforcement interests, U.S. policymakers enacted the CLOUD Act of 2018 to create special procedures for law enforcement to circumvent foreign data privacy laws and access cross-border evidence anyway. Yet no one is creating similar procedures for criminal defense investigators.

In the U.S. adversarial legal system, criminal defense counsel are the sole actors formally tasked with investigating evidence of innocence. While the prosecution team must disclose exculpatory evidence that it happens to possess, law enforcement officers have no formal duty to actively seek out such evidence. As a result, selectively advantaging law enforcement investigations of guilt without creating parallel procedures for the defense means selectively suppressing evidence of innocence. This asymmetry gets privacy backwards. Privacy protections ostensibly meant to constrain government power may accomplish that goal in an absolute sense, but relatively speaking, they specially

* Assistant Professor of Law, University of California, Berkeley, School of Law. Thank you to Jonathan Abel, Ty Alper, Ayodele Akenroye, Katy Glenn Bass, Julie Cohen, Stephanie Campos-Bui, Seth Davis, Jim Dempsey, Andrew Ferguson, Michael Froomkin, Mark Gergen, Edward J. Imwinkelried, Jameel Jaffer, Amy Kapczynski, Matthew Kugler, Mark Lemley, Tejas Narechania, Paul Ohm, Daniel Richman, David Schwartz, Paul Schwartz, David Sklansky, Peter Swire, Kate Weisburd, Josephine Wolff, and Christopher Yoo for invaluable comments on earlier drafts and helpful conversation. Thank you to my research team: Alexa Daugherty, Summer Elliot, Esha Goyal, Kshitij Goyal, Chelsea Hanlock, Joseph Kroon, Ping Liu, Rhea Elizabeth Paul, Izzy Simon, Cheyenne Smith, Nivedita Soni, Tyler Takemoto, and Dani del Rosario Wertheimer. Marci Hoffman and Dean Rowan provided invaluable reference support. This Article benefitted from presentations at the Yale Law School and Knight First Amendment Institute Data and Democracy Symposium, the Privacy Law Scholars Conference, the American Bar Association Criminal Justice Workshop, the Berkeley Faculty Workshop, the Berkeley JWIG Workshop, the UCLA Faculty Colloquium, the Technology Law and Policy Colloquium at Georgetown Law School, and the Junior Faculty Forum for Law and STEM. Finally, thank you to Marie Mullins and her colleagues on the *Texas Law Review* for excellent editorial suggestions.

empower the government as compared to the defense. They thereby undermine the criminal defense process that is itself supposed to guard against government abuse.

This Article exposes this structural anti-defendant bias in U.S. responses to global data privacy laws. It then uses this problem as a case study to examine the constitutionality of a more general category of laws: privacy laws that disadvantage criminal defense investigations as compared to their law enforcement counterparts. It diagnoses why constitutional challenges to these types of laws have failed in the past and proposes a novel definitional argument to strengthen these challenges moving forward. Ironically, the very CLOUD Act procedures that exclude defense investigators also hold a key to advocating on their behalf.

Introduction

Prosecutors investigating evidence stored on a foreign server and protected by a foreign privacy law can use a treaty—and in some cases a U.S. court order—to pierce the privacy law and seize the evidence anyway.[1] Prosecutors seeking testimony from a witness who has asserted their Fifth Amendment privilege against self-incrimination can circumvent the privilege by promising not to use the testimony to prosecute the witness and then compelling the testimony anyway.[2] And prosecutors investigating communications-content data possessed by a U.S. technology company can get a court order compelling disclosure of the data despite Fourth Amendment and U.S. statutory privacy protections for that information.[3]

Not so for those who are wrongfully accused of a crime and seeking evidence to prove their innocence.[4] Most treaties for cross-border evidence gathering are exclusive to law enforcement, leaving defendants helpless in the face of foreign privacy laws that block their access to exculpatory evidence stored abroad, even when the evidence is essential to exonerate the wrongfully accused.[5] Meanwhile, courts have consistently denied criminal defendants the ability to pierce a witness's Fifth Amendment privilege, even if that witness's testimony is the sole means to avoid a wrongful conviction.[6] And courts have construed U.S. federal privacy law to categorically bar criminal defense counsel from subpoenaing U.S. technology companies for the contents of another's stored electronic communications, even when those

1. *See infra* notes 165, 171–173 and accompanying text.

2. *See infra* notes 263–264 and accompanying text.

3. *See infra* note 173 and accompanying text.

4. This Article refers to access to evidence of innocence and access to exculpatory evidence interchangeably. The arguments developed here apply broadly to any evidence relevant to the defense, including the defense of individuals without a factual innocence claim. *Cf.* Carol S. Steiker & Jordan M. Steiker, *The Seduction of Innocence: The Attraction and Limitations of the Focus on Innocence in Capital Punishment Law and Advocacy*, 95 J. CRIM. L. & CRIMINOLOGY 587, 597 (2005) (observing that focusing exclusively on innocence risks "indifference if not hostility to other types of injustice," such as "arbitrary and unequal treatment of offenders as well as disproportionate punishment"). *See generally* Margaret Raymond, *The Problem with Innocence*, 49 CLEV. ST. L. REV. 449 (2001) (critiquing "the wrongful convictions movement" for placing a premium on establishing factual innocence in post-conviction proceedings to the potential detriment of systemic reforms and other defendants).

5. *See infra* notes 36, 178, 180, 195–198 and accompanying text.

6. Notably, there are rare situations when courts have compelled the prosecution to grant use immunity on behalf of a criminal defendant to pierce a defense witness's assertion of the Fifth Amendment privilege. *See infra* notes 263–270 and accompanying text.

communications are essential to prove innocence and unavailable from other sources.[7]

These asymmetries get privacy backwards. While privacy protections ostensibly meant to *constrain* government power may accomplish this goal in an absolute sense, relatively speaking they specially *empower* the government as compared to the defense, thereby undermining the criminal defense process that is itself supposed to guard against government abuse.[8] In the U.S. adversarial criminal legal system, law enforcement is responsible for investigating inculpatory evidence,[9] while criminal defense counsel are the sole actors formally responsible for investigating exculpatory evidence.[10] (*Brady v. Maryland*[11] and its progeny merely require the prosecution team to

7. *See infra* notes 178–180, 276, 318 and accompanying text.

8. *Cf.* Charles J. Ogletree, Jr., *Beyond Justifications: Seeking Motivations to Sustain Public Defenders*, 106 HARV. L. REV. 1239, 1258 (1993) (highlighting the role of defense advocacy in guarding against tyranny). To be sure, privacy laws that generally restrict access to data accomplish the policy goal of increasing overall privacy, even if those laws have limited exceptions for law enforcement access. Nonetheless, when these laws disadvantage criminal defense investigations as compared to those of law enforcement, the laws get backwards the element of privacy policy that seeks to constrain government overreach.

9. *See, e.g.*, Andrew Manuel Crespo, *Probable Cause Pluralism*, 129 YALE L.J. 1276, 1279–80 (2020) ("[T]o satisfy the Fourth Amendment's core substantive requirement, the government must point to facts that provide some basis to believe that 'an offense has been or is being committed' . . . ." (quoting Safford Unified Sch. Dist. # 1 v. Redding, 557 U.S. 364, 370 (2009))).

10. U.S. law enforcement officers have no constitutional, statutory, or formal ethical duty to actively investigate innocence. That duty belongs to defense counsel alone, aided by defendants' constitutional and statutory rights to see and contest the evidence against them and to compel the production of evidence in their favor. *See generally* U.S. CONST. amends. V–VI, XIV (establishing the constitutional rights of an individual accused of a crime, including the right to assistance of counsel for his defense, but not prescribing a duty on law enforcement to investigate an individual's innocence); FED. R. CRIM. P. 16 (describing disclosure rules in criminal cases but stating that with regards to government disclosure, "this rule does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating . . . the case"). *See also* Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212, 223–24 (2021) (observing that "defense counsel must conduct independent investigations on behalf of their clients" in order to uncover a variety of defenses, alibis, and inconsistencies that may aid defense counsel in presenting an "effective defense"). Prosecutors have some domain-specific duties—for instance, to seek out information suggesting that a confidential informant may be unreliable. *See* STANDARDS FOR CRIMINAL JUSTICE: PROSECUTORIAL INVESTIGATIONS Standard 2.4(e) (AM. BAR ASS'N 2014) ("Before deciding to rely upon the information provided by a confidential informant for significant investigative steps, the prosecutor should" vet informants for unreliability using ten distinct criteria.). But law enforcement has no general responsibility to investigate exculpatory evidence. A recent story of a man accused of vehicular homicide, and whose defense attorneys used facial recognition software to locate a witness who exonerated him when police and prosecutors were either unable or unwilling to locate that witness, illustrates why the defense should not be forced to rely on the results of police and prosecutor investigations. Kashmir Hill, *Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands*, N.Y. TIMES, https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html [https://perma.cc/YTP6-YBC3] (Sept. 21, 2022).

11. 373 U.S. 83 (1963).

disclose favorable material evidence that they already know exists; these cases do not require law enforcement to investigate exculpatory evidence.[12]) Hence, privacy protections that allow for law enforcement investigations but not for criminal defense investigations systematically advantage the search for evidence of guilt while selectively suppressing that for evidence of innocence.[13]

To date, this phenomenon has largely escaped scrutiny.[14] Growing state,[15] national,[16] and global[17] privacy movements aim to curb the excesses of law enforcement and corporate surveillance enabled by the data-driven economy. These movements have garnered robust debate in legal

12. *See, e.g.*, United States v. Hughes, 211 F.3d 676, 688 (1st Cir. 2000) (stating that the prosecution was not obliged to produce exculpatory evidence beyond its control). Nor do the ethics rules generally require prosecutors to actively investigate evidence of innocence except in the very narrow circumstance of a postconviction prosecutor who "knows of new, credible and material evidence" of innocence, in which case the prosecutor should investigate whether the defendant was wrongfully convicted. MODEL RULES OF PRO. CONDUCT r. 3.8(g)(2)(ii) (AM. BAR. ASS'N 2020) (describing the requirement to investigate in that situation).

13. *Cf.* Daniel Richman, *Framing the Prosecution*, 87 S. CAL. L. REV. 673, 680–81 (2014) (arguing that "[d]efense counsel need to get adequate information not just about what the prosecutor included in her case, but also about what she left out," so as to air "reasonable doubt" for the jury).

14. Prior scholars have identified other pretextual uses of data privacy concepts to serve institutional interests at the expense of individuals. *See generally, e.g.*, Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1 (2023) (discussing the weaponization of privacy by institutions at the expense of individuals).

15. *See, e.g.*, California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.100–.199.100 (West 2018) (California's privacy legislation). The CCPA "gives consumers more control over the personal information that businesses collect about them" and "secures new privacy rights for California consumers." *California Consumer Privacy Act (CCPA)*, CALIF. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/WW5N-59DU] (Feb. 15, 2023).

16. CAMERON F. KERRY, JOHN B. MORRIS, JR., CAITLIN T. CHIN & NICOL E. TURNER LEE, BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION 5, 28 (2020), https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf [https://perma.cc/85F5-RZ8Y] (asserting that privacy law and its enforcers (e.g., the FTC) should take special care and craft accountability measures that force corporate entities to "respect the privacy of individuals" and reduce discrimination).

17. *See, e.g.*, Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 109–10, 116 (2020) (explaining that the European Union's General Data Protection Regulation (GDPR) protects data by establishing "individual rights" and "a set of company obligations" in order to increase corporate accountability).

scholarship,[18] media,[19] litigation,[20] and public policy[21] fora. Yet, despite urgent and widespread attention to privacy issues generally and to privacy concerns surrounding law enforcement specifically,[22] commentators have consistently overlooked privacy law's selective erosion of criminal defense access to evidence of innocence.[23] As a result, existing scholarly and public

18. *See, e.g.*, NEIL RICHARDS, WHY PRIVACY MATTERS 3–5 (2021) (disagreeing with the conventional wisdom that "privacy is dead," but arguing for the need to better understand privacy and how technologies can "make our lives better and make them worse"); ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 2 (2021) (listing examples that reflect erosion of privacy); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 1–3 (2019) (proposing there exists an inextricable link between the transformation of legal institutions and that of political economy, and studying the trajectory of the former in the networked-information age).

19. *See, e.g.*, Justin Sherman, *Data Brokers Know Where You Are—and Want to Sell That Intel*, WIRED (Aug. 23, 2021, 7:00 AM), https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/ [https://perma.cc/UXJ4-58H5] (detailing the sale of highly sensitive personal information to corporate data brokers); Sara Morrison, *Here's How Police Can Get Your Data—Even if You Aren't Suspected of a Crime*, VOX (July 31, 2021, 9:00 AM), https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant [https://perma.cc/Y8S4-9FK7] (noting that third-party data brokers can hand over personal information to law enforcement absent a warrant, other legal process, or even a crime); *When Law Enforcement Wants Your Social Media Content, Do Data Privacy Laws Hold Up?*, NPR (Aug. 14, 2022, 5:15 PM), https://www.npr.org/2022/08/14/1117465757/when-law-enforcement-wants-your-social-media-content-do-data-privacy-laws-hold-u [https://perma.cc/SPF2-3YND] (discussing law enforcement's broad power to access data generated by social media and other online platforms).

20. *See, e.g.*, Class Action Complaint at 1, Katz-Lacabe v. Oracle Am., Inc., No. 3:22-cv-04792 (N.D. Cal. Aug. 19, 2022) (alleging massive illegal privacy violations worldwide); Class Action Complaint at 1, Brooks v. Thomson Reuters Corp., No. RG20082878 (Cal. Sup. Ct. Dec. 3, 2020) (alleging sale of voluminous data dossiers including individuals' names, pictures, financial information, etc. to "corporations, law enforcement, and government agencies"); Consent Order of Permanent and Time-Limited Injunctions Against Defendant Clearview AI, Inc. at 2–3, ACLU v. Clearview AI, Inc., No. 2020 CH 04353 (Ill. Cir. Ct. May 11, 2022) (ordering that Clearview AI, a facial recognition company, cease sale of its services—built on the aggregation of large quantities of personal data—to private entities and individuals or the government without complying with the Illinois Biometric Information Privacy Act).

21. *See, e.g.*, Nicol Turner Lee & Caitlin Chin, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/VSL5-7SFF] (warning of the dangers of facial recognition and other surveillance technology for individuals in marginalized communities); Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CTR. FOR JUST. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data [https://perma.cc/ML65-MSMD] (writing that law enforcement purchases data in bulk and urging lawmakers to close "loopholes in privacy laws" that allow for this practice).

22. *See, e.g.*, Mariana Oliver & Matthew B. Kugler, *Surveying Surveillance: A National Study of Police Department Surveillance Technologies*, 54 ARIZ. ST. L.J. 103, 107–08 (2022) (presenting an empirical survey of large and small police department surveillance capacities).

23. There are welcome exceptions. *See generally* Rebecca Steele, Note, *Equalizing Access to Evidence: Criminal Defendants and the Stored Communications Act*, 131 YALE L.J. 1584 (2022) (presenting a case law survey of defendants' attempts to access evidence and concluding that

dialogue has almost entirely missed the fact that, when considered in the context of criminal investigations, core privacy protections that purport to limit law enforcement power can have the opposite effect.

This Article examines this broad phenomenon through the lens of global data privacy laws and cross-border access to evidence.[24] Part I begins by describing longstanding disparities between law enforcement's and criminal defense counsel's ability to compel access to evidence stored abroad. It then argues that new foreign data privacy laws, and U.S. policymakers' responses to those laws, are poised to make these disparities far worse. Specifically, it raises the alarm that the U.S. Congress and Executive Branch are in the midst of creating special new avenues for law enforcement to circumvent foreign data privacy laws while leaving U.S. criminal defense investigators with no similar recourse—just as the rise of the global cloud is making cross-border access to digital evidence ever more salient in more types of cases.[25]

---

criminal defendants' rights are violated by the Stored Communication Act's restrictions on disclosure to defendants); Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569 (2007) (exploring restrictions on internet service providers disclosing data to criminal defendants and civil litigants under the Stored Communications Act and proposing a statutory amendment to remedy this feature of the Act); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014) (developing the concept of "digital innocence" based on the theory that technology and data collection tools that have historically been used to prove guilt can also be used to prove innocence).

24. A note on broader context is in order. This Article is the third in a trilogy about privacy protections that specially empower law enforcement to access certain categories of evidence while selectively disadvantaging criminal defense investigations in seeking the same types of evidence. In prior work, I identified these disparities, which I call "privacy asymmetries," in U.S. federal privacy statutes that protect stored electronic communications contents, U.S. postal mail, video rental records, tax filings, educational records, and substance abuse records. Wexler, *supra* note 10, at 232–37. I argued that these disparities are almost certainly legislative accidents rather than deliberate policy choices, and that they are a normatively unreasonable policy default. And I proposed legislative reforms, *id.* at 258–61, and statutory interpretations, Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2774–78 (2021), that would avoid these types of disparities moving forward. This Article builds on that prior work by tackling both the global and constitutional dimensions of these types of asymmetries.

25. This Article is the first legal scholarship to identify and examine this issue from the perspective of U.S. criminal defense rights and in the context of the current global data privacy movement, as compared to the longstanding inequities in access to Mutual Legal Assistance Treaties (MLATs). Notably, scholars and nongovernmental organizations outside the United States have produced important works questioning whether recent efforts to speed up cross-border evidence gathering by law enforcement comply with the human rights principle of "equality of arms" for criminal defense access to evidence. *See, e.g.*, MARLOES C. VAN WIJK, CROSS-BORDER EVIDENCE GATHERING: EQUALITY OF ARMS WITHIN THE EU? 13–64 (2017) (examining "which requirements can be deduced from the principle of equality of arms as to the role of the defence with regard to cross-border evidence gathering"); FAIR TRIALS, POLICY BRIEF: THE IMPACT ON THE PROCEDURAL RIGHTS OF DEFENDANTS OF CROSS-BORDER ACCESS TO ELECTRONIC DATA THROUGH JUDICIAL COOPERATION IN CRIMINAL MATTERS 5, 27–29 (2018), https://www.fairtrials.org/app/uploads/2022/02/JUD-IT-Fair-Trials-Policy-Brief-October-2018.pdf [https://perma.cc/

Part II zooms out to the constitutional dimensions of this issue. Notwithstanding the apparent offense to both accuracy[26] and procedural fairness[27] ideals in the criminal legal system, constitutional challenges to disparities between law enforcement and criminal defense investigative powers have repeatedly failed.[28] Part of the work that this Article performs is a clear-eyed assessment of why these failures occurred. Its diagnosis is definitional. Part II argues that, under current doctrine, whether the constitutional right to present a defense enables defendants to use any particular form of compulsory process depends on whether courts define that process as a Judicial or an Executive Branch power. Existing constitutional challenges have proven unpersuasive to courts to date, I contend, in part because the arguments failed to define the underlying compulsory process power as judicial.[29] Moving forward, then, defense counsel facing barriers to their use of compulsory process should argue that the underlying process is judicial and, thus, that the right to present a defense should attach. If this argument succeeds, defendants could no longer be *categorically* denied access to that form of process. Instead, they would be entitled to use it in especially compelling circumstances, namely when the evidence they seek is important and when blocking access to that evidence would be "arbitrary or disproportionate."[30]

Part III zooms back in and applies the definitional insights from Part II to the cross-border evidence disparities identified in Part I. It focuses on one asymmetry in particular: law enforcement can use court orders to compel U.S. technology companies to disclose electronic communications contents stored on foreign servers, even when doing so violates a foreign data privacy law, but criminal defense counsel cannot. Defense counsel seeking access to

XR72-R6CB] (discussing the defendants' procedural rights in our "increasingly digitalised world"). This Article seeks to build on and engage with these welcome prior works.

26. *See* Daniel Epps, *The Consequences of Error in Criminal Justice*, 128 HARV. L. REV. 1065, 1074–75 (2015) ("While it's possible to debate the degree to which these largely symmetrical civil procedure rules maximize accuracy, it's difficult to dispute that criminal procedure exhibits a greater concern for skewing errors in one direction than does its civil counterpart." (emphasis and footnote omitted)).

27. *See generally* Tracey L. Meares & Tom R. Tyler, *Justice Sotomayor and the Jurisprudence of Procedural Justice*, 123 YALE L.J. F. 525 (discussing the normative values of Justice Sotomayor's—and larger—jurisprudence prioritizing judicial use of authority underwritten by just procedures).

28. *See* subpart II(A). *See also* Facebook, Inc. v. Wint, 199 A.3d 625, 633–34 (D.C. 2019) (rejecting constitutional challenge to SCA asymmetry).

29. *See, e.g.*, Informal Response to Petition for Writ of Mandate/Prohibition and/or Other Extraordinary Relief at 37, Facebook, Inc. v. Superior Ct., No. S256686 (Cal. July 8, 2019) (relying on *Wardius* to challenge SCA asymmetry without distinguishing Judicial from Executive Branch investigative powers); Opposition to Facebook's Motion to Quash Subpoena Duces Tecum; Points and Authorities in Support of SDT at 9–10, California v. Touchstone, No. SCD268262 (Cal. Super. Ct. Apr. 21, 2017) (same).

30. *See infra* notes 292–304 and accompanying text.

such court orders should argue that they are a form of Judicial rather than Executive Branch compulsory process. Ironically, the most recent U.S. law that specially advantages law enforcement investigations of cross-border evidence, the CLOUD Act of 2018, also holds a definitional key to help make this argument work.[31] The CLOUD Act, I argue, supports the view that court orders compelling technology companies to disclose stored electronic communications contents should be categorized as judicial subpoenas rather than warrants. If this argument succeeds, it will improve defense access to evidence in the global cloud.

The Article concludes by considering the policy dimensions of disparities between law enforcement and criminal defense counsel's cross-border investigative power.

I. Defense Access to Evidence in the Global CLOUD

Mr. Al Safoo was charged with providing material support to Islamic State terrorists.[32] In investigations preceding his still-pending terrorism trial, defense counsel received information indicating that the prosecution's star witness had been tortured to coerce his testimony against the defendant.[33] To prove these allegations and impeach the witness, the defense sought access to certain prior inconsistent statements of the witness purportedly contained in Iraqi court filings.[34] But, despite the verdict-altering potential of evidence that impeaches a key prosecution witness, Mr. Al Safoo's defense counsel was unable to access the documents.[35] This experience is not unique. A long-

31. *See infra* notes 341–352 and accompanying text.

32. Criminal Complaint at 4, United States v. Al Safoo, No. 18-CR-00696 (N.D. Ill. Oct. 16, 2018), ECF No. 1.

33. Defendant's Motion for the Court's Order to Continue the Rule 15 Deposition of the Government Witness, al-Anzi; for a Ruling on Defendant's Related Discovery Requests; and for Reconsideration of the al-Anzi CIPA Substitutions at 4, United States v. Al Safoo, No. 18-CR-00696 (N.D. Ill. Feb. 26, 2021), ECF No. 246 [hereinafter Defendant's Motion for the Court's Order to Continue the Rule 15 Deposition]; Defendant's Motion for Discovery, for the Appointment of an Independent Special Master or Court Expert, and to Continue the Deposition of the Government's Rule 15 Witness, Yasir al-Anzi at 7, United States v. Al Safoo, No. 18-CR-00696 (N.D. Ill. Mar. 17, 2021), ECF No. 260 [hereinafter Defendant's Motion for Discovery].

34. Defendant's Motion for the Court's Order to Continue the Rule 15 Deposition, *supra* note 33, at 7; Defendant's Motion for Discovery, *supra* note 33, at 2–3.

35. While the precise resolution of this issue is difficult to ascertain due to extensive sealing, defense counsel appears to have sought assistance from the prosecution and been denied, then sought assistance from a court-appointed special master and been told to meet and confer, following which the issue disappears from the docket. *See* Defendant's Motion for the Court's Order to Continue the Rule 15 Deposition, *supra* note 33, at 1 (requesting that the court "order the government to produce the underlying material in a classified setting" for the defense); Notification of Docket Entry, United States v. Al Safoo, No. 18-CR-00696 (N.D. Ill. Mar. 2, 2021), ECF No. 254 (ordering that the "supplemental unclassified hearing in chambers shall remain under seal"); Notification of Docket Entry, United States v. Al Safoo, No. 18-CR-00696 (N.D. Ill. Mar. 3, 2021),

recognized, complex web of laws and treaties makes evidence located abroad difficult or impossible for U.S. criminal defense counsel to obtain, even if that evidence is essential to exculpate the wrongfully accused, and even though U.S. law enforcement often would have power to compel cross-border access to the same information.[36]

This Part raises the alarm that new global data privacy movements, combined with the rise of digital evidence in the global cloud, are making these disparities worse. In recent years, two-thirds of the world's

ECF No. 257 (granting in part and denying in part the defendant's motions and granting the government's motion, saying "the material and information contained within the ex parte, in camera, submission reviewed by this Court, shall not be disclosed in discovery to the defense" because the Court found "that the material does not contain information that is exculpatory, impeaching, or otherwise relevant and helpful to the defense, and/or the disclosure of such material is likely to harm" U.S. national security); Defendant's Motion for Discovery, *supra* note 33, at 1 (requesting that the court (1) order the production of discovery materials needed for the witness's cross-examination, (2) appoint a special master or independent expert to verify the integrity of the witness's Iraqi court file, and (3) that the court grant a continuance); Notification of Docket Entry, United States v. Al Safoo, No. 18-CR-00696 (N.D. Ill. Mar. 25, 2021), ECF No. 271 (taking the defense's requests made in ECF No. 260 under advisement and directing the parties to meet and confer). The issue may surface again at trial, which has not yet occurred as of December 13, 2022.

36. *See, e.g.*, Michael Farbiarz, *Accuracy and Adjudication: The Promise of Extraterritorial Due Process*, 116 COLUM. L. REV. 625, 677 (2016) (advocating for a standard in federal extraterritorial prosecutions that would require defendants to "be given roughly the same access to evidence and witnesses as the defendant would have had if, instead of committing the criminal acts abroad, the defendant had acted inside the United States and sought judicial assistance with respect to the evidence and witnesses"); L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem*, 26 BERKELEY J. INT'L L. 62, 84–85 (2008) (describing in detail the "significant compulsion disparity in transnational criminal cases" given that defendants are "explicitly exclude[d]" from "the benefits of the compulsory process provisions"); Frank Tuerkheimer, *Globalization of U.S. Law Enforcement: Does the Constitution Come Along?*, 39 HOUS. L. REV. 307, 364 (2002) (noting that increasing use of MLATs will continue to tilt the scales in favor of prosecutors and arguing that this tilt constitutes "a serious flaw in the administration of justice that must receive attention").

jurisdictions,[37] including Europe,[38] China,[39] Russia,[40] South Africa,[41] Uganda,[42] and Brazil,[43] among many others,[44] have enacted sweeping data privacy, protection, and localization laws that constrain cross-border transfers of data, including electronic communications, metadata, and other digital records. India is currently considering doing the same.[45] Meanwhile, the Court of Justice of the European Union issued a landmark ruling making

37. *See* Graham Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, 176 PRIV. L. & BUS. INT'L REP. 1, 3–8 (2022) (identifying data privacy laws in 157 countries, or "two thirds (67%) of the world's 232 independent jurisdictions" as of March 2022).

