A MUTUAL LEGAL ASSISTANCE CASE STUDY: THE UNITED STATES AND FRANCE

PETER SWIRE,[*] JUSTIN D. HEMMINGS,[**] AND SUZANNE VERGNOLLE[***]

[*] 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 November 13, 2016.

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

[***] Suzanne Vergnolle is a Ph.D. candidate at Paris II Panthéon-Assas France.

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provides a case study involving France and the United States for a topic of growing importance—how to reform the outdated system of "Mutual Legal Assistance" (MLA).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 United States, for criminal prosecution, frequently pursuant to a Mutual Legal Assistance Treaty (MLAT).

As discussed in Part I, 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 communication through the Internet means 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,[1] pressing law enforcement to seek evidence through judicial orders on companies that often store data abroad. Our previous research has examined the goals of

[1] Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Inst. for Info. Sec'y & Privacy at Georgia Tech., Working Paper, Feb. 29, 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf; Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud* 7 (Ctr. for Interdisciplinary Law & Policy Studies at the Moritz College of Law, Working Paper No. 175, 2012), http://idpl.oxfordjournals.org/content/early/2012/09/19/idpl.ips025.full?keytype=ref&ijkey=ywFZOVXIzrgbfae.

stakeholders in the process,[2] 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.[3] 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.[4] 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 procedures for criminal law operate,[5] 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 criminal law and procedure in the United States and France. 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: basic subscriber information; metadata such as to/from information; content of stored records; and interception of electronic communications. Part III 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 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 IV explains the current France/US

---

[2] Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance* (Georgia Tech Scheller College of Bus., Working Paper Series, Working Paper No. 2015-32, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2696163.

[3] Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, N.Y.U. L. REV. (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728478.

[4] Peter Swire & DeBrae Kennedy-Mayo, *Why Both Europe and the US are "Better" than Each Other: Privacy and Government Requests for Information*, EMORY L. J. (forthcoming 2017).

[5] 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 205 (Helsinki Univ. Press 2016).

MLA regime, as well as the growing phenomenon of detailed corporate policies about when to comply with non-mandatory requests for evidence.

Part V turns to possible reforms of MLA between France and the United States, with the proposed reform mechanism of an amendment to 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 France and United States' relationship is a good case study of the promise and challenges of reforming ways to share criminal justice evidence. The French and American 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 V 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.

I. 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: DeBrae Kennedy-Mayo, Justin Hemmings, and Suzanne Vergnolle.[6] Other scholars, most notably Professors Jennifer Daskal and Andrew Woods, have been producing recent scholarship on similar topics.[7]

---

[6] The use of "we" in this article refers to its authors, Peter Swire, Justin Hemmings, and Suzanne Vergnolle.

[7] *See e.g.*, Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issue*s, 8 J NAT'L SEC. L. & POL'Y 473 (2016); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016); Zachary Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45 (2016); Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, BERKMAN CTR. INTERNET & SOC'Y HARV. L. S. (Research Pub. 2016-3, 2016); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015). *See also* Jennifer Daskal, *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, JUST SECURITY (Feb. 8, 2016), https://www.justsecurity.org/29203/british- searches-america-tremendous-opportunity; Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, JUST SECURITY (Nov. 24, 2015), https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework; Michael Chertoff & Paul Rosenzweig, *A Primer on Globally Harmonizing Internet Jurisdiction and*

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 MLAT 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.

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.[8] One important source of current challenges is the increased use of encryption has made many local wiretaps ineffective, pressing law enforcement to seek evidence by alternate means.[9] 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 United States.[10] 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*.[11] As such, the article is entitled *Mutual Legal Assistance in an Era of Global*

Regulation, GLOBAL COMM'N ON INTERNET GOV. (Paper Series 10, 2015), https://www.cigionline.org/sites/default/files/gcig_paper_no10_0.pdf; Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. J. (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age; Albert Gidari, *MLAT Reform and the 80 Percent Solution*, JUST SECURITY (Feb. 11, 2016), https://www.justsecurity.org/29268/mlat-reform-80-percent-solution; David Kris, *Preliminary Thoughts on Cross Border Data Requests*, LAWFARE (Sept. 28, 2015), http://www.lawfareblog.com/preliminary- thoughts-cross-border-data-requests.

8 Swire & Hemmings, *supra* note 3.

9 *Id.*

10 *Id.*

11 *Id.*

Communications: The Analogy to the Visa Waiver Program.[12] 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 United States 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.[13]

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.[14] This article looks to the interests of the US government, non-US governments, technology companies, and public interest groups both in the United States and abroad.[15] 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.[16]

The third article, *Understanding the French Criminal Justice System as a Tool for Reforming International Legal Cooperation and Cross-Border Data Requests*,[17] provides our first detailed examination of a particular country's system for exchanging criminal evidence with the United States. This chapter, in the book *Data Protection, Privacy, and European Regulation in the Digital Age*, focuses on the French criminal

---

[12] *Id.*

[13] Devlin Barrett & Jay Greene, *US to Allow Foreigners to Serve Warrants on US Internet Firms*, WALL ST. J. (Jul. 15, 2016), http://www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305. *See also* Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden, President, U.S. Senate at 2-3 (July 15, 2016), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf.

[14] Swire & Hemmings, *supra* note 2.

[15] *Id.*

[16] *Id.*

[17] Vergnolle, *supra* note 5, at 205.

system and the procedural aspects of how France makes or receives MLAT requests, in contrast to the current article's focus on the substantive standards that apply for such requests.[18] 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.[19] 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.[20] Last, 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.[21]

In the fourth article, *Why Both Europe and the US are "Better" than Each Other: Privacy and Government Requests for Information*, 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 United States has stricter safeguards than the EU, this article also informs current debates and litigation about the adequacy of privacy protections in the United States.

Last, 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 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.

---

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*

II. HOW US LAW ENFORCEMENT OBTAINS EVIDENCE

To assist in the comparison of French and US 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 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.[22] 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."[23] 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 "seizure."[24] 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).[25] Probable cause is not clearly defined in the Constitution. Consequently, the US Supreme Court has attempted to clarify the term on several occasions,[26] but has generally favored a flexible approach,

---

[22] 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.

[23] *Id.*

[24] *See infra* Part III.

[25] *See* Beck v. Ohio, 379 U.S. 89, 96 (1964).

