A Mutual Legal Assistance Case Study: The United States and France

By: Peter Swire*, Justin D. Hemmings**, & Suzanne Vergnolle

Table of Contents

I. INTRODUCTION ................................................................. 2

II. WHY MUTUAL LEGAL ASSISTANCE MATTERS NOW: THE RESEARCH PROJECT .......... 4

III. HOW US LAW ENFORCEMENT OBTAINS EVIDENCE ......................................................... 9

   A. The Fourth Amendment ........................................................................................................... 9

   B. Search and Seizure of Electronic Evidence .......................................................................... 12

   C. Alternate Ways to Obtain Evidence ...................................................................................... 21

IV. HOW FRENCH LAW ENFORCEMENT OBTAINS EVIDENCE .............................................. 23

   A. French Search and Seizure Regime ...................................................................................... 25

   B. Interception of communications transmitted by means of telecommunications .................. 27

   C. Real-time interception of data .............................................................................................. 31

   D. Geolocalization ..................................................................................................................... 32

   E. Collection of Evidence Upon Request .................................................................................. 33

   F. Encryption ............................................................................................................................ 34

   G. Exclusion of Illegal Search Evidence: ............................................................................... 34

   H. State of emergency regime .................................................................................................. 35

V. THE CURRENT FRANCE/US MUTUAL LEGAL ASSISTANCE REGIME ......................... 40

VI. POSSIBLE FRANCE/US MLA REFORMS ........................................................................ 44

   A. The Technical, Legal and Political Context for Reform ....................................................... 44

   B. Scope of Possible Reform and Choice of Law ........................................................................ 46

VII. CONCLUSION ......................................................................................................................... 51

* Peter Swire is the Huang Professor of Law and Ethics at the Georgia Institute of Technology’s Scheller College of Business, and Senior Counsel at Alston & Bird, LLP. This article is current as of December, 2016.

** Justin Hemmings is Associate Counsel at Alston & Bird, LLP. He received his J.D. from American University’s Washington College of Law.

1 Suzanne Vergnolle is a Ph.D. candidate at Paris II Panthéon-Assas France.
I. INTRODUCTION

This article provides a case study involving France and the United States for a topic of growing importance – how to reform the outdated system of “Mutual Legal Assistance” (MLA). Mutual Legal Assistance occurs when one country (such as France) requests evidence held in another country (such as the US) for criminal prosecution, frequently pursuant to a Mutual Legal Assistance Treaty (MLAT).

As discussed in Part II, this article is part of a broader research project on MLA reform, a topic that has reached a new level of prominence driven by two technological developments. First, globalized communications through the Internet mean that emails and other evidence for criminal investigations are often held in a different country, such as when Europeans use popular US-based email and social network services. Second, the drastic increase in use of encrypted communications has made many local wiretaps ineffective,\(^2\) pressing law enforcement to seek evidence through judicial orders on companies that often store the data abroad. Our previous research has examined the goals of stakeholders in the process,\(^3\) and highlighted how the precedent of the Visa Waiver Program, created in response to globalization of travel, provides a promising


model for MLA reform, in response to globalization of evidence.\(^4\) A separate article examines ways that the United States and the European Union (EU) offer stricter privacy protections for government access to data; contrary to the common assumption that EU privacy law is generally stricter than US law.\(^5\) That article’s findings are important to assessing MLA reform proposals for the United States and the EU, and also as part of current debates in the EU about whether the United States has “adequate” privacy protections and therefore is a lawful recipient of personal data.

This article, building off prior work on how French criminal law procedures operate,\(^6\) examines French and US law in detail to understand the substantive standards that apply to government access to data for criminal prosecutions. We believe a relatively detailed explanation of the two regimes will be helpful to discussions of MLA reform, because few participants in such debates are experts in both US and French criminal law and procedure. Part II explains the US regime, founded on Fourth Amendment protections against unlawful searches and seizures. The United States also has created a multi-tiered set of standards under the Electronic Communications Privacy Act (ECPA) and Stored Communications Act (SCA), with different rules, for instance, for: basic subscriber information; metadata such as to/from information; content of stored records; and interception of electronic communications. Part IV explains the French regime. As a general theme, the French system has a tradition of relying on the acts that can be performed at each stage


\(^6\) Suzanne Vergnolle, Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests, in DATA PROTECTION, PRIVACY, AND EUROPEAN REGULATION IN THE DIGITAL AGE (Helsinki University Press, 2016, p. 205.)
of the investigation, as well as the investigative authority of a particular actor, such as a magistrate. In contrast, the US system relies more heavily on distinct rules for different categories of electronic evidence. Part V explains the current France/US MLA regime, as well as the growing phenomenon of detailed corporate policies about when to comply with non-mandatory requests for evidence.

Part VI turns to possible reforms of MLA between France and the United States, with the proposed reform mechanism of an amendment to the ECPA. This amendment would ensure the relatively strict US laws would no longer apply to at least some French requests for the content of communications held by US companies. We conclude that the France/US relationship is a good case study of the promise and challenges of reforming ways to share criminal justice evidence. The France/US alliance and shared commitment to the rule of law provide strong reasons to support MLA reform, while the large differences in criminal procedure and substantive standards for access to evidence illuminate the obstacles to such reform. Part VI also examines how choice of law principles can inform discussions of MLA reform, and identifies what factors support current MLA protections and which ones instead suggest the need for reform.

II. **WHY MUTUAL LEGAL ASSISTANCE MATTERS NOW: THE RESEARCH PROJECT**

This article is part of a larger research project examining the current state of international MLA and builds upon those previous articles. The research project to date is headed by Peter Swire, with co-authors to date: DeBrae Kennedy-Mayo, Justin Hemmings, and Suzanne
Other scholars, most notably Professors Jennifer Daskal and Andrew Woods, have been producing recent scholarship on similar topics.8

A simple example shows how the globalization of data is affecting even routine criminal investigations. Consider a burglary that takes place in Paris with a French suspect and a French victim. In investigating the crime, French law enforcement finds that the suspect was using a US-based email service, and the emails can only be retrieved from the relevant email server. Under the current regime, to access the e-mails, French law enforcement would need to file an MLA request through the French Minister of Justice with the US Department of Justice. This request would need to show “probable cause” of a crime (the US legal standard), despite the crime itself having no connection to the United States other than the physical location of the email server. This example shows how MLA issues increasingly arise for routine criminal investigations such as a burglary. The need for MLA requests is even more pervasive for cybercrime, drug smuggling, money laundering, and other categories of crime where the criminal activity itself often crosses borders.

---

7 The use of “we” in this article refers to its authors, Peter Swire, Justin Hemmings, and Suzanne Vergnolle.

The first article in the research project introduces the international MLA regime, by explaining the origins of MLATs and how electronic evidence requests have come to overwhelm these systems. One important source of current challenges is that the increased use of encryption has made many local wiretaps ineffective, pressing law enforcement to seek evidence by alternate means. The article examines the risks of failing to adequately reform the system. It provides a number of potential administrative reforms that could reduce the current average response time of ten months for MLA requests to the US. The article stresses an innovative way to avoid reliance going forward on mutual legal assistance treaties; instead, reform may be more achievable and effective through mutual legal assistance statutes. As such, the article is entitled *Mutual Legal Assistance in an Era of Global Communications: The Analogy to the Visa Waiver Program*. The Visa Waiver Program was a response to the globalization of travel—for the thirty-eight countries that participate today; individuals can travel to and from the US without the need for an individualized visa interview. Similarly, a new MLA statute can respond to the globalization of evidence—countries that meet strict standards would use a streamlined system to share evidence for criminal investigations. Since the article was written, the United States and United Kingdom have announced one such proposal for an MLA statute.

---


10 Id.

11 Id.

12 Id.


The second article, *Stakeholders in Reform of the Global System for Mutual Legal Assistance*, identifies the various stakeholders in this international mutual legal assistance regime, and their respective incentives and goals for reform. This article looks to the interests of the US government, non-US governments, technology companies, and public interest groups both in the US and abroad. The article seeks to describe the interests of these stakeholders accurately to better inform the debate for MLA reform. It identifies major goals of the various actors, notably: (1) effective law enforcement access to evidence; (2) ensuring that such access is consistent with privacy and civil liberty goals; (3) avoiding data localization, which might otherwise result where local law enforcement insists on data being stored locally; and (4) preventing a greater role for the International Telecommunications Union or other institutions that might seek to impose top-down controls, risking splintering of the global Internet.

The third article, *Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests*, provides our first detailed examination of a particular country’s system for exchanging criminal evidence with the United States. This chapter, in the forthcoming book *Data Protection, Privacy, and European Regulation in the Digital Age*, focuses on the French criminal system and the procedural aspects of how France makes or receives MLAT requests, in contrast to the current

---


16 Id.

17 Id.

The chapter reviews the existing standards of the French criminal system to provide a better understanding of the extent to which investigative authorities have broader powers than their American counterparts and the existing safeguards designed to protect individuals’ rights during the French criminal investigation process. The chapter analyzes the French criminal process for gathering evidence during preliminary inquests and formal investigations, focusing on the existing safeguards protecting privacy and data protection. Lastly, the chapter illustrates that each legal system maintains different checks and balances—the roles of judicial and executive actors are quite different in the United States and France, and those differences should be considered in defining how the two systems should cooperate.

In the course of studying obstacles to effective MLA reform, we have come to believe the fact that both the EU and United States provide stricter privacy protections is salient but little understood—each side is reluctant to compromise on a new approach to the extent that there would be a weakening of some specific safeguards that currently exist in their jurisdiction. This article explains how a fuller understanding of the relative strengths of both sides can enable a more fruitful discussion of MLA reform. By showing notable ways in which the US has stricter safeguards than the EU, this article also informs current debates and litigation about the adequacy of privacy protections in the United States.