38. *See* General Data Protection Regulation (GDPR), 2016 O.J. (L 119) art. 6, § 1 [hereinafter GDPR] (laying out stringent restrictions on data processing, which, as paragraph 101 of the GDPR's introductory findings explains, applies to cross-border data transfers).

39. *See generally* Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ 951 (requiring adoption of systems to protect various kinds of data); Rogier Creemers & Graham Webster, *Translation: Personal Information Protection Law of the People's Republic of China—Effective Nov. 1, 2021*, STANFORD UNIV.: DIGICHINA, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021 [https://perma.cc/S7UZ-GL5T] (Sept. 7, 2021) (imposing strict preconditions for the cross-border transfer of data).

40. Federal'nyĭ Zakon RF o Personal′Nykh Dannykh Rossiĭskoĭ Federatsii [Federal Law of the Russian Federation on Personal Data], SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2006, No. 31, Item 3451 (amended Mar. 1, 2021).

41. *See* Protection of Personal Information Act 4 of 2013 § 72 (S. Afr.) (providing that parties responsible for data "may not transfer personal information about a data subject to a third party who is in a foreign country unless . . . the third party . . . is subject to a law . . . which provide[s] an adequate level of protection").

42. *See* Paul Epodoi & Joel Basoga, Data Protection in Africa: An Appraisal of the Data Protection and Privacy Act of Uganda (unpublished manuscript) (on file with *Texas Law Review*) (explaining that the Ugandan Data Protection and Privacy Act "applies to persons outside Uganda who collect and process, hold or use personal data relating to Ugandan citizens"); Cathy-Eitel Nzume, *Slowly But Surely, Data Protection Regulations Expand Throughout Africa*, IAPP (Apr. 2, 2021), https://iapp.org/news/a/slowly-but-surely-data-protection-regulations-expand-throughout-africa/ [https://perma.cc/4FVF-KVTB] (noting the passage of Uganda's Data Protection and Privacy Act 2019).

43. Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 08.15.2018, art. 33 (Braz.).

44. As of March 2022, 157 countries had enacted data privacy laws, and an additional seventeen had draft bills under consideration by the legislature. Greenleaf, *supra* note 37, at 3–8; *see also* Patricia Boshe & Gregor Lienemann, *Data Protection Laws in Africa*, UNIV. OF PASSAU (Oct. 20, 2021), https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/lehrstuehle/hennemann/Mapping_Global_Data_Law/Sample_African_DPL.pdf [https://perma.cc/6NU2-P7QD] (collecting data privacy laws from thirty-nine African countries).

45. The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, §§ 33–34 (Dec. 5, 2019); Sameer Yasir & Karan Deep Singh, *India Withdraws a Proposed Law on Data Protection*, N.Y. TIMES (Aug. 4, 2022), https://www.nytimes.com/2022/08/04/business/india-data-privacy.html [https://perma.cc/FN8C-XNAW] (noting that the Indian government has withdrawn the 2019 version of the privacy bill but is working on a new law).

it harder to transfer EU data into the United States,[46] and forcing the European Commission and U.S. Department of Commerce into ongoing negotiations to develop a replacement data-transfer agreement.[47] These global developments respond to important data privacy and sovereignty concerns, including regulating AI and machine learning,[48] and anticolonial concerns about U.S. surveillance practices.[49]

At the same time, foreign data privacy laws can block access to important overseas evidence in criminal investigations. For some indication of the scale of this issue, European authorities have reported that over half of all criminal investigations in Europe involve some kind of cross-border digital evidence gathering.[50] And the U.S. Department of Justice (DOJ) recently explained that, during an eleven-month period, U.S. law enforcement's inability to access cross-border data thwarted "dozens of investigations, across the country, in every judicial circuit."[51] The "impacted

46. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd (Schrems II), ECLI:EU:C:2020:559, ¶¶ 1, 198–201 (July 16, 2020) (invalidating the EU-U.S. Privacy Shield Decision on the grounds that it was incompatible with individual data protections required under the GDPR and the Charter of Fundamental Rights of the European Union).

47. *See, e.g.*, *Transatlantic Data Flows: What's Next After the EU-U.S. Privacy Shield?*, BROOKINGS (July 23, 2021), https://www.brookings.edu/events/transatlantic-data-flows-whats-next-after-the-eu-u-s-privacy-shield/ [https://perma.cc/6M8H-ASNX] (discussing the importance of transatlantic data flows and the future of such data exchanges following the Court of Justice of the European Union's *Schrems II* decision).

48. *See, e.g.*, MIT SCHWARZMAN COLL. OF COMPUTING EXTERNAL ADVISORY COUNCIL, THE YEAR OF THE AI POLICY LAWS 4 (2021) (noting the lack of harmonization of AI frameworks across countries).

49. *See* SERGIO CARRERA, MARCO STEFAN & VALSAMIS MITSILEGAS, CTR. FOR EUR. POL'Y STUD., CROSS-BORDER DATA ACCESS IN CRIMINAL PROCEEDINGS AND THE FUTURE OF DIGITAL JUSTICE 5, 21–22 (2020) (discussing the Court of Justice of the European Union's ruling in *Schrems II* declaring that EU–U.S. data transfers permitted the U.S. to conduct overly broad "mass surveillance activities" that "jeopardise[d]" EU citizens' rights under the GDPR); Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 712 (2017) (observing that countries have implemented "localization requirements," which served to "limit the extent to which . . . data enters the United States" due to concerns over "U.S. intelligence activities and to create leverage for possible changes in U.S. policy").

50. *Commission Staff Working Document: Impact Assessment*, at 14, SWD (2018) 118 final (Apr. 17, 2018) [hereinafter European Commission Report]. The European Commission Report is based on a survey sent to public authorities in European Union member states, which received seventy-six responses. *Id.* at 135. While there are some possible discrepancies with the Report's findings, *see infra* note 209, they are commonly cited in policy discussions. *See* Peter Swire & Jennifer Daskal, *Frequently Asked Questions About the U.S. CLOUD Act*, CROSS-BORDER DATA F. (Apr. 16, 2019), https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/ [https://perma.cc/FA6V-M7JF] ("According to a 2018 European Commission impact assessment report, more than half of all criminal investigations include a cross-border request to access electronic evidence.").

51. *See Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era*: *Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 2–5 (2017) (statement of Richard

investigations run the gamut," including investigations "where the victim, the offender, and the account holder are all within the United States;"[52] investigations into computer fraud, identity theft, and tax fraud; and investigations where evidence located abroad was crucial to identify foreign co-conspirators and to locate fugitives.[53]

Meanwhile, think tanks and civil society organizations around the world are holding roundtables and publishing white papers on global data privacy and law enforcement concerns.[54] Jennifer Daskal has observed that "[t]he rules governing cross-border access to data are a topic of significant, ongoing importance to law enforcement officials, technology companies, privacy groups, and key foreign partners alike."[55] In Justin Hemmings, Sreenidhi Srinivasan, and Peter Swire's words, "the sheer amount of electronic evidence has made ubiquitous the need for law enforcement to access this kind of evidence stored outside of their physical jurisdiction."[56] And Andrew Keane Woods calls limits on law enforcement access to data in the global cloud "[o]ne of the great regulatory challenges of the Internet era—indeed, one of today's most pressing privacy questions."[57]

Recognizing the threat to law enforcement interests, Congress enacted the CLOUD Act of 2018 to enable law enforcement to compel access to cross-border data, including by circumventing foreign privacy laws.[58] The CLOUD Act has provoked vigorous and ongoing debates in all branches of

W. Downing, Acting Deputy Assistant Att'y Gen. of the United States) [hereinafter Downing Testimony] (describing the issues caused by the Second Circuit's opinion in *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016), which was decided in July 2016).

52. *Id.* at 6 (emphasis omitted).

53. *Id.*

54. *See, e.g.*, ANHAD KAUR MEHTA, ANMOL KOHLI, KSHITIJ GOYAL, LAKSHMI NAMBIAR & SANDLI PAWAR, SOUTH AFRICA: COUNTRY REPORT 2 (2021) (analyzing whether the South African data privacy law is fit to "address the data collection and privacy practices of today"); Stephanie K. Pell & Bill Baer, *Protecting National Security, Cybersecurity, and Privacy While Ensuring Competition*, BROOKINGS (Jan. 19, 2022), https://www.brookings.edu/blog/techtank/2022/01/19/protecting-national-security-cybersecurity-and-privacy-while-ensuring-competition/ [https://perma.cc/SBV3-HPNV] (summarizing a roundtable that addressed "whether there are irreconcilable tensions between antitrust enforcement and promoting competition on the one hand, and protecting our privacy, guarding against threats to our cybersecurity, and defending our country against hostile foreign actors on the other"); CARRERA ET AL., *supra* note 49, at 1 (exploring the question of whether "the increasing use of information and telecommunication technologies, and the digitalisation of everyday social and economic interactions, mean[s] new rules and instruments are needed for the cross-border gathering and exchange of evidence in criminal proceedings").

55. Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. F. 1029, 1030 (2019).

56. Justin Hemmings, Sreenidhi Srinivasan & Peter Swire, *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, 10 J. NAT'L SEC. L. & POL'Y 631, 631 (2020).

57. Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 729 (2016).

58. *See generally* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1714–20 (2018) (describing the SCA and CLOUD Act structure, and the provisions and agreements that provide the Act its international reach).

government,[59] civil society,[60] and legal scholarship.[61] Yet, these extensive debates have largely failed to consider criminal defense investigations.[62] Policymakers, courts, the legal academy, and civil libertarians alike have almost entirely disregarded the fact that the CLOUD Act procedures that enable law enforcement to access overseas data do not apply to criminal defense counsel.[63] The result is an investigative imbalance that, once again, advantages the search for evidence of guilt over that for evidence of innocence.[64]

The following discussion begins with historical context. It describes the evolution of entrenched procedural inequities in criminal defense counsel's and law enforcement's access to evidence located abroad. It then raises the alarm that, today, these inequities are becoming even worse. The wave of recent global data privacy laws, combined with U.S. policymakers' responses to these laws and the increasing salience of digital evidence from the global cloud, are producing troubling new disparities in criminal defense counsel's and law enforcement's access to evidence across borders. In short, history is repeating itself—at internet scale.

---

59. *See, e.g.*, *Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*: *Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 3 (2017) (statement of Prof. Jennifer Daskal) (suggesting changes to law enforcement access to data before the passage of the CLOUD Act); Downing Testimony, *supra* note 51, at 6 (describing, before passage of the CLOUD Act, law enforcement's need for legal changes).

60. *See* David Ruiz, *EFF and 23 Groups Tell Congress to Oppose the CLOUD Act*, ELEC. FRONTIER FOUND. (Mar. 11, 2018), https://www.eff.org/deeplinks/2018/03/eff-and-x-groups-tell-congress-oppose-cloud-act [https://perma.cc/SJW9-P7NR] (describing a coalition letter opposing the CLOUD Act, signed by an array of organizations including the Electronic Frontier Foundation, the Asian American Legal Defense and Education Fund, Constitutional Alliance, Human Rights Watch, and the American Civil Liberties Union).

61. *See, e.g.*, Anupam Chander, Commentary, *Is Data Localization a Solution for* Schrems II*?*, 23 J. INT'L ECON. L. 771, 782–84 (2020) (arguing that calls for data localization in response to the *Schrems II* decision would add to, rather than solve, the problem of cross-border data flow); Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 187–91 (2018) (critiquing the "location-driven approach" from the *Microsoft v. United States* case); Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEXAS L. REV. ONLINE 145, 149–52 (2017) (discussing the unsettled nature of the law governing cross-border data access); Woods, *supra*, note 57, at 745–48 (analyzing jurisdictional issues raised by storing access in the global cloud).

62. For an overview of legislative and public policy debates surrounding enactment of the CLOUD Act, see generally STEPHEN P. MULLIGAN, CONG. RSCH. SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT (2018).

63. For a welcome exception to this general oversight, see FAIR TRIALS, *supra* note 25, at 20 (discussing the "equality of arms" principle whereby the accused should be notified of investigations and afforded "a genuine opportunity to prepare and present their case").

64. In prior scholarship, I identified these recurring imbalances—which I call privacy asymmetries—in multiple U.S. federal privacy statutes, argued that many are unreasonable as a matter of policy and almost certainly enacted by accident, and provided model statutory text for legislators seeking to avoid enacting more of them. *See generally* Wexler, *supra* note 10. I also developed a statutory construction argument drawn from evidentiary privilege law that litigators can use to challenge existing privacy asymmetries in court. *See generally* Wexler, *supra* note 24.

A. Historical Context

Imagine a Canadian truck driver charged in a U.S. court with smuggling cocaine across the Canada–United States border.[65] Now imagine that a Canadian witness could testify that the driver had never inspected the contents of the truck and did not know she was transporting contraband.[66] If that witness is unwilling to appear voluntarily, U.S. defense counsel would be powerless to compel the witness's testimony—even though the prosecution could likely do so if it wished.[67] Or consider a defendant charged with smuggling cocaine in the lining of his suitcase who claims that he did not know the contraband was present, that his primary suitcase was stolen right before his scheduled flight from Mexico into the United States, and that the suitcase he brought with him was a hurried, last-minute purchase.[68] A Mexican police report might corroborate that testimony, but U.S. defense counsel would be unable to compel cross-border access to the report—even though the prosecution could likely do so if it wished.[69]

As the above examples illustrate, problems accessing evidence across borders are not unique to the internet age. They can apply to witnesses and documents as well as to data. Indeed, asymmetries in law enforcement's and criminal defense counsel's access to cross-border evidence are neither new nor inevitable. The following discussion traces their historical trajectory from the late twentieth century to today.

1. Symmetrical Letters Rogatory and Their Limits.—Prior to the 1970s, the primary legal mechanism to compel cross-border access to evidence, called letters rogatory, was available to law enforcement, civil litigants, and defense investigators alike.[70] Letters rogatory respond to the fact that courts generally lack jurisdiction over evidence located abroad.[71] The letters-rogatory process permits courts in one nation to seek discretionary assistance from courts in another to compel access to evidence in the foreign court's

65. This hypothetical was developed by L. Song Richardson based on the facts of a criminal case in which she was involved. Richardson, *supra* note 36, at 64–65, 64 n.3.

66. *Id.* at 65.

67. *Id.*

68. This hypothetical was developed by L. Song Richardson based on the facts of *United States v. Theresius Filippi*, 918 F.2d 244 (1st Cir. 1990). *Id.* at 66 & n.4.

69. *Id.*

70. *See* Dera J. Nevin & Marc Jenkins, *Information, Knowledge, and the Pursuit of Privacy*, 38 AM. J. TRIAL ADVOC. 485, 502 (2015) (setting out "Transnational Discovery Request Mechanics," including letters rogatory and the new mechanisms available after 1970 when the "Hague Convention of the Taking of Evidence Abroad in Civil or Commercial Matters" passed).

71. *See id.* at 505 ("If discovery cannot be obtained directly because the court does not have personal jurisdiction over the person or entity in possession of the relevant information, discovery may be obtained indirectly, by way of a request for assistance to a foreign court through letters rogatory.").

jurisdiction.[72] The foreign court may choose to assist as a matter of comity, or discretionary legal reciprocity between sovereigns.[73]

The letters-rogatory process is notoriously unpredictable and subject to lengthy delays of a year or more.[74] To use the process, litigants first request discretionary assistance from a court inside the United States.[75] This triggers a complicated and time-consuming chain of communications between U.S. and foreign government officials.[76] In many cases, the U.S. court transmits the letter to the U.S. State Department, which in turn transmits it to the appropriate U.S. embassy. The embassy officials then transmit the letter to the requested state's ministry of foreign affairs, which then transmits it to the state's ministry of justice.[77] Finally, the state's ministry of justice transmits the letter to an appropriate foreign court to enforce or not, following that court's comity analysis.[78] Note that applications for letters rogatory require ex parte judicial review from courts in *both* the receiving and requesting nations before anyone can be served with process and that, after service of process, any interested parties may be given notice and an opportunity to move to quash.[79] In 1971, the U.S. Secretary of State described letters rogatory as "complicated, dilatory and expensive."[80] More recently, Andrew Keane Woods characterized them as "rarely used and extremely unreliable."[81] Especially for criminal defendants incarcerated pre-trial, such

72. T. MARKUS FUNK, MUTUAL LEGAL ASSISTANCE TREATIES AND LETTERS ROGATORY: A GUIDE FOR JUDGES 17 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf [https://perma.cc/S76L-LLCJ].

73. *See id.* at 17 ("[I]nternational judicial assistance is discretionary, based upon principles of comity . . . ."); *see also* C. Todd Jones, *Compulsion Over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 NW. J. INT'L L. & BUS. 454, 471 (1992) ("Based on international comity, nations ordinarily grant such requests absent unusual circumstances." (footnote omitted)).

74. U.S. Dep't of Just., Crim. Res. Manual § 275 (2020).

75. *See, e.g.*, United States v. McLellan, 959 F.3d 442, 455–56 (1st Cir. 2020) (describing a U.S. criminal defendant's attempt to obtain documents from the United Kingdom and Ireland via letters rogatory); *In re* Comm'r's Subpoenas, 325 F.3d 1287, 1290 (11th Cir. 2003) (describing how letters rogatory traditionally work when used by a foreign requester).

76. U.S. Dep't of Just., Crim. Res. Manual § 275 (2020).

77. *Id.*

78. FUNK, *supra* note 72, at 22.

79. *See In re* Sapporo Ota Psychiatry Hosp., No. 20-MC-80147, 2020 WL 5526674, at *2 (N.D. Cal. Sept. 15, 2020) (noting that, typically, applications are considered ex parte because "parties will be given adequate notice of any discovery taken pursuant to the request and will then have the opportunity to move to quash the discovery or to participate in it" and that the orders granting applications thus "typically only provide that discovery is 'authorized,' and thus the opposing party may still raise objections and exercise its due process rights by challenging the discovery after it is issued via a motion to quash").

80. Letter of Submittal from William P. Rogers, U.S. Sec'y of State, to the President (Nov. 6, 1971), *in* 12 INT'L LEGAL MATERIALS 324, 324 (1973) [hereinafter Rogers Letter]; *see also* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct., 482 U.S. 522, 531 (1987) (quoting the Rogers Letter).

81. Woods, *supra* note 57, at 748.

lengthy delays may be untenable; even innocent defendants may choose to plead guilty rather than languish in jail awaiting access to exonerating evidence that may or may not ever materialize through such an unreliable procedure.

Beyond their inefficiencies, letters rogatory have another, perhaps even more significant limitation: they are generally unable to pierce foreign privacy laws that conflict with cross-border evidence transfers.[82] For example, bank secrecy laws in Switzerland and the Cayman Islands impose civil and criminal penalties on financial service providers that disclose customer information to third parties, including to foreign governments.[83] These types of foreign privacy laws are often called blocking statutes. It makes sense that a discretionary process like a letter rogatory would not trump such foreign laws. Courts in Switzerland or the Cayman Islands are unlikely to create exceptions to their own national statutes to provide discretionary assistance to a U.S. court. As a result, U.S. litigants using letters rogatory generally cannot access financial information located in Switzerland or the Cayman Islands.[84]

2. The Rise of Asymmetrical Process.—During the 1950s and 1960s, civil litigants began advocating for a better, more efficient process for cross-border evidence gathering.[85] They argued that the rise of international trade and travel had vastly increased the relevance of cross-border evidence to civil litigation and that continued reliance on the discretionary assistance of foreign courts was untenable.[86] Accordingly, in 1970, the United States signed the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters to standardize and expedite cross-border evidence transfers.[87] The Hague Convention offers civil litigants a special, additional means to resolve conflict-of-laws impediments to discovery compliance; it permits civil litigants to pierce foreign blocking statutes so long as those statutes include exceptions for international agreements.[88] For instance, a U.S. district court in Arizona recently channeled civil discovery through the Hague Convention to resolve a conflict with a French blocking statute that

82. *See* James I.K. Knapp, *Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy*, 20 CASE W. RSRV. J. INT'L L. 405, 410 (1988) (indicating that "letters rogatory generally will not be sufficient to overcome local bank secrecy or other similar restrictions on producing documents," including foreign privacy laws).

83. *Id.* at 407 n.5.

84. *See, e.g.*, United States v. Vetco Inc., 691 F.2d 1281, 1290 (9th Cir. 1981) (noting that appellants "concede[d] that letters rogatory will not be honored in Switzerland").

85. *E.g.*, Rogers Letter, *supra* note 80, at 324.

86. *E.g.*, *id.*

87. *See id.* (advocating for the ratification of the Hague Convention).

88. *See* Vivian Grosswald Curran, *United States Discovery and Foreign Blocking Statutes*, 76 LA. L. REV. 1141, 1146–47 (2016) (discussing letters of request under the Hague Convention).

barred cross-border evidence transfers absent an international treaty authorizing the procedures.[89] Hence, scholars and practitioners have recommended the Hague Convention as a procedural mechanism for civil litigants to route around foreign blocking statutes.[90] Importantly, the Hague Convention procedures were not made available to criminal defense counsel.[91]

Meanwhile, the inability of letters rogatory to pierce foreign bank secrecy laws prompted the U.S. government to start entering into Mutual Legal Assistance Treaties, or MLATs.[92] MLATs are bilateral treaties that bind the signatory nations to assist one another in criminal investigations.[93] Courts in the foreign jurisdiction may review MLAT requests and have some limited discretion to deny those that violate the procedural or substantive domestic law of the requested state.[94] But, crucially, MLATs often expressly waive foreign data privacy protections that conflict with cross-border evidence transfers. For example, the first MLAT, signed with Switzerland, waived Swiss bank secrecy laws to enable U.S. investigators to access Swiss bank records.[95]

Beyond solving the conflict-of-laws issues with cross-border investigations, MLATs also made the process less discretionary and more efficient. MLATs are less discretionary than letters rogatory because the treaties are binding on the signatories. They are more efficient because they often bypass diplomatic channels as well as review by U.S. courts. For instance, U.S. prosecutors using an MLAT process may send requests

89. *See* Salt River Project Agric. Improvement & Power Dist. v. Trench Fr. SAS, 303 F. Supp. 3d 1004, 1010 (D. Ariz. 2018) (finding factors weighed in favor of using Hague Convention discovery methods because the French blocking statute created a risk of criminal penalties for those who violated it).

90. *See, e.g.*, Denise E. Backhouse & Philip M. Berkowitz, *Rarely-Used Provision of Hague Evidence Convention May Be a Viable Option for Cross-Border Discovery*, N.Y. L.J., Feb. 4, 2019, at 11 (referencing the *Trench France SAS* decision from the Arizona district court as a "creative way" of maneuvering around blocking statutes).

91. *See, e.g.*, United Kingdom v. United States, 238 F.3d 1312, 1318 (11th Cir. 2001) ("The Convention plainly does not apply to this proceeding. The materials at issue here are sought for use in a criminal proceeding; the Convention, by contrast, by its terms applies only to civil and commercial matters.").

92. *See* Ethan A. Nadelmann, *Negotiations in Criminal Law Assistance Treaties*, 33 AM. J. COMPAR. L. 467, 468–72 (1985) (describing prosecutors' frustration with the process of using letters rogatory and the subsequent turn to MLATs to serve the same investigatory purposes). Nadelmann focuses in particular on the U.S. interest in closing a gap that had widened during the 1960s "between the capabilities of criminals to hide their assets and resources behind foreign borders [with strong bank secrecy laws and norms] and the capacity of law enforcement officials to investigate and prosecute them." *Id.* at 470.

93. *See generally* U.S. DEP'T OF STATE, 7 FOREIGN AFFAIRS MANUAL § 962.1 (2021), https://fam.state.gov/FAM/07FAM/07FAM0960.html [https://perma.cc/UL5E-QPY5]; *see also* Knapp, *supra* note 82, at 412–14 (describing increasing numbers of MLATs during the early 1980s).

94. FUNK, *supra* note 72, at 5 & n.14.

95. Knapp, *supra* note 82, at 405.

directly to their foreign law enforcement counterparts to pursue through the foreign courts.[96] In other words, the MLAT process requires pre-service-of-process ex parte judicial review solely from courts in the receiving nation.[97]

As with the Hague Convention procedures, these advantages of MLATs were not shared with the criminally accused. The first three MLATs—signed with Switzerland, Turkey, and the Netherlands—are silent on use by criminal defense counsel.[98] As a result, some courts initially construed the treaties to enable access by both law enforcement and criminal defense investigators.[99] During the 1980s, however, the United States began negotiating MLAT treaties that were expressly limited to law enforcement use.[100] The United States–Israel MLAT, for instance, states that it "is intended solely for mutual assistance between the [signatory governments]," and "shall not give rise to any right . . . on the part of any private person to obtain . . . evidence."[101] Courts interpreting the United States–Israel MLAT and similar texts in the United States–United Kingdom MLAT,[102] the United States–Ireland

96. *See* FUNK, *supra* note 72, at 2 ("[T]he courts play no part in initiating or processing outgoing MLAT requests." (emphasis omitted)).

97. *See id.* (stating that in contrast to outgoing MLAT requests, incoming MLAT requests require "direct federal district court oversight and involvement"); s*ee also* United Kingdom v. United States, 238 F.3d 1312, 1317 (11th Cir. 2001) (acknowledging that one of the features of the MLAT "is the requirement that a request for assistance be made, not directly to the courts, but rather between the 'Central Authorities,' which the treaty defines as the Secretary of State of the Home Department (for the United Kingdom), and the Attorney General (for the United States), *or their designees*." (emphasis added)).

98. *See* Michael Abbell, *DOJ Renews Assault on Defendants' Right to Use Treaties to Obtain Evidence from Abroad*, CHAMPION, Aug. 1997, at 20, 21 ("The Swiss MLAT, [and] several negotiated in the late 1970s and early 1980s, . . . are silent with respect to the ability of criminal defendants to use the treaties to obtain evidence on their behalf.").

99. *See, e.g.*, United States v. Rosen, 240 F.R.D. 204, 213 (E.D. Va. 2007) (dismissing defendant's argument based on a prior ruling from the federal district court in the Southern District of New York that had ordered the DOJ to "make an MLA Treaty request on behalf of a criminal defendant").

