DATA AND DEMOCRACY



The CLOUD Act and the Accused

By Rebecca Wexler

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

In October 2020, the Knight First Amendment Institute at Columbia University convened a virtual symposium, titled "Data and Democracy," to investigate how technological advances relating to the collection, analysis, and manipulation of data are affecting democratic processes, and how the law must adapt to ensure the conditions for self-government. This symposium was organized by the Institute's 2019-2020 Senior Visiting Research Scholar, Yale Law Professor Amy Kapczynski, and co-sponsored by the Law and Political Economy Project at Yale Law School.

The essays in this series were originally presented and discussed at this two-day event. Written by scholars and experts in law, computer science, information studies, political science, and other disciplines, the essays focus on three areas that are both central to democratic governance and directly affected by advancing technologies and ever-increasing data collection: 1) public opinion formation and access to information; 2) the formation and exercise of public power; and 3) the political economy of data.

The symposium was conceptualized by Knight Institute staff, including Jameel Jaffer, executive director; Katy Glenn Bass, research director; Amy Kapczynski, senior visiting research scholar; Alex Abdo, litigation director; and Larry Siems, chief of staff. The essay series was edited by Glenn Bass and Amy Kapczynski with additional support from Lorraine Kenny, communications director; A. Adam Glenn, writer/editor; Madeline Wood, research coordinator; Chand Rajendra-Nicolucci, research fellow; Kushal Dev, research fellow; and Ashwin Pillai, intern.

The full series is available at knightcolumbia.org/research/

I. INTRODUCTION

IMAGINE A PERSON sentenced to death who is seeking to examine information about a forensic software program used to convict him.[1] Now imagine that a court reviewing the person's postconviction petition for relief finds that the information is material and necessary to the administration of justice and orders the software developer to disclose it. To safeguard the developer's trade secrets and proprietary information, the court orders disclosure under a strict protective order. Even so, the developer refuses to comply. In most cases, this fact pattern would lead to a standard discovery dispute for the court to adjudicate. But now imagine two additional facts. First, the developer is located abroad and thus beyond the subpoena power of U.S. courts. Second, a U.S. cloud service provider possesses a copy of the information that the developer has stored in a private cloud account. If the person sentenced to death tries to subpoena the information from the U.S. cloud service provider, the provider will likely argue that the Stored Communications Act (SCA),[2] a key U.S. data privacy law for the internet, categorically immunizes it from complying with the subpoena. In other words, a person's appeal to get off of death row may depend on data that a

foreign company refuses to hand over and that a U.S. company says it does not legally have to disclose.[3]

Police or prosecutors seeking the same information could compel disclosure directly from the foreign developer through a mutual legal assistance treaty (MLAT), which entitles law enforcement to assistance from foreign governments in accessing evidence located abroad.[4] Or they could also serve a U.S. cloud service provider with an order under the SCA, which was recently amended by the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 to expressly permit governmental entities to compel disclosures of data that U.S. cloud providers store on foreign servers.[5] Significantly, both of these mechanisms have the potential to circumvent conflict-of-law issues that might otherwise impede cross-border evidence transfers. Yet, neither of these mechanisms is currently available to criminal defense investigators.

The thicket of domestic, foreign, and international law that affords some the power to compel cross-border access to data and others the power to keep it secret is tipping further in favor of law enforcement as compared to the criminally accused. This trend matters because it advantages the search for evidence of guilt over that for evidence of innocence. In the U.S. adversarial criminal legal system, law enforcement has no general constitutional, statutory, or ethical obligation to investigate evidence of innocence.[6] 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.[7] Selectively blocking defense access to evidence thus means selectively suppressing evidence of innocence. This essay examines these dynamics in the context of cross-border access to data and argues that the CLOUD Act can help to address them.[8]

More specifically, data privacy, protection, and localization laws around the world are combining with criminal procedure rules to afford U.S. law enforcement the power to compel access to evidence of guilt while granting corporations the power to withhold evidence of innocence.[9] A variety of dynamics contribute to this pattern, which I elsewhere term "privacy asymmetries," or privacy laws that afford law enforcement more or better access to sensitive information than they afford to criminal defense investigators.[10] The rise of the data economy means that corporations, rather than the government, increasingly possess digital evidence relevant to criminal

investigations, including methodological details about investigative and forensic algorithms licensed for law enforcement use, as well as faceprint, DNA, and fingerprint databases that in earlier eras were created and maintained by government agencies.[11] Corporate possession of relevant digital evidence in turn means that 20th century due process protections requiring prosecutors to inform the accused about evidence of innocence within their control are less likely to apply. At the same time, corporations are asserting privacy law and other legal entitlements to block criminal defense subpoenas for evidence within their possession.[12] Meanwhile, law enforcement entities are negotiating expansive powers to compel private companies to disclose evidence of guilt, including cross-border data disclosures, while few if any advocate for parallel investigative powers on behalf of the accused.

Part II traces the evolution of current legal asymmetries between law enforcement and defense access to cross-border evidence. Starting in the 1970s, the U.S. government began entering into a series of MLATs that create special procedures for law enforcement to compel cross-border disclosures of evidence but expressly prohibit defense investigators from using the same procedures. 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. Having described that historical backdrop, Part II then updates and contextualizes the issue of MLAT asymmetries in more recent geopolitical developments. It identifies how the rise of global "informational capitalism,"[13] combined with developing foreign and domestic data privacy, protection, and localization laws, as well as treaties governing cross-border data transfers, risk worsening asymmetries that disadvantage U.S. criminal defendants.

Part III draws on the CLOUD Act of 2018 to help reverse the 50-year trend of growing inequity between law enforcement and criminal defense access to evidence stored abroad. It argues that courts should construe the CLOUD Act to entitle criminal defendants to subpoena U.S. corporations for data stored on foreign servers.[14] Despite significant public policy and scholarly debates over the CLOUD Act, the statute's potential effects on criminal defense investigations have been largely, if not entirely, overlooked. This essay begins to fill that gap, arguing that the statute should be construed to enhance defendants' access to evidence stored abroad while avoiding

the constitutional grounds that courts have used to justify denying defense access to MLAT procedures in the past.

While the arguments developed here will most immediately benefit those wrestling with the law and geopolitics of cross-border data flows,[15] the essay also aims to contribute to broader literatures on the political economy of the criminal legal system,[16] and of information privacy and surveillance law,[17] as well as literatures assessing the possibilities and limitations of transparency as a mechanism for substantive accountability.[18] Legal scholars are developing urgent critiques of structural inequities in criminal procedure and evidence rules,[19] inequities that simultaneously reflect and produce racial, economic, and other forms of oppression.[20] This essay shows that the legal construction of these inequities is not limited to the segment of criminal procedure and evidence rules formally codified as such. To the contrary, economic laws that regulate and respond to markets, including intellectual property[21] and data privacy and protection laws,[22] can also operate as criminal procedure and evidence rules,[23] despite being less typically associated with public law governance of the criminal legal system.[24] The following discussion presents one instance of this broader reality. Put another way, cross-border privacy asymmetries exemplify how "the relationship between the state and the economy, and the interactions between capitalism and democracy" shape the criminal legal system.[25]

II. THE PROBLEM OF CROSS-BORDER "PRIVACY ASYMMETRIES"

Over the past 50 years, the U.S. government has negotiated a series of MLATs with other nations that create special procedures for law enforcement to access evidence abroad while explicitly precluding defense counsel from using those same procedures. As the following discussion shows, the MLAT system began with the goal of enabling law enforcement to circumvent foreign privacy laws, initially foreign bank secrecy laws. This expansion of law enforcement's investigative power without comparable provisions for defense investigators has generated sustained criticism and repeated constitutional challenges. Yet, to date, those efforts

have failed to stem the proliferation of MLAT asymmetries.

This part begins by providing background on the MLAT system and then argues that recent developments in the global data economy are both aggravating these asymmetries and threatening to create new ones. *First*, cross-border access to data matters increasingly in all types of criminal disputes, from global organized crime to common misdemeanors, even when alleged criminal acts occurred entirely within U.S. borders. The result exacerbates existing inequities in the legal structures that determine who can compel and who can withhold cross-border data. *Second*, the rise of the digital services economy is prompting lawmakers around the world to enact new data privacy, protection, and localization laws that risk blocking access to foreign data in U.S. criminal investigations.[26] That erosion of access is most pronounced for defense investigators, who lack the MLAT powers to circumvent foreign laws. Further, in 2018, Congress empowered the U.S. government to enter into a new series of "CLOUD Act Executive Agreements" with other nations designed to supersede the MLAT system and create more efficient law enforcement access. By every indication, these new agreements will also exclude defense investigators. As a result, foreign data privacy, protection, and localization laws threaten to undermine criminal defense investigations and aggravate disparities of power between the government and the accused.