Lastly, we are in the beginning stages of researching how Indian criminal procedure operates for cross-border data requests as an example of an important, non-European Union state.

19 Id.
20 Id.
21 Id.
22 Id.
in need of MLA reform. MLA issues have been prominent in recent US-India diplomatic discussions, and developing reform options for India may be useful in considering how to bring MLA reform to a broader set of countries outside of the United States and EU.

III. HOW US LAW ENFORCEMENT OBTAINS EVIDENCE

To assist in the comparison of US and French standards for obtaining evidence, this part provides a brief introduction to US criminal procedure, with emphasis on how the Electronic Communications Privacy Act (ECPA) and Stored Communications Act (SCA) govern law enforcement investigations seeking electronic evidence. After briefly explaining the foundational constitutional law for criminal investigations, this section explains how the ECPA, SCA, and other relevant US laws apply different standards of proof to different categories of electronic evidence. Lastly, this part explains other means for the US government to collect or compel evidence.

A. The Fourth Amendment

The Fourth Amendment of the US Constitution provides the baseline rule against an officer of the government conducting unreasonable searches or seizures.23 In practice, the Fourth Amendment sets the default rule that any “search” or “seizure” without a warrant is unreasonable and a warrant is only obtainable upon a showing of the key American standard of “probable cause.”24 As discussed below, current law holds that government access to some kinds of records, such as the metadata about a communication, does not constitute a “search” or

23 The Fourth Amendment states that “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[,]” US Const. amend. IV. “Government” in this context means any person acting on behalf of a federal or state entity.

24 Id.
“seizure.”\(^{25}\) To obtain a warrant, the requesting authority must demonstrate a reasonable basis for believing a crime may have been committed (when seeking an arrest warrant) or that evidence of the crime being investigated is present in a location (when seeking a search warrant).\(^{26}\) Probable cause is not clearly defined in the Constitution. Consequently, the US Supreme Court has attempted to clarify the term on several occasions,\(^{27}\) but has generally favored a flexible approach, viewing probable cause as a “practical, non-technical” standard that examines the “factual and practical considerations of everyday life.”\(^{28}\)

One such clarification took place in the seminal wiretap case *Katz v. United States*, which found a violation of the Fourth Amendment when police conducted a wiretap without a search warrant.\(^{29}\) Justice Harlan’s concurrence created the enduring legal test from *Katz*: “a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”\(^{30}\) Courts have applied this “reasonable expectation of privacy” test in the years since.

The third-party doctrine, which states there is no reasonable expectation of privacy in information shared with a third-party business, emerged after *Katz*.\(^{31}\) In *United States v. Miller*, the Court held that a defendant had no reasonable expectation of privacy in the bank records

\(^{25}\) See infra Part III.


\(^{30}\) *Katz* at 361 (J. Harlan, concurring).

associated with revenue he earned through making bootleg liquor on which he did not pay taxes.\footnote{Miller at 436.} The Court pointed to \textit{Katz}’s language, stating that “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”\footnote{Miller at 442 (citing Katz).} The Court in \textit{Miller} noted, the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.\footnote{Miller at 443.}

The same principle was applied in \textit{Smith v. Maryland}, where the Court held that a pen register\footnote{A Pen Register is a device that can record the calls made from a specific phone number. We discuss pen registers in more detail in Section III(B).} was covered under the third-party doctrine.\footnote{Smith at 743-44.} The Court reasoned, “When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, the petitioner assumed the risk that the company would reveal to police the numbers he dialed.”\footnote{Smith at 744.} The third-party doctrine continues today, though as discussed in Section III(B), Congress has enacted specific rules for certain types of information shared with third-party businesses.

The rules for physical evidence include numerous other exceptions and nuances, but are distinct from the rules regarding electronic evidence. We do not expand on the rules regarding the search and seizure of physical evidence here, as electronic evidence constitutes the vast majority of evidentiary MLA requests today compared to physical evidence.\footnote{Telephone Interview with Anonymous Department of Justice Official (Apr. 7, 2015). For more information on US search and seizure law, see Ellen S. Podgor, \textit{et. al.}, \textsc{Mastering Criminal Procedure, Volume 1: The Investigative Stage} (2014).} Instead, the next
section examines the rules and exceptions Congress enacted in the Electronic Communications Privacy Act and the Stored Communications Act to address the specific issues raised by electronic evidence.\textsuperscript{39}

B. Search and Seizure of Electronic Evidence

Under the ECPA and the SCA, the rules for electronic evidence, such as email, are complicated.\textsuperscript{40} Different rules apply to at least five categories of evidence: (1) basic subscriber information (BSI); (2) dialing, routing, addressing, and signaling information (DRAS); (3) other metadata, such as location information; (4) the stored content of electronic communications; and (5) the real-time content of electronic communications.\textsuperscript{41} Rules can also differ by circuit on whether or not a warrant is required to access email. The complex ECPA rules are directly relevant to issues of MLA reform. For evidence governed by the ECPA and the SCA, foreign governments such as France must meet highly varying standards in order to obtain evidence, some of which the foreign government can seek directly from the service provider and some of which is subject to the MLA process.\textsuperscript{42} The complexity of this system requires the investigating authorities to have a clear understanding of what is required, or they might lose precious time during an investigation or even might be deterred entirely from seeking the evidence.

The varying strictness of rules under the ECPA can best be understood as applying to different categories of communication with different privacy expectations—a wiretap is a greater privacy intrusion than basic subscriber information. In understanding these rules, we first examine the rules when the government \textbf{compels} production from the service provider, as


\textsuperscript{40} See generally, \textit{id.}

\textsuperscript{41} \textit{Id.}

\textsuperscript{42} \textit{Id.}
contrasted to situations where the business in possession of electronic information may **voluntarily** disclose it. The content of electronic information cannot be disclosed absent the appropriate legal instrument, but the business can disclose voluntarily for basic subscriber information and to/from information.\textsuperscript{43}

1. Basic Subscriber Information is the easiest category of electronic evidence for the government to obtain.

   IP is defined as the identifying information for the owner or controller of an Internet service account.\textsuperscript{44} BSI can include the name, address, and any assigned number or identity such as a phone number, username, IP address, or email address.\textsuperscript{45} BSI is considered analogous to the types of information at issue under the third-party doctrine in *Miller* and *Smith*, as it is provided in the ordinary course of business.\textsuperscript{46} Consequently, BSI is not protected under the Fourth Amendment.\textsuperscript{47} The government can seek production of BSI through use of an administrative subpoena, grand jury or trial subpoena, or a court order issued under 18 U.S.C. § 2703(d).\textsuperscript{48} As previously noted, a company can also voluntarily disclose BSI to law enforcement upon request without penalty under the ECPA.\textsuperscript{49} This ability to provide the information voluntarily is true for any law enforcement request, whether from within the United States or a foreign sovereign.\textsuperscript{50}

\textsuperscript{43} See 18 U.S.C. § 2703 (2016). Note also that under § 2703(c)(1)(C) any information can be voluntarily disclosed with “the consent of the subscriber or customer to such disclosure.”

\textsuperscript{44} See 18 U.S.C. § 2703(c)(2) (2016).


\textsuperscript{49} *Id.*

\textsuperscript{50} See 18 U.S.C. § 2702(b) (2016).
2. Pen/Trap orders require certification that the evidence sought is relevant to the investigation in order to compel production.

For pen register information (the telephone number dialed) and trap-and-trace information (the telephone number that called), the SCA has long required government certification that the evidence is “relevant to an ongoing criminal investigation.”\(^{51}\) Originally, these orders applied specifically to information about telephone numbers making a call or being called.\(^{52}\) This “to” and “from” information has been considered less privacy invasive than the content of a communication, and so the government is able to gain access with a lesser showing.\(^{53}\) The USA PATRIOT Act (Patriot Act) expanded the scope of pen register and trap-and-trace orders to “dialing, routing, addressing, and signaling” (DRAS) information.\(^{54}\) DRAS includes the entire header, because the “subject” line of an email is considered content.\(^{55}\) The expansion from only telephone numbers to all DRAS information reflected the expansion of types of communication, including emails, text messages, and other types of electronic communications.

The Patriot Act thus applied the metadata/content distinction used for telephone communications to newer electronic communications. First, the new definition applied to any “process” of communication, clarifying that the statute applied beyond hardware “devices” to


\(^{52}\) See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), H.R. 3162, 107th Congress § 214 (2001).


\(^{54}\) Id. at § 215.

\(^{55}\) Note that email subject lines, which are also included as a part of an email’s header information, are specifically not to be read under these orders. See H. Marshall Jarrett, et al., Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations, 153 (2009) available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.
also cover software.\textsuperscript{56} Second, the statute expanded from phone calls to any “instrument or facility from which a wire or electronic communication is transmitted,” clarifying that coverage included “a non-mobile telephone, a cellular telephone, an Internet user account, an email account, or an IP address.”\textsuperscript{57} Third, the application to all “dialing, routing, addressing, and signaling” information clarified that to/from information under the statute would include a wide range of metadata beyond phone numbers, although it did not include location information.\textsuperscript{58}

The Patriot Act expanded the geographic reach of any single pen/trap order. An attorney for the US government can obtain a pen/trap order by certifying “to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation.”\textsuperscript{59} Before 2001, these orders were only valid within the geographic area of the issuing court.\textsuperscript{60} The Patriot Act provided nationwide scope for the order, to “apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.”\textsuperscript{61}

3. The SCA provides for a court order for qualifying categories of electronic evidence upon a showing of a reasonable articulable suspicion.\textsuperscript{62}

\footnotesize{56 Id.} \\
\footnotesize{59 18 U.S.C. § 3123 (2016).} \\
\footnotesize{60 See PL 99-508 (HR 4952) § 3123 (1986).} \\
\footnotesize{61 See USA PATRIOT Act § 216.} \\
\footnotesize{62 18 U.S.C. § 2703 (2016).}
The SCA requires, under § 2703(d), a court order for the production of certain stored records. These “D orders” require a showing of “specific and articulable facts” that the information sought is “relevant and material to an ongoing criminal investigation.” Such orders were historically used to gain access to the content of emails, but the 2010 case, United States v. Warshak has led to the use of probable cause warrants for such access. With the exception of emails, D orders can also be used to obtain the content of an electronic communication, when the target subscriber or customer is given prior notice. Under § 2703 of the SCA, the government can obtain a court order to retrieve metadata for any electronic communication, and D orders have been used widely to retrieve location information, such as from cellphones.