100. *See* FUNK, *supra* note 72, at 12 (noting that, apart from the first few MLATs, "the vast majority . . . explicitly exclude non-government access to U.S. processes" (emphasis omitted)); *see also* Abbell, *supra* note 98, at 21 ("[A]fter the negotiation of [the first three] treaties, the U.S. Department of Justice has insisted on including language in all subsequent United States MLATs that is designed to preclude criminal defendants from using the treaties to obtain evidence from abroad for use in their own defense."); Alan Ellis & Robert L. Pisani, *The United States Treaties on Mutual Assistance in Criminal Matters: A Comparative Analysis*, 19 INT'L LAW. 189, 190 nn.5–7, 190–91, 211 & nn.124–26 (1985) (discussing treaties on mutual assistance in criminal matters and noting that the treaties with Colombia, the Netherlands, Italy, and Morocco "are not intended for use by non-governmental parties," and that "private individuals may not invoke the treaty in order to obtain evidence from the other country for use in solely private matters").

101. Treaty on Mutual Assistance in Criminal Matters, Isr.-U.S., art. 1, ¶ 4, Jan. 26, 1998, T.I.A.S. 12925.

102. *See, e.g.*, *United Kingdom*, 238 F.3d at 1317 ("There is no provision for private parties, such as individual criminal defendants in the English (or American) courts, to request the production of information.") (citing Treaty on Mutual Legal Assistance in Criminal Matters, U.K.-U.S., art. 1, ¶ 3, Jan. 6, 1994, S. Treaty Doc. No. 104-2)).

MLAT,[103] the United States–Nigeria MLAT,[104] and the United States–Mexico MLAT have all held that the language precludes criminal defendants from using the MLAT procedures.[105] Today, nearly all of the United States' MLATs incorporate similar language precluding criminal defense access to their investigative procedures.

The disparity between defendants' letters rogatory power and law enforcement's MLAT power has provoked sustained criticism. Frank Tuerkheimer, a law professor and former Assistant United States Attorney in the Southern District of New York, described the "disparity in access to process" created by the MLAT system as "an endemic flaw in the fact-finding process."[106] L. Song Richardson has argued that "the transnational criminal adjudication process in the United States, particularly its evidentiary method, is deeply flawed."[107] The National Association of Criminal Defense Lawyers (NACDL) has repeatedly lobbied the Senate for amendments to MLAT language that would permit judges to order the DOJ to use MLAT

103. *See, e.g.*, United States v. McLellan, 959 F.3d 442, 472 (1st Cir. 2020) (extending interpretation of United States–United Kingdom MLAT to United States–Ireland MLAT).

104. *See, e.g.*, United States v. Jefferson, 594 F. Supp. 2d 655, 674 (E.D. Va. 2009) (stating that the United States–Nigeria MLAT "expressly provides that only the two governments, and not private parties, can make use of its provisions" (citing Treaty on Mutual Legal Assistance in Criminal Matters, Nigeria-U.S., art. I, ¶ 4, Sept. 13, 1989, S. Treaty Doc. No. 102-26)).

105. *See* United States v. Rosen, 240 F.R.D. 204, 214 (E.D. Va. 2007) ("In short, the language of the U.S.-Israel MLA Treaty cannot be fairly read to authorize the depositions defendants seek."); United States v. Odom, 53 M.J. 526, 537 (N-M. Ct. Crim. App. 2000) (noting that the United States–Mexico MLAT "confer[red] no individual rights to the appellant in regard to obtaining the presence of witnesses from Mexico"); United States v. Amador-Galvan, No. 98-10523, 2000 WL 359981, at *1 (9th Cir. Apr. 7, 2000) (finding that the defendant had "no individual rights under [the] Mexico-United States Mutual Legal Assistance Treaty").

106. Tuerkheimer, *supra* note 36, at 369.

107. Richardson, *supra* note 36, at 64; *see also* Daniel Huff, *Witness for the Defense: The Compulsory Process Clause as a Limit on Extraterritorial Criminal Jurisdiction*, 15 TEX. REV. L. & POL. 129, 161–62 (2010) (noting that criminal defendants who cannot access information abroad are worse off than those who are similarly situated but could obtain such information domestically, and explaining why the government's arguments to not extend this benefit to criminal defendants fall short); David Whedbee, *The Faint Shadow of the Sixth Amendment: Substantial Imbalance in Evidence-Gathering Capacity Abroad Under the U.S.-P.R.C. Mutual Legal Assistance Agreement in Criminal Matters*, 12 PAC. RIM L. & POL'Y J. 561, 580 (2003) (explaining how the United States–China MLAA infringes on criminal defendants' Sixth Amendment compulsory process rights by "dramatiz[ing] the imbalance between the prosecutors' monopoly on the use of the streamlined mechanism [for] ready access to evidence abroad" such that "U.S. prosecutors have quick and extensive access to evidence in [China] while defendants have no way of compelling the [Chinese government] to produce exculpatory evidence"); Ian R. Conner, Note, *Peoples Divided: The Application of United States Constitutional Protections in International Criminal Law Enforcement*, 11 WM. & MARY BILL RTS. J. 495, 504 (2002) ("The problems inherent in the treaty formation have led to a skewing of defendants' rights that can only be solved through reformation, so as to ensure . . . the subject of a treaty request retains the same basic privileges outside U.S. boundaries as he possesses within those boundaries.").

channels on behalf of the defense.[108] Criminal defense bar publications have featured model legal arguments against the inequities.[109] And defendants have repeatedly challenged the constitutionality of the disparities in court.[110]

To date, these critiques have generally failed. The DOJ has consistently opposed granting defendants access to MLAT processes.[111] The DOJ has argued that permitting defense access would deter other nations from entering into MLATs, that defendants do not need such access because they have other purported advantages in accessing certain types of foreign evidence (namely, defendants' own financial documents and other data about themselves), and that the letters-rogatory process should be sufficient for the defense despite its inadequacy for both the prosecution and civil litigants.[112] Meanwhile, the Senate has continued to approve MLATs that explicitly block nongovernmental litigants' access to process. And, apart from a handful of federal district courts that have pressured prosecutors to "voluntarily" use their MLAT power on behalf of the defense,[113] courts have uniformly upheld the constitutionality of these asymmetries between law enforcement and criminal defense access to foreign evidence.[114]

In sum, over the past fifty years, the U.S. government has negotiated a series of MLATs with other nations that create special procedures for law enforcement to compel access to evidence abroad but prohibit defense investigators from using the same procedures. Meanwhile, defense investigators are left to use the unreliable, inefficient, and discretionary letters-rogatory process that cannot circumvent conflicts with foreign privacy laws. This asymmetry in the MLAT regime has been identified and challenged. However, despite decades-long criticism in legal scholarship, Congress, and litigation, the Senate has continued to approve asymmetrical MLATs and courts have consistently found them constitutional.

---

108. *See, e.g.*, Letter from Mark M. Richard, Deputy Assistant Att'y Gen., to Patricia McNerney, Counsel, S. Foreign Rels. Comm. (Oct. 8, 1998), *in Extradition, Mutual Legal Assistance, and Prisoner Transfer Treaties: Hearing Before the S. Comm. on Foreign Rels.*, 105th Cong. app. at 27 (1998) [hereinafter Richard Letter] (recommending rejection of the NACDL's proposal to include a MLAT provision to assist defendants).

109. *See, e.g.*, Abbell, *supra* note 98, at 21 (contesting the government's theory that permitting defense access would lead countries to not enter into MLATs with the United States, because of a lack of evidence in support of that theory and because at least one country uses MLAT procedures to domestically assist criminal defendants).

110. Lauren Briggerman, Linda Friedman Ramirez & Addy Schmitt, *Challenges to Obtaining Foreign Evidence in Cross-Border Criminal Cases*, CHAMPION, Nov. 2019, at 30, 31.

111. Richard Letter, *supra* note 108.

112. Abbell, *supra* note 98, at 21.

113. *See* BRUCE ZAGARIS, INTERNATIONAL WHITE COLLAR CRIME 409 (2d ed. 2015) (describing a case in which the "defendants persuaded the U.S. court to order the government to allow the defendants to use an MLAT").

114. *See* Briggerman et al., *supra* note 110, at 31 (observing that courts "overwhelmingly have declined to require the government" to obtain evidence for defendants through MLAT procedures, "including in cases in which the defendant argues that the evidence is exculpatory").

B. New Foreign Data Privacy Laws

A criminal defendant in New York City was charged with committing a robbery planned using WeChat.[115] WeChat is a Chinese social media platform headquartered in Shenzhen, China.[116] Defense counsel sought, unsuccessfully, to access "any user data relating to the person who set up the robbery."[117] That information could be essential to show third-party guilt, meaning the defendant was misidentified and completely uninvolved in the crime, or to show coercion by a co-conspirator. If the user data that defense counsel sought came from a mainland-Chinese WeChat account, it would likely be stored on servers in China and subject to Chinese laws as well as international treaties and agreements.[118] Thus, U.S. law enforcement officers could, at least theoretically,[119] have compelled WeChat to disclose the data via the United States–China Mutual Legal Assistance Agreement (MLAA).[120] But, as of fall 2021, two new Chinese data privacy laws, discussed in detail below, obstruct U.S. criminal defense counsel from compelling cross-border digital evidence disclosures from China via a letter rogatory.[121]

The WeChat case exemplifies a new and growing source of disparity between criminal defense counsel's and law enforcement's cross-border access to evidence: foreign data privacy laws. To name just a few, Europe's General Data Protection Regulation (GDPR) went into effect in May 2018.[122] Brazil's General Data Protection Law (LGPD) went into effect in August 2021.[123] China's Personal Information Protection Law (PIPL) went into

115. E-mail from Richard Torres, criminal defense counsel, to author (July 24, 2020, 3:09 PM) (on file with author) [hereinafter Torres E-mail].

116. Emily Feng, *China Intercepts WeChat Texts from U.S. and Abroad, Researchers Say*, NPR, https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says [https://perma.cc/EED5-CJXY] (Sept. 19, 2019, 10:23 AM).

117. Torres E-mail, *supra* note 115.

118. WeChat currently stores data for users outside mainland China on servers in Singapore and Hong Kong. *WeChat Privacy Policy*, WECHAT (Sept. 9, 2022), https://www.wechat.com/en/privacy_policy.html#:~:text=Our%20servers%20are%20located%20in,be%20accessed%20from%20such%20locations [https://perma.cc/Y38A-RW82].

119. This would, of course, depend on cooperation from Chinese law enforcement.

120. The United States–China MLAA is unusual in that it has never been formalized into a treaty and remains a non-binding agreement. *See* Loren M. Scolaro, Note, *The Past, Present, and Future of United States-China Mutual Legal Assistance*, 94 N.Y.U. L. REV. 1688, 1709 (2019) (explaining that "the MLAA is not binding under domestic or international law in the same way as a treaty").

121. *See infra* notes 131–139 and accompanying text.

122. Harry P. Rudo & Amy Reagan, *The Global Landscape of Data Privacy: Important Points About New Laws in Three Key Jurisdictions*, DLA PIPER (Sept. 21, 2021), https://www.dlapiper.com/en/us/insights/publications/2021/09/practical-compliance-the-global-landscape-of-data-privacy-important-points-about-new-laws-in-three/ [https://perma.cc/CM5X-NZAR].

123. *Id.*

effect in November 2021.[124] And India has twice proposed a GDPR-like privacy bill: the Personal Data Protection Bill of 2019 and the Data Protection Bill of 2021.[125] Indeed, as of March 2022, a full two-thirds of the world's jurisdictions had enacted a data privacy law, and "substantial numbers of draft Bills" in other countries show that the trend is ongoing.[126]

These foreign laws respond to serious concerns about threats to privacy from corporate and government surveillance.[127] Just as U.S. policymakers are contemplating new federal privacy legislation to address these threats,[128] so too are foreign lawmakers enacting data privacy, protection, and localization laws in response to privacy, security, and sovereignty concerns about the global data economy—and about U.S. intelligence gathering. Post-Snowden concerns over U.S. law enforcement surveillance are playing a prominent role in ongoing international policy debates about the laws and norms governing global data privacy generally, and cross-border data transfers specifically.[129]

---

124. *Id.*

125. The Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (Dec. 5, 2019); *see* Mathew Chacko, Aadya Misra & Shambhavi Mishra, *India: A Guide to the Data Protection Bill, 2021*, MONDAQ (July 20, 2022), https://www.mondaq.com/india/privacy-protection/1213494/a-guide-to-the-data-protection-bill-2021 [https://perma.cc/8WRF-3U74] (explaining that the Data Protection Bill of 2021 was an updated version of the 2019 bill). Note that India has since withdrawn its privacy bill and is working on another revised version. Yasir & Singh, *supra* note 45.

126. Greenleaf, *supra* note 37, at 3–8.

127. *See* COHEN, *supra* note 18, at 247 ("The rapid and dramatic changes in affordances for surveillance, control, and targeted intermediation pose novel challenges for traditional ways of conceptualizing and detecting rights violations."); RICHARDS, *supra* note 18, at 168–206 (discussing the vast technological changes occurring and the resulting need for privacy rules); WALDMAN, *supra* note 18, at 2 (illustrating privacy concerns raised by recent technological developments such as facial recognition surveillance and DNA-testing kits).

128. *See, e.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) ("A Bill [t]o provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.").

129. *See* CARRERA ET AL., *supra* note 49, at 5 (noting that the *Schrems II* case indicated "that EU data-protection standards on cross-border transfers of personal data . . . cannot be compromised by any form of access (including for the purpose of national security)"); Swire & Hemmings, *supra* note 49, at 712 (explaining that the distrust of the U.S. government, technology companies, and surveillance related to Edward Snowden have provided justification for countries "to localize information about a country's residents in order to limit the extent to which such data enters the United States"). *See generally* Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 AM. U. BUS. L. REV. 11 (2015) (discussing the localization movement as a response to concerns about U.S. surveillance practices). For instance, on July 16, 2020, the Court of Justice of the European Union invalidated a "Privacy Shield" agreement between the U.S. Department of Commerce and the European Commission designed to regulate cross-border transfers of personal data. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 1, 198–201 (July 16, 2020); *see also* Ishita Mattoo, *The E.U.-U.S. Privacy Shield Invalidated in "Schrems II,"* BERK. TECH. L.J. (May 17, 2021), https://btlj.org/2021/05/the-e-u-u-s-privacy-shield-invalidated-in-schrems-ii/ [https://perma.cc/GFA8-SWLZ] (describing the *Schrems II* decision). In *Schrems II*, the court held that the Privacy Shield did not sufficiently protect

Yet while foreign data privacy laws may be enacted in the name of human rights, they can undermine them as well. Many of the new foreign privacy laws restrict cross-border transfers of digital evidence, including evidence that may be relevant to prosecuting or defending against criminal charges.[130] U.S. policymakers are responding with new treaties and statutes to circumvent the obstacles that these laws pose for *law enforcement* investigations. But the obstacles that the laws pose for criminal defense investigations are being ignored. While the longstanding MLAT asymmetries discussed above are well-recognized, these new disparities arising from recent global data privacy laws, and U.S. responses to them, are not. This subpart raises the alarm. It describes how new foreign data privacy laws can obstruct criminal defense counsel's cross-border access to evidence. The subsequent subpart argues that U.S. policymakers' asymmetrical responses to these laws are creating new, previously unrecognized disparities that advantage law enforcement investigations over those of the defense.

1. Blocking Statutes.—Some new foreign data privacy laws operate as blocking statutes, meaning they explicitly bar transferring certain data across borders, even in response to a U.S. court order or letter rogatory. China's Data Security Law (DSL), which took effect on September 1, 2021, and Personal Information Protection Law (PIPL), which took effect on November 1, 2021, exemplify this type of foreign law.

DSL Article 36 expressly provides that "[w]ithout the approval of the competent authorities of the People's Republic of China, organizations or individuals in the People's Republic of China shall not provide data stored within the territory of the People's Republic of China to any overseas judicial or law enforcement body."[131] Violators are subject to substantial fines and

EU personal data transferred to the United States from access by U.S. law enforcement and intelligence agencies. *See* Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, LAWFARE (July 17, 2020, 11:31 AM), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision [https://perma.cc/YZ7J-NVWV] (describing and criticizing the *Schrems II* decision). By encouraging companies to store more EU personal data within the EU, further afield from U.S. intelligence agency surveillance and potentially out of reach of U.S. court jurisdiction, *Schrems II* increases U.S. law enforcement investigators' dependence on international treaty processes, rather than domestic U.S. laws that may afford easier access to EU personal data. *See id.* (predicting data localization as a likely response to *Schrems II*).

130. *See infra* sections I(B)(1)–(2).

131. Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ 951; *see also* Philips Med. Sys. (Cleveland), Inc. v. Buan, No. 19 CV 2648, 2022 WL 602485, at *5 (N.D. Ill. Mar. 1, 2022) (quoting this same language). Before the DSL, a variety of Chinese laws imposed similar restrictions on cross-border transfers of distinct categories of data possessed by "critical information infrastructure operators," and data related to securities finance.

revocation of business licenses.[132] Even before the law took effect, commentators expressed concern that it would bar U.S. *civil* litigants' access to evidence in China,[133] as well as "make it harder for [U.S.] law enforcement agencies to get data out of China."[134] And, as it turns out, within months after the law took effect, civil defendants in U.S. federal courts had already begun invoking it to block discovery orders, arguing that documents that they possess and control but that are located on servers in China "may not be transferred to a foreign court or outside [China]."[135] U.S. criminal defense investigators seeking data stored in China will almost certainly face similar objections.

Meanwhile, PIPL Article 41 contains a similar provision, though with an express exception permitting cross-border transfers pursuant to international agreements.[136] Therefore, law enforcement and civil litigants

---

The DSL expanded these restrictions to apply more generally. Todd Liao, *What China's New Data Security Law Means for Multinational Corporations*, JDSUPRA (June 30, 2021), https://www.jdsupra.com/legalnews/what-china-s-new-data-security-law-4175525/ [https://perma.cc/WR6F-7FLX].

132. Xiang Wang, Aravind Swaminathan, Heather Egan Sussman, Mimiao Hu & Ryan McKenney, *China's New Data Security Law: What International Companies Need to Know*, ORRICK (Sept. 23, 2021), https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know [https://perma.cc/ZC9Y-STB9].

133. *See, e.g.*, *China's New Data Security Law Restricts Cross-Border Transfers of All Data to Foreign Authorities*, JONES DAY (Aug. 2021), https://www.jonesday.com/en/insights/2021/08/chinas-new-data-security-law-restricts-crossborder-transfers-of-data [https://perma.cc/C24P-V7NQ] (suggesting that "a conservative interpretation may mean that directly providing any data stored in China to a foreign judicial or law enforcement authority for either a criminal or *civil* proceeding may trigger the need for government approval").

134. Masha Borak, *China to Punish Data Exports to Overseas Courts as Beijing Beefs Up Defence Against US Long Arm*, S. CHINA MORNING POST (Apr. 20, 2021, 6:30 PM), https://www.scmp.com/tech/policy/article/3131453/china-punish-data-exports-overseas-courts-beijing-beefs-defence-against [https://perma.cc/TSM5-ZYSB].

135. *In re* Valsartan, Losartan, & Irbesartan Prods. Liab. Litig., MDL No. 2875, 2021 WL 6010575, at *3 (D. N.J. Dec. 20, 2021); *see also Buan*, 2022 WL 602485, at *3–5 (rejecting defendants' argument that the "DSL inhibit[s] their ability to comply with th[e] court's discovery orders"); *In re* Evenstar Master Fund SPC *ex rel.* Evenstar Master Sub-Fund I Segregated Portfolio, No. 20-MC-418, 2021 WL 5498283, at *4 (S.D.N.Y. Nov. 23, 2021) (describing civil defendant's argument that China's data security laws require approval of the Chinese government before requested information may be obtained). U.S. courts have so far rejected these arguments, reasoning that civil discovery requires disclosure to a party, not to a judicial authority, and that even if the DSL does prohibit U.S. discovery disclosures, the U.S. court would still undertake a comity analysis to determine whether to order discovery anyway. *See, e.g.*, *Buan*, 2022 WL 602485, at *6 (expressing skepticism that "international comity analysis would support curtailing discovery"). Nonetheless, the motion practice itself drains resources and time that criminal defense counsel may not have, and even if a court conducting a comity analysis ultimately ordered disclosure, it could lead to noncompliance causing prejudice to the defense that may be difficult to remedy.

136. *See* Creemers & Webster, *supra* note 39 ("Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies."); Graham Greenleaf, *China's Completed Personal*

may be able to circumvent the PIPL restrictions by routing requests for data through the United States–China MLAA[137] or the Hague Evidence Convention.[138] U.S. criminal defense counsel, who have been repeatedly shut out of international treaties on cross-border evidence gathering, will have no such option. Yet, to date, public policy debates over the Chinese blocking statutes appear to have omitted any mention of the criminally accused.[139]

2. Burden-Raising Statutes.—Other foreign data privacy laws do not expressly bar transferring data across borders in response to a U.S. court order but can have similar effects in practice by imposing onerous burdens on litigants seeking cross-border evidence transfers. Europe's GDPR illustrates this possibility. The GDPR regulates transfers of personal data to countries outside the EU.[140] Within weeks of its going into effect in May 2018, commentators began predicting that the law could impede U.S. *civil* litigants' access to evidence from EU sources.[141] By July 2019, at least eleven federal district courts had considered objections to civil discovery based on

Information Protection Law: Rights Plus Cyber-security, 172 PRIV. L. & BUS. INT'L REP. 20, 20–23 (2021) (analyzing the PIPL conditions for export and concluding that if any "are implemented in very restrictive manner by CAC, export would in effect be prohibited"). Saudi Arabia's newly amended Personal Data Protection Law contains a similar express exception authorizing cross-border transfers "[u]nless required to comply with an agreement to which the [Saudi Arabia] is a party," which suggests that the law will authorize compliance with MLAT requests or the Hague Convention but perhaps not with a criminal defendant's letter rogatory. Habib Saeed, *Saudi Arabia's New Personal Data Protection Law—Key Points for Employers*, NAT'L L. REV. (Mar. 14, 2022), https://www.natlawreview.com/article/saudi-arabia-s-new-personal-data-protection-law-key-points-employers [https://perma.cc/9F42-QA2V].

137. *See generally* Scolaro, *supra* note 120 (discussing the history and application of the United States–China MLAA).

138. China is a member of the Hague Evidence Convention. *China*, U.S. DEP'T OF STATE (May 1, 2019), https://travel.state.gov/content/travel/en/legal/Judicial-Assistance-Country-Information/China.html [https://perma.cc/L8HH-VLBW].

139. And, as the subsequent subpart contends, even a blocking statute that seems to deny evidence equally to law enforcement and defense alike will not operate equally in practice because U.S. domestic statutes give law enforcement, but not the defense, routes to circumvent such laws for at least some data stored on foreign servers. *See infra* subpart I(C).

140. GDPR, *supra* note 38, ch. V; *see also* Michael M. Baylson & Sandra A. Jeskie, *Overseas Obligations: An Update on Cross-Border Discovery*, JUDICATURE, Spring 2019, at 54, 59–60 ("The European Commission makes clear that the mere fact that a foreign court issued an order for the transfer of information outside the EU does not make the transfer lawful under the GDPR.").

141. *See, e.g.*, Backhouse & Berkowitz, *supra* note 90 (indicating that the GDPR might restrict data-transfer rights); Melinda F. Levitt, *GDPR and U.S. eDiscovery—Who Will Win the Game of Chicken*, FOLEY & LARDNER LLP (June 20, 2018), https://www.foley.com/en/insights/publications/2018/06/gdpr-and-us-ediscovery--who-will-win-the-game-of-c [https://perma.cc/WR7V-EFVJ] (discussing potential implications of the GDPR for civil litigation). Jennifer Daskal also predicted that the GDPR could be used to try to block cross-border disclosures to law enforcement pursuant to SCA orders. *See* Jennifer Daskal, Microsoft Ireland, *the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 12 (2018) (noting limitations GDPR placed on EU-held data transfers, "including in response to court orders issued by non-EU countries").

the GDPR.[142] Though the issue has not received the same (or any) attention, the GDPR likely raises even greater impediments for U.S. criminal defense discovery of evidence stored in the EU.[143]

Most significantly, GDPR Articles 48 and 49 restrict cross-border transfers of personal data outside the confines of international treaties.[144] There is an exception permitting cross-border transfers on an occasional or case-by-case basis if they are "*necessary* for the establishment, exercise or defence of legal claims."[145] The European Data Protection Board has clarified that this exception applies "in the context of a criminal or administrative investigation in a third country (e.g. anti-trust law, corruption, insider trading or similar situations) . . . for the purpose of defending oneself."[146] So the GDPR clearly permits *some* cross-border transfers of personal data to U.S. criminal defendants.

The central question is how onerous the requirements will be to satisfy the "necessity" test. What is known right now is that the EU data exporter

142. *See* Michael H. Gladstone, *General Data Protection Regulation in U.S. Litigation Through Mid-Summer 2019*, DEF. COUNS. J., Oct. 2019, at 1, 2 n.2 (collecting cases). To date, most U.S. courts have deemed the U.S. civil discovery orders enforceable under a comity analysis regardless of a conflict with the GDPR. *See, e.g.*, Giorgi Glob. Holdings, Inc. v. Smulski, No. 17-4416, 2020 WL 2571177, at *1–3 (E.D. Pa. May 21, 2020) (holding that defendant could not rely on the GDPR or Polish privacy law to avoid production of relevant documents); *In re* Mercedes-Benz Emissions Litig., No. 2:16-cv-881, 2019 WL 5800270, at *2 (D.N.J. Nov. 7, 2019) (balancing the EU's interest in privacy and the United States legal system's interest in preserving and maintaining broad discovery under the federal rules of civil procedure), *aff'd*, 2020 WL 487288 (D. N.J. Jan. 30, 2020); Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946-JST, 2019 WL 618554, at *3 (N.D. Cal. Feb. 14, 2019) (holding the GDPR did not preclude the court from ordering defendant to produce emails in an unredacted form under an existing protective order). *See generally* Michael H. Gladstone, *GDPR in United States Litigation Through Summer 2020: GDPR-Subject Companies Must Produce*, DEF. COUNS. J., Oct. 2020, at 1, 1–7 (discussing the aforementioned and other GDPR-related discovery cases).

143. Neil Richards has authored a compelling critique of the argument that the GDPR blocks cross-border discovery, which he characterizes as a "co-option of privacy rules to serve institutional rather than individual interests." Neil Richards, *The GDPR as Privacy Pretext and the Problem of Co-Opting Privacy*, 73 HASTINGS L.J. 1511, 1538 (2022). At the same time, Richards recognizes that "there is a significant opportunity for mischief by [civil] defendants advancing a privacy pretext" of this sort. *Id.* at 1524. There is all the more opportunity for such mischief in criminal cases, where most defendants lack access to expert witnesses to challenge complex interpretations of foreign law.

144. *See* COUNCIL OF BARS & L. SOC'YS OF EUR., CCBE ASSESSMENT OF THE U.S. CLOUD ACT 7 (2019), https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf [https://perma.cc/X9XM-Q6V6] (noting that neither a CLOUD Act order nor a warrant meets Article 48's requirement for transferring data to the United States).