[26] *See, e.g.*, Maryland v. Pringle, 540 U.S. 366, 370–71 (2003); Gerstein v. Pugh, 420 U.S. 103, 111 (1975); Carroll v. United States, 267 U.S. 132, 161–62 (1925).

viewing probable cause as a "practical, non-technical" standard that examines the "factual and practical considerations of everyday life."[27]

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.[28] Justice Harlan's concurrence created the enduring legal test from *Katz*, namely, "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.'"[29] 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*.[30] In *United States v. Miller*, the Court held that a defendant had no reasonable expectation of privacy in the bank records associated with revenue he earned through making bootleg liquor on which he did not pay taxes.[31] The Court pointed to *Katz*'s language, stating, "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[32] The Court in *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.[33]

The same principle was applied in *Smith v. Maryland*, where the Court held that a pen register[34] was covered under the third-party doctrine.[35] The Court reasoned, "[w]hen 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

---

[27] *See* Illinois v. Gates, 462 U.S. 213, 231 (1983) (citing Brinegar v. United States, 338 U.S. 160, 176 (1949)).

[28] Katz v. United States, 389 U.S. 347, 358-59 (1967).

[29] *Id.* at 361 (Harlan, J., concurring).

[30] *See, e.g.*, United States v. Miller, 425 U.S. 435, 442-43 (1976); Smith v. Maryland, 442 U.S. 735, 743-45 (1979).

[31] *Miller*, 425 U.S. at 436-43.

[32] *Id.* at 442 (citing *Katz*, 389 U.S. at 351).

[33] *Id.* at 443.

[34] A Pen Register is a device that can record the calls made from a specific phone number. *See* discussion *infra* Section III.B.2.

[35] *Smith*, 442 U.S. at 743–44.

would reveal to police the numbers he dialed.'"[36] The third-party doctrine continues today, though as discussed in Part 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.[37] 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.[38]

B. THE SEARCH AND SEIZURE OF ELECTRONIC EVIDENCE

Under ECPA and the SCA, the rules for electronic evidence, such as email, are complicated.[39] 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.[40] 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 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.[41] 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.

---

[36] *Id.* at 744.

[37] Telephone Interview with Anonymous Official, Dep't of Justice (Apr. 7, 2015). For more information on US search and seizure law, see 1 PETER J. HENNING ET AL., MASTERING CRIMINAL PROCEDURE (Russell L. Weaver ed., 2d ed. 2015).

[38] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1861-63 (codified as amended at 18 U.S.C. § 2703).

[39] *See id.*

[40] *See id.* §§ 201–301, 100 Stat. at 1861-63, 1867, 1869-70.

[41] *See id.* § 201, 100 Stat. at 1861-63.

The varying strictness of rules under 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 *compels* production from the service provider, as 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.[42]

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

BSI is defined as the identifying information for the owner or controller of an Internet service account.[43] BSI can include the name, address, and any assigned number or identity such as a phone number, username, IP address, or email address.[44] 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.[45] Consequently, BSI is not protected under the Fourth Amendment.[46] The government can seek production of BSI through use of an administrative subpoena, grand jury or trail subpoena, or a court order issued under 18 U.S.C. § 2703(d).[47] As previously noted, a company can also voluntarily disclose BSI to law enforcement upon request without penalty under ECPA.[48] This ability to provide the information voluntarily is true for any law enforcement request, whether from within the United States or a foreign sovereign.[49]

---

[42] *See* 18 U.S.C. § 2703 (2016). Note also that any information can be voluntarily disclosed with "the consent of the subscriber or customer to such disclosure." *Id.* § 2703(c)(1)(C) (LEXIS).

[43] *See id.* § 2703(c)(2).

[44] *See id.*

[45] *See Miller*, 307 US 174 (1939); Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[46] *See* § 2703(c)(2).

[47] *Id.* § 2703(d).

[48] *See id.*

[49] *See* § 2702(b).

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."[50] Originally, these orders applied specifically to information about telephone numbers making a call or being called.[51] 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.[52] 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.[53] DRAS includes the entire e-mail header except for the "subject" line, which is considered content.[54] 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 versus 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 also cover software.[55] 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."[56] Third, the application to all "dialing, routing, addressing, and signaling" information clarified that to/from

---

[50] § 3123 (a)(1)-(2).

[51] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 214, 115 Stat. 272, 285-86 (LEXIS through Pub. L. No. 107-56) (codified as amended at 50 U.S.C. § 1842).

[52] *See* Smith v. Maryland, 422 U.S. 735, 745-46 (1979).

[53] § 216, 100 Stat. at 287.

[54] 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* COMP. CRIME & INTELLECTUAL PROP. SECTION, DEPT'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS 152-53 (Comp. Crime & Intellectual Prop. Section, Dep't of Justice ed., 3d ed. 2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[55] *Id.* at 153.

[56] *Id.* at 153-54.

information under the statute would include a wide range of metadata beyond phone numbers, although it did not include location information.[57]

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."[58] Before 2001, these orders were only valid within the geographic area of the issuing court.[59] 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."[60]

3. The SCA provides for a court order for qualifying categories of electronic evidence upon a showing of a reasonable articulable suspicion.[61]

The SCA requires, under § 2703(d), a court order for the production of certain stored records.[62] These "D orders" require a showing of "specific and articulable facts" that the information sought is "relevant and material to an ongoing criminal investigation."[63] 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.[64] 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.[65] Under

---

[57] *See* ELEC. SURVEILLANCE UNIT, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL PROCEDURES AND CASE LAW FORMS 43 (Elec. Surveillance Unit, U.S. Dep't of Justice ed., 2005 ed.), https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf.

[58] 18 U.S.C. § 3123(a)(1) (2016).

[59] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1869 (codified as amended at 18 U.S.C. § 3123).

[60] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288 (LEXIS through Pub. L. No. 107-56) (codified as amended at 18 U.S.C. § 3123(a)(1)).

[61] 18 U.S.C. § 2703(d).

[62] *Id.*

[63] *Id.*

[64] *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[65] 18 U.S.C. § 2703(b). Note that ECPA also provides exceptions for when such an order can be given with delayed notice. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1864-65 (codified as amended at 18 U.S.C. § 2705).

§ 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.[66]

4. Under ECPA and the SCA, the content of stored electronic communications can be obtained with a probable cause warrant.[67]

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 described in the Federal Rules of Criminal Procedure."[68] In other words, a probable cause warrant is sufficient to obtain the content of electronic communications without giving prior notice to the target.[69]

The SCA[70] has complex rules about voluntary and compelled disclosure of emails, as an important example of stored electronic information.[71] 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.[72] 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.[73] 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.[74] 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

---

[66] 18 U.S.C. § 2703(c). The use of these orders for location was confirmed. Telephone Interview with Anonymous Official, *supra* note 37. 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* U.S. *ex rel.* Historical Cell-Site Data, 724 F.3d 600, 608 (5th Cir. 2013); *In re* U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to Gov't, 620 F.3d 304, 319 (3d Cir. 2010); *In re* U.S. *ex rel.* Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (2013).

[67] *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.