A. The global data economy is exacerbating existing asymmetries in law enforcement and defense investigative power

1. THE EVOLUTION OF CROSS-BORDER PRIVACY ASYMMETRIES

Asymmetry in law enforcement and criminal defense access to cross-border evidence is not inevitable. Prior to the Reagan administration, the primary legal mechanism to compel access to evidence located abroad, called "letters rogatory," was available to both law enforcement and defense investigators. Litigants using this process first request discretionary assistance from a court inside the U.S.[27] The U.S. court then transmits the letter rogatory to the U.S. State Department, which in turn transmits it to the appropriate U.S.

embassy, which transmits it to the requested state's ministry of foreign affairs, which transmits it to that state's ministry of justice, which, finally, transmits it to an appropriate foreign court to enforce as a discretionary matter of legal reciprocity between sovereigns, or comity.[28] Note that applications for letters rogatory require ex parte judicial review from courts in *both* the requesting and receiving nations before anyone can be served with process and that, after service of process, any interested parties are given notice and an opportunity to move to quash.[29]

The letters rogatory process is notoriously unpredictable and subject to lengthy delays of a year or more.[30] Advocating during the 1980s for a better, more efficient process for civil litigants, the U.S. secretary of state described letters rogatory as "complicated, dilatory and expensive."[31] Significantly, letters rogatory are generally insufficient to pierce foreign laws, including foreign data privacy, protection, and localization laws that may limit U.S. litigants' service of legal process abroad.[32] 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.[33] As a result, litigants using letters rogatory generally cannot access financial information located in Switzerland or the Cayman Islands.[34]

Beginning in the 1970s, the inability of letters rogatory to pierce foreign bank secrecy laws prompted the U.S. government to start entering into MLATs. MLATs are bilateral treaties that bind the signatory nations to assist one another in criminal investigations.[35] Courts in the foreign jurisdiction may review MLAT requests and have limited discretion to deny those that violate the procedural or substantive domestic law of the requested state.[36] But, crucially, MLATs often expressly waive foreign data privacy protections. For example, the first MLAT, signed with Switzerland, waived Swiss bank secrecy laws to enable U.S. investigators to access Swiss bank records.[37] MLAT procedures are also more reliable and efficient than letters rogatory 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 directly to their foreign law enforcement counterparts.[38] In other words, the MLAT process requires pre-service-of-process ex parte judicial review solely from courts in the receiving nation.[39]

The first three MLATs—signed with Switzerland, Turkey, and the Netherlands—are silent on use by criminal defendants.[40] As a result, some courts construed the treaties to enable access by both law enforcement and criminal defense investigators.[41] During the 1980s, however, as the Reagan administration entered full swing, the U.S. began negotiating MLAT treaties that were expressly limited to law enforcement use.[42] The U.S.-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."[43] Courts interpreting the U.S.-Israel MLAT and similar texts in the U.S.-United Kingdom MLAT,[44] the U.S.-Nigeria MLAT,[45] and the U.S.-Mexico MLAT, have held that the language precludes criminal defendants from using MLAT procedures.[46] Today, nearly all U.S. MLATs lack provisions for criminal defense access to their investigative procedures.

2. THE FAILED CHALLENGES TO EXISTING CROSS-BORDER PRIVACY ASYMMETRIES

The disparity between defendants' letters rogatory power and law enforcement's MLAT power has provoked sustained criticism. For some examples among many, Frank Tuerkheimer, a law professor and former assistant U.S. 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."[47] The National Association of Criminal Defense Lawyers has repeatedly lobbied the Senate for amendments to the MLAT language that would permit judges to order the Department of Justice to use MLAT channels on behalf of the defense.[48] Criminal defense bar publications have featured model legal arguments against the inequities.[49] And defendants have repeatedly challenged the constitutionality of the disparities in court.[50]

To date, these challenges have failed. The Justice Department has consistently opposed granting defendants access to MLAT processes.[51] It 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 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 the prosecution and for civil litigants.[52] Meanwhile, the Senate has continued to approve MLATs that explicitly block defense 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,[53] courts have uniformly upheld the constitutionality of these asymmetries between law enforcement and criminal defense access to foreign evidence.[54]

3. ACCESS TO CROSS-BORDER DATA MATTERS MORE TO MORE CRIMINAL CASES

Evidence located abroad has long been relevant to criminal defendants within the U.S., particularly in cases involving alleged transnational crimes such as trafficking, terrorism, espionage, foreign corrupt practices, and global corporate crime.[55] Some existing procedural rules recognize this fact. For instance, the Federal Rules of Criminal Procedure currently permit defendants, in "exceptional circumstances," to ask a judge for discretionary approval to depose foreign witnesses abroad.[56] Yet, even if defendants meet the high burden necessary to obtain judicial approval for the taking of such foreign depositions, letters rogatory remain defendants' sole means to compel testimony from unwilling foreign witnesses.[57]

While the issue of defense access to cross-border evidence is not new, the global data economy lends new urgency to the problem in a broader swath of cases.[58] People anywhere can use digital services offered by companies headquartered anywhere else. Data generated or used by people within the U.S. can be stored on foreign servers.[59] As a result, legal inequities in law enforcement and defense access to foreign evidence can now affect more and more types of criminal disputes.[60] This is true even when alleged criminal acts occur offline and within U.S. borders. For instance, email and social media service providers may possess evidence relevant to investigating foreign co-conspirators' participation in crimes that were conducted by local co-conspirators within the territorial U.S., to raising a self-defense or coercion defense, or to impeaching government witnesses. And that email and social media evidence may be stored exclusively on foreign servers.[61] Location data, biometrics, health records, private communications, and more can all be relevant to criminal investigations and can all be stored abroad.

Foreign trade secrets and other commercial data are additional examples. U.S. law enforcement agencies may purchase investigative and forensic software tools from foreign companies that store methodological information about their products on foreign servers.[62] Those same companies may refuse to sell their products to criminal defense investigators and withhold methodological information about their tools from defense and public scrutiny.[63] The increased salience of cross-border evidence in the global data economy means that legal inequities in cross-border access to data are poised to affect an unprecedented number and variety of criminal cases.

The following section explains that newly developing legal structures designed to govern the global data economy are poised to both entrench and expand the existing legal asymmetries in law enforcement and defense access to cross-border data.

B. Developing global data governance structures risks creating new asymmetries in law enforcement and defense investigative power

Trends in the global data economy are not merely making foreign evidence more urgent to more types of criminal cases; they also risk making that evidence less accessible to the criminally accused.

1. FOREIGN PRIVACY LAWS RISK IMPEDING ACCESS TO CROSS-BORDER DATA

Just as U.S. policymakers are contemplating new federal and state legislation to address threats to privacy from "informational capitalism,"[64] so too foreign lawmakers are enacting data privacy, protection, and localization laws in response to perceived privacy, security, and sovereignty threats from the global data economy. Data privacy and protection laws often impose broad nondisclosure requirements on companies that possess sensitive personal data, require those companies to notify account holders if and when the companies share sensitive data with others, and entitle account holders to demand that the companies delete certain data.[65] Data localization laws, in turn, require that certain types of data collected within a country, or pertaining to its citizens, must be processed and stored on servers located within that country's borders,[66] sometimes mandating that data remain exclusively

within the country and completely prohibiting cross-border data transfers.[67]

Each of these requirements has the potential to impede U.S. criminal investigations, whether conducted by law enforcement or by defense counsel. Companies that are prohibited from disclosing data are barred from sharing relevant evidence with investigators. Notification requirements can tip off individuals that they are under investigation. When those individuals are dangerous or untrustworthy, notice can threaten someone's life or physical safety, or risk tampering with and destruction of evidence. If account holders can force companies to delete data, then that data will no longer be available to investigators. And data localization makes it more difficult for investigators to route around these other requirements. As a result, demands for data stored abroad that are made outside of sanctioned MLAT procedures for resolving conflict-of-laws problems can, in the words of Google's former general counsel, force companies to "risk violating either the law of the requesting country or the law of the country where we are headquartered."[68]

Notably, the potential effects of new foreign data privacy, protection, and localization laws on cross-border criminal investigations are, at least in part, deliberate policy features designed to regulate law enforcement access to data across borders. Post-Snowden concerns over U.S. law enforcement surveillance conducted through non-MLAT channels are playing a prominent role in ongoing international policy debates about the laws and norms governing cross-border data transfers.[69] For instance, on July 16, 2020, the Court of Justice of the European Union (CJEU) 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.[70] In *Data Protection v. Facebook Ireland Limited and Maximillian Schrems (Schrems II)*,[71] the CJEU held that the privacy shield did not sufficiently protect EU personal data transferred to the U.S. from access by U.S. law enforcement and intelligence agencies.[72] By encouraging companies to store more EU personal data within the EU and out of reach of U.S. court jurisdiction,[73] *Schrems II* is likely to increase investigators' dependence on MLAT processes.