145. GDPR, *supra* note 38, art. 49(1)(e) (emphasis added).

146. European Data Prot. Bd., *Guidelines 2/2018 on Derogations of Article 49 Under Regulation 2016/679*, at 11 (May 25, 2018) [hereinafter European Data Prot. Bd. Article 49 Derogations Guidelines], https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf [https://perma.cc/8X8W-DDRD].

makes the necessity determination,[147] and that satisfying the test requires a showing of "close and substantial connection between the data in question and the specific . . . defense of the legal position."[148] Exactly what this test will mean in practice is up in the air. Some commentators have argued that "[e]stablishing necessity is a high bar,"[149] while others have argued that it requires merely showing the relevance of the data.[150] If the burden turns out to be high, it may become impossible to satisfy for evidence that the seeking party has not yet seen. The result would effectively preclude access altogether. Similar uncertainty appears in other GDPR-like foreign data privacy statutes around the world.[151] For instance, the 2021 version of India's proposed Data Protection Bill generally restricts cross-border transfers of data.[152] Article 36 excepts transfers "*necessary* for . . . defending any charge . . . in any impending legal proceeding."[153]

Meanwhile, GDPR's "two-step" process requires that all other provisions of the law must be satisfied before cross-border transfers may occur.[154] And some of the GDPR's other provisions could also interfere with criminal defense access. For example, the GDPR grants data subjects the rights to demand that companies delete data and to be notified if and when the companies share sensitive data with others, including notice of cross-border transfers.[155] Defense access that requires preservation or confidential disclosures might run afoul of those GDPR guarantees. And even if a U.S. court were to order preservation or confidential disclosures, it would not be

147. *Id.* at 5.

148. *Id.* at 12.

149. Gary Weingarden & Matthias Artzt, *Stuck in the Middle with You: When US Discovery Orders Hit GDPR*, IAPP (Jan. 26, 2021), https://iapp.org/news/a/stuck-in-the-middle-with-you-when-u-s-discovery-orders-hit-the-gdpr/ [https://perma.cc/8TTP-XQDE].

150. *See* Richards, *supra* note 143, at 1530 ("The test is not a 'strict' one as most would understand the term, but one that instead requires a close relationship between the information being sought and the legal claim in question—one that defines necessity in terms of adequacy and relevance for purpose. This guidance is not one requiring strict necessity, but rather actual relevance to a legal claim.").

151. GDPR has served and continues to serve as a model for many other countries' data privacy laws. *See* Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, 169 PRIV. L. & BUS. INT'L REP., 1, 3–5 (2021) ("During 2019-20, at least 13 countries have updated or replaced existing laws (almost always influenced by the EU's GDPR).").

152. *See* The Personal Data Protection (Amendment) Bill, 2019, § 33–34 (2021). India withdrew this version of the bill in the summer of 2022 and is in the process of drafting a new version. Yasir & Singh, *supra* note 45.

153. The Personal Data Protection (Amendment) Bill, 2019, § 36(b) (2021) (emphasis added).

154. Thank you to Paul Schwartz for pointing out the two-step impediment to cross-border discovery. THE EU GENERAL DATA PROTECTION REGULATION (GDPR) 757 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., 2020) ("Under Article 44, all other relevant provisions of the GDPR must be complied with before personal data may be transferred outside the EU (this is the so-called 'two-step' approach to data transfers).").

155. *See id.* (describing some of the rights of data subjects).

enough. The European Data Protection Board has cautioned that U.S. court orders "are not in themselves legitimate grounds for data transfers" to the United States.[156]

The upshot is that GDPR, and other foreign data privacy laws modeled after GDPR, could impose significant burdens on United States criminal defense investigators seeking to access evidence from foreign sources. If those burdens are too high, they could effectively preclude access altogether.

C. The Asymmetrical U.S. Response

U.S. policymakers are addressing the risk that new foreign data privacy laws will impede *law enforcement* investigations.[157] Law enforcement's interest in cross-border data raises challenging tensions between, on the one hand, the privacy rights and sovereignty concerns that the new foreign privacy laws reflect, and on the other hand, access to evidence for criminal investigations.[158] U.S. policymakers are responding by updating statutes and negotiating new treaties to give law enforcement special routes to bypass conflict-of-laws barriers to accessing evidence from the global cloud.

But while the obstacles that new foreign data privacy laws erect for law enforcement investigations have received considerable attention,[159] commentators have almost entirely overlooked how these laws will affect

156. European Data Prot. Bd. Article 49 Derogations Guidelines, *supra* note 146, at 5.

157. Congress made the following findings when it enacted the CLOUD Act:

> Congress finds the following:
>
> (1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.
>
> (2) Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States.

Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V § 102, 132 Stat. 1213, 1213 (2018).

158. *See, e.g.*, MICHAEL J.D. VERMEER, DULANI WOODS & BRIAN A. JACKSON, IDENTIFYING LAW ENFORCEMENT NEEDS FOR ACCESS TO DIGITAL EVIDENCE IN REMOTE DATA CENTERS 6 (2018), https://www.rand.org/pubs/research_reports/RR2240.html [https://perma.cc/G89G-4DDZ] (recognizing that the challenges of extraterritorial data are multifaceted).

159. *See, e.g.*, Peter Swire, *When Does GDPR Act as a Blocking Statute?: The Relevance of a Lawful Basis for Transfer*, *in* BUILDING COMMON APPROACHES FOR CYBERSECURITY AND PRIVACY IN A GLOBALIZED WORLD 76, 76 (Randal S. Milch, Sebastian Benthall & Alexander Potcovaru eds., 2019) (discussing ways law enforcement would have a lawful basis for transferring data out of the EU); Woods, *supra* note 57, at 774–80 (arguing that data should not be "unterritorial"); VERMEER ET AL., *supra* note 158, at 28–30 (reporting that survey respondents identified foreign data localization mandates as both important and difficult).

criminal defense investigations.[160] And the special procedures that U.S. policymakers are negotiating for law enforcement to circumvent foreign data privacy laws do not apply to criminal defendants.

The result is a new set of procedural inequities between law enforcement and criminal defense cross-border investigations. As described in subpart I(A), the longstanding inequities between law enforcement MLATs and criminal defense letters rogatory are well-recognized. However, the new disparities arising from U.S. policymakers' responses to recent global data privacy laws are not. This subpart lays out the problem.

1. CLOUD Agreements.—In 2018, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act to create special procedures for law enforcement to access data stored abroad. The CLOUD Act has two parts. One part empowers the U.S. government to enter into a new series of bilateral executive agreements with "qualifying" foreign nations and is designed to supersede the MLAT system, to expedite law enforcement cooperation across borders, and to ensure U.S. law enforcement power to pierce blocking provisions in foreign data privacy laws.[161] The CLOUD Agreements are effectively a new superhighway for law enforcement to compel access to evidence that is both stored abroad and controlled by a foreign service provider.[162] Defense investigators are being shut out from this superhighway. Without access to CLOUD Agreement procedures, defense counsel seeking the same type of evidence from the same sources as law enforcement must resort instead to the outdated and insufficient letters-rogatory process.

More specifically, the CLOUD Act text enabling these bilateral CLOUD Agreements expressly disadvantages criminal defense investigators. It states that foreign governments entering into such CLOUD Agreements must permit technology companies "to respond to valid legal process sought *by a governmental entity* . . . if foreign law would otherwise prohibit communications-service providers from disclosing the data."[163] Meanwhile, the statute in which the CLOUD Act is embedded (the Stored Communications Act, or SCA) elsewhere defines a "governmental entity" as "a department or agency of the United States or any State or political

160. Meanwhile, scholarship on foreign blocking statutes has focused on civil discovery. *See, e.g.*, Curran, *supra* note 88, at 1141 (analyzing the tensions between United States civil discovery rules and foreign blocking statutes). For a welcome exception to the general oversight of criminal defense cross-border evidence gathering needs, see generally, for example, FAIR TRIALS, *supra* note 25.

161. 18 U.S.C. §§ 2523(b), 2703(h)(1)(A); CLOUD Act § 102(6).

162. *See* 18 U.S.C. § 2713 (stating that providers of an "electronic communication service or remote computing service shall comply with the obligations of this chapter . . . regardless of whether such communication, record, or other information is located within or outside of the United States").

163. *Id.* § 2523(b)(4)(I) (emphasis added).

subdivision thereof,"[164] and courts have interpreted this phrase to exclude criminal defense counsel.[165] In other words, the price of entering into a CLOUD Agreement with the United States is that foreign nations must waive any conflicting privacy laws so as to enable United States law enforcement to access data within their borders. But they only need to do this for *governmental* entities, not for criminal defense counsel. Thus, the very congressional authorization for CLOUD Agreements codifies an asymmetry prioritizing law enforcement investigations over their defense counterparts.

It is hardly surprising, then, that the developing CLOUD Agreement infrastructure mirrors the asymmetries of the MLAT system. The first CLOUD Agreement, which entered into force on October 3, 2022, between the United States and the United Kingdom,[166] expressly excludes criminal defense counsel from its procedural mechanisms for bypassing foreign privacy laws and speeding access to cross-border data. Like its MLAT predecessors, the United States–United Kingdom agreement provides for "timely access to electronic data for authorized *law enforcement* purposes" but expressly disavows the creation of any right for "any private person . . . to obtain . . . any evidence."[167] The second CLOUD Agreement, which was signed between the United States and Australia but which as of January 2023 has yet to go into force,[168] contains the same text.[169] This is precisely the type

164. *Id.* § 2711(4).

165. *See, e.g.*, State v. Johnson, 538 S.W.3d 32, 69–70 (Tenn. Crim. App. 2017) (explaining the court's reasoning for why "defendants . . . do not meet the definition of 'governmental entity'"); United States v. Amawi, 552 F. Supp. 2d 679, 680 (N.D. Ohio 2008) (agreeing with the argument that "the Office of the Federal Public Defender is not a 'governmental entity' within the meaning of § 2703"); *see also* Zwillinger & Genetski, *supra* note 23, at 594 ("The purpose and plain text of the SCA make clear that the exceptions for governmental entities apply only to Fourth Amendment government actors—investigative agencies and prosecuting attorneys—and not to criminal defendants, irrespective of whether they happen to be represented by a publicly funded criminal defender's office.").

166. Press Release, Dep't of Just., Landmark U.S.-UK Data Access Agreement Enters into Force (Oct. 3, 2022), https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force [https://perma.cc/7PDY-3QMJ].

167. Agreement on Access to Electronic Data for the Purposes of Countering Serious Crime, U.K.-U.S., pmbl., art. 3, ¶ 4, Oct. 3, 2019, https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern-ireland [https://perma.cc/CL48-NEAC].

168. *See* Office of the Attorney General; Clarifying Lawful Overseas Use of Data Act; Attorney General Certification and Determination, 87 Fed. Reg. 40274 (July 6, 2022) (noting the agreement will go into force after each country has taken the necessary steps); Press Release, Dep't of Just., United States and Australia Enter CLOUD Agreement to Facilitate Investigations of Serious Crime (Dec. 15, 2021), https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime [https://perma.cc/EYF3-F5S3] (announcing that the agreement had been signed and would go under review processes in both countries).

169. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Austl.-U.S., pmbl., art. 3, ¶ 6, Dec. 15, 2021, https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf [https://perma.cc/Y247-W3DK].

of language that courts have construed to bar defense investigators from accessing MLAT procedures. Given the CLOUD Act text, the first two CLOUD Agreement precedents, and the DOJ's longstanding defense of MLAT asymmetries, there is little reason to think that future CLOUD Agreements will be different and account for defense investigative interests.[170]

2. CLOUD Act Orders and the Stored Communications Act.—The other part of the CLOUD Act specially entitles law enforcement to have U.S. courts compel U.S. technology companies to divulge data stored on foreign servers.[171] In other words, it provides law enforcement with a one-stop shop in U.S. courts to compel disclosures of data stored abroad.[172] If foreign evidence is within the control of a U.S. service provider, such as Microsoft, Google, Facebook, GitHub, or Twitter, then the CLOUD Act expressly empowers law enforcement to compel that company to produce the data through a U.S. court order without resorting to an MLAT (or CLOUD Agreement).[173] Thus, whereas letters rogatory require judicial review by both U.S. and foreign courts, and MLATs require judicial review exclusively by a foreign court, CLOUD Act orders require judicial review exclusively by U.S. courts.

The CLOUD Act also codifies a comity analysis[174] for courts to use in resolving conflicts with foreign laws from certain countries, specifically

170. There is currently a window of opportunity for legislative and diplomatic advocacy to try to change this trend as the United States negotiates additional CLOUD Agreements. This Article focuses instead on doctrinal paths to increase defense access to cross-border evidence through the courts. However, I hope that by identifying the general issue and the specific disparities in the United States–United Kingdom and United States-Australia agreements, the Article will inspire others to try to change this trend through policy channels.

171. 18 U.S.C. § 2713. This Article uses the phrase *U.S. technology companies* to include companies subject to U.S. jurisdiction, regardless of where they are headquartered.

172. *See* Daniel Richman, *Foreign Equities and Informational Restraints on U.S. Prosecutors*, LAWFARE (June 1, 2022, 2:01 PM), https://www.lawfareblog.com/foreign-equities-and-informational-restraints-us-prosecutors [https://perma.cc/S74X-PN59] (noting that the CLOUD Act allows U.S. authorities to "rely on domestic legal processes to obtain data controlled by U.S.-accessible tech platforms but stored abroad," without the same level of cooperation with foreign governments as other data-gathering techniques); Daskal, *supra* note 141, at 11 (explaining that the CLOUD Act requires internet service providers "to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the location of the data").

173. *See* 18 U.S.C. § 2702(b)(2) (providing that data-service providers may divulge data as authorized by several provisions); *id.* § 2703 (stating that "[a] governmental entity may require . . . disclosure"); *id.* § 2713 (requiring the preservation and disclosure of certain records "regardless of whether such . . . information is located within or outside of the United States").

174. *See* Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 384–86 (2018) (providing an overview of the concept of comity and explaining courts' application of it).

those that have entered into CLOUD Agreements.[175] Absent that provision, courts will continue to resolve conflict-of-laws problems with a common law comity analysis to weigh the competing interests from both nations and decide which law to prioritize.[176]

Overall, CLOUD Act orders are narrower than MLATs and CLOUD Agreements in that they reach solely companies subject to U.S. federal or state jurisdiction. However, they are more powerful in that they can require disclosures that violate foreign laws, including foreign laws not pierced or waived by treaty, as long as a court conducts the proper comity analysis and decides to prioritize U.S. law over the foreign sovereign interest.

Once again, these CLOUD Act advantages accrue to law enforcement without parallel benefits for criminal defense counsel. The proximate cause of this disparity is somewhat circuitous in that it involves the SCA statute in which the CLOUD Act is embedded. The SCA is a federal statute from 1986 designed to protect privacy in electronic communications data stored with intermediary service providers such as Google or Facebook.[177] For over a decade, courts have interpreted the SCA to categorically bar criminal defense counsel from subpoenaing U.S. service providers for the contents of another's stored electronic communications, regardless of how necessary that evidence is to exonerate the wrongfully accused—and regardless of whether the data are stored within the United States or abroad.[178] The contents of a communication include things like the body of an email, photographs, text messages, and voicemails. Courts have categorically banned defense counsel from compelling technology companies to disclose this type of data even though the SCA expressly permits law enforcement to compel disclosures of

175. 18 U.S.C. § 2703(h). More specifically, the CLOUD Act specifies a statutory procedure for motions to quash based on conflicts with foreign laws from "qualifying foreign government[s]," *id.* § 2703(h)(3), and defines a "qualifying foreign government" as one that has entered into a CLOUD Agreement with the United States and that provides certain substantive and procedural protections to electronic communication-service providers, *id.* § 2703(h)(1)(A). At the moment, with only two CLOUD Agreements (with the United Kingdom and Australia) in place, almost no foreign nations qualify for the statutory comity analysis.

176. The CLOUD Act also preserves "any other grounds to move to quash." *Id.* § 2703(h)(2)(A)(ii). Hence, conflicts with foreign laws from nonqualifying foreign nations should still trigger a standard common law comity analysis. *See* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct., 482 U.S. 522, 544 (1987) (declining to hold that comity considerations required applying Hague Evidence Convention procedures "without prior scrutiny in each case of the particular facts, sovereign interests, and likelihood that resort to those procedures will prove effective"); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442(1)(c) (AM. L. INST. 1987) (listing factors for courts to consider in deciding whether to order discovery of evidence located outside the United States).

177. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–10 (2004) (explaining that the SCA was designed to provide privacy protections for computer network usage).

178. Wexler, *supra* note 24, 2724–25.

the same types of data from the same sources.[179] As a result, under current law, the CLOUD Act entitles law enforcement seeking communications contents stored abroad to a one-stop shop in U.S. courts, while defense investigators have no ability at all to compel access to this category of evidence from these sources.[180]

D. Increased Salience[181]

It is difficult to know precisely how many criminal defense investigations the rise of the global cloud coupled with new foreign data privacy laws will obstruct or chill.

Evidence located abroad has long been relevant to some U.S. criminal defendants[182] and, for the reasons described in subpart I(A), has long been challenging for those defendants to obtain. Cases alleging terrorism,[183] espionage,[184] treason,[185] drug and human trafficking,[186] immigration crimes,[187] international financial fraud,[188] and extraterritorial prosecutions of crimes committed abroad[189] have implicated transnational facts and cross-border investigations for years.[190] There are even existing procedural rules that recognize criminal defense needs to engage in cross-border evidence gathering. The Federal Rules of Criminal Procedure, for instance, permit U.S. defendants, in "exceptional circumstances," to ask a judge for

179. *Id.* at 2724 & n.11, 2741, 2789.

180. Notably, under current law, defendants are entitled to subpoena U.S. service providers for non-content data such as date, time, and address metadata, including data stored abroad. *See* 28 U.S.C. § 1783 (stating that a court may issue a subpoena to produce a document if the court finds it to be in the interest of justice). This is because nothing in the SCA precludes disclosures of non-content data to nongovernmental entities. *See* 18 U.S.C § 2702 (defining no such prohibition).

181. Jack M. Balkin, *The Path of Robotics Law*, 6 CAL. L. REV. CIR. 45, 46–47 (2015) (suggesting that "[w]hen we consider how a new technology affects law, our focus should [be] . . . on what features of social life the technology makes newly *salient*").

182. *See, e.g.*, Richardson, *supra* note 36, at 64–67, 79 n.76 (noting an increase in transnational crime and describing cases in which the defendants were denied access to cross-border evidence that could have exonerated them).

183. *E.g.*, United States v. Yunis, 924 F.2d 1086 (D.C. Cir. 1991).

184. *E.g.*, United States v. Rosen, 240 F.R.D. 204 (E.D. Va. 2007).

185. *E.g.*, Gillars v. United States, 182 F.2d 962 (D.C. Cir. 1950).

186. *E.g.*, United States v. Borelli, 336 F.2d 376 (2d Cir. 1964).

187. *See, e.g.*, Scolaro, *supra* note 120, 1702 n.74 (framing immigration fraud as a bilateral criminal issue).

188. *E.g.*, United Kingdom v. United States, 238 F.3d 1312 (11th Cir. 2001).

189. *See generally* Farbiarz, *supra* note 36 (lamenting the lack of process available to defendants for cross-border evidence gathering in extraterritorial prosecutions of crimes committed outside the United States).

190. *See generally* Tuerkheimer, *supra* note 36 (discussing the globalization of criminal acts and law enforcement).

discretionary approval to depose foreign witnesses abroad.[191] And the Walsh Act authorizes U.S. courts to issue criminal subpoenas to U.S. persons located abroad.[192] Certainly, for those categories of defendants who have long needed to access evidence located abroad, obstacles from new foreign data privacy laws will only make matters worse.

At the same time, cross-border evidence issues are poised to affect more, and more categories of, criminal defense investigations than ever before. This is because the internet and global cloud substantially increase the likelihood that evidence will be digital and that digital evidence will be located abroad. Cybercrime—hacking, credit card fraud, botnets, identity theft, and trafficking in digital contraband—is one piece of this story.[193] For example, in May 2022, the United States joined twenty-one other countries in signing the Second Additional Protocol to the Budapest Convention on Cybercrime to respond to "the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions."[194] But the issue reaches beyond even the high-stakes context of computer crimes.

In fact, digital evidence relevant to investigating *any* type of crime can now be located abroad, even common crimes like theft, robbery, and assaults that allegedly occur entirely within U.S. borders.[195] One reason is the rise of

191. FED. R. CRIM. P. 15. This rule does not state it applies only to witnesses who will testify voluntarily, but courts appear unlikely to grant such a motion if the witness is likely to refuse to testify. *See, e.g.*, United States v. Rosen, 240 F.R.D. 204, 208 (E.D. Va. 2007) (explaining that the court previously denied a Rule 15 motion because the foreign deponents initially refused to testify, and thus granting that motion "would have been an exercise in futility").

192. 28 U.S.C. § 1783. *But see* Gillars v. United States, 182 F.2d 962, 978 (D.C. Cir. 1950) (indicating that aliens residing abroad cannot be compelled to respond to such a subpoena).

193. *See* JOSEPHINE WOLFF, CYBERINSURANCE POLICY: RETHINKING RISK IN AN AGE OF RANSOMWARE, COMPUTER FRAUD, DATA BREACHES, AND CYBERATTACKS 1–2 (2022) (describing a transnational malware attack); Jennifer Daskal, *Transnational Government Hacking*, 10 J. NAT'L SEC. L. & POL'Y 677, 677 (2020) (noting that cyber investigations often involve devices or data stored abroad); Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1090 (2017) ("Increasingly, criminals use the dark web to facilitate crimes traditionally conducted in the physical world . . . ."); Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58, 61–63 (2017) (detailing international cooperation between law enforcement in investigating "a wide range of crimes," particularly computer crimes).

194. *Second Additional Protocol to the Cybercrime Convention Adopted by the Committee of Ministers of the Council of Europe*, COUNCIL OF EUR. (Nov. 17, 2021), https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe [https://perma.cc/ZD4W-Q9MX].

195. *Cf.* Briggerman et al., *supra* note 110, at 36 ("As criminal cases become increasingly cross-border in nature, the need for defendants to obtain evidence located abroad has become more common."). For discussion of platform-enabled international crimes, such as "genocide, war crimes, [and] crimes against humanity," see generally Rebecca J. Hamilton, *Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators to Commit Atrocities*, 63 B.C. L. REV. 1349, 1414 (2022).

digital evidence generally. "Informational capitalism"[196] has led intermediary service providers to collect and store vast new quantities of data about our locations, habits, associations, physical and mental health, communications, photographs, calendars, documents, and more.[197] Those reams of data are potentially relevant evidence for investigating all kinds of crimes, both to convict and to exonerate.[198]

Another reason is that, because of the global cloud, relevant digital evidence can now be stored anywhere in the world.[199] People in one country can use digital services offered by companies headquartered anywhere else,[200] and those companies may choose to store their users' data in a different jurisdiction entirely.[201] Even electronic communications that start and terminate within a single country may be routed internationally and stored abroad.[202] Meanwhile, efficiency and business purposes can lead service providers to store data outside the jurisdictions where they were

196. COHEN, *supra* note 18, at 5 (defining "informational capitalism" as "the alignment of capitalism as a mode of production with informationalism as a mode of development").

197. *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 258 (2019) ("[Google learns] from your content, context, and behavior not only through search, e-mail, and calendar activity but also from the data in your phone, including movement, location, activities, voice, and apps.").

198. *See, e.g.*, Andrew Guthrie Ferguson, *Digital Habit Evidence*, 72 DUKE L.J. 723, 726 (2023) (explaining that digital evidence "revealing of private habits and workplace practices—will soon become evidence in court" and that "because many civil and criminal trials turn on finding facts in the absence of human witnesses or physical proof, digital evidence will become central to filling in the gaps").

199. *See, e.g.*, United States v. Microsoft Corp., 138 S. Ct. 1186, 1187 (2018) (per curiam) (noting that emails sought by warrant were stored at a datacenter in Ireland); *In re* Search of Info. Associated with [Redacted]@gmail.com, No. 16-mj-00757, 2017 WL 3445634, at *2 (D.D.C. July 31, 2017) ("Google produced subscriber information, chats, 'Google Plus' profile records, search and browsing history, and certain Gmail content (including attachments and headers), but did not produce attachments to emails if those 'documents were determined to be stored on servers located outside the United States.'"); *see also* Swire & Hemmings, *supra* note 49, at 704, 708–09 (discussing the transborder nature of electronic data).

200. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 363 (2015) (describing jurisdictional issues in a case involving data held by Yahoo! China given that Yahoo! is headquartered in the United States); *see* Woods, *supra*, note 57, at 772–73 (discussing a hypothetical involving seeking a warrant for data in Cyprus or Israel).

201. *See, e.g.*, Schwartz, *supra* note 58, at 1693 (describing how the Second Circuit in *Microsoft v. United States* focused on specifically where the sought-after data were located). It is not even clear that technology companies themselves know where user data is stored within their networks of databases. *See* Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, or Where It Goes: Leaked Document*, VICE (Apr. 26, 2022, 8:02 AM), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes [https://perma.cc/WHM2-7C39] (revealing that Facebook does not know where its data goes).

202. *See* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473, 475 (2016) (providing an example of how an email sent from an individual in California to an individual in New York may nevertheless be routed through another country like the United Kingdom or Canada before arriving at its final destination).

created.[203] Indeed, service providers may not even always know where their user data flows.[204]

Further, all those data can be relevant to common crimes with no other international nexus beyond the data's storage location. In the words of the DOJ, foreign law enforcement entities sending mutual legal assistance requests to the United States "often seek electronic information related to individuals or entities located in other countries, and the only connection of the investigation to the United States is that the evidence happens to be held by a U.S.-based global provider."[205] Hence, for example, Brazilian law enforcement might contact a U.S. service provider seeking to access U.S. user data stored in the United States, Brazilian user data stored in the United States, Brazilian user data stored in Brazil, or all of the above. In short, digital evidence concerning routine crimes committed entirely inside one country can be stored on servers located in another.

While the number of criminal defense investigations that seek cross-border data (or would if adequate process existed) remains opaque, some data on cross-border digital evidence requests by law enforcement do exist and provide insight into the scale of the issue. During the six months between January and June 2021, foreign government agencies sent Meta 147,398 requests for data concerning 240,354 accounts,[206] Google 98,442 requests for data concerning 244,089 accounts,[207] and Twitter 9,400 requests concerning

203. *See* Swire & Daskal, *supra* note 50, at n.21 (noting that data storage location is often determined by business considerations). Sometimes processing data within the United States will make the most business sense. For instance, Meta recently threatened to terminate services in Europe if European authorities block it from transferring EU user data to the United States for processing. Isobel Asher Hamilton, *Meta Warns It Could Pull Instagram and Facebook in Europe If It Loses a Data-sharing Rule*, BUS. INSIDER (Feb. 8, 2022, 6:34 AM), https://www.businessinsider.com/meta-could-pull-instagram-facebook-europe-data-sharing-ruling-2022-2 [https://perma.cc/25FY-A88R].