4. Under ECPA and the SCA, the content of stored electronic communications can be obtained with a probable cause warrant.

The SCA states “[a] governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication . . . without required notice to the subscriber or customer, if the governmental entity obtained using the procedures

63 Id.
66 18 U.S.C. § 2703(b) (2016). Note that ECPA also provides exceptions for when such an order can be given with delayed notice under § 2705.
67 18 U.S.C. § 2703(c) (2016). The use of these orders for location was confirmed in telephone Interview with Anonymous Department of Justice Official (Apr. 7, 2015). There has been litigation about whether a probable cause warrant is needed for location data, with some magistrate judges rejecting applications requesting D orders for location records for failure to show probable cause. See, e.g., In re Application of U.S. for Historical Cell-Site Data, 724 F.3d 600 (5th Cir. 2013), In re Application of U.S. for an Order Directing a Provider of Elec. Commc’ns Serv. To Disclose Records to Gov’t, 620 F.3d 304 (3d Cir. 2010), In re Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) vacated.
68 See 18 U.S.C. § 2703 (2016). Note that § 2703(b) provides the ability to obtain content under an administrative subpoena or D order if the target is given prior notice.
described in the Federal Rules of Criminal Procedure." In other words, a probable cause warrant is sufficient to obtain the content of electronic communications without giving prior notice to the target.

The SCA has complex rules about voluntary and compelled disclosure of emails, as an important example of stored electronic information. If a service provider inadvertently comes across the content of a customer’s email related to the commission of a crime, it can share that information with law enforcement. If an email is stored on a server for less than 180 days, and has not been opened, the government entity seeking it is required to obtain a warrant. If the email is stored for more than 180 days, then a warrant, subpoena, or court order issued under §2703(d) of the SCA is acceptable under the statute. Some courts distinguish opened email from unopened email, reasoning that once it has been opened the message is no longer in “electronic storage” but is instead a supplemental “remote storage” and can therefore be accessed with a subpoena, rather than requiring a probable cause warrant.

These rules have been streamlined in practice at the federal level, in large part due to the 2010 decision in United States v. Warshak by the United States Court of Appeals for the Sixth Circuit. In Warshak, the court held that all emails require a warrant. According to the court,

---

71 As enacted, Title II of ECPA.
75 Id.
this holding under the Fourth Amendment applied, notwithstanding the third-party doctrine, the status of whether an individual email has been opened or the length of time the email was stored on a server.\textsuperscript{79} In this case, the government served an order to one of Warshak’s email service providers to preserve emails, and a few months later, obtained the preserved emails with a subpoena under § 2703(b) of the SCA and the rest of Warshak’s emails with an \textit{ex parte} court order under § 2703(d).\textsuperscript{80} The Court held that the contents of a person’s email were equivalent to a person’s letters, and as such can only be obtained with a valid warrant.\textsuperscript{81} The Court also distinguished the third-party doctrine announced in \textit{Miller}, which the government had used to justify access to email content with less than a probable cause warrant.\textsuperscript{82} Unlike bank records provided in the ordinary course of business, emails are not simple business records but rather a “potentially unlimited variety of ‘confidential communications.’”\textsuperscript{83} The Court held that the content of email has a reasonable expectation of privacy, and consequently the government cannot obtain that content without a warrant based on probable cause.\textsuperscript{84} While this holding is only binding in the Sixth Circuit today, it has had a larger effect on federal investigation policy.

After \textit{Warshak}, the DOJ updated its practice to require the acquisition of a probable cause warrant when seizing email content. In addition, the DOJ testified in Congress stating, “there is no principled basis to treat e-mail less than 180 days old differently than e-mail more than 180

\textsuperscript{78} \textit{Id.}
\textsuperscript{80} See \textit{id.} at 283.
\textsuperscript{81} See \textit{id.} at 288.
\textsuperscript{82} See \textit{id.} at 288.
\textsuperscript{83} See \textit{id.} at 287-88.
\textsuperscript{84} See \textit{id.} at 288.
days old.” The DOJ similarly eschewed the difference between opened and unopened email, testifying, “[s]imilarly, it makes sense that the statute [SCA] not accord lesser protection to open e-mails than it gives to e-mails that are unopened.” The DOJ went on to endorse the warrant standard for stored e-mail and “similar stored content,” stating that the DOJ “believe[s] that this approach has considerable merit, provided that Congress consider contingencies for certain limited functions for which this may pose a problem.” The DOJ later updated its own practices to state that it will only obtain emails or similar stored content with a warrant based upon probable cause.

Congress has been considering the Email Privacy Act. The Act as currently written would amend ECPA and the SCA to both codify the ruling in Warshak and apply the probable cause warrant standard to any stored electronic content, not just communications. The Email Privacy Act was passed unanimously in the House with 315 cosponsors, and is currently awaiting review in the Senate. As part of codifying Warshak, the Act would also remove the current differentiation between emails less or greater than 180 days old.

---


86 See id.

87 See id.

88 Note that while this means that for any DOJ-involved federal investigation the Warshak rule essentially applies, the same is not binding on states outside the Sixth Circuit today.


90 See Email Privacy Act.

91 See id.

92 See id.
5. The real-time interception of data requires not only a demonstration of probable cause but also other requirements such as exhausting other investigatory procedures.\textsuperscript{93}

The real-time interception of electronic data is recognized as holding the greatest privacy risks and consequently an order authorizing such interception requires a heightened standard of proof.\textsuperscript{94} First, unlike a pen/trap or D order, which can be general in scope, an interception order requires “a particular description” of both the “nature and location of the facilities from which or the place where the communication is to be intercepted” and “the type of communications sought.”\textsuperscript{95} Second, the application for an interception order must explain “whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or be too dangerous.”\textsuperscript{96} Failure to exhaust alternate, less-intrusive means of obtaining the same information can result in the denial of an application for an interception order absent an adequate showing of why such attempts are too dangerous or are likely to fail.\textsuperscript{97} Third, the application must specify the period of time during which the interception will take place, or a reason why the applicant has probable cause to believe no termination date should be set because additional covered communications will continue to occur.\textsuperscript{98} If the judge then finds:

(a) there is probable cause . . . that an individual is committing, has committed, or is about to commit a particular [covered] offense;
(b) there is probable cause . . . that particular communications concerning that offense will be obtained through such interception;

\textsuperscript{94} Rules affecting real-time interception are relevant beyond the law enforcement rules discussed here, and may come under the legal regime for foreign intelligence investigations, under laws including the Foreign Intelligence Surveillance Act. 50 U.S.C. ch. 36. Since this article focuses solely on the standards used in criminal investigations for purposes of comparing the US and French systems, those topics are not addressed here.
\textsuperscript{97} See Id.
(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or be too dangerous;
(d) . . . there is probable cause . . . the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, . . . or commonly used by such person;
then the court may issue an authorizing order for the interception.99

C. Alternate Ways to Obtain Evidence

Along with the five categories of compelled production, the US government can also obtain certain types of evidence through other means, including voluntary disclosure, subpoena, grand jury subpoena, or through mandatory reporting. A first party to any communication may always consent to sharing the content of that communication with the government.100 The SCA specifically permits the use of administrative subpoenas, grand jury subpoenas, or court orders for acquiring qualified metadata.101 Furthermore, if data is required to be reported to the government under law then that information can be used without additional court authorization.102 For example, when a bank reports the deposit of over $10,000 under the Bank Secrecy Act that information can be used by the government as part of any ongoing investigation without further authorization.103

Under the ECPA, a business can voluntarily disclose basic subscriber information at its own discretion.104 The SCA’s default rule provides that no electronic communication service can “knowingly divulge to any person or entity the contents of a communication while in electronic

---

103 Id.
storage by that service.”

The law does provide exceptions for when voluntary disclosure is permitted, however, including to “any person other than a [US] governmental entity.”

A covered business may disclose to a US governmental entity when it “in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.”

A prosecutor can use a subpoena to compel the production of evidence after a case is brought. The Federal Rules of Criminal Procedure authorize a prosecutor to compel the attendance of a witness or the production of any data the subpoena designates. A defendant can attempt to quash a subpoena if “compliance would be unreasonable or oppressive.” A prosecutor may also serve a subpoena on a third party when authorized by court order, though the victim must be given notice and time to object or move to quash or modify the subpoena.

Failure to comply with a valid subpoena may result in a finding in contempt of court, resulting in fine or imprisonment until the target complies with the court order.