In a parallel and interlocking trend, there is substantial agreement within the U.S. that existing MLAT processes, designed as they were in the pre-internet age, are too slow for criminal investigations in an age of digital data that might be deleted before the legal process resolves,[74] and that

more efficient channels are needed to expedite law enforcement's access to data stored in foreign jurisdictions.[75] (Of course, law enforcement also has access to the letters rogatory process available to criminal defense investigators but generally does not use it due to its unpredictability and delay.)[76] Efforts to develop alternative non-MLAT routes for U.S. law enforcement to more efficiently access foreign data have, in turn, raised alarm among foreign policymakers. For instance, a report by a Centre for European Policy Studies task force on cross-border data in criminal proceedings expresses concern that U.S. law will encourage "direct private-public cooperation for cross-border data gathering [that] cannot be considered a satisfactory alternative to judicial cooperation."[77] In response, foreign lawmakers are seeking to close off routes for cross-border data transfers outside of sanctioned MLAT agreements. The European Data Protection Board (EDPB), for example, has advised that "where there is an international agreement such as an MLAT, EU companies should generally refuse direct requests and refer the requesting third-country authority to an existing mutual legal assistance treaty or agreement."[78]

As explained in more detail below, these developments risk reducing U.S. criminal defense investigators' access to cross-border data because defense counsel cannot use the sanctioned MLAT procedures, and their letters rogatory powers cannot pierce new foreign data privacy, protection, and localization laws designed to close off non-MLAT routes for access.

2. ASYMMETRICAL EFFECTS ON LAW ENFORCEMENT VERSUS DEFENSE INVESTIGATIONS

Foreign data privacy, protection, and localization laws risk imposing new asymmetrical effects on law enforcement and criminal defense investigations. To start, as with domestic U.S. privacy legislation, foreign privacy laws may contain exceptions that enable law enforcement to continue accessing sensitive information without parallel provisions for defense access. India's proposed data privacy bill of 2019, for instance, would allow public sector entities of the Indian government to compel companies to disclose data without users' consent but includes no similar provision for defense counsel to do the same.[79] Similarly, Brazil's Civil Rights Framework for the Internet and its Criminal Procedure Code each permits police or prosecutors to order

data preservation or compel disclosures of subscriber data in certain circumstances but contain no similar provisions for defense counsel.[80]

Further, even when foreign privacy laws lack exceptions for law enforcement investigations and impede U.S. law enforcement efficiency—and indeed foreign lawmakers may intend precisely that effect—the laws do not risk blocking law enforcement access altogether. Channeling cross-border investigations into MLAT processes and closing off alternative access routes still leaves law enforcement with MLAT powers to route around foreign data privacy and protection laws. The same cannot be said for criminal defense investigators, who stand to lose their existing letters rogatory powers.

To illustrate this asymmetry, consider Europe's recent General Data Protection Regulation (GDPR). The GDPR appears on its face to block legally compelled transfers of personal data to the U.S. unless the transfer is made pursuant to an MLAT or other international treaty.[81] Specifically, Article 48 of the GDPR states that a non-EU country's order requiring a service provider "to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty."[82] Hence, the GDPR expressly exempts MLAT transfers from its regulations, affording U.S. law enforcement the power to pierce GDPR restrictions on cross-border transfers of European data.[83] To be sure, Article 49(1)(e) also exempts transfers "necessary for the establishment, exercise or defense of legal claims."[84] And the EDPB has affirmed that the Article 49 exemption encompasses disclosures "necessary" for pretrial discovery, so long as the data go through a predisclosure minimization process.[85] Nevertheless, the requirement to establish the necessity of data rather than their mere relevance, and to comply with the minimization process, may prove too burdensome and expensive for indigent criminal defense teams to manage. The result would mean that U.S. law enforcement will retain its MLAT powers but the defense will have an even harder time obtaining a letter rogatory.

Notably, foreign legislators enacting data privacy and protection laws may be even less likely to account for defense investigative needs than are U.S. lawmakers[86] because many foreign nations have inquisitorial criminal legal systems that task state officials with investigating exculpatory as well as inculpatory evidence.[87] In these inquisitorial systems, MLAT access may also benefit the accused. Foreign policymakers responding to concerns about

U.S. law enforcement's extra-MLAT surveillance practices may be unaware that blocking non-MLAT routes for access can harm criminal defendants.[88] Policymakers in these nations—if they are concerned at all with U.S. criminal defendants—may incorrectly assume that accommodating U.S. law enforcement's investigative needs through MLATs or other bilateral agreements will suffice to protect the rights of the accused. If so, they would be wrong.

3. THE CLOUD ACT

While the combination of new foreign data privacy, protection, and localization laws with asymmetrical MLAT procedures already privileges law enforcement investigations of guilt over defense investigations of innocence, this is not the only structural legal disparity of its kind. Law enforcement's greatest recent buffer against data economy and privacy trends that threaten cross-border access to evidence may be the CLOUD Act. The CLOUD Act has two main parts, both of which—under current judicial readings of U.S. law—aid law enforcement investigative power without providing parallel benefits to criminal defense investigators.

One part of the CLOUD Act empowers the government to enter into a new series of bilateral executive agreements with other nations designed to supersede the MLAT system and expedite law enforcement cooperation across borders. The first such "CLOUD agreement," the U.K.-U.S. Bilateral Data Access Agreement, entered into force in July 2020. Like its MLAT predecessors, the U.K.-U.S. agreement is closed to defense investigators. It 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."[89] Given this precedent and the Justice Department's long-standing defense of MLAT asymmetries, there is little reason to think that future CLOUD Act agreements will account for defense investigative interests.

The other part of the CLOUD Act amended the SCA to provide law enforcement with a one-stop shop in U.S. court to compel disclosures of data stored abroad. 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 permits law enforcement to compel the company to produce that data solely through a U.S. court order, without resort to an MLAT,

even if the data are stored on a foreign server.[90] Specifically, the CLOUD Act amended the SCA to state that electronic communications service providers "shall comply with the obligations of this chapter [the SCA] to ... disclose the contents of a wire or electronic communication ... within such provider's possession, custody, or control, regardless of whether such communication ... is located within or outside of the United States."[91]

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. CLOUD Act orders are narrower than MLATs in that they solely reach companies subject to U.S. jurisdiction but more powerful than MLATs in that they can require disclosures that violate foreign laws, including foreign laws not pierced or waived by treaty.

For a somewhat circuitous reason, this CLOUD Act-decreed application of SCA procedural rules to data stored on foreign servers once again enhances law enforcement's investigative power without parallel benefits for the defense. This is because, under the current judicial consensus view of the SCA, explained in further detail below, SCA orders for communications contents are exclusively available to law enforcement—even for data stored within the U.S.[92] For over a decade, nearly every state and federal court to have squarely ruled on the issue has construed the SCA to unqualifiedly bar criminal defendants from subpoenaing service providers for content data.[93] Accordingly, under current law, the CLOUD Act amendment to the SCA entitles law enforcement seeking electronic communications data to circumvent foreign data privacy, protection, and localization laws by relying unilaterally on U.S. courts to compel access to foreign evidence but does not allow defense investigators to do the same.