[68] *Id.*

[69] *See id.* § 2703(b)(1)(A).

[70] *See* § 201, 100 Stat. at 1860 (codified as amended at 18 U.S.C. §§ 2701-10) (enacted as Title II of ECPA).

[71] *See id.* § 201, 100 Stat. at 1861.

[72] *See* 18 U.S.C. § 2703.

[73] *See id.* §2703(a).

[74] *See id.* §2703(a), (b), (d).

instead a supplemental "remote storage" and can therefore be accessed with a subpoena, rather than requiring a probable cause warrant.[75]

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.[76] In *Warshak*, the court held that all emails require a warrant.[77] According to the court, notwithstanding the third-party doctrine, this holding under the Fourth Amendment applied the status of whether an individual email has been opened or the length of time the email was stored on a server.[78] 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 *ex parte* court order under § 2703(d).[79] 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.[80] The court also distinguished the third-party doctrine announced in *Miller*, which the government had used to justify access to email content with less than a probable cause warrant.[81] 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.'"[82] The court held that the sender has a reasonable expectation of privacy for the content of email, and consequently the government cannot obtain that content without a warrant based on probable cause.[83] Although this holding is only binding in the Sixth Circuit today, it has had a larger effect on federal investigation policy.

After *Warshak*, the DOJ updated its practice to require 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 days old."[84]

---

[75] *See* United States v. Weaver, 636 F. Supp. 2d 769, 770–72 (C.D. Ill. 2009).

[76] *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[77] *Id.*

[78] *Id.*

[79] *Id.* at 283.

[80] *See id.* at 286, 288.

[81] *See id.* at 288.

[82] *See id.* at 287–88.

[83] *See id.* at 288.

[84] *ECPA (Part I): Lawful Access to Stored Content: Hearing before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the Comm. of the Comm. on the Judiciary, H.R.*, 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office

The DOJ also eschewed the difference between opened and unopened email, testifying, "Similarly, it makes sense that the statute [SCA] not accord lesser protection to open e-mails than it gives to e-mails that are unopened."[85] 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."[86] 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.[87]

Congress has been considering the Email Privacy Act.[88] 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.[89] In the 114th Congress, the Email Privacy Act was passed unanimously in the House with 315 cosponsors, but failed to pass in the Senate.[90] The Act was reintroduced in the 115th Congress with 109 cosponsors and recently passed the House on a voice vote. As part of codifying *Warshak*, the Act would also remove the current differentiation between emails less than or greater than 180 days old.[91]

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.[92]

The real-time interception of electronic data holds the greatest privacy risks and consequently an order authorizing such interception

---

of Legal Policy, Department of Justice), https://judiciary.house.gov/_files/hearings/printers/113th/113-16_80065.PDF.

85 *Id.*

86 *Id.*

87 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.

88 *See* Email Privacy Act, H.R. 699, 114th Cong. (2016); *Updating an E-Mail Law From the Last Century*, DIG. DUE PROCESS (July 25, 2013), https://digitaldueprocess.org/2013/07/updating-an-e-mail-law-from-the-last-century/.

89 *See* H.R. 699 § 3.

90 *See id.*

91 *See id.* § 3.

92 18 U.S.C. § 2518(1)(c) (LEXIS through Pub. L. No. 114-28).

requires a heightened standard of proof.[93] 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."[94] 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."[95] Failure to exhaust alternative, 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.[96] 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.[97] 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;
>
> (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;

---

[93] 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. *See, e.g.*, 50 U.S.C. § 1802(a)(1) (2017). 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.

[94] § 2518(1)(b).

[95] *Id.* § 2518(1)(c).

[96] *See id.*

[97] *Id.* § 2518(1)(d).

> then the court may issue an authorizing order for the interception.[98]

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.[99] The SCA specifically permits the use of administrative subpoenas, grand jury subpoenas, or court orders for acquiring qualified metadata.[100] Furthermore, if data is required to be reported to the government under law then that information can be used without additional court authorization.[101] 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.[102]

Under ECPA, a business can voluntarily disclose basic subscriber information at its own discretion.[103] 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 storage by that service."[104] The law does provide exceptions for when voluntary disclosure is permitted, however, including to "any person other than a [US] governmental entity."[105] 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."[106]

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

---

98 *Id.* § 2518(3).
99 *See* § 2702(b)(3).
100 *See* § 2702(b)(3).
101 *See* 12 U.S.C. § 1953(a); *See also* Treas. Reg. § 1010.100(xx) (as amended in 2010).
102 *See* § 1953(a) (LEXIS); Treas. Reg. § 1010.100(xx).
103 *See* § 2702(c).
104 *Id.* § 2702(a).
105 *Id.* § 2702(c)(6).
106 *Id.* § 2702(c)(4).

or the production of any data the subpoena designates.[107] A defendant can attempt to quash a subpoena if "compliance would be unreasonable or oppressive."[108] 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.[109] Failure to comply with a valid subpoena may result in a finding of contempt of court, resulting in fine or imprisonment until the target complies with the court order.[110]

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.[111] A grand jury may subpoena any information it deems relevant to its consideration of whether or not to indict the suspect.[112] The target of any such subpoena maintains the ability to seek to quash or modify a grand jury subpoena.[113] 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.[114]

III. 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. 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

---

[107] *See* FED. R. CRIM. P. 17(a), (c)(1).
[108] FED. R. CRIM. P. 17(c)(2).
[109] FED. R. CRIM. P. 17(c)(3).
[110] *See* FED. R. CRIM. P. 17(g).
[111] OFFICE OF THE U.S. ATTORNEYS, DEP'T OF JUSTICE, US ATTORNEYS' MANUAL § 9-11.140 (2016 ed.), https://www.justice.gov/usam/usam-9-11000-grand-jury#9-11.140.
[112] *See* FED. R. CRIM. P. 17(a).
[113] *See* FED. R. CRIM. P. 17(c)(2).
[114] *See* FED. R. CRIM. P. 17(g).

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 analysis of the roles and powers of different actors in the French criminal procedure system,[115] the discussion here emphasizes the French substantive standards for accessing electronic evidence. Three main principles dominate the French criminal system in regard to 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).[116] This principle of liberty when administrating the evidence has a truth-seeking function. The principle is not absolute since the principle of legality in 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, and are regulated by the law. Second, the principle of "loyalty when administering proof" ensures that the investigator cannot use unfair practices, fraud, or tricks to obtain the evidence.[117] Finally, trial judges must weigh all items of evidence brought before them under the principle of "intimate conviction."[118]

The French Code of Criminal Procedure permits four types of investigations: identity checks;[119] investigations of *in flagrante delicto*;[120] "preliminary" investigations;[121] and formal investigations conducted by an investigating magistrate (*judiciary information*).[122] Specific regimes and rules govern all four investigation types. The present section focuses

---

[115] Vergnolle, *supra* note 5, at 205.