A prosecutor can also use a grand jury subpoena to seek the production of evidence to help prove why a grand jury should indict a suspect. Subpoenas sought in grand jury proceedings are governed by the Federal Rules of Criminal Procedure. A grand jury may subpoena any

109 See id.
110 See id.
111 See id.
information it deems relevant to its consideration of whether or not to indict the suspect.\textsuperscript{113} The target of any such subpoena maintains the ability to seek to quash or modify a grand jury subpoena.\textsuperscript{114} As with other subpoenas, failure to comply can result in the issuance of a court order compelling the target to comply with the subpoena. Failure to do so can result in a finding of contempt of court, resulting in fine or imprisonment until the target complies.\textsuperscript{115}

\textbf{IV. HOW FRENCH LAW ENFORCEMENT OBTAINS EVIDENCE}

This section provides a brief introduction to the French criminal justice system with an emphasis on how the French Code of Criminal Procedure organizes the rules depending on different categories of electronic evidence. After briefly explaining the principles that exist under the French Code of Criminal Procedure, this section examines its various regimes depending on the evidence sought and the stage of the investigation.\textsuperscript{116} Under these various regimes, different standards of proof are required and different actors can ask for different categories of electronic evidence. As a general theme, the French system has a tradition of relying on the acts that can be performed at each stage of the investigation, as well as the investigative authority of a particular actor, such as a public prosecutor or a magistrate. In contrast, the US system relies more heavily on distinct rules for different categories of electronic evidence.

Building on our previous work about the roles and powers of different actors in the French criminal procedure system,\textsuperscript{117} the discussion here emphasizes the French substantive standards for accessing electronic evidence. Three main principles dominate the French criminal

\begin{itemize}
\item \textsuperscript{113} See F. R. Crim. P. 17.
\item \textsuperscript{114} Id.
\item \textsuperscript{115} Id.
\item \textsuperscript{116} See Livre 1 of the C. PR. PÉN.
\end{itemize}
system as regards the gathering and use of evidence. First, the principle of the “rule of evidence by all means” ensures that all types of evidence are admissible (e.g., written, oral, testimonial).\textsuperscript{118} This principle of liberty when administrating the evidence has a truth-seeking function. This principle is not absolute since the principle of legality administrating the criminal process inherently limits the principle of liberty. Thus, all the acts need to comply with the provisions of the French Code of Criminal Procedure, which are all regulated by the law\textsuperscript{119}.

Second, the principle of “loyalty when administering proof” ensures that the investigator cannot use unfair practices, fraud, or tricks to obtain the evidence.\textsuperscript{120} Finally, trial judges must weigh all items of evidence brought before them under the principle of “intimate conviction.”\textsuperscript{121}

The French Code of Criminal Procedure permits four types of investigations: identity checks;\textsuperscript{122} investigations of \textit{in flagrante delicto};\textsuperscript{123} “preliminary” investigations;\textsuperscript{124} and formal investigations conducted by an investigating magistrate (\textit{judiciary information}).\textsuperscript{125} Specific regimes and rules govern all four investigation types. The present section focuses mainly on the

\textsuperscript{118}See e.g., Rép. dr. pén. et pr. pén. Dalloz, I\textdegree {}“Preuve”, 2016, by Jacques Buisson, § 50.
\textsuperscript{119}See Thierry Garé and Catherine Ginestet, Droit pénal et procédure pénale, 9\textsuperscript{e} ed., HyperCours, Dalloz, 2016, § 399, p. 255.
\textsuperscript{121}See FRENCH CODE OF CRIMINAL PROCEDURE [C. PR. PÉN.], articles 353, 427 and 536. See also, Bernard Bouloc, Procédure pénale, 25\textsuperscript{e} ed., Précis Dalloz, 2015, n° 166; Rép. dr. pén. et pr. pén. Dalloz, I\textdegree {}“Preuve”, 2016, by Jacques Buisson, § 94: “the magistrate has the freedom to value each piece of evidence produced.”
\textsuperscript{122}In France, identity checks are strictly regulated in articles 78-1 et seq. of the C. PR. PÉN..
\textsuperscript{123}Under article 53 of the C. PR. PÉN., a “in flagrante delicto” is one that is “in the process of being committed or which has just been committed.”
\textsuperscript{124}The preliminary investigation is used in most cases involving traffic violations, contraventions, and non-\textit{flagrante delicto}. Under article 76 of the C. PR. PÉN., this type of investigation is a non-coercive procedure.
process for gathering evidence during preliminary and formal investigations. The French Code of Criminal Procedure determines the tools that investigating authorities can use and under which conditions they may use those tools. The more serious the offense, the more the investigating authorities will be allowed to use tools that intrude upon the suspect’s freedom. The law permits, and indeed anticipates, that the police authorities, under the supervision of the prosecutor, will investigate the vast majority of criminal cases. Very few cases are actually transferred to the investigating magistrate in order to open a formal investigation.

A. French Search and Seizure Regime

The rules governing searches of electronic evidence are complicated. Different rules apply to different types of investigations. Under French law, a search occurs when there is a “research” in an enclosed space of evidence, which may lead to the existence of infringement or identifying the author of an offense.

Article 56 and subsequent articles of the French Code of Criminal Procedure regulate the regime of search for in flagrante delicto investigation. Here, the search is permitted if the nature of the crime is such that proof can be obtained by the seizure of papers, documents, or electronic evidence. The search is legal if the person whose home is searched is present during the search. If the target of the search is present, the Officers of the Judicial Police then will go to the home to perform the search and seize the evidence.

126 See e.g., Jacqueline Hodgson, ‘The Police the Prosecutor and the Juge d'Instruction. Judicial Supervision in France, Theory and Practice’ (2001) 41 Brit. J. of Criminology 342, 349. The recent reforms reinforced this tendency to strengthen the French prosecutor’s position and influence, thus reducing the investigating magistrate’s role within the criminal process.


128 Article 56 C. PR. PEN.

129 Article 57 of the C. PR. PEN..
For “preliminary” investigations, article 76 and subsequent articles of the French Code of Criminal Procedure require the Officers of the Judicial Police to obtain the written consent of the person whose home is to be searched.\textsuperscript{131} Under very specific circumstances, a search can occur without the person’s written consent. For such a search to be valid, the public prosecutor can ask the liberties and custody judge\textsuperscript{132} to issue a warrant, but only when the investigation so requires and for cases involving criminal offences and misdemeanors carrying a sentence of at least five years imprisonment.\textsuperscript{133}

Finally, for a formal investigation, article 92 and subsequent articles of the French Code of Criminal Procedure provide broad powers to the investigating magistrate allowing her to order the search of any place\textsuperscript{134} where one can discover objects or data. Article 94 uses general terms, so the rogatory commission does not need to precisely name the places to be searched.\textsuperscript{135} To be legal, the search only needs to be necessary to establish the truth of an offense.\textsuperscript{136} Either the resident\textsuperscript{137} or two persons not subject to the administrative authority of the searching official must be present during the search, and must read and sign the official report of the operation.\textsuperscript{138}

When a search is necessary to establish the truth, the Officers of the Judicial Police can seize the

\textsuperscript{130} The Officers of the Judicial Police are responsible for recording criminal offenses, receiving complaints from victims, summoning witnesses, interviewing suspects and gathering evidence.

\textsuperscript{131} Article 7657 of the C. PR. PÉN..

\textsuperscript{132} The “Juge des libertés et de la detention”, which can be translated as “liberties and custody judge.”

\textsuperscript{133} Article 7657 of the C. PR. PÉN..

\textsuperscript{134} Except in certain places that are excluded by law, such as the office of a parliament members and attorneys.

\textsuperscript{135} French Supreme Court, Crim. 22 January 1953, Bull. crim. no. 24; D. 1953. 533, note Lapp.

\textsuperscript{136} See e.g., articles 81, 82, 97 of the C. PR. PÉN. See also, French Supreme Court, Crim. 27 October 1959 Bull. Crim. no. 450.

\textsuperscript{137} When the resident is under custody the investigating magistrate needs to obtain his written consent under article 95 of the C. PR. PÉN..

\textsuperscript{138} The regime depends on the place that is searched, see article 57 or article 96 of the C. PR. PÉN..
data that is located where the search happens. The data is seized under judicial authority. Little guidance is provided in the law regarding the deletion of such evidence at the end of the investigation.

B. Interception of communications transmitted by means of telecommunications

In the 1990s, France was repeatedly sanctioned by the European Court of Human Rights for its legal regime regulating the interception of communications transmitted by means of telecommunications. The Court considered that tapping and other forms of interception of telephone conversations represented a serious interference with private life and correspondence. To comply with the Court’s requirement, the regime had to be based on a precise "law" with clear and detailed rules. The Court outlined the substance of what might be regarded as adequate legislation in this sphere, noting that the French system did not afford adequate safeguards against various possible abuses and thus found that there had been a violation of article 8 of the European Convention on Human Rights. Consequently, in 1991 the French Parliament adopted a specific regime that regulates the collection and interception of electronic communications. “Electronic communications” is defined in article 32 of the Postal and Electronic Communications Code as any transmission, emission or reception of signs, signals, writing, images, sounds, or intelligence of any nature by wire, cable, radio, optical, or

---

139 During the seizure, the judiciary police can either seize the computer on which the data is based or make a copy of the data on another support.
140 Article 97 al. 3 of the C. PR. PÉN.
142 That are both protected under article 8 of the European Convention on Human Rights.
144 Law no. 91-646 of July 10, 1991 on secrecy of correspondence transmitted by means of telecommunications.
other electromagnetic or electronic system.\(^{145}\) Thus, the definition is very broad and encompasses a variety of different types of correspondence, including not only traditional phone communications but also emails.\(^{146}\)

Under article 100 of the French Code of Criminal Procedure, the interception, recording, and transcription of communications transmitted by means of telecommunications is possible only under specific circumstances. Interception can only be ordered in cases involving criminal offences and misdemeanors, sanctioned by imprisonment of at least of two years, and when the circumstances of the case require interception.\(^ {147}\) To be valid, however, the investigation magistrate does not need to justify the request of interception.\(^ {148}\) Where the investigating magistrate delegates this operation through a rogatory commission,\(^ {149}\) the process must be under her authority and control.\(^ {150}\) An interception operation must be ordered in writing and must be for a period of not more than four months.\(^ {151}\) This order is not judicial in nature, and so cannot be appealed.\(^ {152}\) Finally, the order shall provide all the information needed to identify the communication(s) to be intercepted.\(^ {153}\)

---


\(^ {146}\) Similarly, the misdemeanor of violating the secrecy of correspondence transmitted by means of telecommunications also includes emails, see e.g., Court of Appeal, Paris, Div. 2, Chamber 7, 27 January 2012 no. 10/05328.