III. THE CLOUD ACT SOLUTION TO CROSS-BORDER "PRIVACY ASYMMETRIES"

The CLOUD Act amendment to the SCA has provoked substantial public policy debate. From one perspective, the amendment effects an extraterritorial application of U.S. law enforcement's search and seizure power and is an example of the U.S. unilaterally bypassing the multisovereign-endorsed MLAT frameworks for transnational cooperation in gathering evidence.[94] From another perspective, the amendment merely codifies the status quo rule that persons and entities subject to U.S. jurisdiction can be compelled to produce documents within their "possession, custody, or control,"[95] regardless of where they choose to store those materials.[96] Despite this sustained attention, debates over the CLOUD Act appear to have entirely overlooked its potential effect on criminal defense investigations.

This section seeks to remedy that oversight. It builds on an argument I advance in depth elsewhere that, properly construed, the SCA's statutory text should yield to defendants' otherwise valid subpoena power.[97] This essay extends the analysis to contend that a proper reading of the CLOUD Act should grant both law enforcement and criminal defense investigators access to foreign data controlled by U.S. companies. Construing the statute in this manner is doctrinally correct. It would help to reverse the 50-year inequity in cross-border evidence gathering that MLAT asymmetries have imposed while avoiding the constitutional grounds that courts have relied on to justify those MLAT asymmetries. And it would afford defense investigators parallel access to at least one of the buffers that law enforcement enjoys against trends in the global data economy and foreign privacy laws that might otherwise impose disparities based on who has power to access evidence and who to withhold it. This solution is, admittedly, a partial one; it will enhance criminal defendants' access to evidence that U.S. corporations store abroad, but not to data possessed by foreign entities not subject to U.S. court jurisdiction. Nevertheless, it is a productive step toward greater parity in the truth-seeking process, and it is within the power of courts to implement immediately.

A. The plain text of the CLOUD Act's SCA amendment should help criminal defendants access cross-border evidence

As mentioned above, courts across the U.S. have nearly uniformly ruled that the SCA bars technology companies from complying with criminal defense subpoenas seeking certain types of data—specifically communications contents from another user's account—even when that data could establish innocence and are unavailable from other sources.[98] The pertinent language in the SCA statute states that electronic communication service providers "shall not knowingly divulge to any person or entity the contents of a communication,"[99] and then enumerates a series of express exceptions for permissible disclosures, including to law enforcement pursuant to certain forms of legal process.[100] There is no express exception for disclosures to criminal defense investigators.[101] Courts have applied an expressio unius canon of statutory interpretation to this language and concluded that the presence of an enumerated exception permitting disclosures to law enforcement and the absence of a similar enumerated exception for defense investigators means that Congress must have intended to bar disclosures to the defense.[102] As a result, current judicial consensus holds that the SCA permits law enforcement to compel service providers to disclose content data but prohibits defense counsel from doing the same.[103] Under this interpretation of the statutory text, the CLOUD Act's extension of SCA procedures to cover data that U.S. corporations store abroad will asymmetrically enhance law enforcement's access to cross-border data without similar benefit for the defense.

However, as I have argued in depth elsewhere, the current consensus view that the SCA bars criminal defense subpoenas is wrong.[104] This consensus reading erroneously construes silence in the SCA's text to create a statutory evidentiary privilege that blocks otherwise valid legal process. Reading statutory silence in this manner violates binding interpretive rules for evidentiary privileges. Specifically, the Supreme Court has repeatedly declared that courts must construe privileges narrowly because they are "in derogation of the search for truth,"[105] and must not read federal statutes to "suppress otherwise competent evidence unless the statute, strictly construed, requires such a result."[106] Ambiguous silence in statutory text does not require such a result. Thus, courts should read the SCA's ambiguous

silence as to disclosures to defense investigators to yield to criminal defendants' otherwise valid compulsory legal process rights.[107] In other words, they should construe the statutory language commanding that electronic communication service providers "shall not knowingly divulge to any person or entity the contents of a communication" as a mere confidentiality rule that, like banks' or accountants' duties of confidentiality, yields to judicial compulsory process.[108]

Applying this strict construction privilege interpretation to the SCA would mean that the CLOUD Act amendment does not merely permit law enforcement to compel U.S. companies to disclose data stored on foreign servers; it also permits criminal defendants to do the same. There are two reasons for this. The first is readily apparent; construing the SCA privacy provision as a confidentiality rule, rather than a privilege rule, would mean that the SCA no longer blocks criminal defense subpoenas to U.S. technology companies seeking communications contents. And, under the normal subpoena rules, a nongovernmental litigant can compel a company that is subject to U.S. court jurisdiction to disclose evidence within its possession, custody, or control, even if the company stores that evidence abroad.[109] Hence, if defense subpoenas to U.S. technology companies seeking communications contents are SCA-compliant, then they should also be able to reach data stored abroad.

The second reason is somewhat less obvious and pertains to the broad context in which Congress enacted the CLOUD Act. As explained in further detail below, the Act resolved an ongoing ambiguity as to whether law enforcement orders compelling technology companies to disclose the contents of stored communications were warrant-like or subpoena-like for purposes of an extraterritoriality analysis. By ordering technology companies to comply with those orders for data stored abroad, the CLOUD Act favors a subpoena-like view. And the more subpoena-like these orders are, the more squarely they fall within defense investigators' standard tool set.

In short, law enforcement's latest buffer against the erosion of its own access to foreign data—the CLOUD Act amendment of the SCA—should also buffer defense subpoenas.

B. Defense access to data under the CLOUD Act would avoid the grounds that courts have relied on to reject defense access to MLAT procedures

CLOUD Act-enabled defense subpoenas should increase defense access to evidence stored abroad while avoiding the constitutional grounds that courts have relied on to uphold MLAT asymmetries in the past. To date, challenges to the constitutionality of MLAT asymmetries have failed for two key reasons. *First*, courts have reasoned that defendants' Sixth Amendment right to compulsory process does not generally extend beyond U.S. borders. *Second*, courts have reasoned that defendants' Sixth Amendment and due process rights to present a defense merely entitle them to access the compulsory process powers of the judiciary, not those of the executive branch, and that law enforcement's exclusive access to cross-border data derives from the latter. Both lines of constitutional reasoning are irrelevant to the SCA portion of the CLOUD Act because that part of the CLOUD Act is premised on the notion that court orders to U.S. corporations are not extraterritorial, even when the orders require cross-border productions of data. Hence, under the CLOUD Act logic, defense subpoenas for evidence stored abroad would be supported by defendants' constitutional as well as statutory rights to compulsory legal process. The following section lays out these arguments in greater detail.

1. AVOIDS EXTRATERRITORIAL REACH OF DEFENDANTS' COMPULSORY PROCESS RIGHTS

Courts have held repeatedly that criminal defendants' lack of access to MLAT procedures does not violate the Sixth Amendment right to compulsory process because defendants' compulsory process rights do not normally reach beyond the territorial U.S.[110] There are some exceptions to this rule that are triggered by governmental misconduct. For instance, courts may find a Sixth Amendment or due process violation if the government caused the loss of defense access to foreign evidence, such as by deporting material defense witnesses[111] or by denying such witnesses entry into the country to testify voluntarily.[112] But absent such misconduct, courts reason that defendants lack compulsory process rights to evidence "when *a court itself* cannot compel" access to that evidence.[113] Courts themselves generally lack power to compel cross-border evidence disclosures.[114] As a result, courts have found that "a

defendant's constitutional right to compulsory process is not implicated by a court's refusal to order the Executive Branch to invoke [an] MLA Treaty in favor of a defendant."[115]

The CLOUD Act should flip this logic because the Act establishes that subpoenas to U.S. corporations for data stored abroad are not extraterritorial applications of compulsory process. This result is clear from the plain text of the CLOUD Act, which states that corporations "shall comply" with SCA orders "regardless of whether such communication, record, or other information is located within or outside of the United States."[116] To more fully understand the rejection of extraterritoriality that this language embodies, it will be helpful to provide some additional context about the history of the CLOUD Act.

The story of the CLOUD Act began years before its enactment, in December of 2013, when law enforcement officers investigating a drug-trafficking case served Microsoft with an SCA order for the contents of emails from one of its web-email service's customer accounts.[117] Microsoft refused to comply, arguing that the email contents were stored exclusively on a server in Ireland[118] and that the order lacked extraterritorial effect.[119] Microsoft and the Justice Department fought this case, *United States v. Microsoft (Ireland)*, all the way up to the Supreme Court.[120] Before the Court could decide the issue, Congress mooted the case by enacting the CLOUD Act of 2018.[121]

Microsoft (Ireland) focused on certain provisions of the SCA that regulate government access to electronic communications contents.[122] 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.[123] The disagreement focused on whether the SCA procedures for government access qualified as a subpoena, in which case the normal subpoena production rule should apply and permit access to data stored abroad, or whether those procedures instead qualified as a warrant that conscribes the recipient into an agent of law enforcement who must execute a search and seizure, in which case a presumption against extraterritorial searches and seizures should apply and block access to data stored abroad.[124] The CLOUD Act dictated the result that SCA orders are subpoena-like, at least for purposes of an extraterritoriality analysis.