204. *See, e.g.*, Sam Biddle, *Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data*, THE INTERCEPT (Sept. 7, 2022, 6:00 AM), https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/ [https://perma.cc/88YE-TH3Y] (explaining that during the Cambridge Analytica scandal, Facebook engineers stated during hearings that they were not clear where data was held at any given time).

205. U.S. DEP'T OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 2 (2019), https://www.justice.gov/criminal-oia/page/file/1153436/download [https://perma.cc/4B44-AC4B].

206. *Government Requests for User Data*, META, https://transparency.fb.com/data/government-data-requests/ [https://perma.cc/CG2W-9HVY] (reporting, for the period of January to June 2021, a total of 211,055 requests concerning 351,471 accounts, of which 63,657 requests concerning 111,117 accounts came from U.S. law enforcement).

207. *Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview [https://perma.cc/FLB9-SU2U] (reporting, for the period of January to June 2021, a total of 149,349 requests concerning 359,683 accounts, of which 50,907 requests concerning 115,594 accounts came from U.S. law enforcement).

19,100 accounts.[208] And, as mentioned previously, the European Commission has reported that "[m]ore than half of all [European] investigations include a cross-border request to access e-evidence."[209] Even if criminal defense investigations seeking cross-border disclosures amounted to a relatively small percentage of their law enforcement counterparts, the number of affected cases would be significant.

To be sure, to the extent that U.S. technology companies like Meta, Google, and Twitter control the pertinent data, U.S. investigators (whether law enforcement or defense counsel) will enjoy a buffer against impediments to cross-border evidence gathering.[210] Perhaps for that reason,[211] U.S. law enforcement has, to date, reported more modest cross-border evidence concerns than their European counterparts.[212] As Peter Swire and Justin Hemmings put it, "the United States is a primary exporter of electronic

208. *Information Requests*, TWITTER, https://transparency.twitter.com/en/reports/information-requests.html#2021-jan-jun [https://perma.cc/4DJH-LNX9] (reporting, for the period of January to June 2021, a total of 12,400 government requests concerning 26,200 accounts, of which 3,000 requests concerning 7,100 accounts came from the United States).

209. European Commission Report, *supra* note 50, at 14 (emphasis omitted). Notably, there must be orders of magnitude more total criminal investigations in Europe than the number of cross-border evidence requests documented in U.S. technology companies' transparency reports. For comparison, approximately 344,00 crimes were reported in New York State alone in the year 2021. *New York State Index Crime*, N.Y. STATE: CRIM. JUST. SERVS., https://www.criminaljustice.ny.gov/tableau_index_crime.htm [https://perma.cc/Z6TD-DQ4R] (Oct. 2022). It is unclear from the European Commission Report how to resolve this discrepancy. Perhaps the European Commission survey reflects the number of European criminal investigations that could *potentially* benefit from access to cross-border digital evidence, if such evidence were easily available, rather than the number that actually "include a cross-border request to access e-evidence." European Commission Report, *supra* note 50, at 14 (emphasis omitted). Nonetheless, this figure is commonly cited in policy debates. *See, e.g.*, *E-evidence—Cross-border Access to Electronic Evidence*, EURO. COMM'N, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence [https://perma.cc/EG9W-PY35] (noting that "[m]ore than half of all criminal investigations today include a cross-border request to access electronic evidence").

210. For a discussion of the CLOUD Act provision empowering U.S. law enforcement to direct U.S. companies to disclose data that the companies control and store abroad, see *supra* note 180 and accompanying text.

211. Another possible reason is that the large geographic size of the United States places efficiency demands on U.S. service providers to store U.S. user data within the United States, whereas the smaller size of EU member states means that a single data center is more likely to serve multiple European countries.

212. According to the DOJ, obstructions to U.S. law enforcement accessing cross-border digital evidence thwart "dozens of investigations" each year. Downing Testimony, *supra* note 51, at 5. This statement concerns the period from July 14, 2016, which marks the issuance of the Second Circuit's opinion in *Microsoft v. United States*, to June 15, 2017, when Richard Downing, Acting Deputy Assistant Attorney General at the DOJ, testified at the "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era" House Committee hearing. *See id.* (discussing the Second Circuit's decision).

evidence,"[213] meaning U.S. law enforcement receive more requests to assist foreign agencies' evidence-gathering efforts than they make for assistance from the same.[214]

However, the buffer of U.S. tech supremacy is hardly inevitable.[215] Consider TikTok. In August 2020, Chinese service provider TikTok[216] had 100 million monthly active users in the United States[217]—nearly 40% of the active monthly U.S. users that Facebook had by early 2021[218]—and control over U.S. users' TikTok data has been the subject of intense geopolitical negotiations.[219] During the six months between January and June 2021, U.S. law enforcement sent TikTok 801 requests concerning 1,385 accounts.[220] Meanwhile, Chinese service provider WeChat—which, by 2020, had the international version of its app installed 100 million times from the Google

213. Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance*, *in* BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 395, 400 (Fred H. Cate & James X. Dempsey eds., 2017). This has meant that the burdens of the slow letters rogatory system have primarily fallen on law enforcement in other countries. *See, e.g.*, Chinmayi Arun, *How to Prevent Another Bulli Bai or Sulli Deals*, INDIAN EXPRESS (Feb. 18, 2022, 9:14 AM), https://indianexpress.com/article/opinion/columns/preventing-bulli-bai-sulli-deals-to-protect-muslim-women-7779008/ [https://perma.cc/FZH9-BXHG] (indicating that criminal process in countries outside the United States is thwarted because U.S. laws do not allow companies "to share private information unless the request is made through an onerous process," which "is a pre-internet process for law enforcement requests from other countries").

214. Swire & Hemmings, *supra* note 213, at 400.

215. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 287 (2015) (stating that the assumption that the internet is in essence a "U.S.-based Internet, dominated by U.S.-based companies and U.S.-based users" is "obsolete").

216. TikTok belongs to the Chinese company ByteDance, which is headquartered in Beijing and domiciled in the Cayman Islands. Chloe Mayer, *Is TikTok Owned by the Chinese Communist Party?*, NEWSWEEK (Oct. 17, 2022, 1:31 PM), https://www.newsweek.com/tiktok-owned-controlled-china-communist-party-ccp-influence-1752415 [https://perma.cc/DV29-3GRY].

217. Alex Sherman, *TikTok Reveals Detailed User Numbers for the First Time*, CNBC (Aug. 24, 2020, 6:33 PM), https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html [https://perma.cc/8REU-XTPY].

218. *Facebook Monthly Active Users (MAU) in the United States and Canada as of 2nd Quarter 2022*, STATISTA (2022), https://www.statista.com/statistics/247614/number-of-monthly-active-facebook-users-worldwide/ [https://perma.cc/W3L2-ZQGK] (reporting that Facebook had 259 million monthly active users by the end of the first quarter of 2021).

219. *See, e.g.*, Kim Lyons, *The TikTok and Oracle 'Trusted Technology Partner' Deal Might Really Happen*, THE VERGE (Mar. 11, 2022, 10:41 AM) (recognizing the intense need for policy and business solutions to TikTok's use and storage of data by its Chinese parent company after then-President Trump announced a potential ban on the app), https://www.theverge.com/2022/3/11/22972530/tiktok-oracle-china-bytedance-trump-cfius [https://perma.cc/YWM4-KSMP]. TikTok's U.S. user data is currently stored in both Virginia and Singapore. Echo Wang & David Shepardson, *Exclusive: TikTok Nears Oracle Deal in Bid to Allay U.S. Data Concerns-Sources*, REUTERS (Mar. 10, 2022, 4:13 PM), https://www.reuters.com/technology/exclusive-tiktok-nears-deal-with-oracle-store-its-data-sources-2022-03-10/ [https://perma.cc/X8RU-L3WX].

220. *Information Requests Report: January 1, 2021–June 30, 2021*, TIKTOK (Dec. 2, 2021), https://www.tiktok.com/transparency/en-us/information-requests-2021-1/ [https://perma.cc/22VL-FBUK].

Play Store alone[221]—has yet to publish data on law enforcement requests.[222] The more U.S. users adopt foreign services, the more the United States will become an importer of electronic evidence. And the more likely it will be that foreign data privacy laws will obstruct or chill U.S. investigations of all kinds—from terrorism charges to low-level drug offenses and minor property crimes.

Finally, forensic technologies present another circumstance where foreign data can be relevant to investigating even those alleged criminal acts that occur offline and within U.S. borders. U.S. law enforcement agencies may purchase forensic software tools and services from foreign companies that store methodological information about their products on foreign servers.[223] For instance, Cellebrite is an Israeli company that provides hacking services to law enforcement customers worldwide "to reveal the user lock passcode and extract the data" from digital devices.[224] Cellebrite's customer contract asserts that personal data that Cellebrite extracts and analyzes for its law enforcement customers "may be transferred or stored outside . . . the country where [the] Customer is located in order to carry out the Services."[225] If the personal data must be transferred to foreign servers for the services to be performed, then, presumably, methodological details about the data processing and analysis are also located abroad. The personal data may ultimately be transferred back to the U.S. law enforcement customer, while methodological details concerning the service that are potentially relevant to the defense may not be.[226] Corporations often claim that disseminating such methodological details would violate their trade secret rights or undermine the efficacy of their tools by risking leaks that

221. Ronald Deibert, Opinion, *WeChat Users Outside China Face Surveillance While Training Censorship Algorithms*, WASH. POST (May 7, 2020, 3:54 PM), https://www.washingtonpost.com/opinions/2020/05/07/wechat-users-outside-china-face-surveillance-while-training-censorship-algorithms/ [https://perma.cc/EJ96-CQQN].

222. A Canadian public interest organization called the Citizen Lab confirmed that the company does monitor documents and images transmitted through international as well as Chinese domestic WeChat accounts. *See id.* (stating that even communications of WeChat users whose accounts are registered *outside* of China are under political surveillance).

223. *See, e.g.*, Stephanie Kirchgaessner, *How NSO Became the Company Whose Software Can Spy on the World*, THE GUARDIAN (July 23, 2021, 7:00 AM), https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world [https://perma.cc/P57D-EE2D] (explaining that NSO, an Israeli surveillance company, created a deal that would allow other foreign-country clients to expand their use of spyware through targeting mobile phones in other countries).

224. General Terms and Conditions, CELLEBRITE § 1.1.1, https://legal.cellebrite.com/CB-us-us/index.html [https://perma.cc/9BQY-V46N].

225. *Id.* § 10.3.

226. *See generally* Steven M. Bellovin, Matt Blaze, Susan Landau & Brian Owsley, *Seeking the Source*: *Criminal Defendants' Constitutional Right to Source Code*, 17 OHIO ST. TECH. L.J. 1 (2021) (noting how defendants do not always have access to the source code or underlying software that produces evidence, such as from computer forensic analysis, used against them).

could educate future criminals about how to evade detection.[227] Hence, they may choose to store any methodological data locally in the foreign jurisdiction in a deliberate effort to shield that information from discovery.

In sum, the internet and global cloud are poised to increase the salience of cross-border evidence, to render historical asymmetries in cross-border investigations ever more urgent and consequential, and to lead to new disparities in law enforcement and defense access to data located abroad.[228]

***

Privacy law debates are missing consideration of criminal defense investigations. Secreted beneath this oversight, a system of laws and treaties advantages law enforcement investigations of guilt over criminal defense investigations of innocence. This system includes longstanding disparities in law enforcement versus defense access to MLATs for cross-border evidence gathering as well as new disparities that U.S. policymakers are producing by creating special CLOUD Agreements for law enforcement alone to circumvent foreign data privacy laws. Meanwhile, new CLOUD Act rules for law enforcement to obtain court orders that unilaterally compel U.S. technology companies to disclose data stored on foreign servers are also distorted to disadvantage defense investigations. This is because these new procedures layer on top of a pre-existing statutory disparity: U.S. courts have construed the SCA to categorically bar criminal defense counsel from subpoenaing technology companies for the contents of another's stored electronic communications, regardless of where those contents are located or how necessary they may be to prove innocence. The results are privacy protections that systematically advantage the search for evidence of guilt over that for evidence of innocence.

---

227. *See generally* Christina Koningisor, *Police Secrecy Exceptionalism*, 123 COLUM. L. REV. (forthcoming 2023) (describing and critiquing anti-circumvention justifications for police secrecy); Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKELEY TECH. L.J. 503 (2019) (arguing that anti-circumvention concerns produce excessive law enforcement secrecy); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (documenting and arguing against companies' assertions of trade secrecy to block criminal discovery); Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659 (2018) (proposing policy changes to foster greater transparency of criminal justice technologies in response to trade secret assertions).

228. The effects will almost certainly be distributed unequally. Well-resourced defendants may hire white-collar defense attorneys with longstanding collaborations with other attorneys in foreign countries who can assist their investigations. *E.g.*, *Cartel–Government Investigations & Litigation*, MILLER & CHEVALIER, https://www.millerchevalier.com/practice-area/cartel-government-investigations-litigation [https://perma.cc/LTQ8-77K3]. Indigent defendants will generally lack that option.

II. Definitional Logic: Executive Versus Judicial Powers

For years, former prosecutors,[229] members of the criminal defense bar,[230] and legal scholars[231] have all criticized the MLAT procedures that empower law enforcement—but not the defense—to compel access to relevant evidence across borders. And for years, criminal defendants have raised constitutional challenges to these disparities in court.[232] The existing constitutional challenges have been similar. They have drawn on the "right to present a defense," which is guaranteed by Fifth and Fourteenth Amendment due process rights combined with Sixth Amendment rights to confrontation and compulsory process.[233] Among other things, the right to

229. *See, e.g.*, Tuerkheimer, *supra* note 36, at 364 (saying that with regards to the imbalance caused by prosecutorial access to evidence via MLATs, "the ends of the criminal justice system are defeated if its judgments are founded on a partial presentation of the facts, an inevitable result when only one side has meaningful power of process"); Farbiarz, *supra* note 36, at 680 (suggesting a lack of justification for prosecutors' refusal to use MLAT power on behalf of defendants).

230. *E.g.*, Abbell, *supra* note 98, at 21 ("Preventing criminal defendants from utilizing MLATs to obtain evidence from abroad with which to defend themselves places them at an unfair disadvantage to the government, and raises constitutional concerns."); Briggerman et al., *supra* note 110, at 33 (highlighting the lack of visibility defendants and their counsel have in the MLAT process).

231. *See, e.g.*, Richardson, *supra* note 36, at 84 (describing as a flaw the fact that prosecutors have access to MLAT procedures while criminal defendants do not).

232. *See* Briggerman et al., *supra* note 110, at 31 ("[C]ourts overwhelmingly have declined to require the government to act on behalf of the defendant, including in cases in which the defendant argues that the evidence is exculpatory.").

233. *See, e.g.*, Steele, *supra* note 23, at 1635–37 (describing the right to present a defense); Colin Fieman & Alan Zarky, *When Acquittal Is Just a Tweet Away: Obtaining Historical Social Media Evidence from Service Providers that Use the SCA as a Shield*, CHAMPION, Nov. 2015, at 26, 34 ("Closely related to the Sixth Amendment's right to compulsory process is the Fifth Amendment's guarantee of due process and a defendant's 'right to a fair opportunity to defend against the [government's] accusations.'" (quoting Chambers v. Mississippi, 410 U.S. 284, 294 (1973) (alteration in original)); United States v. Jefferson, 594 F. Supp. 2d 655, 674 (E.D. Va. 2009) (finding that "a defendant's constitutional right to compulsory process is not implicated by a court's refusal to order the Executive Branch to invoke the MLA Treaty in favor of a defendant"); United States v. Rosen, 240 F.R.D. 204, 215 (E.D. Va. 2007) (holding that exculpatory evidence available through an MLAT did not "implicate a defendant's constitutional right to compulsory process"); Escalante v. Lizarraga, No. ED CV 17-850-R, 2018 WL 2938520, at *8–9 (C.D. Cal. Apr. 16, 2018) (finding that the MLAT did not grant a defendant a "right to compulsory process for witnesses outside the jurisdiction of the United States" and there was no "clearly established . . . constitutional right to compel the attendance of a witness [at a trial]" when the witness is not in the United States), *adopted by* No. 5:17-cv-00850-R, 2018 WL 2771211 (C.D. Cal. June 5, 2018); United States v. Sedaghaty, 728 F.3d 885, 917 (9th Cir. 2013) (determining that the district court lacked the power to compel process under an MLAT since that was a power left to the Executive Branch (citing *Rosen*, 240 F.R.D. at 213–14)); United States v. Hutchins, No. 17-CR-124, 2018 WL 1695499, at *2 (E.D. Wis. Apr. 6, 2018) (determining that the Due Process Clause did not require the government to provide the defendant with an MLAT request, given that defendants generally do not have "any private right . . . to enforce its terms"); United States v. Kapordelis, No. 1:04-CR-249, 2007 WL 9717351, at *6 (N.D. Ga. Apr. 20, 2007) (finding that a defendant's compulsory process right was not violated because the "United States ha[d] no subpoena power" over MLAT witnesses).

present a defense entitles defendants to bring as-applied challenges to statutes, rules, or orders that block their access to or introduction of exculpatory evidence.[234] To date, these challenges to the MLAT regime have yet to succeed in court.[235] Why have they failed?

This Part begins with current constitutional doctrine. It contends that a core reason constitutional challenges to asymmetrical MLAT procedures have proven unpersuasive to courts to date is definitional.[236] Courts have defined the underlying compulsory process power at issue in cross-border MLAT disclosures as an executive rather than a judicial power.[237] Courts have then concluded that the right to present a defense does not attach to Executive Branch investigative powers.[238] Hence, even *categorically* denying the defense access to the MLAT investigative procedures does not violate the right to present a defense, regardless of how essential the evidence at issue might be. With no rights violation, there is no reason for the court to provide a remedy, even one well within the standard judicial toolkit such as a sanction, adverse inference instruction, or dismissal. Unfortunately for criminal defendants, existing right-to-present-a-defense doctrine does not clearly contradict this rationale.[239]

Moreover, courts' reliance on a definitional distinction between Executive and Judicial Branch powers to uphold disparities between law-enforcement- and defense-investigative capacity extends beyond the MLAT context. Courts have also relied on this distinction to uphold prosecutors' refusal to grant use or derivative use immunity to defense witnesses.[240] And similar logic is at play in DOJ arguments attempting to justify law enforcement's exclusive access to certain types of court orders pursuant to the SCA. Underlying the shape of these doctrines are balance-of-powers concerns that discourage courts from ordering police and prosecutors to exercise Executive Branch powers on behalf of the defense.[241]

---

234. *See infra* at notes 288–294 and accompanying text.

235. See the cases cited *infra* notes 321–323.

236. Thank you to David Sklansky for initially suggesting that I consider the distinction between Judicial and Executive Branch compulsory process powers when analyzing privacy asymmetries.

237. *See infra* notes 243–245 and accompanying text.

238. *See infra* notes 279–281 and accompanying text.

239. *See infra* notes 263–268 and accompanying text.

240. *See infra* notes 269–270 and accompanying text.

241. *See* Funk, *supra* note 72, at 12–14 (explaining how the MLAT process is available only to the prosecution); *see also EPCA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Const., C.R., & C.L. of the H. Comm. on the Judiciary*, 111th Cong. 128 (2010) (written statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP) ("Judges, for their part, can be reluctant based on separation of power issues to require the government to use its investigative powers at the behest of a defendant . . . .").

After identifying the definitional logic embedded in existing doctrine and explaining the broad applicability of that logic, this Part develops a proposal for how criminal defense attorneys should respond. Defendants could conceivably challenge the doctrine in a variety of ways. They could argue that the executive-judicial distinction is superficial; perhaps the underlying power at issue in any of these circumstances is shared between the Executive and Judicial Branches.[242] Alternatively, defendants could concede that the underlying power is executive, yet argue that the accused should be entitled to use executive as well as judicial compulsory process powers. While each of these tactics is worth exploring, the following discussion suggests a different path designed to work within the bounds of current doctrine.

In circumstances where the defense is categorically denied access to compulsory process powers that are available to law enforcement, I propose that defense counsel should attempt to define the powers as judicial and then argue that the right to present a defense attaches. Next, I explain precisely how attachment of the right to present a defense would improve defense access to evidence, again within the constraints of current doctrine. Finally, I detail some limitations of existing alternative constitutional arguments, which make the proposed definitional approach more attractive in comparison. In doing so, I do not mean to endorse the current doctrine but rather to provide a practical path forward for defense advocacy within the realities of existing constraints.

A. The Definitional Logic in Current Constitutional Doctrine

1. MLATs and Extraterritoriality.—Courts have repeatedly upheld the constitutionality of MLAT asymmetries by reasoning that MLAT processes are Executive Branch treaties and that defendants' compulsory process rights do not reach the powers of the Executive Branch. Accordingly, in rejecting one defendant's constitutional argument for access to MLAT process, a court in the Eastern District of Virginia explained that "the right to compulsory process . . . cannot be stretched to include compelling the invocation of treaty process powers available only to the Executive Branch."[243] In another case

242. *Cf.* Erwin Chemerinsky, *Enemy Combatants and Separation of Powers*, 1 J. NAT'L SEC. L. & POL'Y 73, 82 (2005). Discussing the fundamental nature of collaboration between government branches, Professor Chemerinsky explains:

> [T]he system of checks and balances in the Constitution requires that two branches of government concur for almost every major form of government action. Enacting a law generally requires both legislative and executive action. Putting a person in prison requires executive prosecution and judicial conviction.

Id. See also INS v. Chadha, 462 U.S. 919, 951 (1983) (noting that "powers delegated to the three Branches" are "not 'hermetically' sealed from one another").

243. United States v. Rosen, 240 F.R.D. 204, 215 (E.D. Va. 2007).

in the same jurisdiction, the court rejected a similar constitutional argument because "a defendant's constitutional right to compulsory process is not implicated by a court's refusal to order the Executive Branch to invoke the MLA Treaty in favor of a defendant."[244] And the D.C. Circuit held that the government had no obligation to use its MLAT powers to secure tapes and transcripts from an alleged co-conspirator's trial abroad because the mere authority "to seek" evidence does not impose any disclosure obligations on the government.[245]

There can be exceptions triggered by governmental misconduct. For instance, courts may find a due process or Sixth Amendment violation if the government caused the defense to lose access to foreign evidence, such as by deporting material defense witnesses in bad faith[246] or by denying such witnesses entry into the country to testify voluntarily.[247] But absent such misconduct, courts reason that defendants lack rights to compulsory process "when *a court itself* cannot compel" access to that evidence.[248] Courts themselves generally lack power to compel cross-border evidence disclosures.[249] Hence, the reasoning goes, defendants' rights to compulsory process also do not reach beyond the territorial United States.[250] As a result, courts have found that defendants' lack of access to MLATs does not violate the constitutional right to compulsory process.[251]

---

244. United States v. Jefferson, 594 F. Supp. 2d 655, 674 (E.D. Va. 2009).

245. United States v. Mejia, 448 F.3d 436, 444–45 (D.C. Cir. 2006).

246. *See, e.g.*, United States v. Leal-Del Carmen, 697 F.3d 964, 970–71 (9th Cir. 2012) (explaining that "[t]he question of bad faith . . . turns on what the government knew at the time it deported [a] witness," since the government may not deport a witness when it has information suggesting the witness could offer exculpatory information); *see also* United States v. Pena–Gutierrez, 222 F.3d 1080, 1085 (9th Cir. 2000) (holding that there is no bad faith where the government did not depart from normal procedures or pursue an unfair tactical advantage); United States v. Valenzuela-Bernal, 458 U.S. 858, 872–73 (1982) (saying that deporting a witness, without more, "is not sufficient to establish a violation of the Compulsory Process Clause of the Sixth Amendment or the Due Process Clause of the Fifth Amendment" and that "some showing that the evidence lost would be both material and favorable to the defense" is required to demonstrate such a violation).

247. *E.g.*, United States v. Theresius Filippi, 918 F.2d 244, 247–48 (1st Cir. 1990) (finding the government's deliberate failure to act to enable the defendant's only material witness to enter the United States "constitute[d] a violation of the Sixth Amendment right to compulsory process and, derivatively, the right to due process protected by the Fifth Amendment").

248. *Rosen*, 240 F.R.D. at 214.

249. *See* United States v. Moussaoui, 382 F.3d 453, 463–64 (4th Cir. 2004) (referencing the "well established and undisputed principle" that district courts do not have process power over foreign nationals abroad); United States v. Zabaneh, 837 F.2d 1249, 1259–60 (5th Cir. 1988) (stating that U.S. courts do not have the power to subpoena non-citizen witnesses abroad); *cf.* Anna VanCleave, *The Right to Inter-Sovereign Disclosure in Criminal Cases*, 2013 WIS. L. REV. 1407, 1436–37 (explaining that state courts cannot enforce subpoenas against the federal government due to sovereign immunity).

250. *See, e.g.*, *Theresius Filippi*, 918 F.2d at 247 (stating that this limitation on the right of compulsory process is supported by practical considerations).

251. *E.g.*, United States v. Jefferson, 594 F. Supp. 2d 655, 674 (E.D. Va. 2009).

Notably, the exceptions for governmental misconduct show that this doctrine cannot be explained solely by courts' limited institutional capacity to enforce certain constitutional norms.[252] When courts find governmental misconduct, they can remedy the harm in a variety of ways, such as by imposing sanctions, issuing adverse inference orders, striking evidence, or dismissing cases.[253] Courts could presumably use the same tools to remedy harms from MLAT asymmetries, even though they may lack the power to order cross-border evidence disclosures directly.[254] That most courts have chosen not to deploy those remedies when the government simply refuses to use its MLAT processes on behalf of the defense shows not that courts lack power to provide a remedy but rather that the courts have decided there is no harm to remedy.

Moreover, little to nothing in current right-to-present-a-defense doctrine clearly contradicts the conclusion that the right does not entitle defendants to assistance from Executive Branch powers.[255] The due process requirements at the core of the doctrine—the *Brady* requirement that prosecutors disclose evidence that is known, favorable, and material to the defense[256] and the principle articulated in *Wardius v. Oregon*[257] that criminal discovery requires reciprocity[258]—both concern the judicial power to manage discovery

252. *Cf.* Lawrence Gene Sager, *Fair Measure: The Legal Status of Underenforced Constitutional Norms*, 91 HARV. L. REV. 1212 (1978) (propounding that the federal Judiciary has, "failed to enforce . . . provision[s] of the Constitution to [their] full conceptual boundaries" because of institutional concerns like federalism and judicial competence). Thank you to Mark Gergen for suggesting that I clarify how the availability of remedies interacts with the doctrines that refuse to apply the right to present a defense to Executive Branch powers.