[116] *See, e.g.*, Jacques Buisson, *Preuve*, V RÉPERTOIRE DE DROIT PÉNAL ET DE PROCÉDURE PÉNALE [RÉP. DR. PÉN. ET PR. PÉN.] § 50 (2016) (Fr.).

[117] *See id.* at § 125. Coralie Ambroise-Castérot, *Recherche et administration des preuves en procédure pénale : la quête du Graal de la Vérité*, 2005 ACTUALITÉ JURIDIQUE PÉNAL [D.A.J. PÉNAL] 261.

[118] *See* CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] [CRIMINAL PROCEDURE CODE] art. 353, 427, 536 (Fr.). *See also* BERNARD BOULOC, PROCÉDURE PÉNALE (25th ed. 2015); Buisson, *supra* note 116, § 94 ("[T]he magistrate has the freedom to value each piece of evidence produced.").

[119] In France, identity checks are strictly regulated, *see* C. PR. PÉN. art. 78-1 to 78-2.

[120] An "*in flagrante delicto*" is one that is "in the process of being committed or which has just been committed," *id.* art. 53.

[121] The preliminary investigation is used in most cases involving traffic violations, contraventions, and non-*flagrante delicto*. This type of investigation is a non-coercive procedure, see *id*. art. 76.

[122] *See* Christopher Slobogin, *Comparative Empiricism and Police Investigative Practices*, 37 N.C. J. INT'L L. & COM. REG. 321, 323 (2011-12).

mainly on the 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.[123] Very few cases are actually transferred to the investigating magistrate in order to open a formal investigation.

A. THE 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.[124]

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.[125] The search is legal if the person whose home is searched is present during the search.[126] If the target of the search is present, the Officers of the Judicial Police[127] then will go to the home to perform the search and seize the evidence.

---

[123] *See, e.g.*, Jacqueline Hodgson, *The Police, the Prosecutor and the Juge d'Instruction: Judicial Supervision in France, Theory and Practice*, 41 BRIT. J. CRIMINOLOGY 342, 349 (2001). 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. *See* Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale [Law 2016-731 of June 3, 2016 for strengthening the fight against organized crime, terrorism and their financing, and improving the efficiency and guarantees of criminal proceedings], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 4, 2016, p. 129).

[124] *See* Cour de cassation [Cass.] [supreme court for judicial matters] crim., Mar. 29, 1994, Bull. crim., No. 118 (Fr.); Jean Pradel, *Définition de la perquisition: notion de lieu clos*, DALLOZ RECUEIL [D.] 1995, 144 (Fr.).

[125] C. PR. PÉN. art. 56.

[126] *See id.* art. 57.

[127] The Officers of the Judicial Police are responsible for recording criminal offenses, receiving complaints from victims, summoning witnesses, interviewing suspects and gathering evidence.

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.[128] 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[129] to issue a warrant, but only when the investigation so requires and for cases involving criminal offenses and misdemeanors carrying a sentence of at least five years imprisonment.[130]

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[131] 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.[132] To be legal, the search only needs to be necessary to establish the truth of an offense.[133] Either the resident[134] 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.[135] When a search is necessary to establish the truth, the Officers of the Judicial Police can seize the data that is located where the search happens.[136] The data is seized under judicial authority.[137] Little guidance is provided in the law regarding the deletion of such evidence at the end of the investigation.

---

[128] C. PR. PÉN. art. 76.

[129] The "Juge des libertés et de la detention", which can be translated as "liberties and custody judge."

[130] C. PR. PÉN. art. 76.

[131] Except in certain places that are excluded by law, such as the office of parliament members and attorneys, under article 26 of the French Constitution and C. PR. PÉN. 56-1 and following.

[132] *See* Cass. crim., Jan. 22, 1953, Bull. crim., No. 24 (Fr.); Charles Lapp, *Note*, D. 533, 535 (1953) (Fr.).

[133] *See, e.g.*, C. PR. PÉN. art 81, 82, 97; Cass. crim., Oct. 27, 1959, Bull. crim., No. 450 (Fr.).

[134] When the resident is under custody, the investigating magistrate needs to obtain his written consent. C. PR. PÉN. art 57, 95.

[135] The regime depends on the place that is searched. *See id.* C. PR. PÉN. art. 57, 96.

[136] 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.

[137] C. PR. PÉN. art. 97.

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 regime regulating the interception of communications transmitted by means of telecommunications.[138] The Court considered that tapping and other forms of interception of telephone conversations represented a serious interference with private life and correspondence.[139] 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.[140] Consequently, in 1991 the French Parliament adopted a specific regime that regulates the collection and interception of electronic communications.[141] "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 other electromagnetic or electronic system.[142] Thus, the definition is very broad and encompasses a variety of different types of correspondence, including not only traditional phone communications but also emails.[143]

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

---

[138] *See* Huvig v. France, 176 Eur. Ct. H.R. (ser. A) 36, 56-57 (1990); Kruslin v. France, 176 Eur. Ct. H.R. (ser. A) 3, 24-25 (1990).

[139] These are both protected under article 8 of the European Convention on Human Rights. *See* European Convention on Human Rights as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13, art. 8, 4 Nov. 1950, 213 U.N.T.S 221.

[140] *See Huvig*, 176 Eur. Ct. H.R. at 56-57; *Kruslin*, 176 Eur. Ct. H.R. at 24-25.

[141] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques [Law 91-646 of July 10, 1991 on secrecy of correspondence transmitted by means of telecommunications] (Fr.).

[142] Pascal Dourneau-Josette, *Écoutes téléphoniques judiciaires*, V. RÉP. DR. PÉN. ET PR. PÉN. § 52 (2016) (Fr.). Code des postes et des communications électroniques [C.P.C.E] [Postal and Electronic Communications Code] art. 32 (Fr.).

[143] Similarly, the misdemeanor of violating the secrecy of correspondence transmitted by means of telecommunications also includes emails. *See, e.g.*, Cour d'appel [CA] [regional court of appeal] Paris, Chambre 7, Jan. 27, 2012, 10/05328.

criminal offenses and misdemeanors, sanctioned by imprisonment of at least two years, and when the circumstances of the case require interception.[144] To be valid, however, the investigating magistrate does not need to justify the request of interception.[145] Where the investigating magistrate delegates this operation through a rogatory commission,[146] the process must be under her authority and control.[147] An interception operation must be ordered in writing and must be for a period of not more than four months.[148] This order is not judicial in nature thus it cannot be appealed.[149] Finally, the order shall provide all the information needed to identify the communication(s) to be intercepted.[150]

In a recent case, the French Supreme Court[151] 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.[152] 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

---

144 C. PR. PÉN. art. 100.

145 Dourneau-Josette, *supra* note 142, § 68.

146 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* Christian Guéry, *Commission Rogatoire*, V. RÉP. DR. PÉN. ET PR. PÉN. § 1 (2015) (Fr.).