\(^ {147}\) Article 100 of the C. PR. PÉN..


\(^ {149}\) A rogatory commission is the act by which the investigating magistrates delegates her powers to another magistrate or judicial police officer in order to make them proceed for her to one or more acts of investigation (see: Rép. dr. pén. et pr. pén. Dalloz, V° “Commission Rogatoire” 2015, by Christian Guéry, § 1).

\(^ {150}\) Article 100 of the C. PR. PÉN..

\(^ {151}\) Articles 100 and 100-2 of the C. PR. PÉN.. It can be renewed once in the same conditions.

\(^ {152}\) Article 100 of the C. PR. PÉN.. Under the general rules of law, all the investigation phase has to be written. The decision of intercepting the communication is an investigating act, so it does not have a judicial nature, and cannot
In a recent case, the “Cour de cassation” (French Supreme Court)\textsuperscript{154} clarified the regime for interception of emails. In this case, the investigating magistrate, in a rogatory commission on March 11, 2013, ordered the interception, recording, and transcript of emails sent or received from a suspect’s email address.\textsuperscript{155} The Officer of the Judicial Police not only obtained communication of the emails sent and received from March 11, 2013, but also the stock of emails in the archives of the mailbox. The French Supreme Court, in a much commented ruling, decided the interception, recording, and transcript of correspondence sent or received by means of telecommunications before the date of the order had to have been made in accordance with the law on search and seizure.\textsuperscript{156} As such, the French Supreme Court distinguished between the flow of emails that can be intercepted under article 100 CPP (without notifying the suspect) and prior communications, which can be collected under the search and seizure regime (requiring notification of the suspect).\textsuperscript{157} On July 3, 2016, the French Parliament passed the law on fighting against organized crime, terrorism, and terrorist financing, and improving the efficiency and safeguards on criminal procedure.\textsuperscript{158} This law provides a new regime for formal investigations or be appealed even from the prosecutor because the prosecutor can only appeal Decree. See, e.g., Pierre Chambon, \textit{D. 1991}, p. 173.

\textsuperscript{153} Article 100-1 of the C. PR. PÉN.

\textsuperscript{154} French Supreme Court, Crim. 8 July 2015, \textit{Bull. Crim.} no. 450. However, this case has been overruled by the law no. 2016-731 adopted on July 3, 2016.

\textsuperscript{155} \textit{Id}


\textsuperscript{157} \textit{See id.} for the French search regime.

\textsuperscript{158} Law no. 2016-731 adopted on July 3, 2016 on fighting against criminalized crime, terrorism, and their financing, and improving the efficiency and safeguards on criminal procedure.
investigations for the most serious offenses, including organized crime. Indeed, articles 706-95-1 and 706-95-2 of the French Code of Criminal Procedure allow the liberties and custody judge and the investigation magistrate, when it is necessary for the investigation, to issue an “ordonnance motivée” (writ). This writ will allow remote access to the stock of emails without the user’s knowledge. The process must be conducted under the authority and control of the judge who issued the writ. The investigating magistrate or the mandated Officers of the Judicial Police can require access to the emails through a qualified agent. To be considered legal, the search and detection may only concern the specific infractions listed in the writ. This provision does not forbid the discovery of other offenses not mentioned in the writ, however.

From an international perspective, two recent cases are relevant to the French communications interceptions regime when the communications are made with someone in another country. The French Supreme Court upheld telephone interception targeted to foreign numbers because the requisition sent to the French phone companies could only be targeted to communications transiting through the telephone operators located in the national territory. This decision represents another broad interpretation of the national territory and jurisdiction of the French Officers of the Judicial Police. Similarly, the law passed on July 3, 2016, also extended to law enforcement authorities the ability to use International Mobile Subscriber

---

159 A list of the offenses concerned by the provision of the law can be found at article 706-73 and 706-73-1 of the French Code of Criminal Procedure.

160 Article 706-95-3 al. 1 of the C. PR. PÉN.

161 Article 706-95-3 al. 2 of the C. PR. PÉN.

162 Article 706-95-3 al. 2 of the C. PR. PÉN.

163 Article 706-95-3 al. 3 of the C. PR. PÉN.

Identity (IMSI) catchers\textsuperscript{165} for investigating the most serious offenses.\textsuperscript{166} Law enforcement authorities\textsuperscript{167} can use IMSI catchers to collect login data enabling the identification of terminal equipment, the subscription number and localization of the terminal,\textsuperscript{168} or intercept communications.\textsuperscript{169} To be valid, the writ must be in writing and motivated (justified).\textsuperscript{170} The writ does not have a judicial nature, so it cannot be appealed. The process has to be under the authority and control of the judge who issued the writ\textsuperscript{171} and can only be ordered for a brief period of time.\textsuperscript{172}

\textit{C. Real-time interception of data}

The French regime of real-time interception of data was created in 2011\textsuperscript{173} and modified in 2016. Until 2016, only the investigating magistrate had the power to issue a writ ordering real-time data interception without the user’s knowledge. In 2016, the French Parliament extended this power to the liberties and custody judge for \textit{in flagrante delicto} investigations and

\begin{footnotesize}
\footnotetext[165]{An IMSI catcher is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking movement of mobile phone users.}
\footnotetext[166]{A list of the offenses concerned by the provision of the law can be found at articles 706-73 and 706-73 C. PR. PÉN.}
\footnotetext[167]{The liberties and custody judge or the investigating magistrate can order such uses.}
\footnotetext[168]{Articles 706-95-4, I and 706-95-5, I of the C. PR. PÉN.}
\footnotetext[169]{Articles 706-95-4, II and 706-95-5, II of the C. PR. PÉN. For the writ to order to intercept communications, the regime provided by article 100-4 and following of the C. PR. PÉN. also applies.}
\footnotetext[170]{Article 706-95-6 of the C. PR. PÉN.}
\footnotetext[171]{Articles 706-95-4 and 706-95-5 of the C. PR. PÉN.}
\footnotetext[172]{For the collection of login data, the liberties and custody judge’s writ is limited to one month and can be renewed once (article 706-95-4 of the French Code of Criminal Procedure). For the investigating magistrate’s writ is limited to two months and can be renewed once (article 706-95-5 of the C. PR. PÉN.). For the interception of communications, it only can be order for forty-eight hours and renewed once (articles 706-95-4 and 706-95-5 of the C. PR. PÉN.).}
\end{footnotesize}
preliminary investigations of the most serious offenses. Under the new regime, the liberties and custody judge and the investigating magistrate’s decision have to indicate the specific offense, the localization or description of the information system to be accessed, and the duration of the writ (which cannot be more than a month for the liberties and custody judge and four months for the investigating magistrate). The process must be carried out under the authority and control of the judge who issued the writ. To be considered legal, the interception must target the specific infractions listed in the writ. This provision does not forbid the discovery of other offenses not mentioned in the writ, however.

D. Geolocalization

From 2011, the French Supreme Court considered geolocalization legal under article 81 of the French Criminal Procedure Code, as a tool to gather evidence during formal investigations. However, the Court did not allow this use during preliminary inquest (conducted by the public prosecutor) in two decisions of 2013. A law was adopted in 2014 to clarify the conditions of the use of geolocalization in the criminal process. This law was then codified in articles 230-32 to 230-42 of the French Criminal Procedure Code. Under the new legal regime, the public prosecutor or the investigative magistrate can, in cases of certain offenses, use any technical means to track the position of a person, object, or vehicle, in real time, without

---

175 Articles 706-102-1 and 706-102-3 of the C. PR. PÉN.
176 Art. 706-102-4 of the C. PR. PÉN.
177 Article 706-102-4 al 1 of the C. PR. PÉN.
178 Article 706-102-4 al 2 of the C. PR. PÉN.
179 French Supreme Court, Crim. 22 October 2013, no.13-81.945, Bull. crim. no. 196 and no. 13-81.949, Bull. crim. no. 197.
181 Article 230-32 of the C. PR. PÉN.
obtaining the suspect’s consent, on the national territory. In 2016, the French Supreme Court specified its interpretation on the use of evidence gathered outside of the national territory. In this case, the suspected was being tracked with geolocalization tools inside and outside of the French borders.\footnote{French Supreme Court, Crim. 9 February 2016, no. 15-85.070, Bull. crim. no. 32; no. 15-85.068; no. 15-85.071.} The issue was to determine if the evidence gathered outside of France could be used during the French trial. The Supreme Court ruled that the when the geolocalization tracking was not authorized by the foreign authority, it was necessary to determine if the foreign authority authorized the use of the data issued from geolocalization tracking. Thus, the French Supreme Court emphasizes the basic principles of international criminal cooperation, and confirmed that it is necessary to obtain the authorization of a foreign authority when tracking vehicles in its territory.