253. *See, e.g.*, Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998) (stating that an adverse inference instruction may restore "the prejudiced party to the same position [it] would have been in"); United States v. Bowen, 799 F.3d 336, 340 (5th Cir. 2015) (affirming grant of new trial based on prosecutorial misconduct); United States v. Chapman, 524 F.3d 1073, 1077 (9th Cir. 2008) (affirming dismissal of indictment based on prosecution's failure to disclose to the defense more than 650 pages of documents); *In re* Howes, 39 A.3d 1, 5 (D.C. 2012) (disbarring a federal prosecutor for his misconduct).

254. *But see* Farbiarz, *supra* note 36, at 680–81 (suggesting there is no reason why the government could not make a request through MLAT procedures on behalf of defendants, and also that the government is more likely to do so when pressed by a court).

255. *See* 1 EDWARD J. IMWINKELRIED & NORMAN M. GARLAND, EXCULPATORY EVIDENCE § 2-2 (5th ed. 2021) (summarizing the different views on the source of the constitutional right to present a defense and the strength of the right).

256. Brady v. Maryland, 373 U.S. 83, 87 (1963) ("We now hold that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.").

257. 412 U.S. 470 (1973).

258. *Id.* at 472 ("We hold that the Due Process Clause of the Fourteenth Amendment forbids enforcement of alibi rules unless reciprocal discovery rights are given to criminal defendants.").

disclosures between parties before the court.[259] Meanwhile, the confrontation right implicates courts' power to control the examination of witnesses.[260] And the few times that the Supreme Court has found a violation of the Compulsory Process Clause have focused on criminal defendants' rights to assistance from judicial compulsory process powers,[261] not Executive Branch investigatory powers.[262]

2. Fifth Amendment Privilege and Use Immunity.—The reasoning from MLAT cases regarding defendants' rights to assistance from Judicial versus Executive Branch powers extends beyond the MLAT context to other disparities between law enforcement and defense investigations. Consider use and derivative use immunity. Prosecutors deploy this form of immunity to defeat the Fifth Amendment privilege, which entitles witnesses to refuse to provide testimony that would risk self-incrimination.[263] The prosecution can compel a witness who asserts the Fifth Amendment privilege to testify anyway by promising not to use the testimony to prosecute the witness, thereby effectively eliminating the risk of self-incrimination.[264]

---

259. *See* FED. R. CRIM. P. 16(d) (defining the court's role in regulating discovery); *see also* FED. R. CRIM. P. 16 advisory committee's note to 1944 amendment (observing that courts sometimes ordered limited discovery disclosures to criminal defendants even before the enactment of Rule 16).

260. *See, e.g.*, Crawford v. Washington, 541 U.S. 36, 51 (2004) (noting the Confrontation Clause "applies to 'witnesses' against the accused"); FED R. EVID. 611 ("The court should exercise reasonable control over the mode and order of examining witnesses and presenting evidence . . . .").

261. *See* Washington v. Texas, 388 U.S. 14, 22–23 (1967) (holding that a statute excluding certain defense witness testimony from admission into evidence violated the Compulsory Process Clause); Rock v. Arkansas, 483 U.S. 44, 52, 62 (1987) (finding an Arkansas per se rule excluding post-hypnosis testimony from admission into evidence violated a defendant's right to testify on their own behalf, which the Court stated was derived from several constitutional provisions including the Compulsory Process Clause); Crane v. Kentucky, 476 U.S. 683, 690–91 (1986) (finding error when a court excluded a defendant's evidence, and locating that right in the Compulsory Process Clause amongst other constitutional provisions); Chambers v. Mississippi, 410 U.S. 284, 294, 302 (1973) (stating that the right to "call witnesses in one's own behalf" is "essential to due process," and finding that exclusion of certain defense testimony violated the right). *But see* United States v. Scheffer, 523 U.S. 303, 306–307, 317 (1998) (upholding as constitutional Military Rule of Evidence 707, which as a per se rule excluded all polygraph evidence).

262. *See* United States v. Valenzuela-Bernal, 458 U.S. 858, 872–73 (1982) (finding that the government's deportation of a potential defense witness did not violate the Compulsory Process Clause).

263. *See generally* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEXAS L. REV. 767 (2019) (discussing the barrier that the Fifth Amendment privilege against self-incrimination imposes to orders compelling a suspect to enter a password to decrypt a locked device).

264. *See* 18 U.S.C. §§ 6002–03 (providing that federal prosecutors may obtain a court order compelling testimony from a witness who claims the right against self-incrimination, but that such subsequent testimony may not be used "against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order");

Prosecutors rarely use their immunity power to benefit defendants.[265] Rather, they generally refuse to immunize witnesses who would provide exculpatory testimony for the defense.[266] Nonetheless, most courts have found that this refusal does not violate the Constitution.[267] The majority rule in current doctrine is that neither the court nor the defense have power to grant immunity to defense witnesses.[268] A leading justification for this asymmetry in current case law is that, "as a general rule[,] the Government may not be required to confer immunity for the benefit of the defense"[269] because immunity is "pre-eminently a function of the Executive Branch."[270] In other words, the power to grant immunity, and thus the derivative ability to exercise compulsory process in this circumstance, belongs to the

IMWINKELRIED & GARLAND, *supra* note 255, § 2-3[b] n.271 (explaining how "use and derivative use" immunity may supplant a witness's Fifth Amendment privilege); JAMES E. PFANDER, CASES WITHOUT CONTROVERSIES: UNCONTESTED ADJUDICATION IN ARTICLE III COURTS 125–127 (2021) (discussing immunized testimony under the Fifth Amendment privilege and the Judiciary's role in the immunization process).

265. Robin Deborah Mass, Note, *Witness for the Defense: A Right to Immunity*, 34 VAND. L. REV. 1665, 1687 (1981). Mass describes this phenomenon:

> The impact of grants of statutory immunity on the federal criminal justice system is evidenced by the dramatic increase in immunity requests since the Supreme Court held in *Kastigar* that use immunity is coextensive with the fifth amendment. . . . As the Government has increased its reliance on immunity as a prosecutorial tool, defense attorneys have challenged the unfettered discretion of the prosecutor . . . when the prosecutor refuses to honor requests to immunize these witnesses.

Id. See also United States v. Alessio, 528 F.2d 1079, 1080–81 (9th Cir. 1976) (noting that the prosecutor immunized one of its witnesses but refused to immunize three witnesses for the defense); Earl v. United States, 361 F.2d 531, 534 (D.C. Cir. 1966) (stating that the prosecutor and federal district court had refused to grant immunity to a defense witness under the statute that was in effect at the time); United States v. Morrison, 535 F.2d 223, 225 (3d Cir. 1976) (noting that the prosecutor had not only refused to immunize an exculpatory defense witness but went so far as to intimidate her by reminding her multiple times that he would charge her with her past or current crimes if she took the stand).

266. *Cf.* James F. Flanagan, *Compelled Immunity for Defense Witnesses: Hidden Costs and Questions*, 56 NOTRE DAME LAW. 447, 456 (1981) (discussing reasons why use immunity incentivizes broad testimony, which can obstruct ongoing or future investigations).

267. IMWINKELRIED & GARLAND, *supra* note 255, § 11-4[a].

268. *See* Reid H. Weingarten & Brian M. Heberlig, *The Defense Witness Immunity Doctrine: The Time Has Come to Give It Strength to Address Prosecutorial Overreaching*, 43 AM. CRIM. L. REV. 1189, 1191 (2006) (saying that prosecutors are not required to grant immunity to defense witnesses because immunity is considered a function of the Executive Branch). *See generally* Robert M. Schoenhaus, Annotation, *Right of Defendant in Criminal Proceeding to Have Immunity from Prosecution Granted to Defense Witness*, 4 A.L.R.4th 617 (1981) (collecting cases where courts have analyzed requests for use immunity for defense witnesses).

269. United States v. Dolah, 245 F.3d 98, 105 (2d Cir. 2001), *overruled on other grounds by* Crawford v. Washington, 541 U.S. 36 (2004).

270. United States v. Turkish, 623 F.2d 769, 776 (2d Cir. 1980).

Executive alone, and defendants lack a constitutional right to assistance from that executive power.[271]

Once again, as in the MLAT context, government misconduct may trigger some exceptions. Courts may find a due process violation if prosecutors withhold a grant of immunity with the bad-faith intent of distorting the fact-finding process.[272] But in general, courts have upheld the prosecution's exclusive power to grant use immunity to compel testimony from witnesses who assert their Fifth Amendment privilege, and have not found constitutional error because the defense lacks access to the same power.[273]

Notably, again as with MLAT asymmetries, courts have some power to remedy harms to defendants from a witness's assertion of the Fifth Amendment privilege. If a prosecution witness testifies against the defendant during direct examination and then invokes the Fifth Amendment privilege to block cross-examination, courts may strike the direct testimony from the record.[274] That type of remedy lies squarely within the judicial prerogative to regulate the presentation of evidence.[275] But in these circumstances, it is the unfairness of a witness using the privilege selectively as both a sword and a shield that courts are remedying, not the exclusivity of prosecutorial power to deploy use immunity to pierce the privilege in the first place.

B. The Broad Applicability of the Definitional Logic

Although the issue has yet to be widely litigated, definitional distinctions between Executive and Judicial Branch powers could be used to

271. *See* Carter v. United States, 684 A.2d 331, 338–39 (D.C. 1996) (en banc) (rejecting the "concept of judicially imposed immunity" for a witness who invokes the right against self-incrimination (emphasis omitted)).

272. *E.g.*, United States v. Quinn, 728 F.3d 243, 247 (3d Cir. 2013); United States v. Straub, 538 F.3d 1147, 1156 (9th Cir. 2008).

273. *See* Schoenhaus, *supra* note 268, at 625 (presenting cases where "defendant did not have an adequate basis for compelling an immunity grant" in the context of considering whether it violated the Constitution to deny immunity to defense witnesses).

274. *Cf.* Douglas v. Alabama, 380 U.S. 415, 419 (1965) (finding a violation of the Confrontation Clause where a witness's alleged confession incriminating the defendant may have been treated as direct testimony by the jury, and where the witness's assertion of the Fifth Amendment privilege against self-incrimination prevented the defense from engaging in cross-examination). Neither are defense counsel entirely powerless to remedy the harms of a prosecutor's refusal to grant immunity to a defense witness. Defense counsel can inform the jury of the prosecution's refusal and use that refusal to suggest that the prosecution's investigation was "shoddy or one-sided." Richman, *supra* note 13, at 687. This defense strategy would shift the burden to the prosecution to respond and explain what reason, if any, justified the prosecution's refusal to immunize a defense witness in any given case. *See id.* at 691–92 (discussing possible prosecutorial arguments to explain to a jury why a plausible investigative lead was not pursued).

275. *See* FED R. EVID. 611 (directing the court to "exercise reasonable control over the mode and order of examining witnesses").

challenge—or to justify—a far broader set of disparities between law enforcement and criminal defense investigative capacity.

For instance, consider the SCA. Recall that courts have interpreted the SCA to categorically bar criminal defense counsel from subpoenaing U.S. service providers for the contents of another's stored electronic communications, even though law enforcement can compel disclosures of the same evidence from the same sources.[276] Case law examining constitutional challenges to the SCA bar on criminal defense subpoenas is less developed than in the MLAT or use immunity contexts. The D.C. Court of Appeals has speculated that a categorical bar on criminal defense subpoenas to technology companies seeking stored electronic communications contents might impermissibly interfere with a criminal defendant's right to compulsory process in some cases, but determined that the constitutional issue was not properly before the court in that case.[277] Similarly, the California Supreme Court has stated that the SCA bar on criminal defense subpoenas raises "important constitutional and related issues," but has to date declined to decide them.[278]

Nonetheless, a similar underlying logic from the MLAT and use immunity contexts—the view that the right to present a defense tracks the powers of the Judiciary, not those of the Executive—is at play in these cases as well. This is because the DOJ's recurring argument in favor of the SCA asymmetry is to analogize SCA orders to Rule 41 warrants and Title III wiretap authorizations, and then to characterize all three of these procedures as powers of the Executive Branch.[279] For instance, in a recent case before the D.C. Court of Appeals, federal prosecutors argued that SCA procedural rules that "provide for one-sided access to the government" are unremarkable because "the search warrant provisions of Federal Rule of Criminal Procedure 41(b) and the wiretap application provisions of 18 U.S.C. § 2516(1) [(Title III)] both provide a means for the government to obtain evidence without a mechanism for defendants to do so."[280] From the DOJ's perspective then, these three provisions—the SCA, Rule 41, and Title III—grant "means" or powers to the Executive Branch.[281] If the DOJ is correct, then the definitional logic from the MLAT and use immunity doctrines would counsel courts to reject any right-to-present-a-defense challenges to these statutes.

276. 18 U.S.C. § 2703; Warshak v. United States, 532 F.3d 521, 523–24 (6th Cir. 2008) (en banc).

277. Facebook, Inc. v. Wint, 199 A.3d 625, 633–34 (D.C. 2019).

278. Facebook, Inc. v. Superior Ct. of San Diego Cnty., 471 P.3d 383, 402 (Cal. 2020).

279. *E.g.*, Brief for the United States at 27, *Wint*, 199 A.3d 625 (No. 18-CO-0958).

280. *Id.*

281. *Id.*

However, an alternative way to understand these three provisions is that they *constrain* rather than *empower* the government. In other words, SCA procedures, Rule 41 warrants, and Title III wiretap authorizations may not be a "means for the government to obtain evidence" at all.[282] Rather, they may be the opposite: limits on the manner in which law enforcement may exercise its investigative powers.[283] In that case, it would be entirely unremarkable for the statutes to apply solely to the government, as solely the government would be bound to obtain these forms of procedural authorization.

Further, when viewed as constraints on the government, the statutes themselves reveal little about the source of the underlying compulsory process power at issue or about defendants' entitlement to use that power. For instance, while the DOJ is correct that the Rule 41 statutory warrant procedures are available solely to government applicants,[284] warrants in general are not exclusively available to the government. On the contrary, criminal defendants have a right to warrants in certain circumstances, such as bench warrants for the compelled production of defense witnesses who have been properly subpoenaed and failed to appear.[285] Hence, the underlying search and seizure power affiliated with a warrant is at least partially within the power of the courts to initiate without a governmental applicant and is available for use by the defense apart from the Rule 41 procedures.[286]

The upshot is that, at least within the logic of current doctrine, a core issue for the constitutionality of compulsory process asymmetries is definitional: Does the underlying compulsory process power that the defense

282. *Contra id.*

283. *See, e.g.*, Steagald v. United States, 451 U.S. 204, 212 (1981) (observing that the "purpose of a warrant is to allow a neutral judicial officer to assess whether the police have probable cause to make an arrest or conduct a search" and characterizing the warrant as a "checkpoint between the Government and the citizen"); *id.* at 213 ("An arrest warrant . . . primarily serves to protect an individual from an unreasonable seizure. A search warrant . . . safeguards an individual's interest in the privacy of his home and possessions against the unjustified intrusion of the police."); *see also* Lange v. California, 141 S. Ct. 2011, 2022 (2021) (characterizing warrants at common law as "strong protection from government intrusion"); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1235–40 (2016) (describing how nineteenth-century warrant requirements limited the instances where the government could search or seize a person or item).

284. *See* FED. R. CRIM. P. 41(b) (authorizing magistrate judges to issue warrants "[a]t the request of a federal law enforcement officer or an attorney for the government").

285. *See, e.g.*, United States v. Simpson, 992 F.2d 1224, 1229–30 (D.C. Cir. 1993) (holding that a trial court's refusal to issue a bench warrant for a defense witness violated the Compulsory Process right); *see also* BARBARA E. BERGMAN & JOHN D. CLINE, EVERYTRIAL CRIMINAL DEFENSE RESOURCE BOOK § 47:1 (2022) (discussing the process for requesting a bench warrant from the court after having properly subpoenaed a witness who is necessary for a defense theory).

286. There are a variety of potential sources of authority for courts to issue compulsory process *sua sponte*, including warrants. Among these sources is the courts' inherent authority. *See* Chambers v. NASCO, Inc., 501 U.S. 32, 43–46 (1991) (discussing inherent powers of federal courts); All Writs Act, 28 U.S.C. § 1651(a) (providing that federal courts "may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law").

seeks to operationalize emanate from the Executive or from the Judiciary? If the answer is the Executive, then the current MLAT and use immunity case law suggest that access to that form of compulsory process power may be categorically denied to the defense. In contrast, if the underlying power emanates at least in part from the Judiciary, then the right to present a defense may attach and entitle defendants to access the pertinent investigative process.[287]

C. Implications for Criminal Defense Strategy

If defendants were to persuade a court that a particular form of compulsory process is judicial, and hence is subject to the right to present a defense, what benefits would that definitional success provide to defense investigations? This subpart explains that clarifying that any particular type of compulsory process is subject to a right-to-present-a-defense constitutional claim would strengthen defendants' ability to pierce statutory or other barriers to accessing that form of process.

1. Right-to-Present-a-Defense Challenges.—The right to present a defense supports as-applied challenges to statutes or other rules that block defense use of compulsory process. As the following paragraphs describe, there is a substantially high bar to succeeding on such a claim. Yet, if the right attaches, then at least defendants cannot be *categorically* denied the use of compulsory process powers.

The most pertinent part of the current right-to-present-a-defense doctrine concerns defendants' compulsory process rights to pierce statutory and common law evidentiary privileges.[288] While legal scholars have long

287. For a discussion of the types of circumstances in which the right to present a defense can pierce a conflicting statutory barrier to accessing evidence, see *infra* section II(C)(1).

288. *See generally* IMWINKELRIED & GARLAND, *supra* note 255, § 10 (outlining the various evidentiary privileges that exclude logically relevant evidence). The right-to-present-a-defense doctrine has many heads, the majority of which speak to defendants' rights at trial to *introduce* evidence that the defense already possesses. *See id.* § 10-2[a] (distinguishing between situations in which a defendant already possesses the information and in which they do not and discussing whether the same standard should apply to both situations). The Supreme Court has danced around the related issue of defendants' rights to defeat statutory barriers to *subpoena* evidence but has yet to squarely answer the question. *See* Commonwealth v. Barroso, 122 S.W.3d 554, 558 (Ky. 2003) ("The United States Supreme Court has yet to decide whether a criminal defendant has the right to compel a third party to produce exculpatory information protected by an absolute privilege."); *cf.* Davis v. Alaska, 415 U.S. 308, 320–321 (1974) (holding that defendant's constitutional right to cross-examine a witness for bias outweighed a facially absolute statute protecting the confidentiality of a juvenile offender's record); Roviaro v. United States, 353 U.S. 53, 64 (1957) ("The desirability of calling [an undercover narcotics agent] as a witness, or at least interviewing him in preparation for trial, was a matter for the accused rather than the Government to decide."). Nonetheless, there is a compelling argument to conclude that if the right to present a defense entitles defendants to introduce certain evidence at trial, then it should also entitle them to subpoena that same evidence.

debated precisely how compulsory process rights should interact with evidentiary privileges,[289] Edward Imwinkelried and Norman Garland have documented that "the vast majority of contemporary lower courts assume that the accused's constitutional right applies to evidentiary privileges and that if the excluded evidence is reliable and material enough, the right can override a privilege."[290] Scholarly debates aside then, in practice defendants can and often do use the right to present a defense to defeat statutory barriers to subpoenaing evidence on a case-by-case basis by showing that their need for the evidence outweighs the public policy interest in nondisclosure.[291]

In these cases courts consider, on the one hand, whether the evidence that the defense seeks would be cumulative or unique, its reliability, its

---

This is because the Court initially derived defendants' right to introduce evidence from their right to compel its production. *See* Washington v. Texas, 388 U.S. 14, 23 (1967) ("The Framers of the Constitution did not intend to commit the futile act of giving to a defendant the right to secure the attendance of witnesses whose testimony he had no right to use."). So, where there is a right to introduce evidence, there should also be a right to compel its production. Justice Alito's dissent in *Pena–Rodriguez* supports this reading by extending the right to present a defense to investigations, not merely admissibility. Alito explains that the constitutional bar on arbitrary or disproportionate exclusionary rules applies broadly to investigations of jurors, and hence to rules beyond the particular evidence rules that control admissibility at trial. Pena–Rodriguez v. Colorado, 137 S. Ct. 855, 874–76 (2017) (Alito, J., dissenting); *but see* IMWINKELRIED & GARLAND, *supra* note 255, § 10-2 (suggesting that the right to present a defense should apply with lesser force to pre-trial discovery based on the relative importance of evidentiary privileges at that stage).

289. *See* IMWINKELRIED & GARLAND, *supra* note 255, § 10-3 (describing debates); *see also, e.g.*, Jackson Teague, Note, *Two Rights Collide: Determining When Attorney-Client Privilege Should Yield to a Defendant's Right to Compulsory Process or Confrontation*, 58 AM. CRIM. L. REV. 487, 489 (2021) (critiquing current approaches to analyzing the intersection between privileges and the right to confront a witness, and recommending a new standard "for when attorney-client privilege should yield to the Sixth Amendment"); Martin A. Hewett, Note, *A More Reliable Right to Present a Defense: The Compulsory Process Clause After* Crawford v. Washington, 96 GEO. L.J. 273, 281–82 (2007) (discussing the Supreme Court's interpretation of the Compulsory Process Clause as providing the right to present a defense); Alfred Hill, *Testimonial Privilege and Fair Trial*, 80 COLUM. L. REV. 1173, 1173–74 (1980) (discussing the increased prevalence of courts finding that assertions of privilege violate the Compulsory Process Clause and explaining resulting problems); Akhil Reed Amar, *Sixth Amendment First Principles*, 84 GEO. L.J. 641, 699 (1996) ("A defendant should be given compulsion parity with the government."); Robert Weisberg, Note, Defendant v. Witness*: Measuring Confrontation and Compulsory Process Rights Against Statutory Communications Privileges*, 30 STAN. L. REV. 935, 937 (1978) (analyzing the interplay between communications privileges and defendants' Sixth Amendment rights, and recommending procedural solutions for resolving clashes between the two); Peter Westen, *Compulsory Process II*, 74 MICH. L. REV. 191, 199 (1975) (noting how the Wigmorean view, which is that the right of compulsory process does not override other immunities and privileges, was rejected by the Supreme Court as conflicting with the Framers' intent); Peter Westen, *The Compulsory Process Clause*, 73 MICH. L. REV. 71, 121 (1974) (indicating the Supreme Court's shift towards recognizing "that certain kinds of discovery have a sounder conceptual basis in the compulsory process clause"); Christopher Slobogin, *The Right to Voice Reprised*, 40 SETON HALL. L. REV. 1647, 1649 (2010) (arguing that there "is a limited constitutional right to tell exculpatory mental-state stories through experts" and advocating for a "generalized right to voice").

290. IMWINKELRIED & GARLAND, *supra* note 255, § 10-3.

291. *See id.* § 10-4 ("[C]ourts employ a balancing test to determine whether the accused's constitutional right to present a defense overrides an exclusionary rule of evidence.").

probative value, and its importance to the defense case.[292] On the other hand, courts consider whether applying the conflicting statute to bar the defense from accessing evidence would be "arbitrary or disproportionate to the purposes [the statute is] designed to serve."[293] The result is that statutes or other rules barring defense access to evidence are unconstitutional as applied if they block access to important defense evidence and are arbitrary or disproportionate.[294]

This line of right-to-present-a-defense doctrine does not depend on *asymmetry* between law enforcement and defense investigative power. In the evidentiary privilege cases, for instance, a block on compulsory process can violate defense rights even if the same block applies symmetrically to law enforcement. So too, asymmetry on its own does not necessarily make a block on compulsory process unconstitutional. A multitude of asymmetries exist in the criminal legal system, including the prosecution's burden of proof,[295] the defendant's Fifth Amendment privilege against self-incrimination,[296] and the character evidence rules,[297] and many of these asymmetries have non-arbitrary justifications.[298]

Nevertheless, asymmetrical barriers that allow law enforcement more or better access to evidence than they allow to criminal defense investigators—including MLATs, Rule 41 warrants, Title III wiretaps, and SCA court orders for stored communications contents—are particularly promising targets for right-to-present-a-defense challenges. This is because, as multiple prior commentators have proposed, asymmetry that advantages prosecution evidence over that of the defense can indicate that a rule is "arbitrary or disproportionate."[299] Martin Hewett is the most recent commentator to advance this view.[300] Previously, Richard Nagareda argued

292. *Id.* § 2-4[a].

293. Rock v. Arkansas, 483 U.S. 44, 55–56 (1987).

294. *Id.*

295. Richard A. Posner, *An Economic Approach to the Law of Evidence*, 51 STAN. L. REV. 1477, 1505 (1999) (justifying prosecution's burden of proof as a leveling mechanism to counterbalance defense investigators' limited resources).

296. U.S. CONST. amend. V.

297. FED. R. EVID. 404(a)(2).

298. *See, e.g.*, Anna Roberts, *Asymmetry as Fairness: Reversing a Peremptory Trend*, 92 WASH. U. L. REV. 1503, 1549–50 (2015) (arguing that certain asymmetries in criminal procedure make the system more fair, not less). Indeed, Peter Westen has argued that even the asymmetry in the notice of alibi rule that the Supreme Court struck down as unconstitutionally arbitrary in *Wardius v. Oregon* was actually rational. Westen, *supra* note 289, at 181 n.512 (justifying the notice of alibi statute that the Court struck down in *Wardius v. Oregon* as "not irrational" because of differences between the prosecution's and defense's needs for pre-trial discovery of alibi witnesses).

299. *Rock*, 483 U.S. at 56.

300. *See* Hewett, *supra* note 289, at 281–83 (suggesting that discrimination between prosecution and defense was an "important rationale" for the Court's finding that exclusionary rules of evidence were unconstitutionally arbitrary in *Washington v. Texas* and *Holmes v. South Carolina*).

for "a compelling interest test to discriminatory evidence rules."[301] Akhil Amar advanced a related theory of "compulsion parity" whereby in his view "asymmetric witness rules" violate the Compulsory Process Clause.[302] Edward Imwinkelried has argued more broadly that evidence rules that condition admissibility "on the identity of the evidence's proponent" effect a "classification of persons" for purposes of the Equal Protection Clause and should trigger intermediate scrutiny that "can be a powerful weapon against evidentiary doctrines that . . . introduce asymmetries into the adversary system."[303] And Peter Tague concluded that evidence rules that asymmetrically disadvantage criminal defendants "may be unconstitutional under the equal protection clause."[304]

Concededly, the Supreme Court has thinned the definition of unconstitutional arbitrariness and disproportionality over time.[305] But right-to-present-a-defense challenges are worthwhile even if they merely trigger an *inquiry* into whether a bar on criminal defense access to evidence is unconstitutionally arbitrary or disproportionate. At the least, that inquiry would force the prosecution to articulate a justification for the bar on defense access to compulsory process. The arguments thus surfaced could support efforts to amend offensive rules and statutes, would help to educate legislators and rule makers about the downstream consequences of their

301. Richard A. Nagareda, *Reconceiving the Right to Present Witnesses*, 97 MICH. L. REV. 1063, 1146 (1999).

302. Amar, *supra* note 289, at 699–700. For a discussion of the idea that if the MLAT procedure is unavailable to the defense, MLATs are unconstitutional because they create "an imbalance in compulsive power between prosecution and defense," see Robert Neale Lyman, *Compulsory Process in a Globalized Era: Defendant Access to Mutual Legal Assistance Treaties*, 47 VA. J. INT'L L. 261, 282 (2006).