While criminal defense investigators have well-established subpoena power, their entitlement to court orders that compel conduct similar to a law enforcement search or seizure is more ambiguous.[125] By adopting a subpoena-like characterization of SCA orders, rather than a search-like characterization, the CLOUD Act supports the view that defense investigators should be able to subpoena technology companies for stored communications contents. Hence, the CLOUD Act adds further reason to construe the SCA to yield to defense subpoenas, both defense subpoenas in general and, specifically, defense subpoenas to U.S. companies for data stored abroad. Further, if courts do not construe the SCA to yield to these defense subpoenas, the CLOUD Act lays the groundwork for a constitutional challenge. Specifically, the CLOUD Act dictates the conclusion that SCA orders for data stored abroad do not reach beyond the ordinary jurisdiction and powers of the courts. Hence, unlike with MLATs, even current doctrine would support the claim that categorically denying defense access to such orders may violate defendants' Sixth Amendment right to compulsory process.

2. AVOIDS THE COMPULSORY PROCESS POWERS OF THE EXECUTIVE BRANCH

The second reason courts have repeatedly upheld the constitutionality of MLAT asymmetries is related to the first; defendants' compulsory process rights do not generally reach the compulsion powers of the executive branch. Accordingly, courts in the Eastern District of Virginia explained in one case that "the right to compulsory process … cannot be stretched to include compelling the invocation of treaty process powers available only to the executive branch,"[126] and in another case 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."[127] Meanwhile, balance of powers concerns discourage courts from ordering police and prosecutors to exercise executive branch powers on behalf of the defense.[128] For instance, the U.S. Court of Appeals for the D.C. Circuit held that the government had no obligation to use its MLAT powers on behalf of the defense 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.[129]

The MLAT opinions are thin on reasoning about the relationship between judicial and executive powers, but this relationship is illuminated further in related case law on selective immunity. A witness who asserts the Fifth Amendment privilege against self-incrimination can be compelled to testify if the government immunizes that witness from future criminal prosecution based on the testimony.[130] In current doctrine, neither the court nor the defense has a similar power to grant immunity to defense witnesses.[131] Nonetheless, courts have consistently found that the prosecution's refusal to immunize a defense witness in order to enable a defendant to compel exculpatory testimony from that witness does not violate the Constitution.[132] In other words, selective immunity is an asymmetrical investigative power, and courts have upheld that asymmetry as constitutional. Here too, government misconduct may trigger some exceptions. Courts may find a due process violation if prosecutors withhold a grant of selective immunity with the bad faith intent of distorting the fact-finding process.[133] But, in general, courts have upheld the prosecution's exclusive power to compel testimony from witnesses who assert their Fifth Amendment privilege.[134]

Once again, the CLOUD Act should flip this logic to favor defense subpoenas to U.S. companies in general, and specifically to favor such subpoenas seeking data stored abroad. By construing SCA orders as subpoena-like rather than warrant-like, the CLOUD Act has characterized these orders as a form of legal process that lies squarely within the powers of the judiciary. Hence, defendants serving CLOUD Act subpoenas need not petition for assistance from the prosecution. Instead, they can rely on their own constitutionally grounded and statutorily endorsed subpoena rights to request compulsory process from the courts.

IV. CONCLUSION

DEBATES ABOUT GLOBAL DATA PRIVACY have largely overlooked the criminally accused. Data privacy laws may appear as private laws regulating consumer protection for the global data economy. Or they may appear as public laws regulating law enforcement investigations. Both can be true. But myopic focus on either ignores the distributional distortions and democratic harms of data privacy laws that grant more power to law enforcement seeking evidence of guilt than to defense investigators seeking evidence of innocence.[135] This essay has begun to rectify the awareness gap by documenting that, and how trends in the global data economy, combined with foreign data privacy laws, risk selectively suppressing criminal defense access to evidence of innocence. The essay has also taken an initial step toward fixing these harms by arguing that the U.S. CLOUD Act supports not only law enforcement's but also criminal defense investigators' entitlement to judicial process to compel U.S. companies to disclose data stored on foreign servers. We should not grant law enforcement the power to compel private companies to disclose evidence of guilt while granting those same companies the power to suppress evidence of innocence. At this moment of overdue national reckoning with police violence, mass incarceration, racism, classism, and other structural disparities in the criminal legal system, data privacy law must do better.

NOTES

1 This essay is an excerpt from a forthcoming article with the Texas Law Review entitled *Life, Liberty, and Data Privacy: The Global Cloud and the Criminally Accused*, 101 Tex. L. Rev. __ (forthcoming 2023).

2 18 U.S.C. §§ 2701-12.

3 These facts are based on *In re* Application of Colone, No. 20-517083 (Cal. Sup. Ct. July 28, 2020). For additional details, see Colone v. Superior Ct. of Cal., 20-1474 (Cal. Ct. App. Oct. 4, 2021).

4 *See, e.g.*, *Mutual Assistance and Making Requests*, Crown Law, https://www.crownlaw.govt.nz/ [https://perma.cc/4XDK-FLVE] (last visited July 5, 2021) (describing the Mutual Assistance in Criminal Matters Act 1992 (MACMA) and listing the U.S. as a partner country); *Mutual Assistance*, Crown Law, https://www.crownlaw.govt.nz/assistance-for-foreign-authorities/mutual-assistance/ [https://perma.cc/CK28-PUDE] (last visited Sept. 30, 2021) (describing Mutual Legal Assistance Treaty); *Making Requests*, Crown Law, https://www.crownlaw.govt.nz/assistance-for-foreign-authorities/making-requests/ [https://perma.cc/ST2J-K5VW] (last visited Sept. 30, 2021) (describing the U.S. as a party country).

5 *See generally* Paul Schwartz, *Legal Access to the Global Cloud*, 118 Colum. L. Rev. 1681, 1714-20 (2018) (examining the post-CLOUD Act extraterritorial reach of the SCA as applied to different cloud computing models).

6 Brady v. Maryland, 373 U.S. 83 (1963), and its progeny merely require the prosecution team to disclose material exculpatory evidence that is within their control; these cases do not require law enforcement to investigate exculpatory evidence that is beyond the prosecution team's control. *See, e.g.*, United States v. Hughes, 211 F.3d 676, 688 (1st Cir. 2000). Prosecutors have some domain-specific duties, for instance to seek out exculpatory information, such as information suggesting that a confidential informant may be unreliable. *See Criminal Justice Standards for Prosecutorial Investigations: Standard 2.4(e)*, Am. Bar Ass'n (Feb. 2008), https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice_section_archive/crimjust_standards_pinvestigate/#2.4 [https://perma.cc/T8QL-7F5J]. But law enforcement has no general responsibility to investigate evidence of innocence.

7 *See generally* U.S. Const. amends. V, VI, XIV; Fed. R. Crim. P. 16.

8 *Cf.* David Singh Grewal, et al., *Toward a Manifesto: The LPE Project*, LPE Project (Nov. 11, 2017), https://lpeproject.org/blog/law-and-political-economy-toward-a-manifesto/ [https://perma.cc/5YT6-4C6C] (observing that law "conditions race and wealth" as well as "the political order through which we must respond").

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

10 *See* Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. Rev. 212 (2021).

11 *Cf.* Brandon Garrett, *Big Data and Due Process*, 99 Cornell L. Rev. Online 207, 211-13 (2014) (discussing *Brady's* application to digital evidence possessed by the government); Andrew Ferguson, *Big Data Prosecution and Brady*, 67 UCLA L. Rev. 180, 238-41 (2020) (discussing how big data systems controlled by prosecutors risk exacerbating structural weaknesses in the *Brady* doctrine).

12 *See generally* Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 Harv. L. Rev. 2721 (2021) (documenting and arguing against corporate claims that the Stored Communications Act, a key data privacy law for the internet, entitles technology companies to withhold relevant evidence from criminal defendants); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stan. L. Rev. 1343 (2018) (documenting and arguing against corporate claims that trade secret law entitles them to withhold relevant evidence from criminal defendants).