\textit{E. Collection of Evidence Upon Request}

The 2004 reform of criminal procedure\footnote{Law no. 2004-204 of 9 march 2004, adapting the justice system to developments in crime.} expanded the powers of the Officers of the Judicial Police, prosecutor, and investigating magistrate\footnote{Respectively articles 60-1, 77-1-1 and 99-3 of the C. PR. PÉN. See also, Marc Schwendener, Une police aux pouvoirs d’enquête renforcés, AJ Pénal 2004, p. 228.} allowing them to require, by any means, any person to provide information or documents relevant to the investigation, including electronic information and documents. This reform also provided the Officers of the Judicial Police, prosecutor, and investigating magistrate with the power to compel telecommunications operators to retain the content of the information viewed by the target user for up to a year.\footnote{See articles 60-2, 77-1-2 and 99-4 of the C. PR. PÉN.} Except when there is “due cause,” the operator has to answer the request even if the person is
bound by professional secrecy obligations. Failure to promptly answer a request can be sanctioned by a fine of 3,750 euros. When the data is requested from certain categories of people (e.g., doctors, notaries, solicitors, bailiffs, attorneys, or a press or communication company) the specific target must give consent. Failure to promptly answer such a request can be sanctioned by a fine of 3,750 euros.

The French Supreme Court has consistently ruled that the identification of a phone number should not be considered as an interception of communication, nor a technical measure. Thus, the protections provided by article 100 and subsequent and articles 60 and 77-1 of the French Criminal Procedure Code do not apply.

**F. Encryption**

With the increased use of encryption, law enforcement authorities have been facing difficulties conducting effective wiretaps and accessing stored data. A specific section in the French Code of Criminal Procedure allows law enforcement to designate any person to decrypt the data or provide access to the data in plaintext.

**G. Exclusion of Illegal Search Evidence:**

The enforcement of search and seizure rules is a key area of difference between European and American law. While exclusion is the usual response to an illegal search and seizure in the

---

186 Article 60-1 and 77-1-1 of the C. PR. PÉN.
187 Article 60-1 al. 2 of the C. PR. PÉN.
188 See article 77-1-1 of the C. PR. PÉN.
189 Article 60-1 al. 2 of the C. PR. PÉN.
190 French Supreme Court, Crim. 2 April 1997, no. 97-80.269, Bull. Crim. no. 131; Crim. 18 June 2002, no. 01-86.098, Bull. Crim. no. 136.
191 Articles 60 and 77-1 of the C. PR. PÉN. Code regulate the recourse to expertise.
192 Article 230-1 and subsequent of the C. PR. PÉN.
United States, this remedy is rarely used in Europe. Indeed, the European Court of Human Rights has decided in various cases that a failure to exclude illegally seized evidence does not automatically render a trial unfair under the European Convention on Human Rights. The French Supreme Court has consistently ruled that illegally seized evidence does not need to be automatically excluded from the trial when both parties can discuss the evidence. Furthermore, the trial judge is free to weigh each piece of evidence before her.

**H. State of emergency regime**

The Paris terrorist attacks on November 2015 constituted unprecedented incidents in the French history. The night of the attacks, French President François Hollande declared a nationwide state of emergency. Under French law, the President, in consultation with the Council of Ministers, may declare a state of emergency “in situations involving imminent danger resulting from serious breaches of public order” or “in circumstances which, due to their nature and seriousness have the character of public disaster.”

---

196 See no 121.
198 Article 1 of the law on the state of emergency, as amended on July 21, 2016.
Since November 14, 2015, the state of emergency has been prorogated five times by the French Parliament and will be valid through at least July 25, 2017.\textsuperscript{199} The law regulating the state of emergency provides extensive police powers, conferring extraordinary capacities to the Minister of Interior and the Prefect of Regions.\textsuperscript{200} The French State Council considered in a 2006 decision that the extraordinary powers provided by the law on the state of emergency are still compatible with the provisions of the European Convention on Human Rights.\textsuperscript{201} To avoid sanctions, however, as other countries have done before,\textsuperscript{202} France filed a formal notice of derogation from the European Convention on Human Rights with the Secretary-General of the Council of Europe.\textsuperscript{203}

Under article 6 of the law on the state of emergency, the Minister of Interior may order detention under house arrest when there are serious grounds to consider that a person’s behavior may constitute a threat for public security and order.\textsuperscript{204} Article 14 of the law on the state of emergency provides that house arrests will cease to have effect at the latest time when the state

\textsuperscript{199} The French Prime minister announced on November 13, 2016 that the state of emergency will probably be prorogated for a few months. See http://www.bbc.com/news/world-europe-37965708.

\textsuperscript{200} The prefect of region is the State’s representative in the region.


\textsuperscript{202} For a list of the countries and the context of these derogations, see www.echr.coe.int/Documents/FS_Terrorism_ENG.pdf

\textsuperscript{203} \url{http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations?p_auth=N5hF4XrW}, consulted in September 2016.

\textsuperscript{204} Alongside with this house arrest detention, the Minister of Interior can order additional measures, including that the person reports several times each day to the police or gendarmerie services; the surrender to these services of his or her passport or other identification documents; and to be prohibited from associating directly or indirectly with certain persons. Also, when the person has received a custodial sentence following conviction of a crime classified as an act of terrorist act or similar, the Minister of Interior may order that he or she be electronically tagged.
of emergency ends. Thus, some of the house arrests ordered in November 2015 could end in late July 2017 if the state of emergency is not again prorogated. The Constitutional Council considered that the provision regarding house arrest does not constitute a disproportionate violation to the freedom of movement.

From November 13, 2015 to February 2016, 392 house arrests were ordered by the Minister of Interior (including 307 from November 15, 2015 to November 30, 2015). House arrests were also used by the Minister of Interior during the Climate Event COP 21 held in Paris in November and December 2015, although the house arrest of these persons were not related to terrorist threats. In December 2016, there were 91 house arrest in effect.

Article 5 of the law on the state of emergency provides the Prefect of Region the power to restrict freedom of movement in her territory in three ways. First, article 5 offers the possibility to forbid movement of persons and vehicles in certain places and at certain times. Second, it allows, by order of the Prefect, for protection and security zones in which the presence or residence of persons would be regulated. Finally, it provides the power to prohibit the presence or residence of any person seeking to disrupt or otherwise interfere with public policy.

---

205 Even if the Minister ordered in a circular to reassess regularly the necessity of the house arrest. In December 2016, 37 house arrest have been applied for more than a year (see Mercier Report, no. 220 of 14 December 2016 p. 19, https://www.senat.fr/rap/l16-220/l16-2201.pdf).


210 Article 5V of the law on the state of emergency, as amended on July 21, 2016.
Adding to the existing list of associations that can be dissolved under article L 212-1 of the Code for Homeland Security, article 6-1 of the law on the state of emergency provides the power to the Council of Ministers to dissolve associations that participate, facilitate, or incite to commit serious offense to the public order.\textsuperscript{211} The Ministry of the Interior also gains limited control over the press, as he is permitted to take any measure to interrupt online communication services inducing or glorifying terrorist acts.\textsuperscript{212}

This derogatory regime has many implications on the rules regarding collection of and access to evidence, especially with article 11 of the law on state of emergency. With article 11, both the Minister of Interior and the Prefect of region can individually: “order warrantless searches at any location,\textsuperscript{213} during daytime or night hours, if there is serious reason to believe that this location is frequented by a person whose conduct constitutes a threat for security and public order.”\textsuperscript{214} The public prosecutor with territorial jurisdiction shall be informed by this decision without delay. Similar to what is required under the ordinary rules, the search may only be carried out in the presence of the occupant or in his or her absence in the presence of his or her representative or of two witnesses. From November 2015 to May 2016, 3,594 administrative searches were ordered (2,700 of which conducted within the first month).\textsuperscript{215} Half of these searches were made outside of the hours authorized under the regular procedures.\textsuperscript{216}

\begin{flushleft}
\textsuperscript{211} Article 6-1VI of the law on the state of emergency, as amended on July 21, 2016.
\textsuperscript{212} Article 11, II of the law on the state of emergency, as amended on July 21, 2016.
\textsuperscript{213} Except in traditionally protected locations such as a location dedicated to the exercise of parliamentary mandate or the professional activity of a lawyer, judge or journalist.
\textsuperscript{214} Article 11 of the law on the state of emergency, as amended on July 21, 2016.\textsuperscript{1955}
\textsuperscript{216} Rules provided at article 59 of the Code of Criminal Procedure.
\end{flushleft}
these 3,299 administrative searches, only five led to the opening of judicial procedure for terrorism and twenty led to the opening of judicial procedure for glorification of terrorism. From July to December 2016, 590 administrative searches were ordered leading to the opening of 65 judicial procedure including 25 relating to terrorism.\footnote{217}{See Mercier Report, no. 220 of 14 December 2016 p. 18, \url{https://www.senat.fr/rap/l16-220/l16-2201.pdf}.}

Article 11 also provides broad powers to the Officers of the Judicial Police\footnote{218}{Insert definition of Officers of the Judicial Police} regarding the access to electronic evidence. The law allows access to,

data using a computer system or terminal equipment present at the locations where the search is carried out to data stored on the said system or equipment or in another computer system or terminal equipment, provided that these data are accessible from the initial system or available to the initial system.\footnote{219}{Article 11 of the law on the state of emergency, as amended on July 21, 2016.}

If the seizure reveals elements regarding a threat to security and public order, data can be copied or seized. The data copied or seized cannot be exploited before the issuance of a court order.\footnote{220}{Article 11 of the law on the state of emergency, as amended on July 21, 2016.}

At the end of the search and seizure the administrative authority shall bring the matter to the administrative magistrate of expedite\footnote{221}{The administrative \textit{Juge des référés} is an administrative judge who takes decision on emergency cases and matters.} whose ruling on the validity of the seizure and its exploitation must be made within 48 hours. The Constitutional council ruled this provision and part of its revision of July 2016 contrary to the constitution.\footnote{222}{Under both decisions, the provision provided by the law no. 2015-1501 of 20 November 2015 was declared unconstitutional by the Constitutional Council because neither the seizure nor the exploitation of the data thereby collected was authorized by a court, decision no. 2016-536 of 19 February 2016, \url{http://www.conseil-constitutionnel.fr/conseil-constitutionnel/ Francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-536-qpc/ version-en- anglais.147081.html}. Then a revision was made with law no. 2016-987 of 21 July 2016, some part of which was also declared unconstitutional by the Constitutional Council, \url{http://www.conseil-constitutionnel.fr/conseil- constitutionnel/ Francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-600-qpc/ decision-n-2016-600-qpc-du-2-decembre-2016.148276.html}.}
The Constitutional council considered that the provisions were not providing the legal safeguards capable of ensuring a reasonable balance between the objective of constitutional standing of safeguarding public order and the right to respect for private life. Indeed, the first version of the text did not provide any judicial oversight. The provision of July 2016 provides some judicial oversight for the exploitation of the data seized, but the regime remains highly intrusive on the right to private life and can lead to abuse because of the broadness of the terms used in the law. In addition, the judge empowered to review for exploitation is the administrative judge and not the judiciary judge, who ordinarily reviews search and seizure under the criminal procedural rules.\textsuperscript{224}

Many French, European, and international institutions, academics, and NGOs have criticized the French state of emergency’s implications on civil liberties.\textsuperscript{225}

\section*{V. **The Current France/US Mutual Legal Assistance Regime**}

The default mechanism for sharing evidence between the United States and France is a bilateral Treaty on Mutual Legal Assistance (France/US Treaty), which was signed in 1998 and entered into force in 2001.\textsuperscript{226} This treaty embodies the same structures as the other bilateral and multilateral MLA treaties both countries have signed and therefore the examination of this treaty

\textsuperscript{224}The regime applying for the instruction and the prosecution of terrorism acts is provided by articles 706-16 and subs. of the Code of Criminal Procedure.

\textsuperscript{225}CNCTR, défenseur des droits, quadrature du net; Council of Europe, Secrétaire general du Conseil européen; Condamnation rapporteurs spéciaux des NU; 450 academics signed a voluntary intervention in a case asking the French Conseil d’État (CE) to suspend the state of emergency or to ask the President to suspend in part or completely the state of emergency; Human Rights Watch, Amnesty international, Firefox.

\textsuperscript{226}See Mutual Legal Assistance Treaty Between the United States of America and France (1998) available at \url{http://www.state.gov/documents/organization/121413.pdf}.\
introduces MLA treaties more generally. This Part examines how the France/US Treaty operates for the categories of electronic evidence discussed above.

Under the France/US Treaty, the requesting state must have jurisdiction over the criminal offense. The Treaty allows a country to deny a request if either “the offense to which the request relates is a political offense or an offense related to a political offense” or “the execution of the request would prejudice its sovereignty, security, public order, or other essential interests.” In light of the effect that criminal investigations can have on a state’s sovereignty and security, this text provides significant latitude to deny a request.

Current US law provides considerable reason to deploy MLAT requests. For emails and other requests for the content of stored electronic communications, ECPA is widely understood to require France or any other requesting country to make an MLAT request. Such a request is needed for content even in the simple original example, where a burglary in France, involving French citizens, has evidence held by an email provider in the United States. The 2016 Microsoft Ireland case increased the importance of using MLA procedures to US prosecutors as well. In that case, the Second Circuit held that the SCA did not apply “extraterritorially”—a search

---

227 The treaty is limited in scope to the “investigations or proceedings in respect of criminal offenses the punishment of which, at the time of the request for assistance, is a matter for the judicial authorities of the requesting state.” Mutual Legal Assistance Treaty Between the United States of America and France, at Art. 1(1) (1998), available at http://www.state.gov/documents/organization/121413.pdf.

228 See id. at Art. 6.


warrant could not compel a US-based company to provide the contents of an email account where the evidence was stored outside of the United States. To the extent emails and other electronic evidence are stored abroad, the US government can no longer rely on the presence of the corporate headquarters in the United States to justify access to the evidence.231

As discussed previously, there is a multi-step process when France or another country submits an MLAT request to the US, with the total process on average taking roughly ten months to complete.232 Each successful request is evaluated by the DOJ’s Office of International Affairs (OIA), a US Attorney’s office, a federal magistrate judge, and then again by the Federal Bureau of Investigation and the OIA.233 The OIA, US Attorney’s office, and magistrate judge each review to ensure that enough evidence exists for the type of information sought—a probable cause warrant for content, and a 2703(d) order showing a reasonable and articulable suspicion for much non-content data.234 After the magistrate judge approves the request, and the company produces the records, the FBI and OIA review the records so that only data responsive to the

---


232 See id. at *38-39, Telephone Interview with Anonymous Department of Justice Official (Apr. 7, 2015).


234 See supra Part II (standards of proof under ECPA).
request is returned to France, and that no data is included that may violate the US First Amendment, such as prosecution of a political or speech crime.235

Requests from the US to France follow analogous procedures. A US MLAT request goes to the French Ministry of Justice, where it is processed by the “bureau d’entraide pénale internationale.”236 This bureau centralizes both incoming and outgoing MLA requests. Once processed by the bureau, the request goes to the competent magistrate or procureur if under French law there is a need for a warrant or else directly to the company. The bureau sends evidence produced under the treaty to the US DOJ.

The United States and France have different rules for voluntary disclosure of metadata, including both basic subscriber information and information that is often considered more sensitive, such as to/from and location information.237 In the United States, as previously discussed, the ECPA permits a company to voluntarily disclose metadata with a non-US governmental entity.238 In practice, companies in the United States disclose BSI subject to their internal policies, which have become increasingly strict in recent years.239 For instance, if the request appears to be an attempt to prosecute political dissent, blasphemy, or other speech

236 French Office of International Affairs.
crimes, the internal policies of a US company may dictate not to disclose the information, unless required to do so by legal process. Additionally, if the company believes the request is for a valid crime but worries that the requesting country may commit human rights violations in its prosecution of that crime, such as through torture, its policy may also be to refuse the request. In contrast, French companies may only disclose the personal data of users, including basic subscriber information, when officially requested.\textsuperscript{240}

VI. \textbf{Possible France/US MLA Reforms}

This Part first examines the technical, legal, and political context for reform. France and the United States provide an informative case study for considering MLA reform—the two countries are longstanding allies, which supports reform, but have criminal justice systems that differ in multiple respects, which creates an obstacle to reform. The Part then uses a choice-of-law approach to analyze several issues concerning the scope of possible MLA reform.

\textit{A. The Technical, Legal and Political Context for Reform}

The context for considering possible reform in France/US MLA procedures include changing technology, the political and legal context, and the different approaches for gathering electronic evidence. Concerning technological and market change, our research has emphasized two factual changes that drive the growing importance of MLA reform: (1) the globalization of data, resulting in evidence often being held outside of the country; and (2) the growth of encryption and related technical security measures, leading to the country often being blocked when it seeks evidence from a wiretap or access to stored information. The combination of globalization and encryption means that the best source of evidence in a growing fraction of cases will be held in another country, only accessible via an MLA request.

\textsuperscript{240} See articles 60-2, 77-1-2 and 99-4 of the C. PR. PÉN. See Part IV E, Collection of Evidence upon request.
Along with this technological context, consideration of MLA reform between France and the United States takes place in a shared political and legal context. The two countries are allies, from the U.S. Revolutionary War through both Worlds Wars, and today in NATO. France is a Member State of the EUEU, which has innumerable ties with the United States, including recent agreements on protecting personal data such as the Umbrella Agreement and Privacy Shield. Both France and the United States, today and for many years in the past, are democracies under the rule of law. The US heritage of constitutional law, overseen by the Supreme Court, has strong parallels to fundamental rights protection today in France and the EU generally, with recourse to the European Court of Justice and the European Court of Human Rights. This heritage of alliance and protection of the rule of law make the two countries strong candidates for agreeing to new procedures for sharing evidence in an era of where that evidence is more often best accessed abroad.

This article has shown, however, that there are important differences in how the two legal systems govern searches for electronic evidence. Along with most of continental Europe, France’s legal system derives primarily from Roman law and the civil law tradition, while the US system derives primarily from England’s common law. Where the US law insists on a probable cause finding by an independent magistrate, in France the majority of criminal cases are

---


investigated by the police under the supervision of the public prosecutor.\textsuperscript{243} Instead of the US adversarial system, where criminal defendants can exclude evidence that is illegally obtained, in France any information “necessary to establish the truth” is generally available to assist investigating authorities.\textsuperscript{244} France, in turn, can point to its own institutional safeguards on the actions of police, prosecutors, and magistrates, as well as comprehensive data protection laws for providing safeguards against misuse of personal data, in contrast to the lack of such a law in the United States in general and for criminal justice more specifically.

Our current article in the Emory Law Journal examines in greater depth the ways that both the United States and the EU are stricter in some respects for law enforcement access to personal data.\textsuperscript{245} For purposes of this article, the France/US relationship is a meaningful case study of the promise and challenges of reforming ways to share criminal justice evidence. The France/US alliance and shared commitment to the rule of law provide strong reasons to support MLA reform, while the large differences in criminal procedure and substantive standards for access to evidence illuminate the obstacles to such reform.

\textit{B. Scope of Possible Reform and Choice of Law}

Given the strong case for MLA reform, the next question is how broad the scope of such reform should be. For evidence held by US-based information technology companies, the status quo has been that requests made outside of the US generally have to comply with the


\textsuperscript{244} In the United States, the so-called “exclusionary rule” bars evidence obtained through an illegal search from being used at criminal trials, while the “fruit of the poisonous tree” doctrine further bars additional evidence derived from the illegal search. See e.g., \textit{Mapp v. Ohio}, 367 U.S. 643 (1961), \textit{Wong Sun v. U.S.}, 371 U.S. 471 (1963). In France, where evidence is available to assist the investigation, it is not necessarily available for use in an actual court proceeding. See e.g., articles 81, 82, 97 of the C. PR. PÉN. See also, French Supreme Court, Crim. 27 October 1959 \textit{Bull. Crim.} no. 450.

requirements of the ECPA, the SCA, and the Fourth Amendment.\textsuperscript{246} As former Judge and US Secretary of Homeland Security Michael Chertoff has written, MLA reform raises choice of law issues. He states,

\begin{quote}
We should work together to identify an agreed-upon international system for newly designed choice-of-law rules for data, particularly data in the Internet cloud. Such rules would determine which country’s law governs in a dispute, as when we try to decide whose law governs a contract for the sale of goods.\textsuperscript{247}
\end{quote}

Under traditional choice-of-law approaches, we identify the interests that the countries, such as the United States and France, have in a particular case.\textsuperscript{248} In some cases, there may actually be a conflict of law; such as if a country like France requires production of evidence but another country such as the United States says production is not permitted.\textsuperscript{249}

Some MLA reforms are possible without the choice of law analysis. In our previous work, for instance, we have supported measures such as increasing MLA funding for the DOJ, streamlining the request process, and developing online tools to improve communications

\textsuperscript{246} The \textit{Microsoft Ireland} case states an exception to that approach, for evidence about a non-US person held only outside of the US – Irish rules for government access apply under those facts.


\textsuperscript{248} See, e.g., \textit{Restatement (Second) of the Conflict of Laws} § 6(2)(a) (including “the needs of the international systems” as a factor in choice-of-law analysis).

\textsuperscript{249} In 2016, there have been instances in Brazil where a judge ordered WhatsApp to produce evidence, while WhatsApp argued that production was illegal under ECPA. WhatsApp has been shut down temporarily due to such orders, which were overturned on appeal. Vinoid Sreeharsha, \textit{WhatsApp is Briefly Shut Down in Brazil for a Third Time}, N.Y. Times (July 19, 2016) available at http://www.nytimes.com/2016/07/20/technology/whatsapp-is-briefly-shut-down-in-brazil-for-a-third-time.html?r=0. Such cases highlight the importance of international solutions to minimize such conflict. The Brazilian approach, if the initial court orders had been upheld, are an example of what we have called the “extra-territorial” approach. We have previously discussed disadvantages of such an approach, especially for privacy in situations where extra-territorial orders are issued from countries with a weak rule of law. See Peter Swire & DeBrae Kennedy-Mayo, \textit{Why Both Europe and the US are “Better” than Each Other: Privacy and Government Requests for Information}, EMORY L. J. (forthcoming 2017).
between the countries. Such proposals do not raise particularly difficult conflicts between nations. The focus of reform discussions, however, has been on creating exceptions to the requirement that the ECPA applies, to enable France or some other country to go directly to the company for content requests, without requiring the lengthy MLA process.

The strongest case for reform occurs when the interests tilt strongly toward the requesting country, such as France. First, in the burglary example, the crime occurs in France, with both the victim and suspects being French citizens in France, but a US-based email company holds the evidence. In considering the relative interests of France and the United States with these facts, France has a strong case to argue that it has more at stake than the United States—an entirely French violation of law, except for the fact that that the communication was made through the services of a non-French company. For MLA reform, this is the “easiest case.” Second, the case may be less purely French but with no greater interest of the United States. For instance, one of the suspects lives in Germany or some other EU member state with a strong rule-of-law structure. In that instance, the crime and victim are French, and the United States has no greater interest than before. The balance between France and the United States is not as clear-cut as in the easiest case, but the US interest remains limited. Third, the case may involve a suspect who lives in a non-EU country that lacks a strong rule-of-law structure. In this case, one might see the US interest as somewhat stronger, in order to prevent direct access by the French government, perhaps for types of communication protected under US law.


251 The Microsoft Ireland case states an exception to the applicability of ECPA, for evidence about a non-US person held only outside of the US – Irish rules for government access apply under those facts.
A number of factors can strengthen the US interest in the case. Notably, the requested communications might be from a US person, such as a US citizen who is a suspect or a US citizen who happens to communicate with non-US persons whose records are produced directly to the French government. In recognition of the greater US interest in such instances, the proposed US/UK MLA reform agreement does not apply to communications of US persons.\textsuperscript{252} Second, it may be relevant to assess where the evidence is actually located—evidence held only in the United States arguably has a stronger US interest than evidence held only in France, with evidence stored in both countries being an intermediate case. The \textit{Microsoft Ireland} case emphasized this location factor, by holding that a US warrant could not compel production of records held about a non-US person and stored only outside of the United States.\textsuperscript{253} Third, some types of investigations more strongly implicate US constitutional values. For instance, the United States could argue that direct production of evidence should not be made to the French government in cases where the First Amendment would prohibit production of evidence from the United States.\textsuperscript{254} Certain speech-related French crimes might thus be excluded from the scope of an MLA reform proposal.

The shifting possible interests of France and the United States affect the provisions of possible MLA reform. For the easiest case or other settings where the French interest is relatively


\textsuperscript{253} \textit{In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, Microsoft Co. v. US}, 2016 WL 377056, at *19 (2nd. Cir., 2016).

\textsuperscript{254} One example of such a speech-related case concerns the French action against Yahoo-France for allowing hate speech on Yahoo’s sites accessible from France. The case succeeded against Yahoo-France, but based on the First Amendment, US courts would not recognize the judgment against Yahoo. \textit{See Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme}, 433 F.3d 1199 (9th Cir., 2006).
strong compared to the US interest, there is greater reason to support amendments to the ECPA that would allow the French government direct access to records held by a US company. For the cases where the US interest is relatively strong, the current MLA procedures deserve more careful consideration.

Along with this analysis of the relative interests of France and the United States, we will briefly mention three other issues to consider in MLA reform. First, since emails obviously lack a postal address, there is often uncertainty about the nationality of an email’s sender or recipient. An MLA reform proposal thus should police the realm of possible uncertainty, to avoid requests that, reasonably understood, involve a US person or some other criterion that still requires an MLA request. Second, the scope of data covered by MLA reform could be broadened or narrowed. As part of MLA reform, Greg Nojeim of the Center for Democracy and Technology has proposed expanding ECPA protections to traffic data, such as to/from information for an email. This proposal has virtues, notably that a weakening of the ECPA for content would be accompanied by strengthening the ECPA for some metadata. On the other hand, expansion to traffic data creates a disincentive for countries to enter the new system—participating countries would lose access to traffic data, which is often used early in an investigation to identify suspects and develop enough evidence to meet the probable cause standard. Third, participation should be permitted only with periodic review about whether the


other country continues to comply with the rule-of-law and other requirements in the MLA reform package. Some civil society groups have sought an independent, non-governmental way to do the periodic assessment.\textsuperscript{257} We have not seen a workable proposal where a non-governmental entity does the assessment. In the absence of such a proposal, we instead support the VWP model, with certification by the US Attorney General, after consultation with the Secretary of State, and containing periodic reviews.\textsuperscript{258}

In conclusion, on the scope of MLA reform, a choice-of-law approach helps organize many of the issues that have arisen in recent MLA debates. The relative interest of France is strongest in the easiest case, where all the activity is French. As the relative interest of the United States becomes stronger, then the case strengthens for comity, where France respects US law and uses the traditional MLA process, hopefully with improved and faster procedures that would apply to all MLA requests.

\textbf{VII. CONCLUSION}

As shown in this article, both France and the United States have complex legal regimes, under the rule of law, for a government to access evidence used in criminal prosecutions. The two approaches particularly differ on how they treat the substance of different kinds of electronic evidence, with the United States making finer distinctions between types of data than France. At


\textsuperscript{258} The VWP itself, applying to border issues under the jurisdiction of the Homeland Security Department, has certification by the Secretary of Homeland Security, in consultation with the Secretary of State. MLA reform is under DOJ jurisdiction, so we have supported the approach in the text, which also is included in the proposed UK/US MLA reform. Peter Swire & Justin D. Hemmings, \textit{Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program}, N.Y.U. L. REV. (forthcoming 2017), \url{https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478}. 

51
the same time, the French system provides more systematic protections for the length of time data can be seized, who must oversee investigations, and how data lawfully seized can be used. Comparison of the two regimes thus offers a useful case study for ways in which democratic legal systems govern privacy and government access to evidence.

The interest in MLA reform is growing due to technical and market changes such as the globalization of data and the newly pervasive use of encrypted communications. For such reform to be successful, allied countries such as France and the United States will need to find solutions that bridge the significantly different legal systems. More nuanced understanding of the similarities and differences is a precondition for finding solutions that in the end are consistent with each country’s requirements, including the protections offered by constitutional law.

As we have discussed in more detail elsewhere, there are potentially serious consequences if MLA reform efforts do not succeed. The US government has set forth goals for Internet governance with which we agree: “The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.” Failure to find common ground on MLA reform, under the rule of law, could lead to different and less desirable mechanisms for governments to


seize evidence. These could include increased use of unilateral and extra-territorial mandates to access evidence, as well as requirements to hold data locally rather than permit flow of data across borders. The result would be a global communications structure that is less “open, interoperable, secure, and reliable.”\footnote{INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (May, 2011) (emphasis added), \url{https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf}; For further discussion, see PRESIDENT’S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT’S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY, 209 (Dec. 12, 2014), \url{https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf}.} It is better to overcome the obstacles to MLA reform.