303. Edward J. Imwinkelried, *Of Evidence and Equal Protection: The Unconstitutionality of Excluding Government Agents' Statements Offered as Vicarious Admissions Against the Prosecution*, 71 MINN. L. REV. 269, 286, 299, 301–02, 314–15 & n.266 (1986).

304. Peter W. Tague, *Perils of the Rulemaking Process: The Development, Application, and Unconstitutionality of Rule 804(b)(3)'s Penal Interest Exception*, 69 GEO. L.J. 851, 858 (1981).

305. The Court's most recent formulation in *Holmes v. South Carolina*, 547 U.S. 319 (2006), defines unconstitutionally "arbitrary" rules as "rules that exclude[] *important* defense evidence but that d[o] not serve *any* legitimate interests," *id.* at 324–25 (emphasis added), and that also infringe a "weighty interest" of the accused, *id.* at 324, 326 (quoting United States v. Scheffer, 523 U.S. 303, 308 (1998)). Logically, this must mean an interest *other* than freedom from arbitrary or disproportionate exclusions, without more. Substantive due process case law also suggests that arbitrary conduct, without more, is not unconstitutional. *See* Richard H. Fallon, Jr., *Some Confusions About Due Process, Judicial Review, and Constitutional Remedies*, 93 COLUM. L. REV. 309, 325 (1993) ("[T]he Supreme Court has not definitively held that all arbitrary official conduct violates the Constitution, and it suggested in one recent case that conduct could be 'arbitrary . . . in a constitutional sense' only if it shocked the conscience." (footnote omitted) (quoting Collins v. City of Harker Heights, 503 U.S. 115, 128 (1992))). Under *Holmes*, then, even a rule that excludes "important" defense evidence is not unconstitutionally arbitrary if it serves any legitimate governmental interest, and even one that does not so serve may still be constitutional if it infringes less than a "weighty interest." *Cf.* Jane R. Bambauer & Toni M. Massaro, *Outrageous and Irrational*, 100 MINN. L. REV. 281, 297–98 (2015) (discussing the "rational basis" test).

statutory or rule language, and would, hopefully, increase care and attention to defense access to evidence in the future.

2. The Limitations of Existing Alternatives.—While the right-to-present-a-defense definitional strategy described above imposes a high bar for success, the argument substantially improves over a number of existing alternatives.

One alternative recurring argument raised in MLAT and other contexts is that courts should require prosecutors to use their unique investigative powers to compel access to exculpatory evidence on behalf of the defense.[306] Prior critics of this argument have observed that it introduces a new problem of its own: requiring the defense to seek assistance from the prosecution also requires the defense to notify the prosecution about the evidence it seeks, potentially exposing trial strategy and other information that the defense would prefer to keep confidential.[307] But another obstacle for the success of this prosecutorial assistance proposal is finding a hook in current doctrine that would enable a court to order the prosecution to use Executive Branch powers on the defendant's behalf.

Some commentators have attempted to hook the prosecutorial assistance proposal to the due process requirements of *Brady v. Maryland* and its progeny.[308] *Brady* and its progeny mandate that the prosecution team disclose known, favorable, material evidence to the defense.[309] A central difficulty with this approach, however, is that the *Brady* doctrine does not generally compel law enforcement to actively investigate new evidence on the defendant's behalf.[310] Another way to understand this is that a defendant's *Brady* due process rights arise from the judicial power to manage discovery disclosures between parties before the court, meaning disclosures of

306. *E.g.*, Farbiarz, *supra* note 36, at 677, 679.

307. Zwillinger & Genetski, *supra* note 23, at 593.

308. *E.g.*, Briggerman et al., *supra* note 110, at 32.

309. *See* Brady v. Maryland, 373 U.S. 83, 87 (1963) (holding that prosecutors may not suppress evidence that is favorable to the accused if it would be material to either guilt or punishment); *see also* United States v. Agurs, 427 U.S. 97, 112 (1976) (discussing the materiality standard); Giglio v. United States, 405 U.S. 150, 154 (1972) (same); United States v. Bagley, 473 U.S. 667, 669 (1985) (same); Kyles v. Whitley, 514 U.S. 419, 432 (1995) (characterizing *Brady* disclosures as an "affirmative duty" for prosecutors).

310. *See* United States v. Hughes, 211 F.3d 676, 688 (1st Cir. 2000) (noting that "the government has no duty to produce evidence outside of its control" (citing United States v. Sepulveda, 15 F.3d 1161, 1179 (1st Cir. 1993))). Limited exceptions prove the rule. *See, e.g.*, Jonathan Abel, *Cop-"Like" ("[]"): The First Amendment, Criminal Procedure, and the Regulation of Police Social Media Speech*, 74 STAN. L. REV. 1199, 1207, 1236 (2022) (arguing that *Brady* and its progeny may impose a duty on the prosecution team to "proactively monitor" police officer's speech if but only if an "officer's credibility problems . . . are known to some member of the prosecution team").

information that the parties already have, and do not more generally reach Executive Branch investigative conduct.

A more nuanced version of the prosecutorial assistance argument is the view that judges could route around their limited power to compel prosecutors to exercise Executive Branch powers by instead incentivizing them to do this with the threat of finding a due process violation on some other ground. Michael Farbiarz, a legal scholar and former Assistant United States Attorney in the Southern District of New York, recently advocated this position in the MLAT context.[311] Farbiarz contends that courts should declare a due process violation where defendants have less access to evidence located abroad than they would have to evidence within the United States.[312] The threat of the due process violation would, in turn, "strongly incentivize prosecutors . . . to obtain the foreign evidence and witnesses on behalf of the defendant."[313] Yet this argument once again fails to fully grapple with the distinction between Judicial and Executive Branch process. Attending to that distinction opens the door to a counterargument that defendants already have equal access to *process* for evidence located within the United States and abroad; in each case, they have access to judicial compulsory process with all its limitations and not to Executive Branch treaty or search and seizure powers with all their capacity.

A second recurring argument that advocates and commentators have raised draws from the Court's statement in *Wardius v. Oregon* that due process regulates the balance of forces between the prosecution and defense.[314] For instance, Frank Tuerkheimer has drawn on *Wardius* to criticize MLAT asymmetries, arguing that "the due process clause requires some sort of balance in terms of access to evidence."[315] *Wardius* struck down a state statute that required defendants to give pre-trial notice of alibi witnesses without requiring prosecutors to give reciprocal notice of alibi rebuttal witnesses.[316] The Court explained that due process requires that, "in the absence of a strong showing of state interests to the contrary, discovery . . . be a two-way street."[317] Applying this principle to the SCA asymmetry, criminal defense counsel have argued that it is "fundamentally unfair that the government can obtain the contents of

311. *See* Farbiarz, *supra* note 36, at 680 ("[I]f due process were thought to require obtaining a foreign document for the defense, it is hard to see why the United States could not, on behalf of the defendant, make an MLAT request for that document.").

312. *Id.* at 677.

313. *Id.* at 679.

314. 412 U.S. 470, 474 (1973); *see* Fieman & Zarky, *supra* note 233, at 34 ("A constitutional problem arises from the sharp difference between how the SCA (in the view of social media providers) treats the prosecution and defense.").

315. Tuerkheimer, *supra* note 36, at 366.

316. *Wardius*, 412 U.S. at 475.

317. *Id.*

communications . . . while the defense is statutorily barred from obtaining them by any means, no matter how exculpatory they might be."[318]

A major limitation of this position, however, is that *Wardius*—like *Brady*—concerned discovery between parties, not access to evidence possessed by nonparties.[319] Courts would therefore have to read *Wardius* expansively to touch the MLAT and new CLOUD Agreement scenarios. This is an unlikely outcome given that the Supreme Court has not revisited or even discussed the *Wardius* holding in depth since issuing it in 1973.[320] Further, the lower courts have shown little enthusiasm for reading *Wardius* broadly.[321] Indeed, some jurisdictions have directly rejected efforts to extend *Wardius*'s reciprocity principle from discovery between parties to investigations of nonparties.[322] Defense counsel could attempt to route around this problem by arguing that asymmetrical investigative powers effectively compel nonreciprocal disclosures between the parties because they entitle solely the government to engage in confidential investigations through partnerships with foreign law enforcement or via delayed-notice subpoenas to technology companies. Hence, the government can collect information without notice reaching the defense, while it is more challenging for the defense to do the same without notice reaching the government. Yet, courts have rejected analogous arguments in similar circumstances.[323] In short, applying

318. Fieman & Zarky, *supra* note 233, at 34; *see also* Informal Response to Petition for Writ of Mandate/Prohibition and/or Other Extraordinary Relief, *supra* note 29, at 37–38 (arguing that the SCA statutory scheme creates an "inherent imbalance in the ability of the parties to seek information" and "creates a structurally unfair process"); Opposition to Facebook's Motion to Quash Subpoena Duces Tecum; Points and Authorities in Support of SDT, *supra* note 29, at 4 (citing *Wardius* for the proposition that "a statute cannot lawfully foreclose a criminal defendant from obtaining information while simultaneously providing an avenue of discovery for law enforcement").

319. Fieman & Zarky, *supra* note 233, at 34.

320. As of a Westlaw search on March 5, 2023, the Supreme Court has cited the opinion a mere fourteen times.

321. *See, e.g.*, Davis v. Workman, 695 F.3d 1060, 1078 (10th Cir. 2012) ("The holding in *Wardius* is only that the government cannot require the defendant to disclose an alibi defense witness unless the government will also disclose its witnesses rebutting that defense."); United States v. Harbin, 250 F.3d 532, 540 (7th Cir. 2001) (stating, in discussing *Wardius*, that "[d]ue process does not require absolute symmetry between rights granted to the prosecution and those afforded the defense").

322. *See* People v. Valdez, 281 P.3d 924, 954–55 (Cal. 2012) (finding that the defendant's claim that the prosecution was impermissibly granted nonreciprocal discovery benefits failed because the trial court's order did not "tilt the balance toward the state"); State v. Percy, 548 A.2d 408, 415–16 (Vt. 1988) (finding no reciprocity issue when the defense lacks access to a witness, as long as the defense has access to information the prosecution obtained through its interview of the witness). Most problematic for the defense position, the Oregon Supreme Court has explicitly rejected a *Wardius* reciprocity challenge to the SCA's asymmetrical subpoena bar, concluding it would require an excessive expansion of current doctrine, and relegating its discussion of the issue to a footnote. State v. Bray, 422 P.3d 250, 260 n.10 (Or. 2018).

323. *See, e.g.*, *Valdez*, 281 P.3d at 954–55 (asserting that lack of reciprocity in discovery does not necessarily violate due process, including in discovery concerning opposing party witnesses).

Wardius's "balance of forces" principle to nonparty subpoenas is an uphill battle.

***

A definitional logic is at work in current right-to-present-a-defense doctrine. If a court defines an underlying investigative power as purely executive, then MLAT and use immunity case law says that the court can categorically deny that power to a criminal defendant without violating the constitutional right to present a defense. This is so regardless of how essential the investigative power is to obtain exculpatory evidence. In contrast, if the underlying investigative power can be characterized as judicial, the definitional logic says that the right to present a defense attaches and entitles defendants to use that power in qualifying circumstances (i.e., when the evidence sought is important to the defense and the defense can show that blocking access to that evidence would be arbitrary or disproportionate to the purpose of the blocking rule). While this view of the law is particularly entrenched in MLAT and use immunity case law, the underlying logic can theoretically extend more broadly either to challenge or to justify a wide array of asymmetries between law enforcement and criminal defense investigative powers, including access to warrants, wiretaps, and court orders for stored electronic communications contents.

After identifying this definitional logic, this Part has argued that criminal defense counsel should exploit the logic in their litigation strategy. Hence, defense counsel facing asymmetrical barriers to access to process should seek to define the underlying power as at least partially judicial, and then argue that the right to present a defense attaches. Limitations of alternative *Brady*- and *Wardius*-based due process arguments for expanding defense access to evidence possessed by third parties make this definitional approach comparatively more attractive.

III. Applying the Definitional Logic to the Global CLOUD

This Part applies the definitional insights from Part II to map out a novel argument that criminal defense attorneys could use to challenge the disparities between law enforcement and defense access to cross-border evidence described in Part I. It focuses on one asymmetry in particular: the SCA rule that law enforcement, but not the defense, may subpoena U.S. technology companies for the contents of another's stored electronic communications, including content data stored on foreign servers that is protected by a foreign data privacy law. Ironically, the CLOUD Act of 2018—the very law that Congress enacted to give law enforcement special investigative powers without accounting for criminal defense needs—holds a key to challenging the SCA bar on defense subpoenas to technology companies and thereby to expanding defense access to exculpatory evidence both within the United States and across borders. The key is definitional.

The CLOUD Act, I contend, supports the view that court orders compelling the disclosure of stored electronic communications contents should be characterized as subpoenas rather than warrants. Meanwhile, other provisions of the SCA statute in which the Act is embedded help to establish that the subpoenas are judicial rather than administrative. Hence, even within the constraints of current doctrine, criminal defendants' constitutional right to present a defense should attach to these court orders and entitle defendants to pierce the SCA's bar on defense use of such orders in qualifying circumstances, even when the orders reach evidence stored on foreign servers and even when complying with the orders would violate a foreign data privacy law. This entitlement would expand defendants' cross-border access to evidence in the global cloud and improve their access to domestic evidence to boot.

A. Defining the Underlying Compulsory Process Power

How does the CLOUD Act support the view that court orders to service providers for stored electronic communications contents are a form of Judicial rather than Executive Branch process? There are two components to this claim. Defense counsel should argue, *first*, that the CLOUD Act implies that court orders for stored electronic communications contents are a form of subpoena for compelled disclosure, rather than a warrant for a direct search or seizure. *Second*, the pertinent provision of the SCA establishing that these orders must be issued by "a court of competent jurisdiction"[324] shows that the subpoenas are judicial rather than the Executive Branch variety.

1. Subpoenas, Warrants, and Extraterritoriality.—To understand the CLOUD Act's definitional implications, it will be helpful to start with some additional context about judicial subpoenas, warrants, and extraterritoriality. A subpoena is a form of compulsory process that orders the recipient to find and produce materials within their possession, custody, or control.[325] Judicial subpoenas for documents stored abroad generally do not run afoul of rules against courts exercising extraterritorial jurisdiction as long as the subpoena recipient is otherwise subject to the court's normal, domestic jurisdiction.[326] In that case, the reasoning goes, the court is simply exercising its standard

---

324. 18 U.S.C. § 2703(a).

325. FED. R. CRIM. P. 17(c)(1); FED. R. CIV. P. 45(a); *see In re* Grand Jury Proc. Bank of N.S., 740 F.2d 817, 828–29 (11th Cir. 1984) (upholding contempt sanctions against a bank that failed to timely comply with a grand jury subpoena for documents stored abroad).

326. *See* Mark R. Anderson, *Stranger in a Strange Land: Discovery Abroad*, LITIG., Winter 1998, at 41, 42 (noting U.S. courts' reliance on standard civil procedure rules to direct discovery of evidence abroad from parties and nonparties subject to the courts' jurisdiction). *But see* U.S. Dep't of Just., Just. Manual § 9-13.525 (2018) (observing that federal prosecutors must obtain prior approval from the Office of International Affairs before "issuing any unilateral compulsory measure to persons or entities in the United States for records located abroad").

jurisdiction over the recipient who must produce the documents, not extending extraterritorial jurisdiction to the documents themselves.[327]

In contrast, a warrant is a judicial order or authorization for law enforcement officers to search and seize evidence directly.[328] For instance, in executing a warrant for paper documents, law enforcement officers themselves will forcibly find and produce the documents. If a warrant targets paper documents stored abroad, then executing the search or seizure may require law enforcement officers to physically enter the foreign jurisdiction, which does implicate extraterritoriality concerns. Without consent from the foreign sovereign, such conduct violates international norms against extraterritorial enforcement authority.[329]

Unsurprisingly then, there is a strong presumption against courts issuing warrants for extraterritorial searches and seizures. Federal magistrates generally lack authority to issue such warrants.[330] And while Congress might theoretically have the power to authorize them, in the words of Judge Gerard Lynch, "it would be virtually inconceivable under ordinary notions of international law that Congress would ever attempt to authorize any such thing."[331] Moreover, there is an exception that proves the rule. Federal Rule of Criminal Procedure 41 authorizes federal magistrates to issue what are nominally extraterritorial warrants for searches and seizures of property

327. *See* Ghappour, *supra* note 193, at 1103–05 (noting that "courts regularly issue and uphold orders that compel disclosure of foreign-located evidence from third parties, so long as the third party falls under the court's personal jurisdiction and has control over the evidence").

328. *Id.* at 1101–02.

329. *See, e.g.*, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (AM. L. INST. 1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); Daskal, *supra* note 200, at 354 & n.99 (stating this principle and collecting authorities).

330. *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 279 (1990) (Stevens, J., concurring) (arguing that "American magistrates have no power to authorize" any "searches of noncitizens' homes in foreign jurisdictions"); *id.* at 297 (Blackmun, J., dissenting) (noting an "American magistrate's lack of power to authorize a search abroad"); *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 169 (2d Cir. 2008) (observing an absence of known examples of "any instances in our history where a foreign search was conducted pursuant to an American search warrant"); Letter from Mythili Raman, Acting Assistant Att'y Gen., Crim. Div., U.S. Dep't of Just., to Judge Reena Raggi, Chair, Advisory Comm. on Crim. Rules (Sept. 18, 2013), *in* ADVISORY COMMITTEE ON CRIMINAL RULES 171, 174 (2014), http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf [https://perma.cc/NU4P-9GAK] (noting the presumption against warrants for extraterritorial searches and seizures and explaining that an amendment to Rule 41 authorizing courts to issue warrants for anonymized data stored in an unknown location was not intended to authorize courts to issue warrants for data known to be located abroad); Daskal, *supra* note 200, at 354 (observing that "judges are presumed to lack authority to unilaterally authorize extraterritorial searches and seizures").

331. *In re* Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 226 (2d Cir. 2016) (Lynch, J., concurring), *vacated*, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam).

located within the limited bounds of U.S. diplomatic and consular missions abroad.[332] But the extraordinarily narrow carve-out of that authorization for property abroad that serves diplomatic purposes or is controlled by the United States—presumably with approval from the foreign sovereign—is all the more indication that extraterritorial warrants are generally disfavored.

Notably, courts' lack of authority in this respect does not bar federal law enforcement from unilaterally engaging in extraterritorial searches and seizures.[333] That distinction makes sense presuming that federal officials are better equipped than courts to assess and address the foreign policy consequences of extraterritorial enforcement actions.[334] Further, whether or to what extent the international law rules and norms against extraterritorial enforcement authority apply at all to remote electronic searches of data stored abroad—as opposed to direct searches and seizures of persons, paper documents, or other tangible objects in a foreign jurisdiction—is the subject of ongoing scholarly debate.[335] Yet, neither the possibility of unilateral executive action, nor the existence of scholarly debate, clearly authorizes

332. FED. R. CRIM. P. 41(b)(5)(B)–(C). Thank you to Orin Kerr for identifying these provisions of Rule 41.

333. *See Verdugo-Urquidez*, 494 U.S. at 274–75 (holding that the Fourth Amendment does not require warrants for extraterritorial searches and seizures concerning non-U.S. persons). Meanwhile, an Office of Legal Counsel opinion from 1989 asserts that U.S. law enforcement may unilaterally override international law prohibitions on extraterritorial searches and seizures. *See* Authority of the Federal Bureau of Investigation to Override International Law in Extraterritorial Law Enforcement Activities, 13 Op. O.L.C. 163, 163 (1989) (asserting that the Federal Bureau of Investigation has authority to "investigate and arrest individuals for violations of United States law even if those investigations and arrests are not consistent with international law"); *see also* Brian Finucane, *Revisiting the Office of Legal Counsel's Override Opinion*, JUST SEC. (Nov. 17, 2020), https://www.justsecurity.org/73412/revisiting-the-office-of-legal-counsels-override-opinion/ [https://perma.cc/V8PA-FS6Z] (explaining that the Office of Legal Counsel opinion from 1989 authorizes the Federal Bureau of Investigation to conduct activities in violation of customary international law).

334. *See* U.S. Dep't of Just., Just. Manual § 9-13.525 (2018) (noting sovereignty issues with the unilateral exercise of enforcement authority in foreign jurisdictions).

335. *See* Asaf Lubin, *The Prohibition on Extraterritorial Enforcement Jurisdiction in the Datasphere*, *in* RESEARCH HANDBOOK ON EXTRATERRITORIALITY IN INTERNATIONAL LAW (Austen L. Parrish & Cedric Ryngaert eds., forthcoming 2023) (manuscript at 5–7), https://ssrn.com/abstract=4012007 [https://perma.cc/55JU-KYV9] (observing a disjunct between judicial, government, scholarly, and treatise statements endorsing a traditional territorial limit on enforcement authority, even for cyberoperations, and many states' practice of unilateral non-consensual extraterritorial cyber-investigations). For debates on this issue in legal scholarship, compare Ghappour, *supra* note 193, at 1100–02, arguing that law enforcement hacking investigations that reach data stored abroad risk violating international law norms about extraterritorial enforcement, with Kerr & Murphy, *supra* note 193, at 66–67, arguing that existing international law rules against extraterritorial enforcement may apply solely to enforcement actions that involve "the physical sending of law enforcement officers into the territory," and not to digital searches. *See also* Daskal, *supra* note 200, at 355 (noting lack of clarity as to whether the appropriate reference point for a search and seizure analysis is "the location of the data, the provider, or the government agent accessing the data").

courts to issue warrants for direct searches and seizures of electronic data that the court knows are located abroad.[336]

On the contrary, current practice appears to preclude courts from issuing warrants for direct searches and seizures of evidence known to be located abroad, including digital evidence. For example, consider the DOJ's interpretation of a recent change to Federal Rule of Criminal Procedure 41 that authorizes courts to issue warrants for remote searches and seizures of digital evidence when the location of that evidence "has been concealed through technological means."[337] The DOJ is explicit that the rule "does not authorize courts to issue warrants for the search of electronic information stored abroad" and mandates that "[a]ny warrant should be limited to authorizing a search only in the United States."[338] The policy rationale behind this limitation, according to the DOJ, is that "such searches can implicate foreign sovereignty and criminal law issues."[339] Hence, courts should not be ordering or authorizing such conduct. Meanwhile, the DOJ contemplates that prosecutors might engage in such conduct without judicial approval but requires that they first "consult with the Office of International Affairs about appropriate coordination with foreign law enforcement partners as well as potential diplomatic and sovereignty issues."[340] According to the DOJ then, it is not for the courts to authorize remote electronic searches of data stored abroad.

2. Subpoenas, Warrants, and SCA Orders.—Now, enter the CLOUD Act. The CLOUD Act states, in pertinent part, that service providers "shall comply" with a court order issued pursuant to the SCA to disclose communications contents "within such provider's possession, custody, or control, *regardless of whether such communication . . . is located within or outside of the United States*."[341] In other words, SCA court orders can compel a service provider that is otherwise subject to the court's jurisdiction to hand over data, even if the court knows in advance that the data are stored on a foreign server.

---

336. *See, e.g.*, Kerr & Murphy, *supra* note 193, at 69 (observing that a warrant to use a hacking tool to search data directly "doesn't actually authorize the search if the computer turns out to be abroad"); Daskal, *supra* note 200, at 357–58 (noting that, despite a proposed Rule 41 change authorizing warrants for anonymized data in *unknown* locations in certain circumstances, ongoing questions remain about the warrants if the data turns out to be located abroad).

337. FED. R. CRIM. P. 41(b)(6)(A).

338. U.S. Dep't of Just., Just. Manual § 9-13.525 (2018). Note that, while DOJ's interpretation restricts what types of warrants *courts* can issue, it does not bar federal prosecutors from conducting remote searches of electronic data located abroad without judicial approval as long as they consult with the Office of International Affairs. *Id.*

339. *Id.*

340. *Id.*

341. 18 U.S.C. § 2713 (emphasis added).

This CLOUD Act text has at least two possible competing implications. To start, it might be that Congress directly authorized courts to issue warrants for extraterritorial searches and seizures of electronic data. But that reading would either violate the norms against courts issuing such warrants[342] or create a unique, dramatically unregulated exception to those norms for digital data.[343] Reading the CLOUD Act as authorizing extraterritorial warrants would mean that state and federal courts all across the country could order or authorize federal, state, county, or local law enforcement officers to search and seize data that they know is located anywhere in the world with no nexus to a U.S. diplomatic or consular mission. Put another way, it would mean that officers from any law enforcement agency in the United States[344] could engage in conduct that implicates "diplomatic and sovereignty issues"[345] without any requirement or even guidance to first consult the Office of International Affairs or another foreign policy agency of the United States. It is highly unlikely that Congress would have intended this result.

An alternate—and I submit more reasonable—implication is that the CLOUD Act text reflects that SCA court orders compelling service providers to disclose stored electronic communications contents should be characterized as subpoenas rather than warrants. According to this view, the CLOUD Act does not extend courts' jurisdiction extraterritorially or create a novel digital evidence exception to the norms on extraterritoriality. Rather, the Act simply clarifies that courts may exercise their standard compulsory process power over electronic communication-service providers that are otherwise subject to the courts' normal jurisdiction, including ordering the providers to disclose documents or data within their possession, custody, and control, regardless of where those documents or data are stored.[346] This subpoena interpretation would avoid concerns about extraterritorial enforcement authority, remain consistent with current expectations that courts lack authority to issue extraterritorial warrants, and leave foreign policy decisions about extraterritorial enforcement actions to the Executive Branch.

Reading the CLOUD Act's text according to a presumption against courts issuing extraterritorial warrants, and concluding that SCA court orders

342. *See supra* note 331 and accompanying text.

343. *See* Ghappour, *supra* note 193, at 1082–83 (noting the "well-established international law axiom that one state may not unilaterally exercise its law enforcement functions in the territory of another state, which has not been adequately addressed by courts or scholarship in the context of cyberspace" (footnote omitted)).

344. By one count, there are around eighteen thousand law enforcement agencies in the United States. DUREN BANKS, JOSHUA HENDRIX, MATTHEW HICKMAN & TRACEY KYCKELHAHN, NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 6 (2016), https://bjs.ojp.gov/content/pub/pdf/nsleed.pdf [https://perma.cc/C7ND-ZCJC].