13 Julie E. Cohen, Between Truth And Power: The Legal Constructions of Informational Capitalism 5 (2019) (defining "informational capitalism" as "the alignment of capitalism as a mode of production with informationalism as a mode of development").

14 Throughout, I use the term "U.S. corporations" to include corporations subject to U.S. jurisdiction.

15 *See, e.g.*, Anupam Chander, *Is Data Localization a Solution for* Schrems II?, 23 J. Int'l Econ. L. 771 (Sept. 2020); Jennifer Daskal, *Borders and Bits*, 71 Vand. L. Rev. 179, 186-91 (2018); Kristen Eichensehr, *Data Extraterritoriality*, 95 Tex. L. Rev. 145 (2017); Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729, 745-48 (2016).

16 *See, e.g.*, *Transforming a Broken System: A Symposium on Criminal (In)justice in America*, L. & Pol. Econ. Blog

(Sept. 21, 2020), https://lpeproject.org/blog/transforming-a-broken-system-a-symposium-on-criminal-injustice-in-america/ [https://perma.cc/2XKD-BMAR].

17 *See, e.g.*, Julie E. Cohen, *How (Not) to Write a Privacy Law*, Knight First Amend. Inst. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/UT7U-WLXD]; Amy Kapczynski, *The Law of Informational Capitalism*, 129 Yale L. J. 1460 (2020) (reviewing Shoshana Zuboff, The Age of Surveillance Capitalism (2019) and Julie E. Cohen, Between Truth nd Power (2019)).

18 *Cf.* Troubling Transparency 5-8 (David Pozen & Michael Schudson eds., 2018) (surveying critiques of FOIA and arguing that an uncritical acceptance of government transparency ideals "at worst, smuggles in antigovernment biases on the sly").

19 For example, Anna Roberts has identified and challenged uses of the word "victim" in state constitutions, criminal codes, and procedural rules that risk declaring guilt pre-adjudication by presuming a crime occurred. *See* Anna Roberts, *Victims, Right?*, 42 Cardozo L. Rev. 1449 (2021).

20 For instance, Jocelyn Simonson has powerfully critiqued the "people/defendant dichotomy" in criminal procedure rules and practices that presume prosecutors, rather than defense counsel, represent the public interest in court. *See* Jocelyn Simonson, T*he Place of "The People" in Criminal Procedure*, 199 Colum. L. Rev. 249, 255 (2019).

21 *See* Wexler, *Life, Liberty, and Trade Secrets*, *supra* note 12.

22 *See* Wexler, *supra* note 10 (identifying multiple privacy statutes that impose procedural disparities on law enforcement versus defense investigative power).

23 *See* Wexler, *Privacy as Privilege*, *supra* note 12 (arguing that courts have erroneously construed a key data privacy law for the internet *as* an evidentiary privilege).

24 *See* Grewal et al., *supra* note 8 (call to reject an "artificial division between the economy and politics"). *See also* Elizabeth Joh, *Police Surveillance Machines: A Short History*, L. & Pol. Econ. Blog (June 13, 2018), https://lpeproject.org/blog/police-surveillance-machines-a-short-history/ [https://perma.cc/V887-3F42]; Elizabeth Joh, *Undue Influence of Surveillance Technology Companies on Policing*, 91 N.Y.U. L. Rev. Online 101 (2017).

25 *See* Jedediah Britton-Purdy et al., *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 Yale L. J. 1784, 1790-93 (2020).

26 *See, e.g.*, Meg Leta Jones & Margot Kaminski, *An American's Guide to the GDPR*, 98 Denver L. Rev. 93, 97-101 (2020) (distinguishing concepts of privacy from concepts of data protection in U.S. and EU law).

27 *See, e.g.*, *In re* Commissioner's Subpoenas, 325 F.3d 1287, 1291 (11th Cir. 2003).

28 T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Fed. Jud. Ctr. Int'l Litig. Guide 2 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf [https://perma.cc/GJP4-Y2R5]. *See also* C. Todd Jones, *Compulsion over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 Nw. J. Int'l L. & Bus. 454, 472 (1992).

29 *See In re ex parte* Application of Sapporo Ota Psychiatry Hosp., Applicant, No. 20-MC-80147-VKD, 2020 WL 5526674, at *2 (N.D. Cal. Sept. 15, 2020) (quoting IPCom GmbH & Co. KG v. Apple, Inc., 61 F. Supp. 3d 919, 922 (N.D. Cal. 2014)).

30 Department of Justice, *Letters Rogatory*, Crim. Just. Manual § 275.

31 Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 531 (1987) (letter to president advocating the Hague Evidence Convention on the Taking of Evidence Abroad, which offers civil litigants more efficient mechanisms to collect foreign evidence). Notably, the Hague Convention, a multilateral treaty which took effect in 1972, somewhat expedited the process "in civil or commercial matters," 20 U.S.C. § 1781, by permitting litigants to submit letters directly to a designated Central Authority in each contracting State. *See generally* Tony Abdollahi, *The Hague Convention: A Medium for International Discovery*, 40 N.C. J. Int'l L. & Com. Reg. 771, 796 (2015). The Hague Convention is not available to criminal defendants. *See, e.g.*, United Kingdom v. United States, 238 F.3d 1312, 1317-18 (11th Cir. 2001).

32 *See* James Knapp, *Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy*, 20 Case W. J. Int'l L. 405, 410 (1988) (letters rogatory are generally insufficient to pierce foreign bank secrecy and other privacy laws).

33 *Id.* at 410 & n.5.

34 *See, e.g.*, United States v. Vetco, 644 F.2d 1324, 1333 (9th Cir. 1981).

35 *See generally* U.S. Department of State, 7 Foreign Affairs Manual, § 962.1, https://fam.state.gov/FAM/07FAM/

07FAM0960.html#M962_1 [https://perma.cc/9VJG-RFUM].

36 *See* Funk, *supra* note 28, at n.14.

37 *See* Knapp, *supra* note 32, at 405.

38 *See* Funk, *supra* note 28, at 2.

39 *See* United Kingdom v. United States, 238 F.3d 1312, 1315 (2001).

40 *See* Michael Abbell, *DOJ Renews Assault on Defendants' Right to Use Treaties to Obtain Evidence from Abroad*, The Champion, Aug. 1997, at 20-21.

41 *See* United States v. Rosen, 240 F.R.D. 204, 213 & n.22 (E.D. Va. 2007).

42 *See* Funk, *supra* note 28, at 12. *See also* Abbell, *supra* note 40, at 21 (Justice Department "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 Lawyer 189, 190 & nn. 5-7 (1985).

43 MLA Treaty Art. 1 ¶ 4.

44 *See* United Kingdom v. United States, 238 F.3d 1312, 1317 (11th Cir. 2001).

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

46 *See* United States v. Rosen, 240 F.R.D. 204, 214 (E.D. Va. 2007); United States v. Odom, 53 M.J. 526, 537 (N.M. Ct. Crim. App. 2000); United States v. Amador-Galvan, 215 F.3d 1334, 1334 (9th Cir. Apr. 7, 2000).

47 Frank Tuerkheimer, *Globalization of U.S. Law Enforcement: Does the Constitution Come Along?*, 39 Hous. L. Rev. 307, 369 (2002). For additional scholarship on the issue, see Daniel Huff, *Witness for the Defense*, 15 Tex. Rev. L. & P. 129, 16-62 (2010); 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 (2008); 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 Wash. Int'l L. J. 561, 580 (2003).

48 *See, e.g., Extradition, Mutual Legal Assistance and Prisoner Transfer Treaties: Hearing Before the S. Comm. on Foreign Rel's*, 105th Cong. 8 (1998), at 27 (letter from Mark M. Richard, Deputy Assistant Attorney Gen., to Patricia McNerney, Counsel, Foreign Relations Comm. (Oct. 8, 1998)).

49 *See, e.g.*, Abbell, *supra* note 40, at 21.

50 Lauren Briggerman et al., *Challenges to Obtaining Foreign Evidence in Cross-Border Criminal Cases*, The Champion, Nov. 2019, at 31.

51 *Extradition, Mutual Legal Assistance and Prisoner Transfer Treaties*, *supra* note 48.