147 C. PR. PÉN. art. 100.

148 *Id.* art. 100, 100-2. *See id.* art. 706-95.

149 *Id.* art. 100. Under the general rules of law, all of 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 be appealed even from the prosecutor because the prosecutor can only appeal Decree. *See, e.g.*, Pierre Chambon, *Analyse et commentaire de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications*, D. 173 (1991) (Fr.).

150 *See* C. PR. PÉN. art. 100-1.

151 *See* Cass. crim., July 8, 2015, Bull. crim., No. 450 (Fr.). However, this case has been overruled the law No. 2016-731 adopted on July 3, 2016. *See* Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale [Law 2016-731 of June 3, 2016 for strengthening the fight against organized crime, terrorism and their financing, and improving the efficiency and guarantees of criminal proceedings], J.O., June 4, 2016, p. 129.

152 Cass. crim., July 8, 2015, Bull. crim., No. 450 (Fr.).

in accordance with the law on search and seizure.[153] 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).[154] On July 3, 2016, the French Parliament passed a law on fighting against organized crime, terrorism, and terrorist financing, and improving the efficiency and safeguards on criminal procedure.[155] This law provides a new regime for formal investigations or investigations for the most serious offenses, including organized crime.[156] Indeed, articles 706-95-1 and 706-95-2 of the French Code of Criminal Procedure allow the liberties and custody judge and the investigating magistrate, when 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.[157] The investigating magistrate or the mandated Officers of the Judicial Police can require access to the emails through a qualified agent.[158] To be considered legal, the search and detection may only concern the specific infractions listed in the writ.[159] This provision, however, does not forbid the discovery of other offenses not mentioned in the writ.[160]

From an international perspective, two recent cases are relevant to the French interception of commncations 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

---

[153] *See* Cécile Benelli-de Benazé, *Instruction : Précision sur la Notion d'Interception des Correspondances*, Sept. 2015 DALLOZ ACTUALITE [D.A.] (Fr.); Anne-Sophie Chavent-Leclère, *Irrégularité des Interceptions de Courriers Électroniques Stockés Antérieurement à l'Autorisation*, Oct. 2015 PROCDURES No. 10, 309 (Fr.); Albert Maron & Marion Haas, *Vifs Échanges et Données Mortes (Pas Pour Tout le Monde)*, 2015 DROIT PÉNAL [DR. PÉNAL] No. 10, 131 (Fr.).

[154] For the French search regime, see Benelli-de Benazé, *supra* note 153; Chavent-Leclère, *supra* note 153, at 309; Maron & Haas, *supra* note 153, at 131.

[155] Law 2016-731 of June 3, 2016 (Fr.).

[156] A list of the offenses concerned by the provision of the law can be found at articles 706-73 and 706-73-1 C. PR. PÉN.

[157] C. PR. PÉN. art. 706-95-3.

[158] *See id.*

[159] *See id.*

[160] *See id.*

telephone operators located in the national territory.[161] 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 Identity (IMSI) catchers[162] for investigating the most serious offenses.[163] Law enforcement authorities[164] can use IMSI catchers to collect login data enabling the identification of terminal equipment, the subscription number and localization of the terminal,[165] or intercept communications.[166] To be valid, the writ must be in writing and motivated (justified). 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[167] and can only be ordered for a brief period of time.[168]

C. REAL-TIME INTERCEPTION OF DATA

The French regime of real-time interception of data was created in 2011[169] 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 *in flagrante delicto* investigations and preliminary investigations of the

---

[161] *See* Cass. crim., Feb 8, 2011, Bull. crim., No. 15; Cass. crim., Jan. 14, 2014, Bull. crim., No. 8; Lionel Ascensi, *Les Faits Étrangers à la Saisine du Juge d'Instruction et le Trafic de Stupéfiants*, 2014 ACTUALITÉ JURIDIQUE PENAL [A.J. PÉNAL] 248 (Fr.).

[162] An IMSI catcher is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking movement of mobile phone users.

[163] 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.

[164] The liberties and custody judge or the investigating magistrate can order such uses.

[165] *See* C. PR. PÉN. art. 706-95-4(I), 706-95-5(I).

[166] *See id.* art. 706-95-4(II), 706-95-5(II). For the writ to order to intercept communications, *see id.* art. 100-4 to 100-7.

[167] *See id.* art. 706-95-4, 706-95-5.

[168] For the collection of login data the liberties and custody judge's writ is limited to one month and can be renewed once. *See id.* art. 706-95-4. For the investigating magistrate's writ is limited to two months and can be renewed once. *See id.* art. 706-95-5. For the interception of communications, it only can be ordered for forty eight hours and renewed once. *See id.* art. 706-95-4, 706-95-5.

[169] *See* Loi 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure [Law 2011-267 of March 14, 2011 on Guidance and Planning for the Performance of Internal Security], J.O., Mar. 15, 2011, p. 4582.

most serious offenses.[170] 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 one month for the liberties and custody judge and four months for the investigating magistrate).[171] The process must be carried out under the authority and control of the judge who issued the writ.[172] To be considered legal, the interception must target the specific infractions listed in the writ.[173] This provision, however, does not forbid the discovery of other offenses not mentioned in the writ.[174]

D. GEOLOCALIZATION

Since 2011, the French Supreme Court has considered geolocalization legal under article 81 of the French Criminal Procedure Code, when used as a tool to gather evidence during formal investigations. A law was adopted in 2014 to clarify the conditions of the use of geolocalization in the criminal process, and was codified at articles 230-32 to 230-42 of the French Criminal Procedure Code.[175] Under the new regime, the public prosecutor or the investigating magistrate can, in cases of certain offenses, use any technical means to track, in real time on the national territory, the position of a person, object, or vehicle without obtaining the suspect's consent. In 2016, the French Supreme Court specified its interpretation on the use of evidence gathered outside of the national territory. In this case, the suspect was being tracked with geolocalization tools inside and outside of the French borders.[176] The issue presented to the Court was whether the evidence gathered outside of France could be used during the French trial. The Supreme Court ruled that when the geolocalization tracking was not authorized by the foreign authority, it was necessary to determine if the use of the data the tracking was authorized by the foreign authority. Thus, the French Supreme Court emphasized the basic principles of international criminal cooperation, and confirmed that it is necessary to

---

[170] *See* C. PR. PÉN. art. 706-102-1. Dourneau-Josette, *supra* note 142, § 157.
[171] *See* C. PR. PÉN. art. 702-102-1, 702-102-3.
[172] *Id.* at art. 706-102-4.
[173] *See id.*
[174] *See id.*
[175] *See* C. PR. PÉN. art. 230-42, 230-42.
[176] Cass. crim., Feb. 9, 2016, Bull. crim., No. 15-85.070 (Fr.).

obtain the authorization of a foreign authority if using geolocalization to track vehicles in its territory.