345. U.S. Dep't of Just., Just. Manual § 9-13.001 (2018).

346. *See supra* section III(A)(1).

for communications contents should be understood as subpoenas rather than warrants, supports one side in a longstanding debate about whether to view these orders as subpoena-like or warrant-like.[347] On the one hand, the execution of an SCA court order appears functionally similar to a subpoena. Like subpoenas, but unlike warrants, SCA orders can be served without ever providing notice to the subject of a search, are subject to *ex ante* adversarial judicial review, and their execution does not require the physical presence of a government officer.[348] As Paul Ohm has argued, the "ISP, not the agent, performs the 'search,'" and hence SCA orders "are not search warrants at all."[349] On the other hand, the SCA's text refers to these orders as "warrant[s]" and requires that they comply with standard warrant procedural rules.[350] Meanwhile, current appellate doctrine holds that the Fourth Amendment warrant requirement applies to these orders.[351] The theory underlying this view is that SCA court orders conscribe a service provider

347. This debate between a subpoena-like and a warrant-like reading of SCA court orders reached prominent visibility in the history leading up to the CLOUD Act. The story of the CLOUD Act began years before its enactment, when law enforcement officers investigating a drug-trafficking case served Microsoft with an SCA court order compelling the company to disclose the contents of emails from one of its web-email service customer's accounts. *In re* Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 468 (S.D.N.Y. 2014). Microsoft refused to comply, arguing that the email contents were stored exclusively on a server in Ireland, Brief for Appellant at 2, *In re* Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) (No. 14-2985-cv), and that the court order lacked extraterritorial effect, *In re Warrant*, 829 F.3d at 201.

Microsoft and the DOJ fought this case, *United States v. Microsoft Corp.*, all the way up to the Supreme Court. 138 S. Ct. 1186, 1187 (2018) (per curiam). All parties agreed that under the normal subpoena rules, "an entity lawfully obligated to produce information in its control must do so regardless of the location of that information," including data stored abroad. Brief for the United States at 7, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2) (internal quotations omitted). The disagreement in the parties' briefs focused on whether the SCA procedures qualified as subpoena-like, in which case the normal subpoena production rule should apply to data stored abroad, or whether those procedures instead qualified as a warrant that conscripted Microsoft into an agent of law enforcement that must execute a search and seizure abroad, in which case the presumption against extraterritorial warrants should apply and block access to the data stored abroad. *See In re Warrant*, 829 F.3d at 201 ("Warrants traditionally carry territorial limitations: United States law enforcement officers may be directed by a court-issued warrant to seize items at locations in the United States and in United States-controlled areas . . . but their authority generally does not extend further." (internal citation omitted)).

Before the Supreme Court could decide *Microsoft*, Congress mooted the case by enacting the CLOUD Act. Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018) (codified at 18 U.S.C. § 2713). In expressly authorizing SCA court orders for data stored on foreign servers, the CLOUD Act resolved the *Microsoft* dispute in favor of the government and, by extension, in support of the subpoena-like view of the procedures. 18 U.S.C. § 2713.

348. *See, e.g.*, *In re* Leopold, 327 F. Supp. 3d 1, 10–15 (D.D.C. 2018) (discussing functional differences between subpoenas and warrants that lead the court to characterize SCA orders as subpoenas).

349. Paul K Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1611 (2004).

350. 18 U.S.C. § 2703(a), (b)(1)(A).

351. *E.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

into an agent of law enforcement who then executes a search or seizure on behalf of the government.[352]

It is not my claim here to resolve this debate in its entirety. Indeed, perhaps the answer should differ for purposes of an extraterritoriality analysis, a Fourth Amendment analysis, and a right-to-present-a-defense analysis. What I do contend is that the subpoena-like view better avoids conflict between the CLOUD Act and longstanding concerns surrounding courts issuing extraterritorial warrants. Criminal defense counsel should use this CLOUD Act extraterritoriality argument to advocate for a subpoena-like reading because, combined with text from the SCA described below, it indicates that court orders for stored communications contents are a form of judicial compulsory process rather than an Executive Branch power.

3. Judicial Versus Executive Subpoenas.—Presuming that the extraterritoriality argument mapped out above persuades courts to characterize SCA court orders for stored communications contents as subpoenas rather than warrants, how does this support the ultimate conclusion that the subpoenas are a form of judicial process rather than the Executive Branch variety? The final piece of this puzzle comes from reading the CLOUD Act in relation to pertinent parts of the SCA. Specifically, the plain text of the SCA decrees that such orders must be issued by "a court of competent jurisdiction."[353] That suggests that the orders are judicial subpoenas. If the orders were instead a form of Executive Branch or administrative subpoena, then law enforcement should be entitled to issue them in the first instance without obtaining prior judicial authorization.[354] Therefore, the SCA characterizes these orders as a form of legal process that emanates from the compulsory process powers of the Judiciary.

In sum, defense counsel facing claims that the SCA categorically bars criminal defense subpoenas for stored electronic communications contents should argue, first, for reading the CLOUD Act in light of extraterritoriality concerns. This will support the claim that court orders to technology companies seeking stored electronic communications contents are a form of

352. *See* Daskal, *supra* note 200, at 328, 358–59 (describing Microsoft's argument in *Microsoft*).

353. 18 U.S.C. § 2703(d).

354. *See* U.S. DEP'T OF JUST., REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES 6 (2002) https://www.justice.gov/archive/olp/rpt_to_congress.pdf [https://perma.cc/TA7V-YM64] ("Administrative subpoena authorities allow executive branch agencies to issue a compulsory request for documents or testimony without prior approval from a grand jury, court, or other judicial entity."); 18 U.S.C. § 2709 (detailing procedures for National Security Letters, which are administrative subpoenas issued directly by the Executive that can be challenged *ex post* in court but have no *ex ante* judicial review); Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 805 (2005) ("Administrative subpoenas or summons are issued by government agencies . . . .").

subpoena, not a warrant. Next, the SCA's requirement that the orders be issued by a court suggests that these subpoenas are judicial rather than administrative. Combined, these two implications indicate that the right to present a defense should attach to such court orders and entitle criminal defense counsel to subpoena technology companies for stored electronic communications contents in appropriate circumstances.

B. The Common Law Comity Analysis

If the constitutional right to present a defense attaches and enables U.S. criminal defendants to access court orders compelling U.S. technology companies to disclose communications content data, then, like law enforcement, defendants would also get access to a one-stop shop in U.S. courts to compel the same companies to disclose data stored on foreign servers. This would include the ability to circumvent foreign data privacy laws that might otherwise block the cross-border disclosure of evidence, provided the court conducts a common law comity analysis.

Here is how that common law comity analysis works. The Supreme Court has held that foreign blocking statutes that purport to prohibit—or even to criminalize—cross-border disclosures of data do "not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [foreign] statute."[355] On the contrary, the American court will balance the competing policy interests to determine whether to issue the order despite the foreign law.[356] Historically, most courts have resolved that comity analysis by prioritizing the U.S. legal process and ordering discovery despite a conflict with a foreign blocking statute.[357]

While most of the comity case law has come from civil proceedings, U.S. courts should be even more willing to pierce foreign data privacy laws when criminal defense investigative interests are at stake. This is primarily because of the life and liberty consequences of criminal proceedings. But there is another reason as well. Courts conducting a comity analysis balance the U.S. interests at stake in seeking cross-border evidence against the foreign interests that the blocking law protects.[358] Courts conducting this comity balancing should consider whether the foreign nation has an inquisitorial or adversarial criminal legal system that tasks state officials with investigating

355. Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct., 482 U.S. 522, 544 n.29 (1987).

356. *Id.* at 544 n.28 (establishing factors for the comity analysis).

357. *But see* Motorola Credit Corp. v. Uzan, 73 F. Supp. 3d 397, 404 (S.D.N.Y. 2014) (quashing subpoenas for documents in Switzerland because of the country's interest in bank secrecy).

358. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442(1)(c) (AM. L. INST. 1987).

exculpatory as well as inculpatory evidence.[359] If the foreign laws would permit law enforcement access, and the foreign nation has an inquisitorial legal system, then foreign lawmakers may have presumed that the law enforcement exception would cover the criminally accused.

In other words, foreign policymakers may be entirely unaware that blocking non-MLAT or non-CLOUD Agreement routes for U.S. litigants' access to evidence within their borders will block investigations of exculpatory evidence in the U.S. adversarial system.[360] Indeed, foreign authorities may favor access for U.S. criminal defendants because they realize that it is similar to the outcome they would reach in their own system. Not only might such access not offend their domestic policy preferences; it could be consistent with those preferences. In such circumstances, courts should be exceedingly skeptical that there is any foreign interest in blocking a criminal defense subpoena.

C. Fourth Amendment Concerns

At this point in the Article, some readers may be concerned that permitting defense counsel to subpoena technology companies for stored communications contents, regardless of whether those contents are stored within the United States or abroad, might conflict with the Fourth Amendment. After all, current appellate doctrine holds that the Fourth Amendment requires government entities to obtain a warrant supported by probable cause before those entities may compel technology companies to disclose this type of data.[361] And in *Carpenter v. United States*,[362] a majority of the Supreme Court seemingly endorsed this view.[363] This raises two key questions. *First*, if the Fourth Amendment protects this type of data, then can defense counsel compel access to it by using judicial process? *Second*, would permitting defense counsel to obtain this data with a judicial subpoena undermine the requirement that government entities must obtain a warrant supported by probable cause before those entities may compel access to the

359. *See* Abraham S. Goldstein, *Reflections on Two Models: Inquisitorial Themes in American Criminal Procedure*, 26 STAN. L. REV. 1009, 1019 (1974) (discussing the differences between adversarial and inquisitorial systems).

360. *See* CARRERA ET AL., *supra* note 49, at 32 (informing readers, in a report aimed at an EU audience, of the contrast between "the wide-ranging data-gathering powers granted by the CLOUD Act to US authorities" and the limitations on U.S. defendants' comparable investigative power).

361. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause.").

362. 138 S. Ct. 2206 (2018).

363. *See id.* at 2222 (holding that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in [electronic] records held by a third party"); *id.* at 2230 (Kennedy, J., dissenting) (citing *Warshak* approvingly); *id.* at 2269 (Gorsuch, J., dissenting) (same).

same information from the same sources? The answer to the first question is yes. The answer to the second question is no. This subpart explains why.

Begin with the first question. In a recent case before the D.C. Court of Appeals, the prosecution argued: "It would be illogical . . . to allow non-governmental litigants to obtain the content of communications simply by issuing a subpoena to the service provider, while at the same time requiring that the government obtain a warrant supported by probable cause."[364] This assertion is incorrect. The mere fact that the Fourth Amendment protects certain information does not categorically bar nongovernmental litigants from using judicial subpoenas to compel access to that same information.

An example establishing this reality runs to the "very core" of Fourth Amendment protections: the home.[365] As the Supreme Court recently reiterated, "[w]hen it comes to the Fourth Amendment, the home is first among equals."[366] Hence, the Fourth Amendment requires government officers to obtain a warrant before searching private homes.[367] Yet nongovernmental litigants may use a judicial subpoena to do the same—to compel access to someone else's home. Indeed, Federal Rule of Civil Procedure 45 on its face permits nongovernmental civil litigants to obtain judicial subpoenas that command "inspection of premises at the premises to be inspected."[368] Such subpoenas are not issued pursuant to the court's authority to manage Rule 37 discovery between parties. On the contrary, the Advisory Committee Notes explain that this language "authorizes the issuance of a subpoena to compel the inspection of premises in the possession of a *non-party*."[369] Hence, Rule 45 subpoenas ordering the inspection of premises are examples of standard judicial compulsory process that may be directed to nonparties. It should thus be unsurprising that criminal defense counsel can also obtain similar physical location inspection orders from the courts,[370] including orders compelling access to nonparties' homes.[371] These examples show that nongovernmental litigants are not categorically barred from compelling access to Fourth Amendment-protected information.

Far from being "illogical," it makes good sense that nongovernmental litigants may use judicial subpoenas to compel access to Fourth Amendment-protected information. If instead the Fourth Amendment made information

364. Brief for the United States at 25–26, Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019) (No. 18-CO-0958).

365. Florida v. Jardines, 569 U.S. 1, 6 (2013).

366. Collins v. Virginia, 138 S. Ct. 1663, 1670 (2018) (quoting *Jardines*, 569 U.S. at 6).

367. *See, e.g.*, *id.* at 1670.

368. FED. R. CIV. P. 45(c)(2)(B).

369. FED. R. CIV. P. 45 advisory committee's note to 1991 amendment (emphasis added).

370. *See, e.g.*, N.Y. CRIM. PROC. LAW § 245.30 (McKinney 2020) (codifying this right of the defense).

371. *See* Wexler, *supra* note 10, at 252.

available exclusively to the government, then the Amendment would aggrandize rather than constrain government power; it would specially empower government officials while imposing a limit on private entities. This result would get the Fourth Amendment backwards. As Paul Schwartz aptly stated, the language of the Fourth Amendment is designed to "create[] restrictions on the investigatory powers of government officials."[372] What would be "illogical," then, is to construe the Fourth Amendment as granting government entities special powers to compel access to sensitive information simply by obtaining a warrant, while at the same time construing the Amendment as categorically barring all other litigants from accessing the information with any form of process whatsoever.

Given that Fourth Amendment protection does not categorically bar nongovernmental litigants from accessing information, the second question remains: Does recognizing defense counsel's right to use judicial subpoenas to access Fourth Amendment-protected information undermine the warrant requirement for the government to compel access to the same information? It is clear from the home-search scenario that nongovernmental litigants' access to information pursuant to appropriate forms of judicial process does not automatically eliminate the government's warrant requirement. There are at least three plausible explanations for this result.

First, perhaps defense counsel's ability to subpoena Fourth Amendment-protected information is irrelevant to the government's warrant requirement because the Fourth Amendment does not apply to nongovernmental litigants' use of compulsory process. That scenario, while possible, is unlikely to be correct. Judicial compulsory process is a governmental power that risks undue privacy invasions, albeit a different power with different risks than either police-power searches and seizures or administrative and congressional subpoenas. It would be surprising if the Fourth Amendment were entirely unconcerned with judicial invasions of privacy merely because they are initiated by nongovernmental litigants. To be sure, courts have asserted that "[u]se of the courts by private parties does not constitute an act under color of state law."[373] Yet, other Bill of Rights constraints apply to judicial compulsory process even when exercised on behalf of nongovernmental litigants. For instance, First Amendment associational rights protect anonymous speakers from civil court orders to unmask their identities.[374] It is more plausible that the Fourth Amendment imposes lesser procedural requirements on compulsory process exercised by

372. Paul Schwartz, Privacy Supremacy 23 (Oct. 1, 2021) (unpublished manuscript) (draft on file with author).

373. Harvey v. Harvey, 949 F.2d 1127, 1133 (11th Cir. 1992).

374. *See generally* JEFF KOSSEFF, THE UNITED STATES OF ANONYMOUS: HOW THE FIRST AMENDMENT SHAPED ONLINE SPEECH (2022) (discussing the interaction between online anonymity and the First Amendment).

nongovernmental than by governmental litigants, since the risk of government abuses is arguably reduced when a nongovernmental entity instigates compulsory process. There is little to no case law discussing this issue. But if the Fourth Amendment did impose lesser procedural requirements on nongovernmental than governmental litigants, this would help to explain the constitutionality of civil subpoenas for nonparties' Fourth Amendment-protected information.

Second, perhaps the Fourth Amendment applies to judicial subpoenas requested by nongovernmental litigants and imposes equivalent process requirements for those subpoenas as it does for warrants that authorize police-power searches and seizures. In that case, to be constitutional, criminal defense subpoenas for Fourth Amendment-protected information would have to satisfy the same requirements as warrant applications, thus cementing rather than undermining the government's warrant requirement. As it turns out, the requirements to obtain a criminal defense subpoena under current law likely do satisfy the requirements to obtain a warrant. The Fourth Amendment requires that no warrants shall issue without probable cause, particularity, and *ex ante* judicial review.[375] Similarly, criminal defense subpoenas must seek information that is relevant, likely to be admissible at trial, and identified with specificity.[376] The relevance and admissibility determinations arguably also satisfy the probable cause standard. Meanwhile, the specificity showing likely satisfies the Fourth Amendment particularity requirement.[377] Finally, while criminal defense counsel may be authorized to serve attorney subpoenas that have not been pre-approved by the court, the subpoenas generally require that responsive information be delivered to the court, not the attorney, and the subpoenas are not enforceable without judicial review.[378] If the requirements to obtain a criminal defense subpoena are equivalent to the probable cause, particularity, and *ex ante* judicial review requirements of a Fourth Amendment warrant, then permitting defense counsel to obtain communications content data with a judicial subpoena will not undermine the government's warrant requirement to obtain the same information.

Third, perhaps the Fourth Amendment applies equally to all subpoenas—or at least to all judicial subpoenas—and imposes lesser

375. U.S. CONST. amend. IV.

376. *See* United States v. Nixon, 418 U.S. 683, 700 (1974); FED. R. CRIM. P. 17(a).

377. *See* Bihter Ozedirne, Note, *Fourth Amendment Particularity in the Cloud*, 33 BERKELEY TECH. L.J. 1223, 1224 (2018) (explaining that, as described by a Tenth Circuit opinion, a "warrant is sufficiently particular" in compliance with the Fourth Amendment if it would "enable the searcher to reasonably ascertain and identify the things authorized to be seized" (quoting United States v. Dunn, 719 F. App'x 746, 748 (10th Cir. 2017))).

378. *See, e.g.*, People v. Natal, 553 N.E.2d 239, 241–42 (N.Y. 1990) (finding that attorney subpoenas must make documents returnable to the court).

requirements for those subpoenas than it does for police-power searches and seizures, even when the two forms of process result in disclosures of the same information from the same sources.[379] If that is so, then it is civil subpoenas that are most likely to undermine the warrant requirement for government access, not criminal defense subpoenas, because it is civil subpoenas that are most likely to fail the probable cause standard and thereby create a precedent for government litigants to subpoena Fourth Amendment-protected information with less than probable cause. For instance, perhaps Rule 45 subpoenas commanding the inspection of premises possessed by a nonparty fail to satisfy the heightened process demands of the warrant requirement. Those subpoenas may be constitutionally suspect under the Fourth Amendment, or they may support a view that the Fourth Amendment requires mere reasonableness for subpoenas. Either way, authorizing criminal defense subpoenas is not the Fourth Amendment threat.

Regardless of which explanation is correct, one thing is clear. The fact that a form of investigative power emanates at least in part from the Judiciary and is available to criminal defense counsel does not mean that the Fourth Amendment warrant requirements of probable cause and particularity do not apply to government entities. Thus, recognizing that court orders to technology companies compelling disclosures of communications contents are a form of judicial process to which the defense may be constitutionally entitled will not undermine Fourth Amendment requirements for law enforcement to obtain the same information from the same sources.

Conclusion

This Article has focused on identifying the increasing disparities between law enforcement's and criminal defense counsel's cross-border access to evidence, on surfacing the doctrinal logic distinguishing executive from judicial compulsory process powers that courts have relied on to uphold these and similar disparities as constitutional, and on offering a litigation strategy for defense counsel to begin to close the gap in cross-border investigative power while working within the constraints of this existing

379. This is a somewhat less extreme version of the view that Justice Alito advanced in his dissent in *Carpenter v. United States*. 138 S. Ct. 2206, 2250 (2018) (Alito, J., dissenting) (arguing that "the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all"). A majority of the Court squarely rejected this position, stating that:

> [T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy . . . .
>
> . . . .
>
> If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement.

Id. at 2221–22.

doctrine. In conclusion, it is worth pausing to consider why these contributions matter from a policy perspective.

To start, consider procedural disparities between criminal defense and law enforcement investigations generally.[380] As with law enforcement investigations, the legal rules that control criminal defense investigations should advance goals of truth seeking while balancing competing values, such as the privacy interests of victims, witnesses, and other nonparties.[381] Rules that selectively curtail defense investigative power as compared to that of law enforcement, then, raise red flags not merely because such rules may deny defendants access to evidence that is relevant or even necessary to their case, but also, crucially, because the rules may deny this access without good reason. When law enforcement can access compulsory process powers despite competing values such as privacy, it begs the question of whether defense counsel differ from law enforcement sufficiently to justify denying them the same.

One important difference between law enforcement and defense counsel is that the former is tasked with investigating guilt and the latter with investigating innocence. It should be uncontroversial that this difference does not justify legal rules disadvantaging defense investigators as compared to their law enforcement counterparts. Deliberate favoritism for uncovering evidence of guilt rather than evidence of innocence would undermine both the neutral truth-seeking ideals of the adversarial system[382] and the goal of minimizing wrongful convictions.[383]

Another potential difference that, at first glance, might appear to provide stronger justification for such investigative disparities is the risk of abuse of process. Perhaps law enforcement officers are less likely than criminal defense counsel to serve process for illegitimate reasons, such as undertaking a fishing expedition for purposes of delay or harassment. There are, admittedly, some reasons to think this might be so. For instance, prosecutors have obligations to serve the tribunal and the public that, at least

380. For an in-depth analysis of policy concerns surrounding "privacy asymmetries," see Wexler, *supra* note 10, at 242–58.

381. *See id.* at 224–29 (describing how the criminal procedure and evidence rules impose a series of reasonable limitations on criminal defense subpoena power to protect important nonparty privacy interests).

382. For instance, consider the Supreme Court's oft-repeated pronouncement that "it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." United States v. Nixon, 418 U.S. 683, 709 (1974); Taylor v. Illinois, 484 U.S. 400, 409 (1988) (quoting *Nixon*, 418 U.S. at 709).

383. For an in-depth discussion of values of accuracy in the criminal legal system and the conventional account that the system should disfavor false positives, see generally Daniel Epps, *The Consequences of Error in Criminal Justice*, 128 HARV. L. REV. 1065 (2015).

in theory, should lead them to neutrally seek justice.[384] In contrast, defense counsel have duties of zealous advocacy on behalf of their clients, which should lead them to prioritize the client's interest in access above many competing values.[385]

However, there are also good reasons to think that the risk of abuse of process by law enforcement could be greater than or equal to that of defense counsel.[386] For example, prosecutors' qualified immunity for investigative conduct and absolute immunity for prosecutorial conduct reduce deterrents against abuse.[387] Meanwhile, while prosecutors may in theory be neutral, in practice their role as advocates in an adversary system can incentivize a zealousness similar to that of their defense counterparts.[388] In the absence of empirical evidence establishing that the risk of abuse is greater from one source versus the other, I submit that such a risk does not clearly justify disadvantaging defense investigations.

Focusing on particular forms of compulsory process makes disparities disadvantaging defendants' *cross-border* investigative power seem even more unreasonable. Recall that courts have relied on much the same constitutional rationale of distinguishing executive from judicial power to uphold disparities in both use and derivative use immunity and access to MLATs.[389] From a policy perspective, however, there are substantially different reasons why disparate access might be justified in one scenario versus the other.[390] The refusal to immunize defense witnesses is often rationalized by concern over an "immunity bath," whereby witnesses testify far more broadly than anticipated to maximize their immunity for past

384. *See* Eric S. Fish, *Against Adversary Prosecution*, 103 IOWA L. REV. 1419, 1426–32 (2018) (discussing prosecutors' theoretical role as both neutral justice seekers and adversarial advocates). Thank you to David Sklansky for encouraging me to address this possible justification for treating law enforcement and defense investigators differently.

385. *See* Charles J. Ogletree, Jr., *Beyond Justifications: Seeking Motivations to Sustain Public Defenders*, 106 HARV. L. REV. 1239, 1246–47 (1993) (explaining the traditional view of zealous advocacy by defense counsel). This does not mean that the legal system as a whole lacks constraints on defense counsel's exercise of zealous advocacy. On the contrary, judges can curtail any abusive defense use of process on a case-by-case basis without resort to categorical bars on defense investigative power. For an explanation of how the evidence and procedure rules empower judges to balance defense subpoenas with competing values, see *supra* note 381.

386. Wexler, *supra* note 10, at 255–56.

387. Margaret Z. Johns, *Reconsidering Absolute Prosecutorial Immunity*, 2005 B.Y.U. L. REV. 53, 53–54.

388. See Fish, *supra* note 384, at 1432–34 (discussing how prosecutors' dual roles as justice seekers and adversary advocates play out in practice).

389. *See supra* section II(A)(2).

390. Thank you to Daniel Richman for encouraging me to highlight the policy differences between defense access to cross-border investigative power and defense access to immunity power.

criminal acts.[391] Indeed, defendants might call their co-conspirators to the stand deliberately to enable such conduct.[392] As a result, granting defendants a right to immunize witnesses could enable them to constrain the government's subsequent prosecution of other crimes.[393] While in some cases a defendant's need for exculpatory testimony might outweigh this concern, the fact that the prosecution and defense are differently situated in relation to the risk of an immunity bath could conceivably justify an asymmetry in the default rules of access.

In contrast, there is no comparable difference between law enforcement and criminal defense counsel when it comes to cross-border investigative powers. To be sure, cross-border investigations can raise foreign policy considerations that traditionally fall within the purview of the Executive Branch. Perhaps then, an argument could be made that solely Executive Branch officials should be able to undertake those investigations. Yet, use of MLATs and CLOUD Agreements is not currently limited to federal agencies with foreign policy powers, or indeed even to federal agents. On the contrary, there are approximately eighteen thousand separate state and local law enforcement agencies in the United States,[394] all of whom have access to cross-border compulsory legal process through the MLAT and CLOUD Agreement systems. The United States–United Kingdom CLOUD Agreement, for instance, states expressly that it covers legal process "issued by state, local, territorial, tribal, or any other authorities within the United States."[395] If empowering municipal police to access the treaty procedures does not create undue foreign policy risks, then it is unclear why empowering criminal defense counsel to access the same procedures would do so. The fact that private civil litigants have access to cross-border investigative powers through the Hague Convention makes it all the more unreasonable to exclude criminal defendants.

391. *See* Flanagan, *supra* note 266, at 456 (discussing this problem in detail); *see also* Michael J. Schaffer, Note, *The Constitutional Right to Defense Witness Immunity*, 57 N.D. L. REV. 187, 222 (1981) (noting that the "immunity bath" problem also includes a risk that granting defense witness immunity may encourage cooperative perjury to secure immunity for oneself).

392. *See* Flanagan, *supra* note 266, at 456 (raising this concern).

393. *Id.*

394. *See supra* note 344.

395. Agreement on Access to Electronic Data for the Purposes of Countering Serious Crime, U.K.-U.S., art. 1, ¶ 9, Oct. 3, 2019, https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern-ireland [https://perma.cc/CL48-NEAC].

Legislatures all over the world are crafting urgent new legal regimes to safeguard privacy interests in the global data-driven economy. These privacy safeguards matter. Yet to date, privacy law and policy debates have recognized law enforcement's interests in accessing sensitive information for investigative purposes—whether to expand or to curtail that access—while largely overlooking criminal defense investigators' interests in the same. This Article has begun to remedy that oversight.