52 Abbell, *supra* note 40, at 21-22.

53 *See* Transcript of Proceedings, Status Conference, United States v. Nanne Nogendoom, No. A98-0087-CR (D. Alaska July 15, 1999) (cited in Bruce Zagaris, International White Collar Crime: Cases and Materials 409, n.12 (2015)).

54 Briggerman, et al., *supra* note 50, at 31.

55 *See, e.g.*, Richardson, *supra* note 47, at 64-67, 79 & n.76 (describing fact patterns in which criminal defendants in the U.S. were denied process to obtain relevant and material evidence located abroad, and contextualizing the issue in "the rise of global crime").

56 Specifically, Federal Rule of Criminal Procedure 15 permits defendants to seek discretionary approval from a court to take depositions of witnesses outside the U.S., Fed. R. Crim. P. 15(c)(3), which a court "may" grant "because of exceptional circumstances and in the interests of justice," Fed. R. Crim. P. 15(a)(1). Defendants are not guaranteed court approval for the taking of these depositions. The Walsh Act also authorizes U.S. courts to issue criminal subpoenas to U.S. nationals or residents located abroad on a showing of "necessary in the interest of justice," but does not apply to foreign nationals. 28 U.S.C. § 1783. For a discussion of the Walsh Act and criminal defendants' compulsory process rights, see Gillars v. United States, 182 F.2d 962, 978 (D.C. Cir. 1950).

57 *See, e.g.*, United States v. Rosen, 240 F.R.D. 204, 208-09 (E.D. Va. 2007) (applying *Brady* "materiality" standard plus "[necessity] to prevent a failure of justice").

58 *Cf.* Briggerman et al., *supra* note 50, at 36 ("As criminal cases become increasingly cross-border in nature, the need for defendants to obtain evidence located abroad has become more common.").

59 *See, e.g.*, Schwartz, *supra* note 5, at 1693 (describing a "Data Shard cloud … [which] breaks data into small components, or shards, which the system routes around the globe, with different bits shifted between various locations").

60 *See, e.g.*, 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*, 6 (White Paper, Apr. 2019) (noting that effective criminal investigations increasingly require cross-border data disclosures).

61 *See* 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. of Am. L. 687, 704, 708-09 (2017).

62 *See, e.g.*, Stephanie Kirchgaessner, *How NSO Became the Company Whose Software Can Spy on the World*, 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/WWB4-W5RE].

63 *See* U.S. Gov't Accountability Off., GAO-21-435SP, Forensic Technology: Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcomes 42 (July 2021) (documenting a forensic software vendor's refusal to grant research licenses to independent academics).

64 Cohen, *supra* note 13.

65 *See, e.g.*, Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)* 3-4 (Santa Clara Univ. Legal Studies Rsch. Paper, July 1, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 [https://perma.cc/W5W3-H8S7].

66 *See* Courtney Bowman, *Data Localization Laws: An Emerging Global Trend*, Jurist (Jan. 6, 2017), https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/ [https://perma.cc/8RKD-77NM].

67 For example, a 2019 "Personal Data Protection Bill" introduced in India would entirely prohibit transferring "critical personal data," such as biometric and genetic data, outside of India. *See* The Personal Data Protection Bill, Bill No. 373 (2019) (India), http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf [https://perma.cc/C6Y3-LPGM].

68 Kent Walker, *Realign Laws on Evidence-Gathering on the Internet, Google GC Says*, A.B.A. J. (Aug. 24, 2017, 8:00 AM), https://www.abajournal.com/legalrebels/article/realign_laws_on_evidence_gathering_on_the_internet_google_gc_says [https://perma.cc/RW68-RB8C].

69 *See generally* Sergio Carrera et al., Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice 5 (Oct. 2020), https://www.ceps.eu/download/publication/?id=30689&pdf=TFR-Cross-Border-Data-Access.pdf [https://perma.cc/V55T-KZQP]; Swire & Hemmings, *supra* note 61, at 712.

70 *See generally* Ishita Mattoo, *The E.U.-U.S. Privacy Shield Invalidated in "Schrems II,"* Berkeley Tech. L. J. Blog (May 17, 2021), https://btlj.org/2021/05/the-e-u-u-s-privacy-shield-invalidated-in-schrems-ii/ [https://perma.cc/73UE-VZBF].

71 Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. and Maximillian Schrems, [2020] ECLI:EU:C:2020:559 (Ir.).

72 *See* Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, Lawfare Blog (July 17, 2020, 11:31 AM), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision [https://perma.cc/B6XT-W4DN].

73 For a description of the conundrum that *Schrems II* placed companies in concerning personal data transfers, see Caitlin Fennessy, *A Multilateral Surveillance Accord: Setting the Table*, Lawfare Blog (Apr. 23, 2021, 8:01 AM), https://www.lawfareblog.com/multilateral-surveillance-accord-setting-table [https://perma.cc/88FL-4SYX].

74 *See, e.g.*, Mirko Hohmann & Sophie Barnett, System Upgrade: Improving Cross-Border Access to Electronic Evidence (Jan. 2019), https://www.gppi.net/media/GPPi_2018_Hohmann_Barnett_System_Upgrade.pdf [https://perma.cc/N72R-AVAV]; Greg Nojeim, *MLAT Reform: A Straw Man Proposal*, Ctr. for Democracy & Tech. (Sept. 3, 2015), https://cdt.org/insights/mlat-reform-a-straw-man-proposal [https://perma.cc/XUH3-M7HN].

75 *See generally* Swire & Hemmings, *supra* note 61, at 708-10 (observing an average ten-month delay in obtaining evidence through the MLAT process and advocating for more efficient MLAT procedures).

76 *See* Robert Neale Lyman, Note, *Compulsory Process in a Globalized Era: Defendant Access to Mutual Legal Assistance Treaties*, 47 Va. J. Int'l L. 261, 273-75 (2006).

77 Carrera et al., *supra* note 69, at 42 (internal quotation marks omitted).

78 European Data Prot. Bd., *Annex, Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence*, at 3 (July 10, 2019), https://

edpb.europa. eu/sites/default/files/files/file2/edpb_edps_joint_response_ us_cloudact_annex.pdf [https://perma.cc/MRK8-J9HW].

79 *See* The Personal Data Protection Bill, Bill No. 373 (2019) (India), http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf [https://perma.cc/C6Y3-LPGM].

80 *See* Civil Framework of the Internet, Law No. 12.965 Subsect. I, § 2 (Braz.); C.P.P. Art. 13-A (Braz.). *See also* Laws No. 12.850 and 9.613 (permitting police or prosecutors to request subscriber data in money laundering and organized crime investigations but containing no similar provision for defense investigators).

81 *See, e.g.*, Council of Bars and L. Socy's of Eur. [CCBE], *CCBE Assessment of the U.S. CLOUD Act*, at 7 (Feb. 28, 2019).

82 Commission Regulation 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119), 48.

83 *Id.* (concluding that, under GDPR Article 48, "only MLATs or comparable international agreements provide a permissible basis for the extraterritorial transfer of personal data").

84 Commission Regulation 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119), 49.

85 *See* N.Y.C. Bar E-Discovery Working Grp., Cross-Border E-Discovery: Navigating Foreign Data Privacy Laws and Blocking Statutes in U.S. Litigation 8 (Feb. 2020), https://s3.amazonaws.com/documents.nycbar.org/files/2017324-EDiscovery_Working_Group_Memo.pdf [https://perma.cc/PT4W-AKXZ]. If the word "claims" is construed to include criminal charges, then the GDPR might yield to defendants' letters rogatory if defendants can make a sufficiently strong showing of need for the information. However, even here the GDPR may impose higher burdens on criminal defense investigators than on law enforcement to show that the information they seek is "necessary," rather than merely relevant.

86 *Cf.* Wexler, *supra* note 10 (documenting that U.S. legislators enacting privacy laws often unintentionally overlook defense investigative needs).

87 *See* Abraham S. Goldstein, *Reflections on Two Models: Inquisitorial Themes in American Criminal Procedure*, 26 Stan. L. Rev. 1009, 1019 (1974) (explaining that the investigating magistrate in inquisitorial legal systems "seeks all logically probative evidence").

88 *Cf.* Carrera et al., *supra* note 69, at 32 (instructing European readers about the asymmetrical investigative powers of U.S. law enforcement and U.S. criminal defense counsel).

89 Agreement Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purposes of Countering Serious Crime, Gr. Brit. & N. Ir.-U.S, Preamble; Art. 3.4, Oct. 3, 2019 [hereinafter CLOUD Act].