E. THE COLLECTION OF EVIDENCE UPON REQUEST

The 2004 reform of criminal procedure[177] expanded the powers of the Officers of the Judicial Police, prosecutors, and investigating magistrates[178] 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, prosecutors, and investigating magistrates with the power to compel telecommunications operators to retain the content of the information viewed by the target user for up to one year.[179] Except when there is "due cause," the operator has to answer the request even if the person is bound by professional secrecy obligations.[180] Failure to promptly answer a request can be sanctioned by a fine of 3,750 euros.[181] 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.[182] Failure to promptly answer such a request can be sanctioned by a fine of 3,750 euros.[183]

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.[184] Thus, the protections provided by article 100 and subsequent articles, and by articles 60 and 77-1 of the French Criminal Procedure Code do not apply.[185]

---

[177] *See* Loi 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité [Law 2004-204 of March 9, 2004 adapting justice to developments in crime], J.O., Mar. 10, 2004, p. 4567.

[178] *See* C. PR. PÉN. art. 60-1, 77-1-1, 99-3. *See also* Marc Schwendener, *Une police aux pouvoirs d'enquête renforcés*, 2004 ACTUALITÉ JURIDIQUE PÉNAL [D.A.J. PÉNAL] 228 (Fr.).

[179] *See* C. PR. PÉN. art. 60-2, 77-1-1, 99-4.

[180] *See id.* art. 60-1, 77-1-1.

[181] *See id.* art. 60-1.

[182] *See id.* art. 56-1 to -3, 77-1-1.

[183] *See id.* art. 56-1 to -3, 60-1.

[184] *See* Cour de cassation [Cass.] [supreme court for judicial matters] crim., June 27, 2001, Bull. crim., No. 01-82578 (Fr.).

[185] *See* Cass. crim., June 27, 2001, Bull. crim., No. 01-82578 (Fr.).

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.[186]

G. THE EXCLUSION OF ILLEGAL SEARCH EVIDENCE

The enforcement of search and seizure rules is a key area of difference between European and US law. While exclusion is the usual response to an illegal search and seizure in the United States, this remedy is rarely used in Europe.[187] 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.[188] 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.[189] Furthermore, the trial judge is free to weigh each piece of evidence before her.

H. THE STATE OF EMERGENCY REGIME

The Paris terrorist attacks on November 2015 constituted unprecedented incidents in French history. The night of the attacks, French President François Hollande declared a nationwide state of

---

[186] Articles 60 and 77-1 of the C. PR. PÉN. regulate the recourse to expertise.

[187] *See* Charles Whitebread & Christopher Slobogin, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS 19 (5th ed. 2008).

[188] *See* Schenk v. Switzerland, 140 Eur. Ct. H.R. (ser. A) at 29-30 (1988); Kostovski v. Netherlands, 166 Eur. Ct. H.R. 4 (ser. A) at 21 (1989); Khan v. United Kingdom, 2000-V Eur. Ct. H.R. 279, 282; Delta v. France, 191 Eur. Ct. H.R. 3 (ser. A) P 36, at 16 (1993).

[189] *See e.g.*, Cass. crim., 11 Feb. 1992, Bull. crim. No. 66 (Fr.); Cass. crim., 15 June 1993, Bull. crim. No. 210 (Fr.); Cass. crim., 27 Jan. 2010, Bull. crim. No. 16 (Fr.). *See also* Jérôme Lasserre Capdeville, "*La preuve fournie par les parties privées : confirmation de la tolérance quant au principe de loyauté*," 2010 ACTUALITÉ JURIDIQUE PÉNAL [D.A.J. PÉNAL] 280; (Fr.); Anne-Sophie Chavent-Leclere, "*Preuve : indifférence du caractère illicite ou déloyal*," 2010 PROCÉDURES, no. 156 (Fr.); Sébastien Fucini, "*Preuve illégale produite par la victime et caractérisation de la tentative de chantage*," Feb. 2015, [D.] (Fr.).

emergency. Under French law,[190] 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."[191]

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.[192] The law regulating the state of emergency provides extensive police powers, conferring extraordinary capacities to the Minister of Interior and the Prefect of Regions.[193] 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.[194] To avoid sanctions, however, as other countries have done before,[195] France filed a formal notice of derogation from the European Convention on Human Rights with the Secretary-General of the Council of Europe.[196]

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.[197] Article 14 of the law on the state of emergency provides that house arrests will cease to have effect at the

---

[190] Loi 2016-1767 Étendant l'application de la loi No. 55-385 du 3 avril 1955 sur l'état d'urgence [Law 2016-1767 extending the application of Act No. 55-385 of April 3, 1955 on the state of emergency], J.O., July 21, 2016.

[191] *Id.*

[192] *Paris Attacks: France state of emergency to be extended – PM Valls*, BBC (November 13, 2016), http://www.bbc.com/news/world-europe-37965708.

[193] The prefect of region is the State's representative in the region.

[194] CE Ass., Mar. 24, 2006, 288460, Rec. Lebon [154] (Fr.) https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000008239595.

[195] *See generally* European Court of Human Rights Factsheet, Terrorism and the European Convention on Human Rights (September 2016), www.echr.coe.int/Documents/FS_Terrorism_ENG.pdf.

[196] *See generally* Council of Europe Full List, Reservations and Declarations for Treaty No.005 – Convention for the Protection of Human Rights and Fundamental Freedoms (January 19, 2017).

[197] 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.

latest time when the state of emergency ends.[198] Thus, some of the house arrests ordered in November 2015 could end in late January 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.[199]

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).[200] 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.[201]

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.[202] 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.

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.[203] The Ministry of the Interior also gains limited control over the press, as he is permitted to take any

---

[198] 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* Senate Report No. 220, Dec. 14, 2016, p. 19 (Fr.) https://www.senat.fr/rap/l16-220/l16-2201.pdf.

[199] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2015-527 QPC, Dec. 22, 2015 (Fr.) http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-527-qpc/version-en-anglais.146959.html.

[200] *See* Senate Report No. 368, Projet de loi prorogeant l'application de la loi No. 55-385 du 3 avril 1955 relative à l'état d'urgence [Draft law extending the application of Act No. 55-385 of April 3, 1955 on the state of emergency], Mr. Michel Mercier, on behalf of the Law Commission (2015-2016) [hereinafter "Mercier Report"].

[201] CE Ass., Mar. 24, 2006, 288460, Rec. Lebon [134] (Fr.) https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000008239595.

[202] Loi 2016-1767 Étendant l'application de la loi No. 55-385 du 3 avril 1955 sur l'état d'urgence [Law 2016-1767 extending the application of Act No. 55-385 of April 3, 1955 on the state of emergency], [J.O.], art. 5V, July 21, 2016. [hereinafter "Law on the state of emergency"].

[203] *Id.* at Art. 6-1VI.

measure to interrupt online communication services inducing or glorifying terrorist acts.[204]

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 (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), 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."[205] 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).[206] Half of these searches were made outside of the hours authorized under the regular procedures.[207] Among these 3,299 administrative searches, only five led to the opening of a judicial procedure for terrorism and twenty led to the opening of a judicial procedure for glorification of terrorism. From July to December 2016, 590 administrative searches were ordered, which led to the opening of sixty-five judicial procedures, including twenty-five related to terrorism.[208]

Article 11 also provides broad powers to the 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.[209]

---

[204] *Id.* at Art. 11, II.
[205] *Id.* at Art. 11.
[206] *See* Mercier Report, *supra* note 200; *See also* Senate Report No. 220, *supra* note 198.
[207] *See* C. PR. PÉN. art. 59.
[208] *See* Senate Report No. 220, *supra* note 198, at p. 18.
[209] *Id. See also* Law on the state of emergency, *supra* note 202, at art. 11.

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.[210] At the end of the search and seizure the administrative authority must bring the matter to the administrative magistrate of expedite[211] whose ruling on the validity of the seizure and its exploitation must be made within 48 hours. The Constitutional Council ruled this article and part of its revision of July 2016 contrary to the constitution.[212] Under both decisions,[213] the 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 July 2016 provision 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.[214] Many French, European, and international institutions, academics, and NGOs have criticized the French state of emergency's implications on civil liberties.[215]

---

[210] *Id.*

[211] The *Juge des référés* is an administrative judge who takes decision on emergency cases and matters.

[212] *See* CC decision No. 2016-536, Feb. 19, 2016, (Fr.) 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; *See also* CC decision No. 2016-600, Dec. 2, 2016, (Fr.) http://www.conseil- constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-600-qpc/version-en-anglais.148512.html.

[213] *See* CC decision No. 2016-536, Feb. 19, 2016, (Fr.) 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; *See also* CC decision No. 2016-600, Dec. 2, 2016, (Fr.) http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-600-qpc/version-en-anglais.148512.html. In the decision of December 2016, the Constitutional council considered that the lack of a deadline, once the state of emergency has ended, upon which the data that was seized shall be destroyed was unconstitutional.

[214] The regime applying for the instruction and the prosecution of terrorism acts is provided by articles 706-16 and subs. of the C. PR. PÉN.

[215] *See, e.g.*, Geoffroy Clavel, *Law Information: the CNTR, railing or masquerade of mass surveillance?*, Huffington Post (May 5, 2015), http://www.huffingtonpost.fr/2015/05/05/loi-renseignement-la-cnctr-garde-fou-ou-cache-sexe-de-la-surve/; *France: Renewal of State of Emergency risks normalizing exceptional measures*, Amnesty International (Dec. 16, 2016),

IV. THE CURRENT MUTUAL LEGAL ASSISTANCE REGIME OF FRANCE AND THE UNITED STATES

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.[216] 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 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.[217] 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."[218] 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.[219] Such a request is needed for content even in the simple original example,

---

https://www.amnesty.org/en/latest/news/2016/12/france-renewal-of-state-of-emergency-risks-normalizing-exceptional-measures/; Andrew Chung, *French state of emergency facing court challenges*, Reuters (Dec. 18, 2015), http://www.reuters.com/article/us-france-shooting-complaints-idUSKBN0U10VI20151218.

[216] Mutual Legal Assistance Treaty, Fr.-U.S., Dec. 10, 1998, 1 U.S.C. 113, http://www.state.gov/documents/organization/121413.pdf.

[217] *Id.* (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.").

[218] *See id.* at 4.

[219] *See, e.g.*, Andrew K. Woods, *Data Beyond Borders Mutual Legal Assistance Treaties in the Internet Age*, GLOBAL NETWORK INITIATIVE, 15 (Jan. 2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf; *Legal Process – Google Transparency Report*, GOOGLE.COM, https://www.google.com/transparencyreport/userdatarequests/legalprocess (last visited Nov. 9, 2016); Greg Nojeim, *MLAT Reform: A Straw Man Proposal*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Sep. 3, 2015), https://cdt.org/insight/mlat-reform-a-straw-man-proposal/ ("[ECPA] as interpreted by both the DOJ and major US providers, prohibits companies from disclosing communications content to foreign governments absent a warrant issued by a US judge based on a finding of probable cause.").

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.[220] In that case, the Second Circuit held that the SCA did not apply "extraterritorially." As such, a search 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.[221]

As discussed previously, there is a multi-step process when France or another country submits an MLAT request to the United States, with the total process on average taking roughly ten months to complete.[222] 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.[223] The OIA, US Attorney's office, and magistrate judge each review to ensure that enough evidence exists for the type of information sought, probable cause for a warrant for content, and for a 2703(d) order a showing of a reasonable and articulable suspicion for much non-content data.[224] 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 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.[225]

Requests from the United States 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 internationa*le."[226] 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

---

[220] *See In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, Microsoft Co. v. US*, 829 F.3d 197, 221 (2nd Cir. 2016).

[221] *See* Swire & Hemmings, *supra* note 3 (For discussion of procedures for an MLAT request compared to an alternative procedure, a letter rogatory).

[222] *See id.* at 38–39.

[223] Swire & Hemmings, *supra* note 3. *See also* Vergnolle, *supra* note 5.

[224] *See supra*, Part III (standards of proof under ECPA).

[225] *See* Swire & Hemmings, *supra* note 3 (For a more detailed explanation of this process).

[226] The *bureau d'entraide pénale internationa*le is part of the French Ministry of Justice.

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.[227] In the United States, as previously discussed, ECPA permits a company to voluntarily disclose metadata to a non-US governmental entity.[228] In practice, companies in the United States disclose BSI subject to their internal policies, which have become increasingly strict in recent years.[229] For instance, if the request appears to be an attempt to prosecute political dissent, blasphemy, or other speech 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.[230]

V. POSSIBLE MUTUAL LEGAL ASSISTANCE REFORMS FOR FRANCE AND THE UNITED STATES

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 because the two countries are longstanding allies, which supports reform, but have criminal justice systems that differ in multiple respects, which creates an obstacle to

---

[227] *See* 18 U.S.C. § 2702 (2016); *Rules on obtaining subscriber information from the Cybercrime Convention Committee*, COM (2014) (November 21, 2014) (draft only).

[228] 18 U.S.C. § 2702(c)(6); 18 U.S.C. 2711(4) (2016).

[229] *See* Greg Nojeim, *MLAT Reform Proposal: Protecting Metadata*, Lawfare (Dec. 10, 2015), https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata (For discussion of companies' discretionary policies of when to respond to requests from non-US governments). *See also* Nate Cardozo et al., *The Electronic Frontier Foundation's Sixth Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data* (May 2016), https://www.eff.org/files/2016/05/04/who-has-your-back-2016.pdf (In recent years, a growing number of companies release transparency reports, providing statistics and information about their response to government requests for customer data).

[230] *See* CODE DE PROCEDURE PENALE [C. PR. PEN.] [CODE OF CRIMINAL PROCEDURE] arts. 60-2, 77-1-2 & 99-4 (Fr.). *See also* Part IV E, *infra* (discussing collection of evidence upon request).

reform. The Part then uses a choice-of-law approach to analyze several issues concerning the scope of possible MLA reform.

A. THE TECHNICAL, LEGAL, AND POLITICAL CONTEXT FOR REFORM

The context for considering possible reform in France and the United States 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.

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 US Revolutionary War through both World Wars, and today in NATO.[231] France is a Member State of the EU, which has innumerable ties with the United States, including recent agreements on protecting personal data such as the Umbrella Agreement and Privacy Shield.[232] 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

---

[231] Manuel Lafont Rapnouil & Julianne Smith, *NATO and France*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Mar. 2, 2009), https://www.csis.org/analysis/nato-and-france.

[232] The name "Umbrella Agreement" is used to refer to the Agreement between the European Union and the United States of America on the Protection of Personal Data When Transferred and Processed for the Purpose of Preventing, Investigating, Detecting or Prosecuting Criminal Offences. *EU—US Umbrella Agreement*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/intl/data-agreement/ (last visited Feb. 4, 2017). *See also The EU—U.S. Privacy Shield*, European Commission (Nov. 24, 2016), http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm (discussing the Privacy Shield).

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.[233] Instead of the US adversarial system, where criminal defendants can exclude from trial evidence that is illegally obtained, in France any information "necessary to establish the truth" is generally available to assist investigating authorities.[234] 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.[235] For purposes of this article, the relationship between France and the United States is a meaningful case study of the promise and challenges of reforming ways to share criminal justice evidence. The alliance between France and the United States and the 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.

---

[233] *See* Hodgson, *supra* note 123.

[234] 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.*, Mapp v. Ohio, 367 U.S. 643 (1961); 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 generally* C. PR. PÉN. arts. 81, 82 & 97. *See also* Cass. crim., July 8, 2015, Bull. crim., No. 450 (Fr.).

[235] Swire & Kennedy-Mayo, *supra* note 4.

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 United States generally have to comply with the requirements of ECPA, the SCA, and the Fourth Amendment.[236] As former Judge and US Secretary of Homeland Security Michael Chertoff has written, MLA reform raises choice of law issues. He states,

> 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.[237]

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.[238] 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.[239]

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

---

[236] The *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. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 829 F.3d 197 (2d Cir. 2016).

[237] Michael Chertoff, *Statement for the Record in House Judiciary Committee Hearing on "International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests*," (Feb. 25 2016), https://judiciary.house.gov/wp-content/uploads/2016/02/michael-chertoff-testimony.pdf.

[238] *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6(2)(a) (including "the needs to the . . . international systems" as a factor in choice-of-law analysis).

[239] 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, *WhatsApp is Briefly Shut Down in Brazil for a Third Time*, N.Y. TIMES (July 19, 2016), 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, is 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* Swire & Kennedy-Mayo, *supra* note 4.

process, and developing online tools to improve communications between the countries.[240] 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 ECPA applies, to enable France or some other country to go directly to the company for content requests, without requiring a lengthy MLA process.[241]

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 and 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 as there is 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.

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

---

[240] Swire & Hemmings, *supra* note 3 at 4.

[241] 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. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 829 F.3d 197 (2d Cir. 2016).

apply to communications of US persons.[242] 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 *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.[243] 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.[244] 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 strong compared to the US interest, there is greater reason to support amendments to 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.[245] An MLA reform proposal thus should police the realm of

---

[242] *See* Ellen Nakashima & Andrea Peterson, *The British Want to Come to America – with Wiretap Orders and Search Warrants*, WASHINGTON POST (Feb. 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america—with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

[243] *Microsoft Co. v. US*, 829 F.3d at 230–31.

[244] 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. *See Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisémitisme*, 433 F.3d 1199 (9th Cir. 2006).

[245] How to handle geographic uncertainty of an Internet actor has become controversial in proposed changes to Fed. R. Crim. Proc. 41. *See* Google Inc., *Google Inc. Comments on the Proposed Amendment to Federal Rule of Criminal Procedure 41* (Feb. 13, 2015) *available at* https://assets.documentcloud.org/documents/1670588/13feb2015-google-inc-comments-on-the-proposed.pdf; Rainey Reitman, *With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government*, ELECTRONIC FRONTIER FOUNDATION (Apr. 30, 2016),

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.[246] This proposal has virtues, notably that a weakening of ECPA for content would be accompanied by strengthening ECPA for some metadata. On the other hand, expansion to traffic data creates a disincentive for countries to enter the new system, as 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.[247] 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.[248]

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,

---

https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government.

[246] *See* Nojeim, *supra* note 229.

[247] *See* Greg Nojeim, *MLAT Reform: A Straw Man Proposal*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Sep. 3, 2015), https://cdt.org/insight/mlat-reform-a-straw-man-proposal/; Eliza Sweren-Becker, *DOJ's Data-Sharing Proposal Threatens Privacy of Americans and Citizens Around the World*, AMERICAN CIVIL LIBERTIES UNION (July 18, 2016), https://www.aclu.org/blog/free-future/dojs-data-sharing-proposal-threatens-privacy-americans-and-citizens-around-world.

[248] 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. Swire & Hemmings, *supra* note 3.

hopefully with improved and faster procedures that would apply to all MLA requests.

VI. 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 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.[249] 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."[250] Failure to find common

---

[249] *Id. See also* Swire & Kennedy-Mayo, *supra* note 4.

[250] THE WHITE HOUSE, INT'L STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 3 (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. *See also Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (Dec 12, 2013) ("Review Group Report"), archived at http://perma.cc/FG3M-QE8K.

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." [251] It is better to overcome the obstacles to MLA reform.

[251] *Id.*