90 *See* 18 U.S.C. §§ 2702(b)(2), 2703 & 2713.

91 18 U.S.C. § 2713 (2018).

92 *See* Wexler, *Privacy as Privilege*, *supra* note 12.

93 *Id.*

94 *See, e.g.*, Johannes Thumfart & Paul De Hert, *Both the US's Cloud Act and Europe's GDPR Move Far Beyond Geography, But Will Not Solve Transatlantic Jurisdictional Conflicts*, Just Sec. (June 4, 2018), https://www.justsecurity.org/57346/uss-cloud-act-europes-gdpr-move-geography-solve-transatlantic-jurisdictional-conflicts/ [https://perma.cc/6UE5-V8MK].

95 See Fed. R. Civ. P. 45(a)(1)(A)(iii); Fed. R. Crim. P. 17.

96 U.S. courts have authority to subpoena documentary evidence from anyone within the court's personal jurisdiction, including documentary evidence stored abroad. *See, e.g.*, In the Matter of a Grand Jury Subpoena Directed to Marc Rich & Co., 707 F.2d 663, 667 (2d Cir. 1983). The courts also have authority to subpoena U.S. nationals and residents located abroad. *See* 28 U.S.C. § 1783. Perhaps to help alleviate controversy, the Justice Department has instructed federal prosecutors to seek enterprise customer data directly from an enterprise where possible, rather than using a CLOUD Act SCA order to obtain the data from a service provider. U.S. Dep't of Just., *supra* note 60, at 17.

97 *See generally* Wexler, *Privacy as Privilege*, *supra* note 12.

98 For foundational work on this issue, see Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 Cornell L. Rev. 981, 1057-64 (2014); Marc J. Zwillinger & Christian S. Genetsky, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. Crim. L. & Criminology 569 (2007).

99 18 U.S.C. § 2702(a)(1).

100 *See id.* § 2702(b)(1)-(9).

101 *Id.*

102 *See, e.g.*, Facebook, Inc. v. Wint, 199 A.3d 625, 629 (D.C. 2019) (collecting criminal subpoena cases).

103 *Id*. *See also* P.P.G. Indus., Inc. v. Jiangsu Tie Mao Glass Co., Ltd., 273 F. Supp. 3d 558, 560-61 (W.D. Pa. 2017) (collecting civil subpoena cases).

104 *See generally* Wexler, *Privacy as Privilege*, *supra* note 12.

105 United States v. Nixon, 418 U.S. 683, 710 (1974).

106 St. Regis Paper Co. v. United States, 368 U.S. 208, 218 (1961).

107 Wexler, *Privacy as Privilege*, *supra* note 12.

108 *Id*.

109 *See* 28 U.S.C. § 1783. Note that Fourth Amendment constraints on governmental litigants' power to issue certain subpoenas may limit their extraterritorial reach. See Jim Dempsey & Greg Nojeim, *Neither Warrants nor Subpoenas Should Reach Data Stored Outside the US*, Ctr. for Democracy and Tech. (July 30, 2014), https://cdt.org/insights/neither-warrants-nor-subpoenas-should-reach-data-stored-outside-the-us/ [https://perma.cc/U3FF-Q6KY].

110 *See, e.g.*, United States v. Theresius Filippi, 918 F.2d 244, 247 (1st Cir. 1990).

111 *See, e.g.*, United States v. Pena-Gutierrez, 222 F.3d 1080, 1085 (9th Cir. 2000); Unites States v. Valenzuela-Bernal, 458 U.S. 858, 872-73 (1982).

112 *Filippi*, 918 F.2d at 247-48.

113 United States v. Rosen, 240 F.R.D. 204, 214 (E.D. Va. 2007).

114 *See* United States v. Moussaoui, 382 F.3d 453, 463-64 (4th Cir. 2004); United States v. Zabaneh, 837 F.2d 1249, 1259-60 (5th Cir. 1988). *Cf.* Anna Vancleave, *The Right to Inter-Sovereign Disclosure in Criminal Cases*, 2013 Wis. L. Rev. 1407, 1436-37 (2013) (federal sovereign immunity from state court compulsory process). To be sure, courts do have authority to issue letters rogatory. *See* United States v. Staples, 256 F.2d 290, 292 (9th Cir. 1958); *Rosen*, 240 F.R.D. at 213. But letters rogatory draw on the discretionary exercise of judicial comity between courts of different nations, rather than on the judicial compulsion power arising from courts' duty to resolve cases and controversies within their jurisdiction. *See, e.g.*, *In re* Pacific Railway Comm'n, 32 F. 241, 256-67 (C.C.N.D. Cal. 1887).

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

116 18 U.S.C § 2713.

117 In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 15 F. Supp. 3d 466, 468 (S.D.N.Y. 2014) (hereinafter *In re Warrant*).

118 Br. of Appellant at *2, *In re Warrant*, No. 14-2985-cv, 2014 WL 7004807 (2d Cir. Dec. 8, 2014).

119 *In re Warrant*, 15 F. Supp. 3d at 467-68, 470. *See also In re Warrant*, 829 F.3d 197, 201-02 (2d Cir. 2016) (agreeing with Microsoft and quashing the warrant).

120 United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

121 18 U.S.C. § 2713.

122 *See* 18 U.S.C. § 2703(b).

123 Br. of United States at *7, United States v. Microsoft Corp., No. 17-2, 2017 WL 6205806 (U.S. Dec. 6, 2017) (internal citations and quotation marks omitted).

124 *In re Warrant*, 829 F.3d at 201.

125 This is a murky and underexamined legal question. Examples of judicial orders that are available to defendants, and that are at least superficially similar to law enforcement searches and seizures, include physical location inspection orders and bench warrants for witnesses who fail to appear. For a discussion of the relationship between defendants' use of these forms of compulsory process and the Fourth Amendment, *see* Wexler, *supra* note 10, at 250-54.

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

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

128 *See generally* Funk, *supra* note 28, at 12-14.

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

130 *See* 18 U.S.C. § 6002.

131 *See generally* Robert M. Schoenhaus, *Right of Defendant in Criminal Proceedings to Have Immunity from Prosecution Granted to Defense Witness*, 4 A.L.R. 4th 617 (1981).

132 *Id*.

133 *See, e.g.*, United States v. Quinn, 728 F.3d 243 (3d Cir. 2013); United States v. Straub, 538 F.3d 1147 (9th Cir. 2008).

134 *See* Schoenhaus, *supra* note 131.

135 *Cf.* Britton-Purdy et al., *supra* note 25, at 1784-93 (critiquing the "twentieth-century synthesis," a conceptual orientation that "sidelined questions of distribution, power, and democracy in economic laws, while "render[ing] economic power hard to find and correct" in political laws).

About the Author

Rebecca Wexler is an assistant professor of law at the University of California, Berkeley, School of Law, where she works on issues concerning data, technology, and criminal justice. She is also a faculty co-director of the Berkeley Center for Law & Technology, a nonresident fellow at the Brookings Institution, and an affiliated fellow at the Yale Law School Information Society Project. Wexler's research includes "Privacy as Privilege: The Stored Communications Act and Internet Evidence," Harvard Law Review; "Privacy Asymmetries: Access to Data in Criminal Investigations," UCLA Law Review; and "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System," Stanford Law Review. Prior to attending law school, she made documentary films for national broadcast television, museums, and educational distribution.

© 2022, Rebecca Wexler.

Acknowledgments

Thank you to Ayodele Akenroye, Julie Cohen, Seth Davis, Jim Dempsey, Andrew Ferguson, Jameel Jaffer, Amy Kapczynski, Paul Ohm, and Kate Weisburd for helpful comments and discussion. A special thank you is due to Katy Glenn Bass for comments on prior drafts and for shepherding this essay to publication. Alexa Daugherty, Chelsea Hanlock, Joseph Kroon, Ping Liu, and Nivedita Soni provided excellent research assistance. Marci Hoffman and Dean Rowan provided invaluable reference support. This essay benefited from presentations at the Yale Law School and Knight First Amendment Institute's "Data and Democracy" symposium, the American Bar Association "Criminal Justice Workshop," and the "Technology Law and Policy Colloquium" at Georgetown Law School.

About the Knight First Amendment Institute

The Knight First Amendment Institute at Columbia University defends the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. It promotes a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government.

knightcolumbia.org

Design: Point Five
Illustration: ©Erik Carter


KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY