HEINONLINE

Citation:
Susan Freiwald; Sylvain Metille, Reforming the Surveillance Law: the Swiss Model, 28 Berkeley Tech. L.J. 1261 (2013)
Provided by:
Seton Hall Law Rodino Library

Content downloaded/printed from *HeinOnline*

Thu Mar 28 14:25:04 2019

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at https://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

-- To obtain permission to use this article beyond the scope of your HeinOnline license, please use:

Copyright Information

Use QR Code reader to send PDF to your smartphone or tablet device

REFORMING SURVEILLANCE LAW: THE SWISS MODEL

Susan Freiwald[†] *& Sylvain Métille*[††]

ABSTRACT

As implemented over the past twenty-seven years, the Electronic Communications Privacy Act ("ECPA"), which regulates electronic surveillance by law enforcement agents, has become incomplete, confusing, and ineffective. In contrast, a new Swiss law, CrimPC, regulates law enforcement surveillance in a more comprehensive, uniform, and effective manner. This Article compares the two approaches and argues that recent proposals to reform ECPA in a piecemeal fashion will not suffice. Instead, Swiss CrimPC presents a model for more fundamental reform of U.S. law.

This Article is the first to analyze the Swiss law with international eyes and demonstrate its advantages over the U.S. approach. The comparison sheds light on the inadequacy of U.S. surveillance law, including its recurrent failure to require substantial judicial review, notify targets of surveillance, and provide meaningful remedies to victims of unlawful practices. Notably, through judicial oversight and the requirement that surveillance practices be first approved by the legislature, the Swiss significantly restrict several law enforcement methods that U.S. law leaves to the discretion of the police. This Article explains the differences in approach as stemming from the greater influence of international human rights law in Switzerland and the Swiss people's willingness to engage in a wholesale revision of their procedural law.

In the United States, the courts and Congress have struggled to establish appropriate surveillance rules, as evidenced by recent controversial judgments in the courts and congressional hearings on ECPA reform. In the wake of recent disclosures about massive NSA surveillance programs that have relied on both foreign and domestic surveillance, U.S. citizens have grown increasingly concerned about the excessive use of new surveillance technologies to gather information about their private communications and daily activities. This Article analyzes the Swiss approach to domestic electronic surveillance, which, if adopted here, would significantly improve our laws.

© 2013 Susan Freiwald & Sylvain Métille.

† Professor of Law, University of San Francisco School of Law. I thank research librarian John Shafer and research assistants Sydney Archibald, Amy Leifur Halby, Everett Monroe, and David Reichbach for their valuable help. Josh Davis, Jim Dempsey and Judge Stephen Wm. Smith also contributed significantly to my thinking about this paper.

†† Doctor of Law and attorney at the Swiss bar, Lecturer, University of Lausanne, Faculty of Law and Criminal Justice and University of Fribourg International Institute of Management in Technology, Switzerland. This Article was mainly written during my time as a visiting scholar at the Berkeley Center for Law and Technology, University of California, Berkeley, School of Law. I thank research librarian Jean Perrenoud for his valuable help.

We appreciate the comments made by participants at the Privacy Law Scholars' Conference in June 2012, where we presented a draft of this paper: Bryan Cunningham, Danielle Citron, John Grant, Orin Kerr, Greg Nojeim, and Brian Pascal. We particularly thank Stephen Henderson, who moderated the panel devoted to our paper and furnished excellent guidance.

TABLE OF CONTENTS

I. INTRODUCTION 1264

II. THE SWISS LEGAL FRAMEWORK FOR SURVEILLANCE 1269

A. SWISS LEGAL STRUCTURE 1269
B. RIGHTS TO PRIVACY UNDER THE SWISS CONSTITUTION 1270
C. RIGHTS TO PRIVACY UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS 1272

III. THE U.S. FRAMEWORK FOR SURVEILLANCE—COMPARED 1277

A. U.S. LEGAL STRUCTURE 1277
B. RIGHTS TO PRIVACY UNDER THE U.S. CONSTITUTION 1278
C. RIGHTS TO PRIVACY UNDER INTERNATIONAL LAW 1284

IV. SWITZERLAND: APPLICABLE LAW ENFORCEMENT SURVEILLANCE ACTS 1285

A. THE LAWS PRIOR TO THE SWISS CRIMINAL PROCEDURE CODE ("CRIMPC") 1285
B. CRIMPC 1287
C. OTHER ACTS PERTINENT TO LAW ENFORCEMENT SURVEILLANCE 1289

V. UNITED STATES: APPLICABLE SURVEILLANCE ACTS 1290

A. THE WIRETAP ACT 1290
B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") 1291
C. THE USA PATRIOT ACT AND OTHER AMENDMENTS 1292

VI. COMMON ELEMENTS IN SURVEILLANCE PROCEDURES 1294

A. LEVELS OF OVERSIGHT 1294
B. CONDITIONS 1296
1. *Procedural Hurdles* 1296
2. *Predicate Offenses* 1297
3. *Other Limits* 1298
C. NOTICE 1299
D. CONSEQUENCES OF ILLEGAL SURVEILLANCE 1301
E. REPORTING 1303

VII. SURVEILLANCE REGULATION COMPARED 1303

A. INTRODUCTION 1303
B. MONITORING OF POST AND TELECOMMUNICATIONS 1304

1. *In Switzerland* 1304
2. *In the United States* 1306
a) Several Distinctions 1306
b) Interception of Postal Mail Contents 1306
c) Interception of Wire Communications Content 1307
d) Interception of Electronic Communications Content 1308
e) Acquisition of Stored Electronic Communications Content 1310
C. ACQUISITION OF USER IDENTIFICATION DATA 1314
1. *In Switzerland* 1314
2. *In the United States* 1315
a) Several Distinctions 1315
b) Collection of Postal Mail Attributes 1316
c) Collection of Electronic Communication Attributes in Real Time 1316
d) Collection of Electronic Communication Attributes from Electronic Storage 1318
e) Cell Site Location Data Acquisition 1319
D. TECHNICAL SURVEILLANCE EQUIPMENT 1320
1. *In Switzerland* 1320
2. *In the United States* 1321
E. SURVEILLANCE OF CONTACTS WITH A BANK 1322
1. *In Switzerland* 1322
2. *In the United States* 1324
F. UNDERCOVER OPERATIONS 1324
1. *In Switzerland* 1324
2. *In the United States* 1325
G. PHYSICAL OBSERVATION 1325
1. *In Switzerland* 1325
2. *In the United States* 1327
H. NEW TECHNIQUES 1328
1. *In Switzerland* 1328
2. *In the United States* 1329

VIII. CONCLUSION 1330

I. INTRODUCTION

Calls for reform of American laws governing electronic surveillance have multiplied as members of Congress,[1] the judiciary,[2] and the public[3] have recognized that our outdated laws do not adequately protect citizens from law enforcement's abuse of modern surveillance technologies.[4] Congress passed the Electronic Communications Privacy Act ("ECPA")[5] in 1986 to bring government surveillance into the electronic age but has not meaningfully updated it since the advent of the World Wide Web.[6] Bills currently pending in Congress would make small, though significant, changes to ECPA. For example, they would strengthen the protection of location data[7] and stored email.[8] None of the bills proposed, however, would engage in a wholesale overhaul of the electronic surveillance legal regime.

---

1. *See Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 62 (2011) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary) (describing current electronic surveillance law as out of date and insufficient and in need of legislative update).

2. *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the S. Comm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 76–77, 85–91 (2010) (statement of Stephen Wm. Smith, U.S. Mag. J.) (explaining, for example, that because citizens do not receive notice of surveillance, they do not appeal issuance of warrants and thus the judiciary has insufficient opportunities to interpret and clarify vague aspects of the law); United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

3. *See, e.g.*, Editorial, *The End of Privacy?*, N.Y. TIMES, July 14, 2012, at SR10 ("Clearly, federal laws need to be revamped and brought into line with newer forms of surveillance."); *About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Mar. 10, 2013).

4. *See It's Time for a Privacy Upgrade*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Oct. 21, 2011), www.cdt.org/blogs/2010ecpas-25th-anniversary-time-change; Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1551 (2010) ("I agree with essentially everybody who has ever written about ECPA that the law is sorely in need of reform.").

5. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). Commentators tend to refer to the Act by its acronym, "ECPA," pronounced "eck-pah," and to drop the definite article when doing so.

6. *See infra* Part V (discussing the evolution of surveillance law in the United States).

7. *See* Online Communications and Geolocation Protection Act, H.R. 93, 113th Cong. (2013) (requiring a warrant for access to both stored email and location data).

8. *See* Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013) (requiring a warrant for access to stored email); Press Release, Patrick Leahy, U.S. Senator for Vt., Leahy Marks 25th Anniversary of ECPA, Announces Plan to Mark Up Reform Bill (Oct. 20, 2011), *available at* www.leahy.senate.gov/press/leahy-marks-25th-anniversary-of-ecpa-announces-plan-to-mark-up-reform-bill.

That overhaul is exactly what Switzerland accomplished when it unified its procedural laws. Switzerland took the opportunity to entirely update its surveillance laws to cover new technologies as well as traditional ones. In January 2011, the Swiss enacted a brand new statute, the Swiss Criminal Procedure Code ("CrimPC"), which covers all provisions for law enforcement surveillance under Swiss law.[9] Extending federal authority to enact CrimPC was complicated because it required an amendment to the Federal Constitution of the Swiss Confederation ("Swiss Constitution" or "Federal Constitution").[10] A series of decisions from the European Court of Human Rights, however, had set forth detailed requirements for law enforcement surveillance by signatories to the European Convention on Human Rights,[11] and the Swiss enacted CrimPC to comply with those decisions.[12]

With surveillance law reform on the agenda in the United States, the Swiss experience offers a unique opportunity to look at a law enforcement surveillance statute started from scratch. Rather than making piecemeal amendments to an entrenched set of rules, as pending bills in the United States currently propose, Swiss legislators started over, writing on a blank slate. Analyzing the resulting statute affords an unusual opportunity to consider what the United States might accomplish if its legislators were also willing to start entirely anew in the field of law enforcement surveillance. A sustained look at CrimPC can open U.S. eyes to new possibilities for surveillance law that reformers have not yet seriously entertained.

A comparison of the two countries' approaches also highlights systematic differences that strongly impact the balance of law enforcement powers and

---

9. CODE DE PROCÉDURE PÉNALE [CRIMPC] [Code of Criminal Procedure] Oct. 5, 2007, RS 312 (Switz.).

10. Before the amendment, the Confederation did not have the power to legislate over criminal law procedure or civil law procedure. The Federal Constitution of the Swiss Federation describes the process by which the people can amend the Swiss Constitution. A partial revision of the Constitution can be decreed by the Federal Assembly or any 100,000 persons eligible to vote. CONSTITUTION FÉDÉRALE [CST] [CONSTITUTION] Apr. 18, 1999, RO 101, art. 139 (Switz.). A revision needs to be adopted only by a majority of the Cantons and a majority of the eligible voters. CST art. 195. It is much easier to amend the Swiss Constitution than to amend the U.S. Constitution. *See generally*, SANFORD LEVINSON, OUR UNDEMOCRATIC CONSTITUTION: WHERE THE CONSTITUTION GOES WRONG (AND HOW WE THE PEOPLE CAN CORRECT IT) 160 (2006) ("no other country . . . makes it so difficult to amend its constitution").

11. Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, E.T.S. 5 [hereinafter ECHR], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

12. Switzerland is a member state of the Council of Europe but not of the European Union. *See infra* Section II.C.

privacy rights in each country. For example, Swiss law precludes the use of surveillance techniques not authorized and regulated by CrimPC; if the law does not explicitly permit and regulate a surveillance technique, such as using a brand new technology to gather data, law enforcement may not use it.[13] In the United States, by contrast, law enforcement considers itself free to use techniques that U.S. law does not yet regulate.[14] Consequently, as new surveillance methods come online, U.S. agents freely use them unless and until Congress tells them not to through regulation,[15] but Swiss agents may not use them unless and until their legislature authorizes them to do so. For example, before CrimPC, law enforcement agents could use GPS surveillance only in those Cantons that authorized it by statute. In the United States, the FBI felt free to use GPS devices to conduct surveillance without warrants, and scrambled to remove them only after the Supreme Court ruled that such surveillance was a search.[16]

This Article describes the passage of CrimPC and its key surveillance provisions, which govern surveillance of mail and telecommunications, the acquisition of user identification data, the use of technical surveillance devices, surveillance of contacts with a bank, the use of undercover agents, and surveillance through physical observation of people and places accessible to the general public.[17] After briefly explaining the structure and history of U.S. surveillance law, this Article contrasts those CrimPC provisions with existing U.S. law.

Before beginning a detailed comparison of the two countries' approaches to law enforcement surveillance, it is important to explain that the two countries, though radically different in size, are worthy subjects of comparison. Switzerland has always been a relatively independent country

13. *See infra* Section VII.H.1.

14. *Compare* Orin Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 645–47 (2003) (arguing that prior to their inclusion in a 2001 law, surveillance devices that recorded electronic addressing information were entirely unregulated and hence permitted without restriction), *with* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 72–73 (2004) (describing how courts have sometimes viewed practices not subject to statutory regulation as nonetheless subject to Fourth Amendment restrictions). The views of Professor Kerr, a principle author of an early version of the federal prosecutor's training manual, have generally prevailed. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS vii (3d ed. 2009), *available at* www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

15. State legislators may also constrain law enforcement use of new technologies, as may courts through application of constitutional constraints.

16. *See infra* note 83.

17. *See infra* Part VII.

that currently operates outside the strictures of the European Union,[18] although it shares many cultural values with other European countries.[19] As a Western European country, Switzerland is also a close cultural relative of the United States. While it has a lower homicide rate than the United States, it has a comparable number of burglaries and thefts per capita, a comparable number of professional judges and magistrates per capita, and a comparable number of police officers per capita.[20] Other comparative law articles have considered the United States and Germany, a country with geographic and language ties to Switzerland, but which is a member of the European Union and therefore less independent than Switzerland.[21]

Through a detailed, section-by-section comparison of each major surveillance provision of CrimPC to its U.S. counterpart, clear patterns

---

18. The European Council, sometimes called the Council of the European Union, is a body of the European Union; it consists of state or executive leaders from the member states who meet for the purpose of planning E.U. policy. *See* COUNCIL OF THE EUROPEAN UNION, www.consilium.europa.eu (last visited Mar. 13, 2013). Twenty-eight States are members of the European Union, but Switzerland is not among them. The European Council is sometimes confused with the Council of Europe, of which Switzerland is a member. *See infra* note 46.

19. The decisions of the European Court of Human Rights have significantly influenced Swiss law. *See infra* Section II.C.

20. *See* U.N. Office on Drugs & Crime, Theft at the National Level, Number of Police-Recorded Offences, www.unodc.org/documents/data-and-analysis/statistics/crime/CTS12_Theft.xls (last visited Mar. 14, 2013) (reporting theft rate per 100,000 population for the year 2010 as 1993.0 in the United States and 1560.3 in Switzerland); *Statistics on Burglary*, United Nations Office on Drugs and Crime, Burglary Breaking and Entering at the National Level: Number of Price-Recorded Offenses, www.unodc.org/documents/data-and-analysis/statistics/crime/CTS12_Burglary.xls (last visited Mar. 14, 2013) (reporting burglary rate per 100,000 population for the year 2010 as 695.9 in the United States and 812.1 in Switzerland); U.N. Office on Drugs & Crime, Statistics on Criminal Justice Resources: Total Police Personnel at the National Level, www.unodc.org/documents/data-and-analysis/statistics/crime/CTS12_Criminal_justice_resources.xls (last visited Mar. 14, 2013) (reporting police force per 100,000 population in the year 2008 as 232.3 in the United States and 215.6 in Switzerland); European Institute for Crime Prevention and Control, *International Statistics on Crime and Justice*, at 139, HEUNI Publication Series No. 64 (2010) (reporting the rate of professional judges per 100,000 population as 10.8 in the United States in the year 2001 and 10.6 in Switzerland in the year 2002). *But see* U.N. Office on Drugs & Crime, Intentional Homicide: Count and Rate per 100,000 Population, www.unodc.org/documents/data-and-analysis/statistics/crime/Homicide_statistics2012.xls (last visited Mar. 14, 2013) (reporting homicide rate per 100,000 population for the year 2010 as 4.2 in the United States and 0.7 in Switzerland.).

21. *See, e.g.*, Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751 (2002); Paul M. Schwartz, *Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study*, 72 GEO. WASH. L. REV. 1244 (2003); Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493 (2007).

emerge, which illustrate the superior attributes of the Swiss approach. CrimPC provides greater coverage, less complexity, and more comprehensive protections for the Swiss people. First, CrimPC regulates more surveillance techniques than ECPA, the closest U.S. analog. For example, CrimPC restricts the use of undercover agents in law enforcement, but neither ECPA nor any other U.S. statute or constitutional provision regulates undercover operatives.[22] Also, as mentioned above, Swiss law precludes the use of unregulated techniques, whereas, subject to the Fourth Amendment, U.S. law enforcement agents make unlimited use of techniques not covered by ECPA.[23] Second, CrimPC is fundamentally easier to understand, which will surely make it easier for judges to apply. While commentators have criticized the complexity of ECPA rules that govern electronic communications surveillance, CrimPC's nearly uniform and technology-neutral approach contrasts strikingly with ECPA's thicket of categories and distinctions.[24] Finally, for those techniques that are covered by both CrimPC and ECPA, CrimPC almost always provides substantially greater protections against law enforcement abuse. In particular, CrimPC offers significantly greater judicial oversight, including by providing notice to targets that they have been the subjects of surveillance and real remedies for those who have been surveilled in violation of the law.

U.S. reformers should keep the Swiss approach in mind as they turn to ECPA reform in the coming months and years. In particular, Switzerland's requirement that statutory law must first authorize new surveillance techniques with appropriate restrictions before law enforcement may use them should encourage U.S. legislators to act quickly when faced with reports that U.S. agents are using new surveillance techniques to violate privacy. In addition, legislators should take critiques of the U.S. system more seriously, especially those founded on claims that current laws provide inadequate due process and call for better notice to targets, adequate remedies for improper investigations, and meaningful judicial oversight of

22. The Supreme Court has held that the Fourth Amendment does not apply to undercover surveillance. *See infra* Section VII.F.2. If undercover agents use wiretaps or other techniques regulated by ECPA, then those techniques are regulated, but the use of agents per se is not. *See id.*

23. *See infra* Section VII.B. Some states provide greater restrictions than ECPA for agents acting under the jurisdictions of those state statutes. *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006) (providing a comprehensive overview of state statutes that provide greater protection to targets of some surveillance practices than federal law).

24. *See infra* Sections VII.B and VII.C.

surveillance practices. Finally, legislators should seriously consider starting over with a regime that scraps ECPA's outdated and confusing categories and starts anew with a scheme that, like CrimPC, is clear, comprehensive, and, at least on its face, adequately protective of privacy rights.

II. THE SWISS LEGAL FRAMEWORK FOR SURVEILLANCE

A. SWISS LEGAL STRUCTURE

As in the United States, the Swiss legal system operates at both a federal and state level, with the states in Switzerland known as "Cantons."[25] The Swiss Confederation (also known as "Switzerland" or "Confederatio Helvetica") has 7.9 million inhabitants.[26] Each Canton may exercise the power over its own institutions given by the terms of the Federal Constitution.[27] Until the Federal Constitution was amended to provide federal power over all aspects of criminal and civil procedure, criminal law procedures, including surveillance for criminal law enforcement, were solely within the legislative competence of the Cantons.[28]

As in most European countries, the Constitution limits public activities.[29] The constitutional principle of legality requires that all activities of the State, including surveillance by state authorities, shall be based on and limited by enacted law.[30] CrimPC provides the specific legislative enactment required for law enforcement surveillance. Because everyone must abide by public regulations, whether or not they have individually consented to them, rights

25. CST art. 1.

26. 5.1 million people are eligible to vote in Switzerland. Arrêté du Conseil fédéral, constatant le résultat de la votation populaire du 23 septembre 2012 [Decree ascertaining the result of the vote of September 23, 2012] FF 1053, 1055 (2013), www.bfs.admin.ch/bfs/portal/fr/index/themen/01/02/blank/key/bevoelkerungsstand.html.

27. Jean-François Aubert & Etienne Grisel, *The Swiss Federal Constitution*, *in* INTRODUCTION TO SWISS LAW 15–25 (François Dessemontet & Tuğrul Ansay eds. 2004); THOMAS FLEINER, ALEXANDER MISIC & NICOLE TÖPPERWIEN, SWISS CONSTITUTIONAL LAW 122 (2005).

28. The Federal Constitution provides that the Cantons shall exercise all rights that are not vested in the Confederation. CST art. 3; JEAN-FRANÇOIS AUBERT & PASCAL MAHON, PETIT COMMENTAIRE DE LA CONSTITUTION FÉDÉRALE DE LA CONFÉDÉRATION SUISSE DU 18 AVRIL 1999 [SHORT COMMENTARY ON THE SWISS CONSTITUTION OF APRIL 18, 1999] 30–31 (2003); FLEINER, MISIC & TÖPPERWIEN, *supra* note 27, at 122–26; RENÉ A. RHINOW & MARKUS SCHEFER, SCHWEIZERISCHES VERFASSUNGSRECHT [SWISS CONSTITUTIONAL LAW] 147 (2009).

29. CST art. 5.

30. *See* CST art. 5; AUBERT & MAHON, *supra* note 28, at 39–50; Thomas Fleiner, *Cantonal and Federal Administrative Law of Switzerland*, *in* INTRODUCTION TO SWISS LAW, *supra* note 27, at 35–37.

and obligations can be imposed only if they arise from a statute, such as CrimPC.[31]

Written law, enacted by the legislature, is by far the most important source of law in Switzerland.[32] Different forms of written law have different hierarchical values that operate similarly to the hierarchical values of American laws. Constitutional rules prevail over ordinary acts, federal law takes precedence over cantonal law, and legislative statutes take priority over regulations promulgated by the Federal Council[33] or administrative authorities.[34] Both the Swiss Constitution and the European Convention on Human Rights ("ECHR") provide significant privacy rights that the legislature had to respect when enacting CrimPC.[35] The next two Sections discuss those privacy rights.

B. RIGHTS TO PRIVACY UNDER THE SWISS CONSTITUTION

At the constitutional level, the right to privacy derives primarily from Article 13 of the Swiss Constitution, which states that "everyone has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications," and "everyone has the right to be protected against the misuse of their personal data."[36] The first sentence protects privacy in general and emphasizes the protection of the person and of his or her living quarters and workspace and his or her communications with others. The second sentence establishes the traditional protection of personal data, or what U.S. commentators refer to as "information privacy."[37] This informational self-determination right gives every person the power to decide whether and for which purpose personal information shall be processed.[38] As a fundamental right, the right to privacy limits the power of the State but cannot be invoked against other private persons.

---

31. A statute's legitimacy derives from the consent of the people expressed through the democratic adoption of the law.

32. In fact, the Swiss do not have judge-made common law as we do in the United States.

33. In Switzerland, the term "government" describes the executive branch, which is the Federal Council, composed of seven members. Each member is the head of one of seven departments that together form the federal administration. CST arts. 175, 178.

34. ANDREAS AUER, GIORGIO MALINVERNI & MICHEL HOTTELIER, DROIT CONSTITUTIONNEL SUISSE I [SWISS CONSTITUTIONAL LAW] 491–517 (2d ed. 2006).

35. Courts must also consider these rights when evaluating the application of a surveillance law to a particular person.

36. CST art. 13.

37. *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (4th ed. 2011) (assembling cases and readings for law school courses on the protection of personal data).

38. Tribunal Fédéral [TF] [Federal Supreme Court] July 9, 2003, 129 ARRÊTS DU TRIBUNAL FÉDÉRAL SUISSE [ATF] I 232, 245–45; TF, May 29, 2002, 128 ATF II 259, 268.

The Swiss Supreme Court has refused to define the right to privacy, but it has made clear that the right covers every piece of personal data that is not publicly accessible.[39] Europeans generally view privacy as relating to the dignity and autonomy of the person.[40] Article 7 of the Swiss Constitution provides that human dignity must be respected and protected.[41] The right to personal freedom under Article 10 also protects human dignity.[42]

Although the right to privacy is considered a fundamental right, it is not absolute and can be subject to limitation. According to Article 36 of the Swiss Constitution, a restriction on the right of privacy, such as a statute that permits law enforcement surveillance, must satisfy four conditions: (1) it must have a legal basis, (2) it must be justified in the public interest or for the protection of the fundamental rights of others, (3) it must meet the standard of proportionality of means and ends,[43] and (4) it may not violate the essence of the fundamental right at stake.[44] When possible, courts interpret laws consistently with the Constitution.[45]

---

39. Some examples of personal data are: identification data, TF, Apr. 23, 1998, 124 ATF I 85, 87; medical data, TF, June 19, 1996, 122 ATF I 153, 155; data about sexual identity and orientation, TF, Mar. 3, 1993, 119 ATF II 264, 268; data about relationships with other human beings; and files of judicial proceedings, TF, Mar. 17, 1993, 199 ATF Ia 99, 101.

40. For further comparisons of American and European notions of privacy, see Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIF. L. REV. 1925 (2010); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004); Francesca E. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609 (2007).

41. AUBERT & MAHON, *supra* note 28, at 67; JÖRG PAUL MÜLLER & MARKUS SCHEFER, GRUNDRECHTE IN DER SCHWEIZ IM RAHMEN DER BUNDESVERFASSUNG, DER EMRK UND DER UNO-PAKTE [BASIC RIGHTS IN SWITZERLAND ACCORDING TO THE FEDERAL CONSTITUTION, THE ECHR AND THE U.N. COVENANTS] 1–4 (2008).

42. CST art. 10 ("Everyone has the right to life. The death penalty is prohibited. Everyone has the right to personal liberty and in particular to physical and mental integrity and to freedom of movement. Torture and any other form of cruel, inhuman or degrading treatment or punishment are prohibited.").

43. Article 5 of the Swiss Constitution also mentions the principle of proportionality, which governs all activity of the State. CST art. 5.

44. According to the Swiss Constitution, the essence of fundamental rights is sacrosanct. CST art. 36; *see also* ANDREAS AUER, GIORGIO MALINVERNI & MICHEL HOTTELIER, DROIT CONSTITUTIONNEL SUISSE II 79–119 (2d ed. 2006); ULRICH HÄFELIN, WALTER HALLER & HELEN KELLER, SCHWEIZERISCHES BUNDESSTAATSRECHT 90–101 (7th rev. ed. 2008); WALTER HALLER, THE SWISS CONSTITUTION IN A COMPARATIVE CONTEXT 157–62 (2009).

45. Courts in the United States use the same interpretative approach, which is known as constitutional avoidance. *See, e.g.*, Edward J. DeBartolo Corp. v. Fla. Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("[E]very reasonable construction must

In summary, because CrimPC authorizes the restriction of fundamental rights during an investigation, the Swiss Constitution required that it be enacted as a federal law, that it be justified in the public interest to protect other fundamental rights, and that it respect the principle of proportionality and the essence of the right to privacy. These constraints no doubt contributed to CrimPC's comprehensive protections, which distinguish it from its significantly less protective U.S. counterparts.

C. RIGHTS TO PRIVACY UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS

As a member of the Council of Europe,[46] Switzerland enacted the European Convention on Human Rights ("ECHR") in 1974, at which time it became directly binding in the Swiss legal system.[47] ECHR is an international treaty under which the member States of the Council of Europe promise to secure fundamental civil and political rights, both to their own citizens and to everyone within their jurisdictions. The European Court of Human Rights ("ECtHR"), a permanent international court based in Strasbourg and known for its progressive and dynamic interpretation of the Convention, enforces the ECHR. Judgments from the ECtHR are binding on the defendant country and persuasive in other signatory countries. The Court's case law spans more than fifty years.

The ECHR has played and continues to play an important role in shaping surveillance law in Switzerland and many other countries. The ECtHR develops its own case law and interprets the Convention so as to keep it current.[48] As a superior international body, the ECtHR governs how national courts apply the ECHR. Swiss courts are required to apply international law, and when domestic law conflicts with international law, international law

be resorted to, in order to save a statute from unconstitutionality." (quoting Hooper v. California, 155 U.S. 648, 657 (1895))).

46. The Council of Europe is an international organization located in Strasbourg, comprised of forty-seven European countries and established to promote democracy, protect human rights, and enforce the rule of law in Europe. *Who We Are*, COUNCIL OF EUROPE, www.coe.int/aboutcoe/index.asp (last visited Mar. 10, 2013).

47. In Switzerland, ratification of an international treaty like ECHR immediately incorporates the terms of that treaty into federal law. *See* FLEINER, MISIC & TÖPPERWIEN, *supra* note 27, at 43–45.

48. The European Court of Human Rights considers the ECHR to be a living instrument, which must (1) be interpreted in a dynamic and evolutionary way, (2) meet present day conditions, (3) be interpreted according to the purpose of the Convention, and (4) be interpreted such that the rights it grants are practical and effective. In addition, the Court must elucidate, safeguard, and develop the rules instituted by the Convention. *See* Golder v. United Kingdom, App. No. 4451/70, Eur. Ct. H.R. (1975) (hudoc.echr.coe.int).

prevails.[49] Swiss courts may not invalidate Swiss statutes on the grounds that they violate the Swiss Constitution. However, if a statute violates a provision contained in the Constitution and in the ECHR, the ECHR prevails on statutes and the provision of the statute that cannot be interpreted in accordance with the ECHR will not be applied to the case reviewed by the court.[50]

Like the Swiss Constitution, the ECHR establishes a right to privacy and provides similar protections. Article 8 of the ECHR states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[51] The ECtHR views any State that chooses to employ new surveillance technologies as bearing a special responsibility to strike the right balance between the potential benefits of such surveillance techniques and the private lives with which they interfere.[52]

Like the Swiss Supreme Court, the ECtHR has not precisely defined "private life." It certainly covers the physical and psychological integrity of a person and incorporates the notion of personal autonomy.[53] It also protects a right to one's own identity and personal development, such as the right to establish relationships with other human beings and the outside world.[54] This right may also include protection for activities of a professional or business nature.[55] There is, therefore, a category of interaction people have with others that falls within the scope of one's "private life," even if conducted in the public sphere. A person's reasonable expectations of privacy may be a significant, although not necessarily conclusive, factor in determining whether he has a right to privacy.[56]

---

49. CST art. 190.

50. AUBERT & MAHON, *supra* note 28, at 1453–62.

51. ECHR art. 8.

52. S. & Marper v. United Kingdom, App. Nos. 30562/04, 30566/04, § 112, Eur. Ct. H.R. (2008) (hudoc.echr.coe.int) (finding that the retention of DNA profiles, samples, and fingerprints of persons not convicted of a crime violates Article 8 of the ECHR).

53. *Id.* § 66 (finding that the retention of DNA profiles, samples, and fingerprints of persons not convicted of a crime violates Article 8 of the ECHR).

54. Amann v. Switzerland, App. No. 27798/95, § 65, Eur. Ct. H.R. (2000) (hudoc.echr.coe.int).

55. *Id.*

56. *See, e.g.*, *Marper*, § 66 (hudoc.echr.coe.int) (finding that retention of DNA profiles, samples, and fingerprints of persons not convicted of a crime violates Article 8); Gillan & Quinton v. United Kingdom, App. No. 4158/05, § 61, Eur. Ct. H.R. (2010) (hudoc.echr.coe.int) (finding that U.K. law authorizing mandatory searches of persons at the discretion of police within a predetermined geographic area violates Article 8 of the European Convention on Human Rights).

A number of elements determine whether surveillance conducted outside a person's home or private property infringes on that person's private life. The Court has not enumerated those elements explicitly; rather, it considers each case as a whole and engages in fact-specific inquiries based on common norms. For example, in *Niemietz v. Germany* the ECtHR held that the notion of a "private life" is not restricted to an inner circle that entirely excludes the outside world; it also comprises the right to establish and develop relationships with other human beings.[57] The court held that a warrant for the search and seizure of any documents found in the applicant's office impinged on professional secrecy to an extent that was not proportional to the ends achieved under the circumstances.[58]

Like the Swiss Constitution, the ECHR permits some restrictions on the right to a private life. Article 8.2 provides:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[59]

Accordingly, any governmental interference in private lives must, among other things, (1) have some basis in domestic law, (2) have a legitimate aim, and (3) be necessary in a democratic society. The last requirement incorporates the notion that the means (e.g., surveillance) must be proportional to the ends achieved (e.g., law enforcement benefits).

Under the ECtHR's jurisprudence, surveillance generally constitutes an intrusion into private life.[60] In cases involving surveillance laws, the Court emphasizes seven requirements for any law authorizing government surveillance,[61] which explain why CrimPC provides much more

57. Niemietz v. Germany, App. No. 13710/88, § 29, Eur. Ct. H.R. (1992) (hudoc.echr.coe.int).

58. *Id.* (interpreting the words "private life" and "home" in Article 8 to include certain professional or business activities or premises).

59. ECHR art. 8.2.

60. Malone v. United Kingdom, App. No. 8691/79, § 64, Eur. Ct. H.R. (1984) (hudoc.echr.coe.int).

61. The recent cases of Kvasnica v. Slovakia, App. No. 72094/01, Eur. Ct. H.R. (2009) (hudoc.echr.coe.int), Calmanovici v. Romania, App. No. 42250/02, Eur. Ct. H.R. (2008) (hudoc.echr.coe.int), and Popescu v. Romania (No. 2), App. No. 71525/01, Eur. Ct. H.R. (2007) (hudoc.echr.coe.int), have confirmed the previous jurisprudence in cases such as Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (1978) (hudoc.echr.coe.int), Malone, *supra* note 60, Kruslin v. France, App. No. 11801/85, Eur. Ct. H.R. (1990)

comprehensive privacy protection than comparable U.S. law. First, exploratory surveillance for preventive monitoring is prohibited.[62] Second, any surveillance should have a basis in domestic law and this law should be compatible with the rule of law and accessible to the person concerned who must, moreover, be able to foresee its consequences for him or her.[63] Third, data may only be used for the specific purposes for which it was collected.[64] Fourth, surveillance should be authorized by an independent body, preferably a judicial body, which is not in any way associated with the executive power.[65] In a later decision, the ECtHR elaborated that an independent judicial authority should authorize surveillance either before or after it takes place.[66] As the comparison between the two systems will show, CrimPC provides for significantly more judicial review than do the U.S. legal rules.

Fifth, the ECtHR requires such effective remedies as notification to the surveillance target within a reasonable time after the grounds necessitating the surveillance have ceased,[67] an opportunity to contest the surveillance or its effects on protected rights before an independent judicial authority,[68] and standing to bring a civil claim for any damage suffered as a result of the surveillance. Accordingly, CrimPC provides more extensive notice and more significant remedies than are available to the targets of surveillance in the United States. The sixth and seventh requirements provide data privacy rights that U.S. law generally does not afford.[69]

(hudoc.echr.coe.int), and Huvig v. France, App. No. 11105/84, Eur. Ct. H.R. (1990) (hudoc.echr.coe.int).

62. *See Klass*, § 51 (hudoc.echr.coe.int).

63. *See Kvasnica*, §§ 78–79 (hudoc.echr.coe.int); *Kruslin*, § 27 (hudoc.echr.coe.int); *Huvig*, § 26 (hudoc.echr.coe.int), *Popescu*, § 61 (hudoc.echr.coe.int), *Calmanovici*, §§ 118, 121 (hudoc.echr.coe.int).

64. *Calmanovici*, §§ 118, 121 (hudoc.echr.coe.int).

65. *See Klass*, § 56 (hudoc.echr.coe.int).

66. *See Popescu*, §§ 69–75 (hudoc.echr.coe.int). The Swiss Federal Supreme Court requires a judicial body to authorize surveillance beforehand and to consider objections to it afterwards when the surveillance pertains to communications. TF, Dec. 27, 1994, 120 ATF Ia 314, 318.

67. *See Popescu*, § 73 (hudoc.echr.coe.int).

68. *See Kruslin*, § 33–34 (hudoc.echr.coe.int); *Popescu*, §§ 73, 77 (hudoc.echr.coe.int).

69. Under the sixth requirement, the defendant should have access to data that could be used against him or her in a trial, at least by end of the investigation, and the defendant should have access to the original recordings until the end of the trial. *Popescu*, §§ 80–109 (hudoc.echr.coe.int). The surveillance target should also have the right to obtain review by a public or private expert of the authenticity or accuracy of the recording or associated transcript. *See Kruslin*, § 20(m) (hudoc.echr.coe.int); *Popescu*, §§ 80–81 (hudoc.echr.coe.int). The seventh requirement is that the law should indicate when and how data collected by surveillance shall be destroyed. *See Kruslin*, §§ 35, 52 (hudoc.echr.coe.int); *Popescu*, §§ 78–79

To summarize, to the extent it imposes a restriction on private life, surveillance law in Switzerland must have a legitimate aim and be necessary in a democratic society. It must be conducted only in accordance with enacted law, and the law must require that any surveillance be authorized by an independent body not associated with the executive branch. During that review, the independent body will also determine if the means of surveillance is proportional to the ends to be achieved. The target of surveillance must (1) be notified of the surveillance, (2) be provided access to the results of the surveillance, (3) have the opportunity to bring those results to an expert who can evaluate their authenticity, (4) have the opportunity to challenge the surveillance in court,[70] if so desired, and (5) be awarded damages if that challenge is successful. As we shall see, no comparable restrictions or rights underlie much of the surveillance that occurs in the United States.

Surveillance conducted according to CrimPC, therefore, is subject to challenge on the grounds that the statute conflicts with the ECHR.[71] Such a challenge, however, would likely fail because the Swiss legislature drafted CrimPC specifically to conform to ECtHR decisions and other national precedents involving the ECHR.[72] For example, to erase any uncertainty regarding the sufficient legal basis to use government monitoring software and IMSI-Catchers, the Federal Council proposed an amendment to the Parliament in 2013, which would add two new articles permitting the use of government monitoring software and IMSI-Catchers.[73]

In theory, the ECHR plays a similar role in Swiss law as the Fourth Amendment plays in U.S. law.[74] In practice, however, the ECHR has arguably shaped current Swiss law much more than the Fourth Amendment has influenced U.S. law because Swiss lawmakers have drafted legislation to comply with its mandates and because all law enforcement surveillance in Switzerland may proceed only according to that law.

(hudoc.echr.coe.int). Under U.S. law, the only comparable right is the wiretap target's right to request a copy of the recording. *See* 18 U.S.C. § 2518(8)(d) (2012).

70. CRIMPC art. 393.

71. If a court finds that a particular surveillance technique exceeds the mandates of CrimPC, it could render the results of the surveillance unusable. Typically, the legislature amends the law to address the technique.

72. Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale [Message about Unification of Criminal Procedure Law], FF 1057, 1075 (2006).

73. Conseil Fédéral, Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication [LSCPT] [Message About the Modification of the Surveillance of Post and Telecommunications Act], FF 2379 (2013).

74. For further discussion of the Fourth Amendment, see *infra* Section III.A.

In the United States, by contrast, the Fourth Amendment protects against excessive surveillance more in theory than in practice. As Part III discusses, the U.S. Supreme Court has interpreted the Fourth Amendment to apply to a small subset of surveillance practices. Litigators for the Department of Justice ("DOJ") have endeavored to limit the scope of the surveillance practices subject to the Fourth Amendment and have generally achieved success in the courts. As a result, unlike the meaningful limits that the Swiss Constitution and the ECHR impose on surveillance practices in Switzerland, the Fourth Amendment constrains a limited subset of surveillance methods in the United States.

III. THE U.S. FRAMEWORK FOR SURVEILLANCE—COMPARED

A. U.S. LEGAL STRUCTURE

The structure of U.S. law is, at least superficially, similar to the structure of Swiss law. Both federal and state laws in the United States regulate law enforcement surveillance practices, with the U.S. Constitution providing a means to strike down laws that do not satisfy its mandates. In the United States, however, determining the applicable legal rule to govern a given act of law enforcement surveillance may not be easy. Government agents may conduct surveillance activities for law enforcement purposes and to gather foreign intelligence; different rules apply depending on the purpose of the surveillance.[75] Although federal legislation trumps inconsistent state legislation and provides a single law for federal actors all over the United States,[76] federal appellate courts differ as to how they interpret the federal surveillance provisions; consequently, the applicable rules vary by jurisdiction.[77] Finally, states have passed their own laws to regulate the surveillance practices of state and local law enforcement agents as well as private actors.[78] Those laws, which must respect the floor set by federal law,[79]

---

75. Other than a short discussion, *infra* Section V.C, this Article will not cover surveillance for foreign intelligence gathering.

76. Under federal statutory law, applications for wiretapping are made by federal law enforcement officials to federal magistrate judges for violations of federal law, and to state judges for investigation by state law enforcement agents of violations of state laws. *See* 18 U.S.C. § 2516(2)–(3) (2012).

77. *See, e.g.*, Ohm, *supra* note 4, at 1538–42 (describing how the Ninth Circuit interprets an ECPA provision pertaining to email surveillance differently from the Department of Justice).

78. *See, e.g.*, Charles H. Kennedy & Petper P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971, 977 (2003) (surveying state wiretap laws enacted since September 11, 2011). State statutes are subject to judicial review in either state

may be more restrictive of law enforcement practices and therefore more protective of privacy interests.[80] To avoid undue complexity, this Article will focus on federal statutes and federal constitutional law.

The most important difference between the Swiss and American legal systems lies not in the hierarchy of laws, but in the defaults that operate in the absence of legislation. Laws, both statutory and constitutional, *restrict* government action in the United States. That means that ECPA and the Fourth Amendment restrict government surveillance practices, but if they do not preclude a particular surveillance technique, government actors feel free to engage in it.[81] An example is the use of undercover agents, which neither a statute nor the Fourth Amendment regulate in the United States.[82] As previously discussed, the Swiss Constitution and the ECHR require enacted law to *authorize* their surveillance practices before they may be used. Once one understands what CrimPC covers, one knows the scope of law enforcement surveillance in Switzerland. Because law enforcement agents in the United States conduct surveillance until a statute or a court decision restricts them from doing so,[83] however, it is just as important to understand what statutory law (usually ECPA) and the Fourth Amendment do not cover as what they do. The comparison to CrimPC helps to bring that to light.

B. RIGHTS TO PRIVACY UNDER THE U.S. CONSTITUTION

Historically, judges have used the Fourth Amendment[84] to set standards when evaluating law enforcement surveillance practices.[85] Concerns about

---

or federal courts to ensure their compliance with both the federal and applicable state constitutions).

79. *See* Lane v. CBS Broad. Inc., 612 F. Supp. 2d 623, 637 (E.D. Pa. 2009) (reviewing legislative history to find that Congress intended for the federal law to set a baseline of protection above which states could legislate).

80. *See supra* note 23.

81. *See supra* note 14 and accompanying text.

82. *See infra* Section VII.F.2. CrimPC regulates the practice. *See id.*

83. *See, e.g.*, Kevin Johnson, *FBI Cuts Back on GPS Surveillance After Supreme Court Ruling*, USA TODAY, Feb. 7, 2012, www.usatoday.com/news/washington/story/2012-02-03/fbi-gps-surveillance-supreme-court-ruling/52992842/1 (reporting that the FBI had been operating under the assumption that use of GPS trackers did not require a court order or warrant prior to the Supreme Court's decision that it constituted a Fourth Amendment search); Julia Anguin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WSJ.COM (Feb. 25, 2012), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling.

84. U.S. CONST. amend. IV. The Fourth Amendment requires that:

> [T]he 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 warrant shall issue, but upon probable cause, supported by Oath

First Amendment rights of free speech have also animated courts' reasoning in some surveillance cases,[86] but they have not yet provided an independent basis for review.[87]

The Fourth Amendment governs electronic surveillance practices more in theory than in practice. Courts have required challengers to overcome such hurdles as the requirement that they have standing to sue,[88] that the controversy be ripe for review,[89] and that the court cannot avoid the constitutional issue by statutory construction.[90] In addition, because many people targeted for law enforcement surveillance never learn about that surveillance, they cannot bring challenges to those practices of which they are unaware.[91] Finally, the federal appellate courts have taken few cases that

---

> or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

85. *See, e.g.*, Berger v. New York, 388 U.S. 41, 51–53 (1967) (reviewing the history of the U.S. Supreme Court's surveillance decisions); United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010) (finding federal surveillance statute unconstitutional to the extent it permits law enforcement access to stored email without a warrant).

86. *See, e.g.*, United States v. U.S. Dist. Court, 407 U.S. 297, 314 (1972) ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation.").

87. *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 165–76 (2007) (identifying implications of electronic surveillance for First Amendment interests).

88. *See, e.g.*, Jewel v. NSA, 673 F.3d 902, 912 (9th Cir. 2011) (reversing lower court decision that plaintiffs lacked standing to challenge widespread warrantless surveillance of their communications phone calls and emails as part of terrorist surveillance program); ACLU v. NSA, 493 F.3d 644, 657 (6th Cir. 2007) (finding that plaintiffs lacked standing under Fourth Amendment to challenge the same practices).

89. *See, e.g.*, Warshak v. United States 532 F.3d 521, 525–34 (6th Cir. 2008) (en banc) (denying claim for injunctive relief from law enforcement surveillance on the grounds that claim was not ripe).

90. *See supra* note 45 and accompanying text; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 695 (2011) [hereinafter Freiwald, *Cell Phone Location Data*] (discussing successful arguments in recent case that courts should avoid constitutional ruling); Susan Freiwald, *The* Davis *Good Faith Rule and Getting Answers to the Questions That* Jones *Left Open*, 14 N.C. J. L. & TECH. 341 (2013) (discussing how courts are avoiding constitutional analysis by relying on a recent expansion in the exceptions to the exclusionary rule).

91. *See infra* Section VII.C. (discussing how some statutes require notice to targets of surveillance); *see also* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. J. L. & POL'Y REV., 313, 328 n.83 (2012) (discussing huge number of electronic surveillance orders that do not lead to prosecutions and of which the targets never obtain notice).

pertain to surveillance.[92] Among those few instances when higher-level courts do take on cases involving modern day surveillance questions, those courts often avoid the constitutional analysis altogether.[93]

The Supreme Court did issue a constitutional decision in 2012 in *United States v. Jones*, a case that addressed law enforcement's use of a GPS tracker attached to a car for an extended period.[94] Although all nine Justices agreed that the practice implicated the Fourth Amendment, the fractured opinion yielded no clear constitutional test beyond the facts of the case.[95] Importantly, the Court provided little guidance on how the Fourth Amendment applies, if at all, to location data surveillance accomplished by remote GPS tracking surveillance such as when officers monitor devices installed in cars or smartphones or when they acquire location data records from cell phone providers.[96] A broadly written decision might have motivated Congress to dramatically revamp ECPA, but the narrow decision in *Jones* certainly did not.[97] Even after *Jones*, litigants continue to debate how to apply decades-old precedents to modern surveillance methods.[98]

The older cases do make some things clear. In *Berger v. New York*, the Supreme Court found unconstitutional a New York statute that regulated electronic surveillance because the state law did not impose sufficient

92. *See* Smith, *supra* note 91, at 326–31 (discussing lack of appellate oversight of electronic surveillance cases).

93. *See* City of Ontario v. Quon, 560 U.S. 746, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

94. United States v. Jones, 132 S. Ct. 945 (2012).

95. *See id.* at 954 (noting that a later case may require the Court to resort to a reasonable expectation of privacy but that the present case could be resolved on the basis of trespass); *see also* Paul Ohm, *United States v. Jones Is a Near-Optimal Result*, FREEDOM TO TINKER (Jan. 23, 2012), https://freedom-to-tinker.com/blog/paul/united-states-v-jones-near-optimal-result (describing it as positive that Court issued a narrow decision and avoided the debate over "reinventing Katz"). For further discussion, see *infra* Section VII.C.2.e.

96. *See* sources cited *supra* note 90 (discussing cases addressing surveillance through acquisition of location data from cell phone service providers and the questions *Jones* left unanswered).

97. For example, had Justice Sotomayor's concurrence been the majority decision, it would presumably have made any use of GPS tracking a search and dramatically undermined ECPA's lesser protection for electronic communications held by third parties. *See Jones*, 132 S. Ct. at 955–57 (Sotomayor, J., concurring).

98. *See, e.g.*, Brief for the United States at 16–26, *In re* Application of the U.S. for Historical Cell-Site Data, No. 11-20884 (5th Cir. Feb. 15, 2012), 2012 WL 1197699 [hereinafter Government Brief 5th Circuit] (arguing that Supreme Court cases from the 1970s and 1980s determine the outcome of the case).

procedural hurdles on law enforcement agents.[99] In *Katz v. United States*, concurring Justice Harlan formulated the reasonable expectation of privacy test[100] and the majority opinion announced that surveillance practices that intrude upon such expectations must comply with the restrictions set out in *Berger*.[101] In a series of cases in the late 1980s and early 1990s, seven federal courts of appeal extended the core Fourth Amendment protections established in *Berger* to government use of video surveillance cameras that record activities subject to a reasonable expectation of privacy.[102] The appellate courts found video surveillance to share the features of wiretapping that make it particularly prone to abuse in that such surveillance is hidden, indiscriminate, intrusive, and continuous and therefore it must be subject to the same restrictions as wiretapping.[103]

The crucial question in the United States is whether the law enforcement practice at issue constitutes a "search" under the Fourth Amendment like wiretapping, bugging, and some types of silent video surveillance. Unlike in Switzerland, constitutional privacy principles apply only to that subset of practices that are considered to be such searches. Practices that are not searches under the Fourth Amendment are subject to no constitutional regulation, and are regulated, if at all, by Congress, subject to no constitutional constraints.

In two important cases, the Supreme Court significantly limited what surveillance-type practices count as constitutional searches. In *United States v. Miller*, the Court found no Fourth Amendment search when law enforcement agents compelled a bank to produce records of the defendant's transactions

---

99. Berger v. New York, 388 U.S. 41, 60 (1967) (emphasizing the need for "adequate judicial supervision or protective procedures").

100. Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).

101. *See Katz*, 389 U.S. at 354–56 (noting that a judicially-authorized warrant that had "carefully limited use of electronic surveillance" could have been acceptable).

102. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 53–56.

103. *See id.*; *see also* Freiwald, *Cell Phone Location Data*, *supra* note 90, at 746–49 (arguing that these four factors—"hidden, indiscriminate, intrusive, and continuous"—should be used to find cell site location data protected by the Fourth Amendment); Brief for Yale Law Sch. Info. Soc'y Project Scholars et al. as Amici Curiae Supporting Respondent at 34–35, United States v. Jones, 132 S. Ct. 945 (2012) (arguing that the four factors should be used to find GPS tracking data protected by the Fourth Amendment). Arguments to extend the category of searches subject to the *Berger* standard beyond wiretapping, bugging and silent video surveillance to their modern analogues, such as that made in the *Jones* case, have not been successful. *But see In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d. 585, 586 n.7 (W.D. Pa. 2008) (discussing four factors in reference to cell site location information).

with the bank such as his deposit slips and account statements.[104] The Court stated:

> [T]he 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.[105]

Government litigators and academics have disagreed over the implications of *Miller*. Some have argued that it establishes that the Fourth Amendment does not protect information obtained from a third party, which would include records of electronic communications stored with service providers.[106] Others have promoted a narrow construction of *Miller*,[107] under which, for example, customers would not forfeit their Fourth Amendment interests by sharing information with intermediaries such as electronic communication providers.[108] Whatever the proper application of *Miller* to new technologies, it clearly inspired Congress to provide only limited restrictions on law enforcement access to stored electronic records in ECPA.[109]

The Supreme Court extended *Miller* to the communications context in 1979 when it found law enforcement acquisition of dialed telephone numbers not to be an unconstitutional search in *Smith v. Maryland*.[110] Law enforcement agents used a device known as a "pen register" to obtain the

---

104. United States v. Miller, 425 U.S. 435, 442–45 (1976).

105. *Id.* at 443.

106. *See, e.g.*, Final Reply Brief for Defendant-Appellant United States of America at 17, Warshak v. United States, 532 F.3d 521 (6th Cir. 2008), 2007 WL 2085416 (proposing the rule that "the government may compel an entity to disclose any item that is within its control and that it may access").

107. *See, e.g.*, Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1403–09 (2004) (arguing that a broad reading of *Miller* is inconsistent with *Katz*); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004). Under a narrow construction, the *Miller* case would apply only when the target has knowingly and voluntarily shared his information with a service provider and the provider has stored the records in the ordinary course of its business. *See, e.g.*, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010) (rejecting applicability of *Miller* to the acquisition of cell site location data).

108. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. CHI. LEGAL F. 121, 158–69 (2008). In *Miller*, government agents acquired Miller's records from his bank, which was considered a party to his bank records. *Miller*, 425 U.S. at 438, 440–41.

109. *See* H.R. Rep. No. 99-647, at 23, 73 (1986) (referring to the *Miller* case when explaining lesser protections for electronic communications in storage); *see also infra* Section VII.B.2e.

110. 442 U.S. 735, 745–46 (1979).

telephone numbers dialed on a telephone.[111] The Supreme Court considered the limited intrusiveness of the pen register investigation as well as the target's voluntary and knowing disclosure of his telephone numbers to telephone company employees when it found the technique to intrude on no reasonable expectation of privacy.[112] As with the *Miller* case, the *Smith* decision does not have to be read to imply a lack of constitutional protection for modern electronic communications information.[113] Justice Department litigators, however, have maintained that *Smith* establishes that all "non-content" information lacks Fourth Amendment protection.[114] Whatever the appropriate reading of the case, it inspired Congress to provide for relatively little restriction in ECPA on law enforcement access to communication attributes, which include all non-content features of communications.[115]

Miller and *Smith* established that the practices they considered—compelled disclosure of stored bank records and acquisition of telephone numbers dialed—fell entirely outside the protection of the Fourth Amendment because they were not "searches" that intruded upon the targets' reasonable expectations of privacy. Some U.S. courts have read *Miller* and *Smith* more expansively and have found modern surveillance practices, such as IP address and cell site location acquisition, to be similarly outside the protection of the Fourth Amendment.[116] Some courts have recently rejected such broad readings, and found new practices, such as stored email acquisition, to be constitutionally protected because they differ significantly

111. Pen registers were mechanical surveillance devices that originally recorded only the numbers dialed, and did not determine whether a call had succeeded, its duration or the identity of the parties to it. *See generally* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982–89 (1996) (describing the mechanics of early pen registers and reviewing their evolution over time).

112. *Id.* at 741–44.

113. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . ." (citing *Smith*, 442 U.S. at 742, and *Miller*, 425 U.S. at 443)).

114. *See, e.g.*, Gov't Reply Brief at 2–3, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (arguing that "non-content" cell-site location records are not subject to Fourth Amendment protection).

115. *See infra* Section VII.C.2; Freiwald, *supra* note 111, at 969–75, 993–1007 (describing how Congress accorded weak protections to communications attributes in the federal surveillance statutes).

116. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (finding real-time collection of IP addresses by law enforcement agents to be unprotected by the Fourth Amendment); Government Brief 5th Circuit, *supra* note 98, at 25–26 (listing five federal "district court cases [that] have relied on Smith and Miller and rejected Fourth Amendment challenges to acquisition of historical cell-site records without a warrant.").

from the practices considered in *Miller* and *Smith* and instead more analogous to wiretapping and acquisition of postal mail.[117]

Congress retains complete discretion over how to regulate those practices that do not implicate the Fourth Amendment. Unlike Swiss legislators, Congress has not produced a comprehensive surveillance law that covers all types of surveillance used during law enforcement investigations. Instead, restrictions derive from piecemeal legislation such as ECPA, which has fallen out-of-date in the more than twenty-five years since its passage. As the next section shows, in the United States, there is nothing comparable to the restrictions imposed by the ECtHR to inspire or require Congress to bring U.S. laws up to date.

C. RIGHTS TO PRIVACY UNDER INTERNATIONAL LAW

The United States is not a signatory to the European Convention on Human Rights and is not a member of the Council of Europe. Nor is the United States a party to an international treaty that would regulate its national law enforcement practices directly, with the exception of the Convention on Cybercrime. Article 15 of the Convention on Cybercrime requires that parties to the treaty include safeguards which "provide for the adequate protection of human rights and liberties."[118] Individual state parties may determine which specific safeguards to impose, however, and the treaty imposes no specific due process requirements on the United States, nor does it empower an international enforcement body.[119]

The United States does not fully submit to treaty obligations that could impose restrictions like those imposed by the ECHR. For example, the United States is a party to the International Covenant on Civil and Political Rights, but during ratification the Senate declared non-self-executing[120] that part of the treaty that protected against unlawful interference with a person's

117. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that acquisition of stored email without a warrant is unconstitutional); *see also In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (finding warrantless acquisition of historical cell site location information to violate the Fourth Amendment), *vacated*, 724 F.3d 600 (2013).

118. Council of Europe, Convention on Cybercrime art. 15, Nov. 23, 2001, T.I.A.S. No. 13174.

119. Miriam Miquelon-Weisman, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, 23 J. MARSHALL J. COMPUTER & INFO. L., 329, 340–41 (2005).

120. *See* S. Treaty Doc. No. 95-20 (1992) (providing resolution that sections of the International Covenant on Civil and Political Rights listing the rights of individuals are not self-executing).

"privacy, family, home, or correspondence."[121] In the absence of additional legislation, a U.S. citizen cannot challenge surveillance on the basis of that treaty language. While the United States is a party to the International Court of Justice, only other state parties, not individuals or non-state organizations, can bring matters before it.[122] Therefore, no United States citizen can use its dispute resolution mechanisms to challenge domestic law enforcement surveillance.

The absence of a higher order treaty like the ECHR has left law enforcement surveillance in the United States to the discretion of Congress, constrained to a limited degree by the Fourth Amendment. As later sections of this paper will show, Congress has used its discretion to produce an electronic surveillance regime with less expansive coverage, more complexity, and less comprehensive privacy rights than the Swiss statutory regime of CrimPC, to which we now turn.

IV. SWITZERLAND: APPLICABLE LAW ENFORCEMENT SURVEILLANCE ACTS

A. THE LAWS PRIOR TO THE SWISS CRIMINAL PROCEDURE CODE ("CRIMPC")

Current regulations for the various types of surveillance practices stem from the historical regulation of the mail and telephone networks. In 1889, the federal Act on Telephones made the content of telephone calls secret.[123] This first law protected all users by treating all phone calls as private matters. Thirty years later, however, two laws gave significant surveillance power to the State by providing law enforcement authorities the right to access the content of telephone calls, telegraph messages, and mail.[124] Decades later,

121. International Covenant on Civil and Political Rights art. 17, Dec. 19, 1966, 999 U.N.T.S. 171.

122. Charter of the United Nations and Statute of the International Court of Justice art. 34 para. 1, June 26, 1945, 59 Stat. 1055.

123. Loi Fédérale Sur Les Téléphones (du 27 Juin 1889) Avec Les Changements Y Apportés Par La Loi Fédérale Du 7 Décembre 1894, Et Ordonnance Sur Les Téléphones (du 24 Septembre 1895), FF III 902 (1889), RO 11 256, *available at* www.amtsdruckschriften.bar.admin.ch/viewOrigDoc.do?id=10069429.

124. Loi fédérale du 14 octobre 1922 réglant la correspondance télégraphique et téléphonique [Federal Act Regulating Telegraph and Telephone Communications] RS 7872 (1922); Loi fédérale du 2 octobre 1924 sur le Service des postes [Federal Act on the Postal Service] (1924).

both acts were modified again to restrict surveillance so that it could no longer be used to investigate civil matters or minor crimes (non-felonies).[125]

Viewing private life as insufficiently protected by the law, the federal Parliament amended the Criminal Code to add offenses for breach of privacy or secrecy in 1968.[126] The new Criminal Code provisions should have protected citizens' privacy from individual and state surveillance, but the Swiss Supreme Court held that an official who conducted surveillance in violation of the Criminal Code was not guilty on the grounds that he was doing his official duty.[127] This case spurred reform proposals in the Swiss Parliament.

A few years after Switzerland enacted the ECHR in 1974, the ECtHR held in a case brought against Germany that any interference with an Article 8 privacy right needed some basis in domestic law.[128] Even with those changes to its Criminal Code, Switzerland had no clear rule of law for surveillance that satisfied the requirement of proportionality of means and end. Switzerland needed to update its surveillance law to conform to the requirements of ECHR as recently interpreted by the Court.

As a result, Parliament enacted the federal Act on Privacy Protection in 1979,[129] which endeavored to regulate secret surveillance using the same principles that regulated the search of a house or the conduct of an arrest. It enumerated the conditions for surveillance and provided legal protection for individual subjects. The Act's provisions covered surveillance of post, telephone, and telegraph traffic. CrimPC retains several of the Act's basic principles such as the conditions imposed on surveillance, the requirement of proportionality, and the subject's right to go to court to contest surveillance. Parliament also amended the Criminal Code to preclude courts from excusing official surveillance merely on the grounds that the breach was conducted as part of official duties.[130]

---

125. In the Swiss Criminal Code, felonies are distinguished from misdemeanors according to the severity of the penalties that the offense carries. CODE PÉNAL SUISSE [CP] [Criminal Code] Dec. 21, 1937, RS 311, art. 10. Felonies carry a custodial sentence of more than three years and misdemeanors carry a monetary penalty or a custodial sentence not exceeding three years. Contraventions are punishable by a fine. CP art. 103.

126. CP art. 179bis–179septies.

127. Tribunal Fédéral [TF] [Federal Supreme Court] Mar. 8, 1974, 100 ARRÊTS DU TRIBUNAL FÉDÉRAL SUISSE [ATF] Ib 13, para. 5.

128. Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (1978) (hudoc.echr.coe.int).

129. Loi fédérale sur la protection de la vie privée du 23 mars 1979 (modifications de lois fédérales) RO 1170 (1979). The Act amended the Federal Act on Telegraph and Telephone Traffic and the Federal Postal Service Act.

130. CP art. 179octies.

The Swiss Parliament enacted the law that inspired the new CrimPC in 2002.[131] That law, known as the Surveillance of Post and Telecommunications Act ("SPTA"), brought all provisions pertaining to the surveillance of post and telecommunications together in the same act.[132] Parliament designed SPTA to be as uniform as possible and to protect every kind of letter, parcel, and telecommunication from surveillance.[133] It covered the content and attributes of letters and parcels,[134] phone calls (including Voice over IP), email, text messages, faxes, and pager transmissions.[135] The next section describes the passage of CrimPC.

B. CRIMPC

After seven years of work, a committee of experts charged with unifying criminal procedure developed a draft of CrimPC.[136] The experts designed

131. Loi fédérale sur la surveillance de la correspondance par poste et télécommunication ("LSCPT") [The Federal Act of October 6, 2000 on the Surveillance of Post and Telecommunications ("SPTA")], RS 780.1. Parliament passed the Federal Law on Undercover Investigation on June 20, 2003 and CrimPC now includes important rules from that law as well.

132. SPTA did not cover the use of tracking devices and video surveillance equipment because such surveillance was not yet within the federal power and was therefore allowed only pursuant to cantonal law, if at all. For more on the situation prior to the SPTA and SPTA in general, see THOMAS HANSJAKOB, *BÜPF/VÜPF*: KOMMENTAR ZUM BUNDESGESETZ UND ZUR VERORDNUNG ÜBER DIE ÜBERWACHUNG DES POST- UND FERNMELDEVERKEHRS [COMMENTARY TO THE SURVEILLANCE OF POST AND TELECOMMUNICATIONS ACT AND ORDINANCE] 1–18 (2006).

133. Conseil Fédéral, Message concernant les lois fédérales sur la surveillance de la correspondance postale et des télécommunications et sur l'investigation secrète du 1er juillet 1998 [Message concerning the Federal Acts on the Surveillance of Post and Telecommunications and Undercover Investigation of July 1, 1998], FF IV 3689, 3703 (1998).

134. GÉRARD PIQUEREZ, TRAITÉ DE PROCÉDURE PÉNALE SUISSE [TREATY OF SWISS CRIMINAL PROCEDURE] 615 (2006); Bernhard Sträuli, La surveillance de la correspondance par poste et télécommunication: aperçu du nouveau droit [Surveillance of Post and Telecommunications: an Overview of the New Law], in PLUS DE SÉCURITÉ—MOINS DE LIBERTÉ? LES TECHNIQUES D'INVESTIGATION ET DE PREUVE EN QUESTION [MORE SECURITY—LESS FREEDOM? INVESTIGATION TECHNIQUES AND EVIDENCE IN QUESTION] 95–99 (2003).

135. SPTA did not cover communications made in Internet public forums or chat rooms. Police officer interventions in such conversations would be covered under the CrimPC rules pertaining to undercover agents. Beat Rhyner & Dieter Stüssi, *Kommentar zu Art. 269–279 StPO (Commentary to articles 269–279 CrimPC)*, in POLIZEILICHE ERMITTLUNG 443 (Gianfranco Albertini, et al. eds., 2008); Beat Rhyner & Dieter Stüssi, *Kommentar zu Art. 286-298 StPO (Commentary to articles 286–298 CrimPC)*, in POLIZEILICHE ERMITTLUNG, *supra*, at 498–99.

136. The Federal Council submitted the draft to the legislative process along with the committee of experts in 2001; the committee had begun their work in 1994.

CrimPC to treat every method of surveillance consistently with the treatment of surveillance of post and telecommunications under SPTA.[137]

Although CrimPC passed with great support from the Swiss people in 2007, it required a constitutional amendment to pass into law.[138] CrimPC represented a significant change in that it replaced twenty-seven different codes of criminal procedure (twenty-six cantonal and one federal).[139] Because some Cantons had to make extensive administrative or organizational changes to conform to the new federal CrimPC, the legislature decided to delay the new law's introduction until January 1, 2011.[140]

CrimPC provides for a public prosecutor, among other duties, to lead preliminary proceedings, conduct the examination of witnesses and others, bring charges, and represent cases before the courts.[141] Newly created Compulsory Measures Courts offset the public prosecutor's power.[142] In addition to overseeing surveillance activities, the new courts approve pretrial and security detentions and authorize the deployment of undercover investigators.[143]

Swiss law significantly deters violations of CrimPC. Only government officials may use one of the surveillance measures listed under CrimPC, and only after satisfying its statutory requirements.[144] The Criminal Code prohibits the use of surveillance without authorization and treats any information gathered by such surveillance as illegally obtained and subject to

137. Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale (Message about Unification of Criminal Procedure Law), FF 1057, 1099–1100, 1230 (2006).

138. All Cantons and 86.4% of the people eligible to vote approved the constitutional amendment needed. Arrêté du Conseil fédéral du 17 mai 2000 constatant le résultat de la votation populaire du 12 mars 2000, FF 2814–2820 (2000). According to the Swiss Constitution, the Confederation had the power to legislate over criminal and civil law but not over criminal law procedure or civil law procedure.

139. Under CrimPC, cantonal bodies continue to enforce substantive federal criminal law but comply in addition with the federal CrimPC.

140. CrimPC required many practical changes for some Cantons, especially those in the French part of Switzerland. Such Cantons, which used to have an independent and impartial investigating magistrate responsible for gathering the necessary evidence and conducting other pretrial steps, had to adopt the more adversarial prosecutorial role established in CrimPC.

141. CRIMPC art 16.

142. CRIMPC art 18.

143. *Id.* The Compulsory Measures Court is a regular court. *Id.* For more about the Compulsory Measures Courts, *see* André Kuhn, Procédure pénale unifiée: reformatio in pejus aut in melius? [Unified Criminal Procedure: Reformation in Pejus aut in Melius?] 45–49 (2008); Mark Pieth, Schweizerisches Strafprozessrecht: Grundriss für Studium und Praxis [Swiss Criminal Procedure Law: Basics for Academia and Practice] 63–64 (2009).

144. CP art. 179octies.

the exclusionary rule when challenged by the subject.[145] In addition, officials who conduct surveillance in violation of CrimPC risk disciplinary measures and prosecution.[146]

C. OTHER ACTS PERTINENT TO LAW ENFORCEMENT SURVEILLANCE

Swiss intelligence agencies do not conduct surveillance pursuant to CrimPC,[147] but instead operate according to the Internal Security Act ("ISA"), which addresses dangers relating to terrorism, illegal intelligence, violent extremism, and illegal arms and radioactive materials trade.[148] ISA permits preventative surveillance of those not suspected of criminal activity but limits surveillance under its auspices to publicly available information.[149] The Swiss Constitution does not require the limited intelligence surveillance under ISA to proceed with prior judicial authorization, unlike law enforcement surveillance under CrimPC.[150]

Since the enactment of CrimPC, the Swiss Criminal Code,[151] the Swiss Civil Code,[152] and the Federal Act on Data Protection do not generally

145. For more on the remedies for unlawful surveillance, *see infra* Section VI.D.

146. The provisions contained in the Criminal Code aim to avoid private surveillance and official surveillance without authorization, or "wild surveillance."

147. CrimPC does not apply to intelligence activities. Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale (Message about Unification of Criminal Procedure Law), FF 1057, 1112 (2006).

148. Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure [The Federal Act on Measures to Safeguard Internal Security of March 21, 1997 ("LMSI")] RS 120 (1997). The ISA is used for all civil (non-military) surveillance conducted inside the country, whether or not the target is a Swiss citizen.

149. Intelligence agents may gather information through sources open to the public, and cantonal and federal authorities may transmit information to intelligence agencies. ISA art. 14. They may also conduct physical observation, video, and audio recording of public and freely accessible places.

150. *See supra* text at notes 65–66. The Government is currently drafting a bill that may allow for preventive surveillance. This surveillance would be subject to similar requirements to the ones in CrimPC (judicial plus political oversight, notice, and exclusionary rules). *See* Avant-projet de Loi fédérale sur le Service de renseignement civil (First Draft of Civil Intelligence Service Act), *available at* www.admin.ch/ch/f/gg/pc/ind2013.html.

151. The Swiss Criminal Code penalizes as misdemeanors unlawful entry (CP art. 186) and breach of postal or telecommunications secrecy (CP art. 321ter). It treats as felonies: breach of the privacy of a sealed document (CP art. 179), listening in on and recording the conversations of others (CP art. 179bis), unauthorized recording of conversations (CP art. 179ter), breach of secrecy or privacy through the use of an image-carrying device (CP art. 179quater), marketing and promotion of devices for unlawful listening or sound or image recording (CP art. 179sexies), misuse of a telecommunications installation (CP art. 179septies), and obtaining personal data without authorization (CP art. 179novies). *See* Sylvain Métille, *L'utilisation privée de moyens techniques de surveillance et la procédure pénale* (*Private Use of Surveillance and Criminal Procedure*), in "LE DROIT DÉCLOISONNÉ", INTERFÉRENCES ET INTERDÉPENDANCES ENTRE DROIT PRIVÉ ET DROIT PUBLIC ("DECOMPARTMENTALIZED

govern surveillance by law enforcement, but they do contain rules relevant to surveillance by private parties.[153] Law enforcement agents who conduct surveillance in accordance with CrimPC commit no offenses under these laws.[154]

V. UNITED STATES: APPLICABLE SURVEILLANCE ACTS

A. THE WIRETAP ACT

In 1968, Congress passed the Wiretap Act,[155] the precursor to ECPA, to codify the Fourth Amendment protections the Supreme Court had established in *Berger* the year before.[156] The Wiretap Act's procedural safeguards are closest to those provided by CrimPC, offering the highest level of judicial oversight of any of the surveillance laws in the United States. Under the Wiretap Act, for example, law enforcement agents must show that other less intrusive methods will not work before they may wiretap, and they must establish a tight nexus between the communications they seek to obtain and the criminal activity they are investigating.[157] Like CrimPC, the Wiretap Act requires that targets receive notice of the surveillance and provides real remedies for victims of improper investigations.[158]

But while the Wiretap Act has comprehensive protections like CrimPC, its coverage is dramatically more limited. The Wiretap Act applies to the use of traditional wiretaps (for telephone calls), bugs (to record oral conversations), and silent video surveillance conducted where targets have a reasonable expectation of privacy.[159] All other types of law enforcement

LAW," INTERFERENCES AND INTERDEPENDENCES BETWEEN PRIVATE LAW AND PUBLIC LAW) (Jean-Philippe Dunand & Pascal Mahon eds., 2009).

152. Art. 28 provides a general protection of legal personality: any person whose personality rights are unlawfully infringed may apply to the court for protection against any infringers. An infringement is unlawful unless it is justified by the consent of the person whose rights are infringed or by an overriding private or public interest or by law. STÉPHANE BONDALLAZ, LA PROTECTION DES PERSONNES ET DE LEURS DONNÉES DANS LES TÉLÉCOMMUNICATIONS (PROTECTION OF PERSONS AND THEIR DATA IN TELECOMMUNICATIONS) 146–56 (2007).

153. They apply, for example, to monitoring at the workplace or on private property.

154. CP art 179octies.

155. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)). Commentators refer to the law as either "Title III" or the more intuitive "Wiretap Act."

156. Berger v. New York, 388 U.S. 41, 56–59 (1967); *see supra* Section III.B.

157. 18 U.S.C. § 2518 (2012); *see also* James G. Carr & Patricia L. Bellia, The Law of Electronic Surveillance § 4.17–4.48 (2011 ed.) (describing the requirements of the Wiretap Act).

158. *See infra* Section VII.B.2.

159. 18 U.S.C. § 2511 (2012); *see infra* Section VII.D.2. (describing how most federal appellate courts applied the substantive provisions of the Wiretap Act to silent video

surveillance must satisfy other statutes, such as ECPA, or are unregulated by federal statutory law.[160]

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

While Congress endeavored to regulate the surveillance of modern communications technologies by passing ECPA in 1986 to amend the Wiretap Act,[161] ECPA's complexity has created considerable controversy about exactly what it covers.[162] ECPA extended some but not all of the Wiretap Act's protections to electronic communications' content and also includes entirely new provisions to govern some new surveillance practices Congress viewed as less intrusive than traditional wiretapping.[163]

ECPA contains three titles. The first extends the Wiretap Act provisions to the acquisition in real time of electronic communications such as email.[164] As this Article will discuss in more detail, it is easier for agents to obtain approval for such surveillance than for a traditional wiretap.[165] Significantly, and unlike under CrimPC, no information obtained in violation of ECPA is subject to a statutory exclusionary remedy, which significantly reduces ECPA's deterrent effect.[166] ECPA's second title, the "Stored Communications Act," addresses the acquisition of stored electronic information.[167] It has significantly fewer protections for such information than the first title and accords different protections to the contents of electronic communications and the non-content information associated with

surveillance by analogy despite the absence of explicit language in the Act); *see also supra* text accompanying notes 101–02 (describing federal appellate courts' finding that silent video surveillance is protected by the Fourth Amendment).

160. State law may provide greater regulation than federal law, both by providing greater coverage and by providing more comprehensive rights. But a discussion of state law is beyond the scope of this article. *See supra* note 23.

161. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

162. *See, e.g.*, Mink v. Salazar, 344 F. Supp. 2d 1231, 1239 (D. Colo. 2004) ("As several courts have noted, the [ECPA] is 'famous (if not infamous) for its lack of clarity.' " (citations omitted)).

163. *See supra* text accompanying notes 103–14.

164. Title I, Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848 (1986) (codified in scattered sections of 18 U.S.C.). There is no short form name given to the first title of ECPA.

165. *See infra* Section VII.B.2d).

166. It also reduces the number of cases brought to contest surveillance conducted according to its authority. *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 817 (2003); *see also* Freiwald, *supra* note 102, ¶¶ 19–35 (arguing that difficulties in determining constitutional questions have also inhibited their resolution).

167. Title II, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–11 (2012)).

such communications—"communication attributes."[168] The third title, known as the "Pen Register Act,"[169] covers law enforcement use of pen registers and "trap and trace devices" to obtain dialing and addressing information for both wire and electronic communications.[170] Provisions in both the Stored Communication Act and the Pen Register Act restrict law enforcement surveillance significantly less than do comparable provisions in CrimPC.

C. THE USA PATRIOT ACT AND OTHER AMENDMENTS

Congress passed the USA PATRIOT Act in 2001 ("Patriot Act"),[171] just six weeks after the terrorist attacks of September 11.[172] Most of the Patriot Act's many provisions have nothing to do with surveillance, but a few of them further eased the restrictions on law enforcement surveillance.[173] For example, the Patriot Act amended ECPA so that acquisition of voicemail would receive the same reduced protection as stored electronic messages instead of the stronger protections that the Wiretap Act accorded telephone calls.[174] The Patriot Act also clarified that the weak provisions of the Pen Register Act would apply to the acquisition of electronic communication

168. *See* Freiwald, *supra* note 111, at 951 (introducing and explaining use of the term "communication attributes"). The statute treats different subcategories of communication attributes differently. *See infra* Section VII.C.2.

169. Title III, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1873 (1986) (codified as amended at 18 U.S.C. §§ 3121–27 (2012)).

170. Traditional pen registers acquired the telephone numbers dialed by the target's phone while trap and trace devices acquired the telephone numbers of the calling parties, revealing the same information as does caller ID. Modern pen registers acquire more detailed information.

171. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA PATRIOT Act].

172. For an insightful description of the legislative process that produced the Patriot Act, see generally Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145 (2004). Ms. Howell was a senior Democratic staffer at the time, and she argues that several Democrats valiantly resisted, sometimes successfully, some of the Administration's demands. *See id.* at 1165–66.

173. *See generally* Mark Eckenwiler, U.S. Dep't of Justice, Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001, 701 PLI/PAT 1227, 1234 (2002) [hereinafter DOJ Field Guidance] (providing the government's perspective); *see also* Cindy Cohn, EFF Analysis of the Provisions of the USA Patriot Act that Relate to Online Activities, 701 PLI/PAT 1201 (2002) (critiquing several provisions' impact on electronic privacy rights).

174. *See* USA PATRIOT Act § 209, 115 Stat. 272, 283 (2001); DOJ Field Guidance, *supra* note 173, at 1232–33.

attributes, such as electronic mail addressing information, when that was previously unclear.[175]

Other than the Patriot Act, Congress has not significantly altered the statutory scheme just described. In 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA")[176] to ensure that providers of telecommunications services maintained the accessibility of their systems to wiretapping notwithstanding the introduction of digital communications technologies.[177] That Act did not significantly change the substantive restrictions on law enforcement surveillance.[178]

Unlike surveillance to detect terrorist threats in Switzerland,[179] surveillance for foreign intelligence gathering and to prevent terrorism in the United States has significantly fewer constraints.[180] Agents who operate under the Foreign Intelligence Surveillance Act[181] have considerably more discretion and may use all the surveillance tools of traditional law enforcement agents, subject to review only by a secretly impaneled court whose proceedings are not public.[182] Again, in contrast to Switzerland, where the ISA permits only the review of publicly available information, in the United States, extensive and secret surveillance generally proceeds without notice to the targets.[183]

---

175. The Patriot Act established that pen registers could be used to obtain "dialing, routing, addressing or signaling information" associated with electronic communications when it was previously unclear whether pen registers could obtain only the attributes of traditional telephone calls. *See* USA PATRIOT Act § 216, 115 Stat. 272, 288–90 (2001) (amending 18 U.S.C. § 3127(3)); DOJ Field Guidance, *supra* note 173, at 1233–34.

176. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012) and in scattered sections of 18 U.S.C.).

177. *See generally* Freiwald, *supra* note 111 (describing the debates that accompanied the passage of CALEA).

178. *See id.*

179. *See supra* text accompanying notes 146–49.

180. A thorough discussion of foreign intelligence surveillance is beyond the scope of this Article. *See generally* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS (2007) (presenting the law governing investigations for national security rather than domestic law enforcement purposes); Peter Swire, *The System of Foreign Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004) (reviewing the history of foreign surveillance laws and practices).

181. Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801–1862 (2012) (covering the use of electronic surveillance and other investigatory techniques to pursue foreign intelligence).

182. *See* KRIS & WILSON, *supra* note 180, § 27; William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 89 (2000).

183. *See* KRIS & WILSON, *supra* note 180, § 31:2 (discussing how FISA applications and orders may not have to be disclosed to surveillance targets if the Attorney General files an

VI. COMMON ELEMENTS IN SURVEILLANCE PROCEDURES

Before detailing Swiss and U.S. surveillance regulations side-by-side, it helps to understand the types of procedures that regulate law enforcement surveillance. The following Sections describe the different procedural mechanisms and the range of choices among them that legislators have to choose from when drafting surveillance regulations. They cover such topics as the depth of judicial scrutiny and the scope of remedies for victims of improper surveillance.

A. LEVELS OF OVERSIGHT

CrimPC, which divides surveillance into six different methods,[184] requires surveillance under it to meet one of three different authorization processes depending on the intrusiveness of the surveillance method. For the most intrusive methods, CrimPC imposes the highest level of scrutiny, under which the Compulsory Measures Court[185] must confirm the propriety of the public prosecutor's order for police surveillance.[186] By contrast, the police may conduct the least intrusive methods of surveillance for up to a month without any prior judicial or prosecutorial authorization.[187] Intermediately intrusive methods require the prosecutor's prior authorization before law enforcement may conduct surveillance.[188]

affidavit stating disclosure would harm national security). In response to controversial large-scale monitoring programs conducted in the wake of the September 11th attacks, Congress amended FISA to provide immunity to service providers who aided such monitoring. *See* FISA Amendments Act of 2007, § 802, Pub. L. No. 110-261, 122 Stat. 2435, codified at 50 U.S.C. § 1885(a) (2012) (granting retroactive immunity to service providers). Recent disclosures of the extensive monitoring of domestic communications in the name of foreign intelligence came out too close to press time for the authors to assess them in this article. *See* The NSA Files, THE GUARDIAN, www.guardian.co.uk/world/the-nsa-files (last visited July 10, 2013) (compiling articles discussing, among other related pieces, the information revealed to the public by Edward Snowden).

184. The six methods are surveillance of post and telecommunications, acquisition of user identification data, use of technical surveillance equipment, surveillance of contacts with a bank, use of undercover agents, and physical observation of people and places accessible to the general public. *See infra* Part VI.

185. CrimPC established independent Compulsory Measures Courts to oversee law enforcement surveillance requests and perform other duties. *See supra* note 143.

186. If the Court does not confirm the prosecutor's order, the surveillance must terminate, and the results obtained from it cannot be used.

187. Police may continue surveillance after a month if they obtain the public prosecutor's authorization.

188. Both the police and the public prosecutor are considered to be law enforcement authorities. CRIMPC arts. 15–16.

U.S. law also requires a law enforcement agent to obtain the approval of a member of the judiciary, such as a trial judge or magistrate judge, before conducting intrusive forms of surveillance.[189] Fourth Amendment cases have noted the importance of having "a neutral magistrate" pre-approve searches and seizures to constrain the executive's zeal for law enforcement.[190]

Various members of the executive branch must also approve some surveillance methods before they may commence. Approval by high-level officials in the executive branch helps to inhibit unjustified investigations.[191] In some cases, the Attorney General himself must initially approve of a surveillance practice, although sometimes lower-level senior officials may approve. The requirement of high-level executive branch approval usually accompanies rather than substitutes for the requirement of judicial approval.

For a large number of surveillance methods, however, agents may conduct surveillance without submitting to any judicial oversight. For example, agents in the United States conduct a great deal of surveillance by issuing subpoenas, or demands for records.[192] In those cases, judges review the surveillance only when the target learns of it and brings a challenge.[193]

As this Article will discuss, ECPA treats some surveillance methods as insufficiently intrusive to require judicial oversight. In addition, surveillance

---

189. In some emergency situations, agents may conduct surveillance first and then obtain approval afterwards, with the statute specifying how much time the agent has to obtain judicial approval. *See, e.g.*, 18 U.S.C. § 2518(7) (2012) (permitting emergency wiretap orders which last up to forty-eight hours in limited circumstances).

190. *See* Dalia v. United States, 441 U.S. 238, 255–56 (1979).

191. *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 739 (FISC Ct. Rev. 2002) (noting that the requirement of written approval from senior officials provides an important check on arbitrariness).

192. *See* James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data,* 970 PLI/PAT 687, 702 (2009) (describing how prosecutors can issue subpoenas without any judicial involvement to access a variety of modern communications based on relevance to an investigation); *see also* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 824–25 (2005) ("The Supreme Court has applied *Miller*'s rationale to phone company records and loan applications, and lower courts have used it to uphold subpoenas for personal records from medical institutions, auditors and accountants, trustees in bankruptcy, and government institutions." (footnotes omitted)).

193. Department of Justice lawyers have argued that the when agents deliver a subpoena or similar order to a service provider, the subject of the records they seek may contest only on the basis that the subpoena or order seeks irrelevant information or that compliance would be too burdensome for the party who has to furnish the records, notwithstanding the subject's privacy interest in the records. *See* Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored Email: The Law Professors' Brief in* Warshak v. United States, 41 U.S.F. L. REV. 559, 579–85 (2007) (describing and responding to the government's argument in the context of the compelled disclosure of stored email).

that proceeds outside of the bounds of ECPA (and related statutes), either by virtue of not being historically covered, or by virtue of being too new to be included, can proceed without any judicial review, so long as a court has not yet held that the Fourth Amendment requires regulation.[194]

B. CONDITIONS

1. Procedural Hurdles

CrimPC requires that agents have some suspicion of criminal activity before they may undertake surveillance; it does not permit preventative monitoring, where government agents use surveillance to prevent crimes from occurring in the first place.[195] Agents cannot use surveillance to create suspicion, as for example in so-called fishing expeditions.[196] Surveillance may not be undertaken unless a criminal offense has already been committed or is currently being committed;[197] it aims to discover the perpetrator or gather evidence related to a committed offense.[198] Swiss law supplies an equivalent to our probable cause standard by forbidding surveillance unless there is a strong suspicion that an offense has been committed. Physical observation, which may proceed according to an intermediate standard lower than strong suspicion but higher than simple suspicion,[199] is the only method that does not proceed according to the strong suspicion standard.[200]

Procedural hurdles in the United States vary considerably in terms of the burden they impose on law enforcement agents and the scope of discretion

194. Note that courts have limited jurisdiction, so only the Supreme Court can issue decisions that affect the entire United States. A Sixth Circuit decision requiring a warrant for access to stored email, for example, affected only investigations taking place in that Circuit. *See infra* text accompanying notes 293–97.

195. *But see* text accompanying notes 145–48 (noting that intelligence monitoring of public information can be used preventatively).

196. Peter Goldschmid, Der Einsatz technischer Überwachungsgeräte im Strafprozess: Unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern [Use of Technical Surveillance Equipment for Criminal Investigation: with Particular Attention to the Rules of Criminal Procedure in Canton of Bern] 95 (2001); HANSJAKOB, *supra* note 132, at 145.

197. CrimPC regulates the surveillance law enforcement conducts during an inquiry proceeding, which occurs when a criminal investigation is open and there is an (sometimes unidentified) accused person.

198. Acts in preparation for the commission of some particularly serious offenses are themselves independent offenses. They are intentional homicide (CP art. 111), murder (CP art. 112), serious assault (CP art. 122), robbery (CP art. 140), false imprisonment and abduction (CP art. 183), hostage taking (CP art. 185), arson (CP art. 221), genocide (CP art. 264), crimes against humanity (CP art. 264a) and war crimes (CP art. 264c–264h).

199. "Simple suspicion" is the standard for opening an investigation that does not use surveillance. CRIMPC art. 309.

200. *See infra* Section VII.G.1.

they afford to reviewing judges to deny government applications for surveillance. For the most restricted surveillance methods, judges require government agents to establish probable cause to believe the target "is committing, has committed, or is about to commit" a particular offense and that the surveillance will obtain incriminating communications about that offense.[201]

Some surveillance methods have standards that are much easier to meet than probable cause. One intermediate standard requires that the surveillance will yield information relevant to an ongoing criminal investigation instead of yielding evidence of criminal activity. Another even lower intermediate standard requires that the information sought will be relevant to a law enforcement inquiry. Standards are made less demanding both by using language with a broader scope, as just described, and also by limiting the judge's review to one that checks a surveillance application for completeness rather than conducting an independent review of the facts.[202] The lowest level of judicial review applies when judges review challenges to subpoenas. The recipient of a subpoena may generally challenge it only on the basis that it seeks irrelevant information or that compliance would be too burdensome for the party who has to furnish the records.[203]

Of course procedural standards that judges impose come into play only when judges themselves have a role in the surveillance process. Because a large amount of surveillance proceeds in the United States without any judicial review, or with unlikely and limited judicial review as in the case of subpoenas, judges are much less able to block problematic surveillance in the United States than in Switzerland.

2. Predicate Offenses

Although different methods of surveillance require different levels of seriousness, CrimPC permits law enforcement surveillance to investigate only serious criminal offenses. Agents may use some methods of surveillance only

201. *See* 18 U.S.C. §§ 2516(1), 2518(3)(a) (2012) (establishing the requirement under the Wiretap Act). That hurdle may be raised higher by a requirement that the communications device being surveilled has itself been used in the crime. *See* 18 U.S.C. § 2518(3)(b).

202. 18 U.S.C. § 3122(b) (2012).

203. A target may challenge a subpoena only when it is unreasonable or oppressive. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1191 (9th Cir. 2010) (en banc) (Bea, J., concurring in part and dissenting in part); Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J. L. & TECH. 543, 547 (2011) (listing as "most widely accepted test for [the] reasonableness" of a subpoena: (1) whether the requested information is relevant, (2) whether the request is reasonably particularized, (3) whether the information requested covers a reasonable period of time).

to investigate a specific list of serious crimes,[204] while they may use others to investigate a wider range of crimes.

Similarly, some surveillance methods in the United States may be used only to investigate certain types of offenses, such as particularly serious crimes. Other statutes, however, permit surveillance methods for a wide variety of crimes or place no limit on the types of crimes that justify certain surveillance methods.

3. Other Limits

All Swiss surveillance practices must respect the subsidiarity principle and the need for proportionality between means and end. Subsidiarity requires that other less intrusive investigatory activities already conducted have not been successful or have no prospect of success; surveillance must not be the first investigatory activity.[205] Proportionality requires that the scope and duration of surveillance be as limited as possible. It means that the more invasive the surveillance method, the harder it will be to pass muster.[206] When courts conduct proportionality review they consider the seriousness of the offense, the invasion of privacy, the likelihood of success, and the length and type of the surveillance.

Unlike in Switzerland, where the subsidiarity rules apply to all surveillance covered by CrimPC, only surveillance methods covered by the Wiretap Act (wiretapping and bugging) require that less intrusive methods have failed or been shown to be infeasible.[207] Similarly, only the Wiretap Act requires that agents minimize the collection of non-incriminating conversations.[208] For all other surveillance methods in the United States, such as the vast majority of techniques that apply to modern communication methods, ECPA does not require that agents either minimize the collection of non-incriminating information or exhaust other types of surveillance

204. Several scholars have criticized the lists of offenses for reflecting politics rather than legal analysis. *See, e.g.*, Sträuli, *supra* note 134, at 124–27; HANSJAKOB, *supra* note 132, at 154–76.

205. *See* HANSJAKOB, *supra* note 132, at 152–54; NIKLAUS SCHMID, SCHWEIZERISCHE STRAFPROZESSORDNUNG, PRAXISKOMMENTAR [SWISS CRIMINAL PROCEDURE CODE: PRAXISCOMMENTARY] 505–06 (2009).

206. Other limits restrict surveillance to those set out in the order, see CRIMPC art. 278, and protect professional secrets. *See* CRIMPC art. 271; Sylvain Métille, *Le secret professionnel à l'épreuve des mesures de surveillance prévues par le CPP* [*Privileged information and surveillance ruled by CrimPC*], 03 MEDIALEX 131–37 (2011).

207. *See* 18 U.S.C. § 2518(3)(c) (2012). These requirements also apply to video surveillance in some cases. *See infra* note 365.

208. *See* 18 U.S.C. § 2518(5). Judges in individual cases may impose their own limits, but those appear to be rather rare.

first.[209] Some surveillance methods are, however and like in Switzerland, subject to a time limit that may be renewed upon a sufficient showing.[210]

The United States has no general requirement of subsidiarity or proportionality. As we shall see in the next Section, the lack of any proportionality requirement probably contributes the most to the comparatively lower restrictions on government surveillance in the United States. The other two significant factors are the ability of American agents to conduct surveillance without an authorizing statute and the lack of notice to targets for many types of surveillance.[211]

C. NOTICE

CrimPC requires notice for all methods of surveillance.[212] Swiss commentators view both the Swiss Constitution and the ECHR as mandating that law enforcement notify the targets of surveillance.[213] Notice provides the only official way for a target to learn about surveillance and opens the way for her to defend her rights.[214]

CrimPC requires notice even when surveillance does not provide any usable information, but notice may be postponed or even omitted if necessary for the protection of overriding public or private interests.

---

209. *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 463 (5th Cir. 1994) (explaining that only the interception provisions of the federal surveillance statutes have minimization requirements because agents can use keyword searching when going through stored communications). *But see infra* Section VII.D.2 (discussing silent video surveillance which federal appellate courts have found subject to the last resort, minimization, particularity, and limited duration requirements as a matter of constitutional, rather than statutory, law).

210. *See, e.g.*, 18 U.S.C. § 3123(c) (2012) (setting a limit of sixty days for investigations using pen registers unless the orders are renewed).

211. *See, e.g.*, Smith, *supra* note 91 (discussing lack of notice for much electronic surveillance, because of gag orders imposed on service providers, the sealing of judicial orders, and delays in conveying notice even when notice is required).

212. *See* SYLVAIN MÉTILLE, MESURES TECHNIQUES DE SURVEILLANCE ET RESPECT DES DROITS FONDAMENTAUX EN PARTICULIER DANS LE CADRE DE L'INSTRUCTION PÉNALE ET DU RENSEIGNEMENT [SURVEILLANCE MEASURES AND FUNDAMENTAL RIGHTS, WITH PARTICULAR ATTENTION TO CRIMINAL AND INTELLIGENCE INVESTIGATIONS] 182-183 (2011); CRIMPC arts. 279, 298. CrimPC calls notice "communication."

213. *See* HANSJAKOB, *supra* note 132, at 310; PIQUEREZ, *supra* note 134, at 627; Conseil Fédéral, Message relatif à la modification de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure [Message related to the modification of the Internal Security Act], FF 4773, 4838 (2007).

214. Sylvain Métille, Mesures de surveillance secrètes: le rôle de l'information dans la protection des droits de l'individu [Secret surveillance measures: Notice as a protection of the rights of the surveilled person], 29 PLAIDOYER (2011).

Typically the court will permit notice to be postponed when notice without delay will ruin another ongoing investigation, but CrimPC requires that recourse to this exception be limited and instructs that courts should rarely permit notice to be omitted altogether.[215] The information obtained from surveillance may not be used if notice of that surveillance has not been provided to the target. After receiving notice, a surveillance target may contest violations of law including misuse or incorrect use of discretion and incomplete or incorrect establishment of the facts of the case before cantonal (trial) courts.[216]

Regardless of its result, the target should be informed of the surveillance by the public prosecutor as soon as possible and at the latest by the conclusion of the preliminary proceedings, which is when the public prosecutor transmits the case to the judge for a trial. Notice must identify the accused person and furnish the list of accused offenses, the reasons for surveillance, the nature and duration of surveillance, the identity of the person who granted the authorization, the conditions imposed on the surveillance, and the rights of the target as a result of the surveillance.[217] CrimPC provides much more extensive notice, and much more often, than does analogous law in the United States. Under American law, evidence obtained from surveillance but not subject to criminal discovery rules, or obtained about those who are not prosecuted, will never come to the target's attention unless an applicable statute requires notification.[218]

ECPA provisions vary in terms of who must receive notice, when agents must provide that notice, and the circumstances under which agents may delay providing notice.[219] ECPA does not require notice for many

215. CRIMPC art. 279.

216. CRIMPC art. 279, para. 3, art. 393, para. 2. Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale [Message about Unification of Criminal Procedure Law], FF 1057–1296 (2006); André Kuhn, *La procédure pénale suisse selon le futur CPP unifié*, 128 REVUE DE DROIT SUISSE 161–62 (2009).

217. SCHMID, *supra* note 205, at 525; HANSJAKOB, *supra* note 132, at 315–16.

218. *See* Smith, *supra* note 91, at 615–16 n.82 (doubting that criminal defense lawyers will learn of many online surveillance orders and noting that uncharged targets will not learn of much surveillance).

219. Several commentators have recommended that the United States amend its electronic surveillance statutes to provide better notice to targets. *See, e.g.*, Smith, *supra* note 91, at 332 ("ECPA should be amended to require notice to the target of any electronic surveillance order, including the customer, subscriber, or user of a targeted phone or Internet service."); Stephanie Pell & Christopher Soghoian, *Can You See Me Now?: Towards Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 185–89 (2012) (recommending notice when law enforcement obtains location data); Gruenspecht, *supra* note 203, at 561 (advocating for notice to be given to data creators instead of just third party intermediaries in the context of cloud computing).

surveillance methods and also precludes service providers that are involved in some surveillance methods from notifying targets.[220] Unregulated surveillance methods may, by definition, proceed without notice to targets.

D. CONSEQUENCES OF ILLEGAL SURVEILLANCE

CrimPC entitles the victim of unlawful surveillance to request from the court reasonable compensation and reparation for non-pecuniary loss such as emotional distress. CrimPC provides damages for economic losses but not punitive damages.[221] Both the accused people and third parties are entitled to compensation.[222]

Under CrimPC, data acquired using some surveillance methods without authorization[223] must be completely excluded from trial under what is known as an exclusionary remedy.[224] Under that approach, findings may not be used and data must be destroyed immediately.[225] For less intrusive surveillance methods like physical observation, CrimPC makes the results of unauthorized investigations relatively unusable: findings can be used only if they are necessary to solve serious offenses.[226] If the evidence could have been obtained legally, the court must weigh the competing interests of the prosecution in confirming suspicions and of the accused targets in protecting their personal rights.[227]

---

220. *See* Smith, *supra* note 91, at 610–14. Many orders to conduct surveillance are issued under seal (to be kept secret from the public, including the target), and remain under seal indefinitely. *See* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177 (2009) [hereinafter Smith, *Kudzu in the Courthouse*].

221. CRIMPC arts. 431, 434.

222. *Id.*

223. Surveillance is unauthorized when authorization has not been requested as needed, when the Compulsory Measures Court has refused to authorize it, and when surveillance proceeds past when it is authorized. CRIMPC arts. 277, 281, para. 4, 289, para. 6; TF, May 3, 2005, 131 ATF I 272, 281 (Switz.); HANSJAKOB, *supra* note 132, at 250–53 (2006). Whether or not an authorization would have been granted if requested is irrelevant. *See* TF, Oct. 9, 2007, 133 ATF IV 329, para. 4.4 (Switz.).

224. The ECtHR may opine on the fairness of the proceedings as a whole, including the way in which evidence was obtained. Schenk v. Switzerland, App. No. 10862/84, Eur. Ct. H.R. (1988) (hudoc.echr.coe.int).

225. The ECtHR has held that the exclusion at trial of evidence gained through any unlawful surveillance is a necessary but not sufficient remedy for the violation of the right to private life that may have occurred. Khan v. The United Kingdom, App. No. 35394/97, § 44, Eur. Ct. H.R. (2010) (hudoc.echr.coe.int); Taylor-Sabori v. The United Kingdom, App. No. 47114/99, §§ 22–24, Eur. Ct. H.R. (2002) (hudoc.echr.coe.int).

226. Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale [Message about Unification of Criminal Procedure Law], FF 1057, 1163 (2006).

227. TF, Sept. 7, 1983, 109 ATF Ia 244, para. 2.3 (Switz.).

In the United States, unlawful surveillance that violates the Fourth Amendment gives rise to a claim for money damages[228] and the protections of the suppression remedy.[229] The latter prohibits any evidence obtained by or derived from the unlawful surveillance from being introduced at the trial of the target of the surveillance. The suppression remedy is designed to deter law enforcement agents from acting unlawfully, but it is not always available.[230]

As discussed earlier, however, the Supreme Court has limited the Fourth Amendment's protection to that subcategory of investigations that intrude upon a target's "reasonable expectations of privacy" and that therefore constitute a "search." So far the Supreme Court has considered only wiretapping, bugging, and the installation and use of a GPS tracking device to be surveillance practices regulated under the Fourth Amendment.[231]

As distinct from the Constitution, the statutes that govern specific surveillance methods provide a range of remedies for noncompliance. Only the Wiretap Act provides a statutory suppression remedy; no such remedy is available for the improper interception of electronic communications.[232] As to damages, ECPA provides varied levels of monetary relief and the possibility of punitive damages and attorney's fees for some surveillance methods.[233] In limited cases, ECPA imposes criminal punishment or administrative discipline on law enforcement agents who conduct unlawful surveillance.[234] The executive branch rarely prosecutes its own agents, however.

---

228. A victim must bring a claim under 42 U.S.C. § 1983 (2012) (state actors) or the authority of *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971) (federal actors), to obtain such damages. *See, e.g.*, Warshak v. United States, 532 F.3d 521, 528, 532 (6th Cir. 2008) (expressing disapproval of target's pursuit of injunctive relief rather than a civil damages claim).

229. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 28 (2001) (reversing appellate court's denial of defendant's motion to suppress after finding that law enforcement agents conducted a "search" without a warrant).

230. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288–92 (6th Cir. 2010) (denying suppression remedy for constitutional violation when officers relied in good faith on statute that was not plainly unconstitutional).

231. *See supra* Section III.B. The Supreme Court has also treated law enforcement's use of a thermal imaging device to detect the heat emanating from a house as a search under the Fourth Amendment. Kyllo v. United States, 533 U.S. 27 (2001). As we discuss more, *infra* Section VII.G.2, the case's holding is limited. In the United States, moreover, because so few visual investigations require warrants, we tend not to think of them as electronic surveillance.

232. 18 U.S.C. §§ 2515, 2518 (2012).

233. 18 U.S.C. §§ 2520, 2707 (2012).

234. *Id.*

E. REPORTING

CrimPC does not require any particular reports about law enforcement surveillance practices. Information about surveillance practices may be available from the police or other bodies involved in surveillance, including from targets who have been notified of it. Apparently as a voluntary matter, some authorities have published reports about the monitoring of mail and telecommunications.[235] In the United States, Congress receives periodic reports about some surveillance methods. Such reporting facilitates the oversight that may constrain executive branch abuses.[236] Congress may choose to revise surveillance statutes in light of information it receives in surveillance reports. The surveillance statutes vary in how much detail must be provided to Congress, and some surveillance methods require no reporting at all. Compliance with the reporting requirements varies as well.[237]

VII. SURVEILLANCE REGULATION COMPARED

A. INTRODUCTION

Because CrimPC represents a modern and comprehensive statute designed to regulate all surveillance methods in one statute, we have organized the following discussion according to its six categories. CrimPC requires extensive judicial oversight for the most invasive techniques: surveillance of post and telecommunications,[238] use of technical surveillance devices,[239] surveillance of contacts with a bank,[240] and undercover operations.[241] CrimPC treats physical observation[242] as the least invasive method, requiring the least oversight by either a judge or public prosecutor. The acquisition of user identification data[243] is a subcategory of post and telecommunications surveillance and is considered less invasive than that method but more invasive than physical observation. As the following

235. *See Statistical Data*, POST AND TELECOMMUNICATIONS SURVEILLANCE SERVICE, www.li.admin.ch/en/themes/stats.html (last visited Feb. 2, 2013).

236. *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 741 n.25 (FISC Ct. Rev. 2002) (citing Senate report accompanying FISA).

237. Christopher Soghoian, *The Law Enforcement Surveillance Reporting Gap*, http://ssrn.com/abstract=18066628 (discussing how much modern electronic surveillance takes place without being publicly reported).

238. CRIMPC art. 269ss; *see infra* Section VII.B.

239. CRIMPC art. 280ss; *see infra* Section VII.D.

240. CRIMPC art. 284ss; *see infra* Section VII.E.

241. CRIMPC art. 286ss; *see infra* Section VII.F.

242. CRIMPC arts. 282–283ss; *see infra* Section VII.G.

243. CRIMPC art. 273ss; *see infra* Section VII.C.

discussion will show, ECPA[244] covers only a subset of the methods that CrimPC does. For some methods, such as tracking contacts with a bank, differences in other regulations and practices explain and make relatively uncontroversial why CrimPC but not ECPA covers them.[245] For other methods, however, such as the use of undercover government agents, the utter lack of regulation by U.S. law contrasts sharply with the many restrictions that Swiss law imposes.[246] The most glaring lack of coverage pertains to new methods of surveillance, which law enforcement agents in the United States have free rein to use until a court or legislature acts, but which require specific, legislative authorization in Switzerland. Regarding those methods of surveillance that both countries regulate, CrimPC clearly emerges as much less complex and much more comprehensive in its restrictions on law enforcement surveillance.

B. MONITORING OF POST AND TELECOMMUNICATIONS

1. In Switzerland

Swiss law enforcement agents must follow the most stringent procedures when conducting surveillance of an accused person's mail and telecommunications.[247] The pertinent category under CrimPC has an extremely wide scope due to its technology-neutral wording; it includes the interception of communications made by phone call, email, fax, text, pager, and Voice over IP, as well as the acquisition of any information in letters, parcels, and stored emails.[248] Surveillance conducted under this category may proceed in real time, for example when agents conduct a traditional wiretap

244. Technically, the Wiretap Act, which ECPA amended to cover electronic communications, still regulates the surveillance of traditional telephone calls and the installation of bugs. *See infra* Section VII.B.2.

245. *See infra* Section VII.E.

246. *See infra* Section VII.F. For a discussion of similar strong differences between U.S. surveillance law and that of other European countries, see Christopher Slobogin, *Transnational Law and Regulation of the Police,* 56 J. LEGAL EDUC. 451, 451–53 (2006) ("[T]ransnational law can provide interesting alternatives that might be worthy of adoption in the United States . . . . Denmark requires warrants for *any* undercover activity that requires infiltration, in stark contrast to our law essentially giving the police carte blanche in their undercover work.").

247. CrimPC permits the surveillance of the accused person's mail and calls and, in some cases, those of a third person directly connected to the accused. CRIMPC arts. 269–270ss.

248. August Biedermann, Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000 [Surveillance of Post and Telecommunications Act (SPTA) of October 6, 2000], 120 REVUE PÉNALE SUISSE [SWISS CRIMINAL LAW REVIEW] 106 (2002); PIQUEREZ, *supra* note 134, at 615; HANSJAKOB, *supra* note 132, at 71–72; Sträuli, *supra* note 134, at 95–112.

of a telephone call or intercept an email, or it may proceed retroactively as when the police compel a third party service provider to produce an email from its system or a letter from its facilities. The Swiss recognize that the latter intrudes on the secrecy of communications because it may proceed without the person of interest being aware of it.[249]

The Compulsory Measures Court must approve all surveillance under this category and must confirm that the public prosecutor has a strong suspicion that an offense has been committed.[250] The offense must come from a list of serious predicate offenses.[251] Surveillance requests must be quite detailed[252] and they must establish, under the subsidiarity principle, that other investigatory activities have not been successful or have no likelihood of success.[253] As with all forms of surveillance in Switzerland, in determining whether to authorize surveillance, the court shall ensure that the scope and duration of the surveillance is as limited as possible to respect the principle of proportionality.[254]

The target must receive notice whenever the government conducts the surveillance of his mail or telecommunications.[255] Victims of unlawful monitoring of their post and telecommunications are entitled to damages and violators face criminal prosecution.[256] Victims are also entitled to have any

249. Police acquisition of such stored communications through search of a home, a computer, or a person, rather than from a service provider, or acquisition of computer materials directly from an accused person or his property constitutes a search and seizure. CRIMPC art. 263ss; Rhyner & Stüssi, *Kommentar zu Art. 269–279 StPO*, *supra* note 135, at 443–45; *see* HANSJAKOB, *supra* note 132, at 81–85; Sträuli, *supra* note 134, at 99–100, 107–08.

250. CRIMPC arts. 269, 273–274.

251. CRIMPC art. 269, para. 2.

252. They must include the reasoning supporting the surveillance and must describe the object of surveillance, the identity of the target, the offense being prosecuted, the kind of surveillance proposed, and the date and time of the beginning and end of the surveillance. *Ordonnance sur la surveillance de la correspondence par poste et telecommunication* [Ordinance on the Surveillance of Post and Telecommunications] Arts. 11, 15, 23 (Oct. 31, 2001), RS 780.11; HANSJAKOB, *supra* note 132, at 403–08, 412–24, 443–49.

253. In practice, police officers first recommend that surveillance be undertaken to the public prosecutor, who then makes a written order. Instead of the police, the Post and Telecommunications Surveillance Service ("PTSS") mainly coordinates and transmits the surveillance order from the public prosecutor to the pertinent service providers.

254. Surveillance orders are generally granted for up to three months, though the court may also impose its own requirements.

255. The Compulsory Measures Court may consent to notice being postponed or omitted. In the case of physical observation, the prosecutor may consent to notice being postponed or omitted. If notice is not given, however, the results of surveillance may not be used. *See supra* text accompanying notes 213–15.

256. CP art. 179ss.

evidence obtained from unauthorized surveillance[257] or obtained without their notice of surveillance excluded from trial under the exclusionary rule.[258]

2. In the United States

a) Several Distinctions

For real-time surveillance like that covered by the above category, laws in the United States distinguish between acquisition of the contents of communications made by mail, communications made by wire, and electronic communications. Unlike in Switzerland, ECPA treats the acquisition of electronic communications in electronic storage as less deserving of protection than real-time acquisition and subjects the former to a set of weaker restrictions.[259] Commentators have criticized ECPA for incorporating many distinctions that no longer make sense, if they ever did, and that make the law unduly complex.[260]

As in Switzerland, United States law treats the acquisition of documents and communications directly from a person's home or computer as a search or seizure. Such acquisitions are subject to a standard Fourth Amendment warrant requirement in most cases. The discussion that follows will focus on acquisitions from third parties, which, as in Switzerland, Congress has treated as a form of surveillance.[261]

b) Interception of Postal Mail Contents

First class mail and sealed packages in the United States have long been protected against warrantless interception.[262] To acquire mail and packages,

257. *See supra* Section VI.D.

258. CRIMPC art. 279, para. 2 lit a. Documents and data storage devices must be destroyed immediately and intercepted mail should be delivered.

259. *See supra* Section III.B (discussing the origins of these distinctions in Supreme Court cases from the 1970s).

260. *See, e.g.*, Ohm, *supra* note 4, at 1551 ("First, ECPA is confusing; epically confusing; grand-champion-of-the-U.S. Code confusing . . . . ECPA's complexities confuse judges who then make a mess of our understanding of the Act."); Dempsey, *supra* note 192, at 704–05, 722 (criticizing the complexity of the online surveillance rules and recommending a warrant standard for all stored email).

261. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 126 (3d ed. 2009) [hereinafter CCIPS SEARCH MANUAL], *available at* www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (explaining that ECPA does not apply to emails that "are not stored on the server of a third-party provider" of services).

262. *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 49–71 (2000) (reviewing history of protection of

agents must establish probable cause to a judge and also deliver notice to the target of the surveillance.[263] Because of the Fourth Amendment regulation, victims of unlawful acquisition of these items have a suppression remedy available to them.[264] In addition, a federal statute makes tampering with mail a criminal offense.[265] No statute provides other remedies for victims of unlawful mail surveillance, however.

c) Interception of Wire Communications Content

Wiretapping, or the real-time interception of the contents of wire communications,[266] is subject to the highest procedural restrictions, which in the United States are in the Wiretap Act.[267] Under the Act, a member of the judiciary oversees all phases of law enforcement surveillance. Applications for approval, which only high level officials can make,[268] must persuade the reviewing judge of probable cause to believe the target has committed or will commit a particular predicate offense and that the surveillance will obtain incriminating communications about that offense.[269]

The Wiretap Act provides for a U.S. version of subsidiarity, under which the reviewing judge must be convinced that the information sought may not be obtained by normal investigative methods and agents must minimize the interception of non-incriminating communications.[270] Surveillance orders are limited to thirty days, unless renewed, and the wiretapping must end when the information sought is obtained.[271] Together, these attempts to limit the scope and duration of wiretapping parallel the Swiss proportionality principle, although the Wiretap Act does not provide for the explicit

mail); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1142–43 (2002) (same).

263. *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (describing warrantless searches of sealed packages and letters as "presumptively unreasonable"); *Ex parte* Jackson, 96 U.S. 727, 733 (1877). The warrant requirement does not protect fourth class mail and the information visible on the outside of envelopes. WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.2(a) (3d. ed. 2007).

264. *See* United States v. Villarreal, 963 F.2d 770 (5th Cir. 1992).

265. 18 U.S.C. § 1703 (2012).

266. *See* 18 U.S.C. § 2510(1) (2012) (defining "wire communication").

267. For an overview of the Wiretap Act requirements, see *In re* Sealed Case, 310 F.3d 717, 739–40 (FISC Ct. Rev. 2002).

268. 18 U.S.C. § 2516(1), (2) (2012).

269. 18 U.S.C. §§ 2516(1), 2518(3), (8) (2012). As in Switzerland, applications under the Wiretap Act require detailed information about facts and circumstances that support the request for an order. 18 U.S.C. § 2518(1).

270. 18 U.S.C. § 2518(3)(c).

271. 18 U.S.C. § 2518(5).

balancing incorporated into that principle.[272] As subsequent sections will show, most of the other modern surveillance practices in the United States proceed without consideration of the principles of proportionality or subsidiarity.

The Wiretap Act incorporates significant provisions to ensure transparency. The reviewing judge must provide notice to anyone named in an application and to anyone else the judge deems appropriate.[273] When Congress passed the Wiretap Act, it viewed the notice provision, in combination with civil remedies, as an important check on unlawful practices in that the community would be alerted if wiretaps were not reasonably employed.[274] In addition, Congress provided for detailed reports on the numbers of orders issued under the Wiretap Act and their efficacy in fighting crime.[275] Based on those reports, the Administrative Office of the United States Courts is supposed to make public a Report on Wiretapping each year.[276]

Courts may punish violations of the Wiretap Act with significant fines and jail time.[277] In addition, any person whose communications were intercepted, disclosed, or used in violation of the Act may bring civil claims for damages against those who violated their rights.[278] Under the Wiretap Act, a victim may receive attorney's fees, punitive damages, and actual or statutory damages.[279] The Wiretap Act provides a statutory suppression remedy to victims, which provides a complete exclusionary remedy.[280]

Between the significant procedural hurdles imposed on wiretap surveillance, the high level of judicial oversight, and the severe consequences for illegal investigations, the Wiretap Act sets the high water mark for restrictions on surveillance in the United States. Judicially-guaranteed notice to the target and the transparency of the public and congressional reports encourage victims to exercise their rights and obtain their remedies.

d) Interception of Electronic Communications Content

ECPA regulates the interception of modern communications such as email and cell phone calls the same way it regulates traditional wiretaps with a

272. *See supra* text accompanying notes 204–05.
273. *See* 18 U.S.C. § 2518(8)(d), (9).
274. *See* S. REP. NO. 90-1097, at 105 (1968), *reprinted in* 1968 U.S.C.C.A.N 2112, 2194.
275. *See* 18 U.S.C. § 2519 (2012).
276. *See* 18 U.S.C. § 2519(3); Soghoian, *supra* note 237, at 5.
277. 18 U.S.C. § 2511(4) (2012).
278. *See* 18 U.S.C. § 2520(a) (2012).
279. *See* 18 U.S.C. § 2520.
280. *See* 18 U.S.C. § 2515 (2012).

few significant differences.[281] The most significant difference is that when ECPA extended the Wiretap Act's provisions from "wire communications" to "electronic communications,"[282] it excluded the statutory suppression remedy.[283] Victims of unlawful interceptions of their electronic communications can have evidence obtained thereby excluded from trial only if they succeed in showing a Fourth Amendment violation.[284] The lack of a suppression remedy no doubt reduces the number of cases brought to vindicate rights under ECPA, even when the rights and remedies are otherwise at their height, as they are with the interception of electronic communications contents.[285]

All of the restrictions described above regarding judicial oversight, procedural hurdles, the last resort method, minimization, notice, and time limits apply to the interception of electronic communications, as do the civil remedies, criminal penalties, and reporting requirements. Agents may use electronic communications interceptions for only some crimes[286] and must get executive branch approval before doing so.[287] Government litigators have convinced courts to interpret "intercepts" to mean "acquisitions contemporaneous with transmission" and therefore to exclude the

281. Congress has expressed as its goal in crafting ECPA ensuring the privacy of electronic communications and extending all of the Wiretap Act's protections to new communications media. *See* H.R. REP. NO. 99-647, at 17–19 (1986); S. REP. NO. 99-541, at 25 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

282. 18 U.S.C. § 2510(12) (2012) (defining "electronic communication").

283. The Senate report reveals that the omission of the statutory suppression remedy was the "result of discussions with the Justice Department." S. REP. NO. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577; *see also* Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 409–11 (1997) (describing Justice Department opposition to the suppression remedy and congressional acquiescence due to the need for its support).

284. 18 U.S.C. §§ 2515, 2518(10) (2012); *see* Steve Jackson Games, 36 F.3d 457, 461 n.6 (5th Cir. 1994) (discussing statute and legislative history); *see infra* Section VII.B.2.e (describing United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010), which held that an unlawful acquisition of stored email, rather than an interception, violated the Fourth Amendment).

285. *See supra* note 166.

286. 18 U.S.C. § 2516(3) (2012) (providing that electronic communications interceptions may be used in pursuit of any federal felony).

287. The Justice Department has required high level approval as a matter of its own policies. CCIPS SEARCH MANUAL, *supra* note 261, at 167. But ECPA permits any "attorney for the government" to authorize the interception of electronic communications. 18 U.S.C. § 2516(3).

acquisitions of electronic communications out of electronic storage.[288] Because of that narrowed scope, very few cases have been brought under the interception provisions.[289] Agents who choose to wait and acquire electronic communications that have come to rest instead of in real time may comply with the much weaker provisions of the Stored Communications Act ("SCA"),[290] which the next Section describes.

e) Acquisition of Stored Electronic Communications Content

The SCA, which applies when law enforcement agents obtain email and related electronic information stored with third party providers of "electronic communications service[s]" and "remote computing service[s],"[291] is much less restrictive than either the Wiretap Act or CrimPC. The SCA places no limits on who may conduct stored content acquisitions, which may be used to pursue any "ongoing criminal investigation," rather than just felonies or serious crimes.[292] Stored contents do not need to be acquired as a last resort, nor do agents need to minimize non-incriminating stored communications. The SCA places no time limits on stored content acquisitions, which allows investigators to ask for emails received over a span of years.[293] As with the remaining surveillance methods this Article describes, the SCA does not require public reporting on law enforcement's acquisition of stored contents.[294]

The remedies for illegal surveillance are less generous under the SCA provision for acquisition of stored email than they are for the interception of email. The SCA provides for civil damages in some cases, but it does not provide for punitive damages or criminal penalties against law enforcement

288. *See, e.g.*, Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460–63 (5th Cir. 1994).

289. *See, e.g.*, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc) (concluding that email may be "intercepted" when it is acquired out of "transient electronic storage that is intrinsic to the communication process").

290. *See* Soghoian, *supra* note 237, at 10 (pointing out that since 1997, federal authorities had obtained only sixty-seven orders to intercept "computer[s] or email (electronic)" reflecting that "law enforcement agencies rarely engage in real-time interception of Internet communications . . . . [I]t is often easier and cheaper for them to do it after the fact rather than in real-time").

291. *See* 18 U.S.C. § 2703(a), (b) (2012).

292. *See* 18 U.S.C. § 2703(d).

293. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (government compelled the disclosure of over 27,000 emails); Bellia & Freiwald, *supra* note 108, at 572 (noting Warshak's claim that some of his emails were nine years old).

294. The Attorney General must report to Congress on disclosures that service providers made on a voluntary basis only. *See* 18 U.S.C. § 2702(d) (2012).

officials who violate its provisions.[295] The SCA also provides no statutory suppression remedy, so unless victims of unlawful surveillance have a Fourth Amendment claim, they may not have unlawfully acquired stored contents information suppressed. In late 2010 in *United States v. Warshak*,[296] the Sixth Circuit found a warrantless acquisition of stored email to violate the Fourth Amendment,[297] and became the first federal appellate court to recognize a Fourth Amendment interest in stored email.[298] Until other federal circuits follow suit or Congress amends ECPA to provide a statutory suppression remedy,[299] victims of unlawful stored content acquisitions outside the Sixth Circuit will continue to lack a suppression remedy.

The provisions described above are common to all investigations proceeding under the SCA. But the SCA provides different procedural hurdles, levels of oversight, and rules on notice based on different features of the stored content. The next Sections describe those different rules.[300] If other courts follow *Warshak* and require a warrant, and certainly if Congress amends ECPA to do so as well, then the protections for stored email contents will be more comprehensive and less complex, which will bring them closer to those found in CrimPC.

i) Subject to the Warrant Requirement

Targets of law enforcement investigations that acquire the contents of email in "electronic storage" for 180 days or less benefit from the highest procedural hurdle and greatest oversight—a warrant based on probable cause that a reviewing judge must issue.[301] The 180-day cutoff for the mandatory warrant reflects Congress' view in 1986 that emails stored a relatively short time were likely protected by the Fourth Amendment,[302] while those stored longer than 180 days could be seen to be abandoned by the user and

295. *See* 18 U.S.C. §§ 2707(a)–(c), 2712 (2012). There is the possibility of administrative discipline for willful violations. *Id.* § 2707(d). The SCA provides immunity for private parties who act in good faith. *Id.* § 2707(e).

296. *Warshak*, 631 F.3d 266.

297. *Id.* at 283–88.

298. The court did not grant Warshak a suppression remedy because it found that the officers in his case relied in good faith on the terms of the SCA. *Id.* at 288–92.

299. The current version of the Electronic Communications Amendment Act of 2013, S. 607, would not add a statutory suppression remedy for the unlawful acquisition of stored emails. *See* Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013).

300. The reader will no doubt find the distinctions to be confusing and hard to follow. Table 1, *infra* Appendix, summarizes the differences.

301. *See* 18 U.S.C. § 2703(a) (2012).

302. *See* H.R. REP. NO. 99-647, at 67–68 (1986) (reporting that email in storage less than 180 days as likely protected by the Fourth Amendment).

therefore the business records of the storing company.[303] The Justice Department, whose agents apply for orders under the SCA every day, interprets the statutory language to mean only unopened (unretrieved) emails are entitled to the protection of a warrant requirement, no matter how long they have been stored, because only those emails are in "electronic storage" under the statute.[304] The Ninth Circuit has not accepted the Justice Department's approach, and applies the warrant requirement to all emails stored 180 days or less.[305] In the other jurisdictions, however, the Justice Department accords opened or retrieved emails lesser protections than a warrant, the specific protections depending on the type of server upon which the emails are stored.

Although federal criminal law generally requires notice to the target when a warrant is required,[306] the Justice Department argues that when it is authorized to use a warrant under the SCA it does not have to provide notice.[307] Without notice, of course, targets may never learn of the surveillance or that they have any rights with regard to it. If, as the *Warshak* court held, use of a warrant is constitutionally mandated, it may be that notice is mandated as well. In *Warshak*, however, agents unlawfully delayed providing notice for over a year, and the Sixth Circuit made no definitive statement that the Constitution requires notice.[308]

ii) Subject to a Lesser Standard

The SCA makes it significantly easier to acquire electronic communications contents that have been stored more than 180 days. Law

303. *See also id.* at 23 n.41 (analogizing emails held in long term storage to business records). As practices have changed and many users store their more important emails with their service providers for years, it makes no sense to protect older emails less.

304. *See* CCIPS SEARCH MANUAL, *supra* note 261, at 123–26, 138.

305. Ohm, *supra* note 4, at 1539 (citing Theofel v. Farey Jones, 359 F.3d 1066 (9th Cir. 2004)) (describing the 9th Circuit's rejection of the DOJ's approach and its requirement of a warrant for access to stored email).

306. *See* Smith, *supra* note 91, at 611 n.51 (citing Fed. R. Crim. Pro. 41(f)(1)(C), (f)(3) and noting that traditional search warrants provide notice to the targets while electronic surveillance orders do not); *see also* City of West Covina v. Perkins, 525 U.S. 234, 240 (1999) ("[W]hen law enforcement agents seize property pursuant to a warrant, due process requires them to take reasonable steps to give notice that the property has been taken so the owner can pursue available remedies for its return.").

307. CCIPS SEARCH MANUAL, *supra* note 261, at 133–34. Without any explanation or elaboration, the CCIPS manual asserts that the "search warrant obviates the need to give notice to the subscriber." *See id.* at 134 (citing 18 U.S.C. § 2703(b)(1)(A) (2012)). The Supreme Court has found notice constitutionally required for traditional electronic surveillance like wiretapping and bugging. *See* Berger v. New York, 388 U.S. 41, 73 (1967).

308. United States v. Warshak, 631 F.3d 266, 289 (6th Cir. 2010).

enforcement agents may apply for a special court order, known as a "D order," that a court may issue when the application "offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation."[309] When agents acquire stored email contents with a D order, they must give notice to the target, but may delay such notice.[310] In fact, the sample D order in the Justice Department's manual provides for delayed notice until such time as the court determines.[311] Instead of obtaining a D order, agents may obtain the available stored email content without a warrant using an administrative, trial, or grand jury subpoena, so long as they provide notice.[312]

As mentioned above, the Justice Department considers retrieved emails, or those opened, accessed, or read, as subject to the D order standard rather than the warrant requirement, even when they are stored for 180 days or less.[313] According to the DOJ, when emails are stored with a service provider that furnishes email services to the public, that provider is a statutory "remote computing service," and agents may acquire the already-retrieved emails from it pursuant to the lesser statutory standard.[314] If the service provider that stores the email does not furnish email to the public, for example if it is a University or corporate provider, the Justice Department considers the retrieved email to be entirely unprotected by the SCA, as discussed next.[315]

---

309. 18 U.S.C. § 2703(d).

310. *See* 18 U.S.C. § 2705(a)(2)(A)–(E) (2012) (listing reasons that justify the order, such as a concern that evidence will be destroyed or tampered with, the investigation will be jeopardized, or the trial delayed). Apparently agents do not always comply with the requirement that they eventually give notice. *See, e.g.*, *Warshak*, 631 F.3d at 289 (finding that law enforcement delayed giving notice of stored email acquisition for over a year despite only having approval to delay giving notice for ninety days).

311. *See* CCIPS SEARCH MANUAL, *supra* note 261, at 213–23 (App. B and attachment); *cf.* Smith, *Kudzu in the Courthouse*, *supra* note 220, at 208–12 (noting that many electronic surveillance orders remained under seal indefinitely).

312. 18 U.S.C. § 2703(b)(B).

313. *See* Freiwald, *supra* note 14, at 57–59 (criticizing the DOJ's approach).

314. *See* CCIPS SEARCH MANUAL, *supra* note 261, at 127 ("[A] single provider can simultaneously provide ECS [electronic communication services] with regard to some communications and RCS [remote computing services] with regard to others, or ECS with regard to some communications and neither ECS nor RCS with regard to others."). Orin Kerr has praised Congress' foresight in devising ECPA. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1243 (2004) ("It is a particularly remarkable achievement given that its enactment dates back to 1986. The SCA has weathered intervening technological advances surprisingly well.").

315. *See* CCIPS SEARCH MANUAL, *supra* note 261, at 126 (describing how the "SCA no longer regulates access" to an email retrieved from a company provider of email). The

iii) Not Covered by the SCA

The DOJ argues that the SCA does not cover the acquisition of already-retrieved email from a non-public provider.[316] According to the DOJ, agents may compel the disclosure of information that falls outside of the SCA with a simple subpoena without any judicial oversight.[317] Recall that the subpoena can generally be challenged only on the basis that it seeks irrelevant or overbroad information.[318] The process is subject to no statutory restrictions, provides no remedies for unlawful investigations, and proceeds without notice to the subject.[319] Because such "surveillance" is covered and protected under CrimPC, a great disparity exists between U.S. and Swiss surveillance law.

C. ACQUISITION OF USER IDENTIFICATION DATA

1. In Switzerland

User identification data includes information related to communications ("communication attributes") but not the contents themselves. Such data also contains information about the location of the target and when and with which people the target is or was communicating by way of post or telecommunications.[320] Additionally, it includes billing data and traffic data, such as information about the duration of a call, the amount of data downloaded, and the like.[321] CrimPC treats tracking or locating someone using cell site location data as the acquisition of user identification data.[322]

Subject to two exceptions, CrimPC regulates the acquisition of user identification data under the same comprehensive and restrictive standards

Justice Department contends that public systems users qualify for more protection than non-public system users because they are less likely to have a personal relationship with their service providers. *See id.* at 135–36.

316. *See id.* at 125–26, 138.

317. *See id.* at 128 (describing the process for using a subpoena to obtain information beyond the scope of the SCA's protections).

318. *See* Slobogin, *supra* note 192, at 806 (identifying privilege, burdensomeness, and irrelevance as possible grounds for challenging the issuance of a subpoena generally and explaining that those challenges usually prove unavailing); *see also supra* note 203 (discussing ways for recipients to challenge subpoenas).

319. *See also* United States v. Scarfo, 180 F. Supp. 2d 572, 581–83 (D. N.J. 2001) (electronic monitoring by law enforcement that recorded keystrokes as they were typed but purportedly did not operate while the modem was "activated" was not subject to statutory regulation as a wiretap or electronic intercept).

320. CRIMPC art. 273, para. 1a.

321. CRIMPC art. 273, para. 1b.

322. It requires use of a telecommunications installation and involves the secrecy of telecommunications but no access to the contents of communications. *See* TF, Nov. 3, 2011, 132 ATF IV 340 (Switz.).

that apply to the surveillance of post and telecommunications. First, law enforcement agents may acquire user identification data for the investigation of any felony or misdemeanor, but they may only use the surveillance of mail and telecommunications to investigate a limited list of offenses.[323] Second, when judges apply the proportionality principle, they consider the acquisition of non-content user identification information to be less intrusive than interception of the contents of mail, email, and calls.[324]

Unlike ECPA and just as with the interception of post and telecommunications, CrimPC accords the same treatment to acquisition of user identification data in real time as it does to acquisition out of storage.[325] That uniformity of treatment substantially simplifies Swiss law relative to the United States. Agents may request historical user identification data up to six months after the data has been generated and a data retention requirement ensures that mail, telecommunications, and internet service providers will make such data available to them.[326]

As mentioned, the same comprehensive and highly protective procedures that apply to surveillance of post and telecommunications regulate the acquisition of user identification data, with the two exceptions noted. The procedures include several provisions: significant judicial oversight, the principles of subsidiarity and proportionality, the notice requirement, criminal penalties, and the significant remedies of damages and exclusion. These protective provisions all work together to ensure that surveillance under this category will not be overused or abused.

2. In the United States

a) Several Distinctions

The last section introduced the different treatment American law accords to the contents of postal mail, telephone calls, and electronic mail. ECPA has

323. CRIMPC arts. 269, 273. Law enforcement can also acquire user identification data to investigate the misuse of a telecommunications installation, which is an offense less serious than a misdemeanor. *See* CP art. 179septies.

324. ATF 137 IV 340, para 5.5.

325. *See* Sträuli, *supra* note 134, at 98–99.

326. SPTA art. 12, para. 2, art. 15, para. 3. The constitutional courts of the Czech Republic, Germany, and Romania consider the systematic conservation of a log without suspicion as against the constitution. Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), at 5–6, COM (2011), 225 final (Apr. 18, 2011), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:EN:PDF; *see also* TF, Jan. 8, 2010, docket no. 6B 766/2009, para. 3.4 (Switz.) (finding that data retention obligation applies to internet service providers). The obligation for service providers to keep logs of user identification data may be extended to twelve months. *See supra* note 73.

not only fallen out of date, but it retains a confusing set of categories that make understanding the applicable legal rules challenging at best. The next sections describe how U.S. law treats the surveillance that CrimPC handles under acquisition of user identification data. Table 2, *infra* Appendix, summarizes the differences.

b) Collection of Postal Mail Attributes

Legislating against the backdrop of the Fourth Amendment, Congress has provided few procedural restrictions on the surveillance of envelope information.[327] U.S. courts have historically distinguished between the contents of a letter that are unreadable until the envelope carrying the letter is opened, and information appearing on the outside of the envelope and therefore observable to postal workers when they process mail.[328] Courts have reasoned that senders of mail can have no reasonable expectation of privacy in information on the outside of envelopes that third party carriers can see.[329]

Under a 1975 Postal Service regulation, law enforcement agents can request that the post office retain "mail cover" information, or information obtained from the outside of postal mail, whenever they "specif[y] . . . reasonable grounds to demonstrate [that] the mail cover is necessary to . . . [o]btain information regarding the commission or attempted commission of a crime."[330] No judge provides oversight of the investigation, no notice needs to be provided, and no remedies are afforded to victims of improper investigations.[331]

c) Collection of Electronic Communication Attributes in Real Time

ECPA's provisions pertaining to pen registers and trap and trace devices provide minimal procedural restrictions comparable to those just described. Modern pen registers acquire the "dialing, routing, addressing and signaling information"[332] associated with wire and electronic communications as well as the date, time, and duration of transmissions, and information in the "cc"

327. Kerr, *supra* note 14, at 631.

328. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (describing line of cases finding a constitutional difference between contents and the information on the outside of mail).

329. *See* United States v. Van Leeuwen, 397 U.S. 249, 250–52 (1970); United States v. Hernandez, 313 F.3d 1206, 1209–10 (9th Cir. 2002).

330. 39 C.F.R. § 233.3(e)(2)(iii) (2012); Kerr, *supra* note 14, at 631.

331. Kerr, *supra* note 14, at 631.

332. *See* 18 U.S.C. § 3121(c) (2012).

and "bcc" fields of emails.[333] The Justice Department contends that any electronic communications information that is *not* the content of an electronic mail message or the subject line may be intercepted with a pen register order.[334] Courts have permitted law enforcement agents to acquire IP addresses with a pen register order, but have suggested that more specific URL information could not be acquired solely with a pen register order.[335]

Several courts and commentators have criticized the weak protections afforded by ECPA's pen register provisions.[336] Law enforcement agents who seek a pen register must apply for a special court order but do not need to establish probable cause. Instead, the investigating agent need only certify his belief "that the information likely to be obtained is relevant to an ongoing criminal investigation."[337] A judge asked to grant a pen register order "shall approve it" so long as she "finds that the application is complete."[338] Unlike CrimPC, the pen register provisions do not provide notice to the target or any remedies to the target for unlawful investigations; no statutory

333. *See* CCIPS SEARCH MANUAL, *supra* note 261, at 230 app. D. The Justice Department claims that any email header information may be acquired using a pen register. *See id.* at 154.

334. *See id.* at 154. The manual expresses ambivalence about whether the subject line is content or not by stating that it "*can* contain content." *Id.* at 152–53 (emphasis added). For a thorough discussion of the ambiguity here, see Freiwald, *supra* note 14, at 69–74 (arguing that there should be a third category of information that is neither content nor addressing information). For a different view, see Kerr, *supra* note 14, at 611–16 (arguing that there are only two categories); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1019–38 (2010) [hereinafter Kerr, *Applying the Fourth Amendment*] (developing claim that there are only two categories online: content and non-content information).

335. United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008).

336. *See, e.g.*, Ohm, *supra* note 4, at 1550 ("Congress should amend the Pen Register Act to require at least reasonable suspicion" to "stamp out fishing expeditions"); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1289 (2004) (describing the Pen Register Act's protections as "limited and ineffective").

337. 18 U.S.C. § 3122(b) (2012).

338. 18 U.S.C. § 3123(a) (2012). Judges do not conduct independent reviews of the factual support for the applications, and the Justice Department has largely persuaded courts to view their role as "ministerial in nature." *See, e.g.*, United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

suppression remedy or damages are available.[339] Additionally, the statute does not provide for reports to Congress or the public.[340]

d) Collection of Electronic Communication Attributes from Electronic Storage

Congress afforded electronic communication attributes in electronic storage the lowest level of statutory protection. Law enforcement agents may compel the disclosure of a large set of information called "basic subscriber . . . information" from service providers by presenting an administrative, grand jury, or trial subpoena.[341] Under this provision, law enforcement agents may learn identifying information about a subscriber, including the electronic communication service to which he subscribes, when he used the service to access the Internet, and what IP address he used to do so.[342] In addition, service providers must turn over electronic records that disclose all of the people with whom a person has corresponded online and the "detailed internet address[es] of sites accessed."[343]

Although the size and duration of electronic log files vary by service provider, they can be quite revealing.[344] Service providers keep log files to protect themselves against hacking and fraud; such files can provide the entire history of one's communications and movements through the World Wide Web, down to an astonishing level of detail.[345]

339. Smith, *supra* note 91, at 612. Courts have found no Fourth Amendment right implicated by use of pen registers. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008). The statute provides for the possibility of a criminal action against violators, but no known cases have been brought. *See* 18 U.S.C. § 3121(d) (2012) (providing for a penalty of a fine and up to one year of imprisonment).

340. 18 U.S.C. § 3123(a)(3)(A) provides for records to be kept when law enforcement agents use their own devices, but does not require that the reports be sent to Congress or published.

341. 18 U.S.C. § 2703(c)(2) (2012); CCIPS SEARCH MANUAL, *supra* note 261, at 128.

342. For example, the information comprises the subscriber's name, address, length of service, telephone number or IP address, and the means and source of payment. 18 U.S.C. § 2703(c)(2)–(3); *see also* USA PATRIOT Act § 210, 115 Stat. 272, 283 (2001) (adding "records of session times and durations" and "any temporarily assigned network address").

343. CCIPS SEARCH MANUAL, *supra* note 261, at 122.

344. *Id.* at 139 (noting that "some providers retain very complete records for a long period of time," while others retain few if any records). Bills have been proposed to impose a mandatory retention period for service provider logs. *See, e.g.*, Protecting Children from Internet Pornographers Act of 2011, H.R. Res. 1981, 112th Cong. (2011) (imposing obligation to hold identifying information for eighteen months).

345. The sample of a letter an agent may send to a provider to require the preservation of stored information under 18 U.S.C. § 2703(f) lists the following to preserve: all stored communications to and from the target, all files the target has accessed or controlled, all connections logs and records of user activity, including the volume of data transferred, all

Any other records "concern[ing]" electronic communications may be obtained with a D order,[346] but are subject to no other limits (such as subsidiarity or proportionality). Law enforcement agents are specifically excused from giving notice to targets under this section,[347] and are immune from criminal liability. Congress obtains no reports about acquisitions of electronic communications attributes from storage. Targets of unlawful surveillance may bring civil claims for improper investigations, but have no statutory suppression remedy.[348]

e) Cell Site Location Data Acquisition

The legal framework for acquisition of cell phone location data rivals the complexity attendant to acquisition of email. In addition, it is unclear how to apply ECPA rules to this method. Recall that interception of the content of cell phone calls and acquisition of the attributes of cell phone records other than location data are covered in the sections above.

Cell phone location data, however, which refers either to Global Position Satellite ("GPS") data associated with smartphone use or to records of the cell towers with which mobile phones communicate, reside in their own category. Courts have recognized that, while they do not fit under the traditional definition of communications content, such location records raise special concerns because they convey so much information about personal lives and activities. One magistrate judge recently explained that "[t]wo months' worth of hourly tracking data will inevitably reveal a rich slice of the user's life, activities, and associations . . . . If the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera."[349] Cases have begun to reach the appellate courts raising

records of files or system attributes accessed, modified, or *added* by the user, and all connection information for other computers to which the user connected. It also includes all correspondence, and other records of contact by the target, the content and connection logs associated with or related to postings, communications or any other activities to or through the target's email or internet connections. *See* CCIPS SEARCH MANUAL, *supra* note 261, at 225–26; *see generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (describing current online information gathering practices in depth).

346. 18 U.S.C. § 2703(c). There are some other limited ways in which government agents may acquire access to such records. *See id.*

347. 18 U.S.C. § 2703(c)(3).

348. 18 U.S.C. § 2707 (2012); *see also* Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181–83 (D. Conn. 2005) (no Fourth Amendment protection for subscriber information disclosed to the service provider's employees in the ordinary course of business).

349. *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (2013).

the issue of whether cell phone location data acquisition is protected by the Fourth Amendment, and if so, just what protections that affords.[350]

In the absence of clear guidance from either appellate courts or Congress, courts vary in the requirements they impose on law enforcement agents who compel disclosure of location data records from service providers. For acquisition of cell phone location data in real time, some courts require a warrant and others require the combination of a D order and a pen register order under what is called the "hybrid theory."[351] For the acquisition of location information out of electronic storage,[352] some courts have required a D order, and some have required a warrant. Because these cases have generally arisen before trial, when the government has requested records as part of its investigation, it is too early to say whether those courts that require a warrant will also require notice to the target and whether they will provide a suppression remedy to those subject to unlawful surveillance.[353] There is currently no reporting of cell phone data acquisitions and no statutory remedies other than civil remedies (but not notice) under the SCA when courts require a D Order.

D. TECHNICAL SURVEILLANCE EQUIPMENT

1. In Switzerland

CrimPC treats the use of technical surveillance devices as sufficiently invasive to be included in the most restricted category and accorded the same comprehensive treatment as the surveillance of mail and telecommunications. Technical surveillance equipment (sometimes called "other surveillance

350. *See* Freiwald, *Cell Phone Location Data*, *supra* note 90, at 732–49 (reviewing a 2010 Third Circuit case in detail and arguing that courts should impose Wiretap Act requirements on acquisition of cell site location data that covers a period of time); Government Brief 5th Circuit, *supra* note 98 (appealing district court case that affirmed Magistrate Judge Smith's opinion cited *supra* note 349).

351. *See, e.g.*, Steven B. Toenisketter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 RICH. J.L. & TECH. 19–28 (2007) (describing cases accepting and rejecting the "hybrid theory").

352. In some cases the government purports to seek information out of electronic storage, but actually requests that information be created on an ongoing basis. *See* Susan Freiwald, *The Vanishing Distinction Between Real-time and Historical Location Data*, CONCURRING OPINIONS, (July 17, 2012, 4:50 PM), www.concurringopinions.com/archives/2012/07/the-vanishing-distinction-between-real-time-and-historical-location-data.html (describing how, in a case on appeal to the Fifth Circuit, agents asked for cell site location records to be created in real time and then stored, and then immediately transmitted to law enforcement agents as soon as they were stored).

353. *See, e.g.*, United States v. Muniz, No. H-12-221, 2013 WL 391161 (S.D. Tex. Jan. 29, 2013) (denying motion to suppress to defendant whose historical cell site location records were acquired without a warrant based on good faith rule).

measures") includes listening or audio recording devices, cameras, movie cameras, tracking devices,[354] and the like.[355] Law enforcement agents conduct surveillance using such devices when they observe or record statements or incidents made in non-public places and when they establish the location of people or things in both public and non-public places.[356] While there may appear to be some overlap among the surveillance categories, each technique belongs in only one category. For example, videotaping or photographing a telephone booth constitutes the use of technical surveillance equipment and not the monitoring of telecommunications when there is no access to the content of the phone call.[357] Audio and video recordings of places not accessible to the general public are covered under this category;[358] audio and video recordings in public spaces are not.[359]

As with the surveillance of post and telecommunications, only particular offenses justify the use of technical surveillance devices.[360] In addition, the same oversight, procedural hurdles, notice requirements, and consequences apply to unauthorized surveillance by technical surveillance equipment as apply to unauthorized surveillance by mail, email, and phone.[361]

2. In the United States

Reflecting the relative complexity of U.S. law, no single statute covers technical surveillance equipment. The closest approach to CrimPC in the United States would be the Wiretap Act, which strictly regulates the use of bugs and video surveillance in private areas. The Wiretap Act restricts the recording of spoken words in the same way as it restricts wiretapping, so long as the bugging takes place in an area in which the target has a reasonable expectation of privacy.[362] As described above, the Wiretap Act provides a

354. Including GPS devices and RFID.

355. The Technical Surveillance Equipment category may come to include later developed technologies that fit within its parameters. *See infra* Section VII.H.1.

356. Non-public places are places that are not accessible to the general public. CRIMPC art. 280. Before CrimPC, cantonal law varied a lot with respect to these practices. *See* GOLDSCHMID, *supra* note 196; Sträuli, *supra* note 134, at 112–17.

357. Thomas Hansjakob, Die ersten Erfahrungen mit dem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs [BÜPF], 120 REVUE PÉNALE SUISSE 268 (2002).

358. CRIMPC arts. 272, 281–282.

359. The recording of public spaces is treated as physical observation. CRIMPC art. 282; *see also infra* Section VII.G.1.

360. CRIMPC art. 281, para. 4.

361. *Id.*

362. 18 U.S.C. § 2510(2) (2012) (defining "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation").

comprehensive set of protections, such as approval of high level officials and extensive judicial oversight, subsidiarity and limited proportionality, transparency and notice, and significant remedies and a statutory suppression remedy.[363] Similarly, seven federal courts of appeals have found silent video surveillance, in areas subject to a reasonable expectation of privacy such as a home or office, to also require the highest restrictions of the Wiretap Act.[364] Because the restrictions derive by analogy from the Fourth Amendment rather than from the explicit text of Wiretap Act, however, the provisions for Congressional reporting and some of the other "technical" requirements do not apply to silent video surveillance.[365]

The Supreme Court has restricted similar surveillance methods using the Fourth Amendment. For example, it found law enforcement's use of a thermal imaging device to record the heat emanating from the target's home to be a search under the Fourth Amendment.[366] Though the *Kyllo* case was privacy-protective, its reasoning contains significant limits. The Court's emphasis on the fact that agents used devices not in general public use to search a home suggests that U.S. law would not restrict many of the techniques that CrimPC would.[367] It remains an open question how much the Court will restrict surveillance that does not implicate traditional property rights, especially when that surveillance uses readily available technology.

E. SURVEILLANCE OF CONTACTS WITH A BANK

1. In Switzerland

CrimPC includes surveillance of a target's contacts with a bank or bank-like institution in the most restricted category of surveillance, but relaxes protections by allowing bank surveillance to investigate any felony or misdemeanor, and by providing a slightly weaker exclusionary remedy.[368]

---

363. *See supra* Section VI.B.2.c.

364. *See supra* text accompanying notes 101–02.

365. United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992) (en banc) (adopting the "last resort rule" for silent video surveillance as one of four Fourth Amendment requirements that also include minimization, particularity, and limited duration).

366. Kyllo v. United States, 533 U.S. 27, 27 (2001).

367. *Id.* at 40 (finding that the "Government use[d] a device that [was] not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion").

368. CRIMPC art. 284; *see also* SYLVAIN MÉTILLE, MESURES TECHNIQUES DE SURVEILLANCE ET RESPECT DES DROITS FONDAMENTAUX EN PARTICULIER DANS LE CADRE DE L'INSTRUCTION PÉNALE ET DU RENSEIGNEMENT [SURVEILLANCE MEASURES AND FUNDAMENTAL RIGHTS, WITH PARTICULAR ATTENTION TO CRIMINAL AND INTELLIGENCE INVESTIGATIONS] 167–70 (2011). The bank itself primarily executes this type of surveillance by following the instructions contained in the surveillance order.

Surveillance of both financial flows and credit card information is available under this category, and authorized techniques include ordering the bank to transmit, in real time, information about every transaction with the bank; information from physical observation; information from communication intercepts; and specific documents relating to the accused person's interactions with a bank.[369] Because an order for real-time transmission of bank transactions requires a bank to transmit information that does not yet exist, it is forward looking.[370] Banks may also be ordered to provide access to their computer systems.[371]

As mentioned, besides the greater number of predicate offenses that can justify surveillance of bank contacts, CrimPC applies the same comprehensive restrictions accorded to surveillance of mail and telecommunications to surveillance under this category. Instead of a complete exclusionary remedy, however, CrimPC treats evidence uncovered by unauthorized surveillance of contacts with a bank as relatively unusable; it can be used only if the evidence could have been obtained legally and if it is necessary to solve serious offenses.[372] More serious committed offenses will increase the weight of the prosecution's interest in the information, tipping the balance against the private interest in not having the illegally obtained evidence used.[373]

---

369. SCHMID, *supra* note 205, at 538.

370. CrimPC's provision on Surveillance of Contacts with a Bank incorporates into Swiss law Article 4 of the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of November 8, 1990. Article 4 requires Swiss law to permit the use of special investigative techniques that facilitate the identification and tracking of proceeds and the gathering of evidence related thereto. *See* Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale [Message about Unification of Criminal Procedure Law], FF 1057, 1236 (2006); DANIEL JOSITSCH, GRUNDRISS DES SCHWEIZERISCHEN STRAFPROZESSRECHTS [OUTLINE OF SWISS CRIMINAL PROCEDURE LAW] 150 (2009);

371. Procedures for acquiring bank records are covered by the rules pertaining to searches and seizures. CPP arts. 241ss, 263ss; STEPHANIE EYMANN, DIE STRAFPROZESSUALE KONTOSPERRE [THE BANK ACCOUNT FREEZE ACCORDING TO CRIMINAL PROCEDURE] 81–90 (2009). However, Rhyner and Stüssi view surveillance of contacts with a bank as both occurring in real time and retroactively. Beat Rhyner & Dieter Stüssi, *Kommentar zu Art. 284–285 StPO*, *in* POLIZEILICHE ERMITTLUNG 484 (2008) (Gianfranco Albertini, et al. eds., 2008).

372. TF, Nov. 4, 1970, 96 ATF I 437, 441 (Switz.).

373. TF, May 3, 2005, 131 ATF I 272, 279 (Switz.). The police may conduct an undercover investigation to establish that the offense has been committed as well as to gather evidence of it.

2. *In the United States*

Undoubtedly because the United States does not share Switzerland's tradition of bank secrecy and because U.S. bank records are not subject to Fourth Amendment protection, no laws in the United States tailor law enforcement surveillance regulation specifically to the bank context.[374]

F. UNDERCOVER OPERATIONS

1. *In Switzerland*

CrimPC treats undercover operations as surveillance methods because they analogize the police hiding their official function to obtain evidence of committed offenses[375] to hiding devices like video cameras or wiretaps.[376] In undercover operations, police generally obtain fake identities to engage with suspects.[377] Because undercover operations intrude on privacy, CrimPC subjects them to the highest restrictions. CrimPC also restricts undercover operations to ensure that they are not used to entrap people; agents must restrict their activities to substantiating a preexisting intention to commit a criminal offense and they may not investigate outside of the context of a criminal investigation.[378]

Undercover investigations may be used to investigate a smaller number of serious offenses than surveillance of post and telecommunications or technical surveillance devices.[379] Except for that difference, CrimPC uses the same protective procedures for undercover investigations that it uses for the

374. The United States has a statute providing some secrecy for bank records, but it does not regulate the surveillance of bank contacts as CrimPC does. *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2012) (requiring a subpoena or warrant for the disclosure of financial information to the government).

375. TF, June 16, 2008, 134 ATF IV 266, 277, para. 3.7 (Switz.).

376. CRIMPC arts. 286–298; Vincent Jeanneret & Roland M. Ryser, *Commentaire ad art. 286-295 CPP* [*Commentary to articles 286–295 CrimPC*], *in* COMMENTAIRE ROMAND DU CODE DE PROCÉDURE PÉNALE [COMMENTARY TO CRIMINAL PROCEDURE CODE] 1315 (André Kuhn & Yvan Jeanneret, eds., 2011); Laurent Moreillon & Miriam Mazou, *Commentaire ad art. 296-298 CPP* [*Commentary to articles 296–298 CrimPC*], *in* COMMENTARY TO CRIMINAL PROCEDURE CODE 1351, *supra.*

377. In some situations a member of a foreign police force or a person temporarily appointed to carry out police work may be deployed as an undercover investigator.

378. If an undercover investigator oversteps the scope of the permissible action, then that shall be taken into consideration in determining the appropriate sentence to be imposed on the person concerned or the court shall refrain from sentencing the person altogether. CRIMPC art. 293, para. 4.

379. CRIMPC art. 286, para. 2 contains the second list pertaining to undercover investigations and contains a smaller number of offenses than the list in CRIMPC art. 269, para. 2 pertaining to post and telecommunications surveillance.

surveillance of post and telecommunications and all of the other methods discussed,[380] apart from the slight variations mentioned.

2. In the United States

In sharp contrast to the Swiss approach, use of undercover agents faces no regulation in the United States. No statute applies, and in a series of cases more than fifty years old, the Supreme Court found no Fourth Amendment search when agents used undercover agents to either record or transmit information divulged by a criminal suspect.[381] As a result, use of undercover agents requires no warrant or judicial oversight. If undercover agents engage in wiretapping or use another restricted surveillance method, however, those restrictions apply.[382]

The difference between the way Switzerland tightly controls undercover agents and the United States does not has tremendous implications for the two countries' systems. First, it illustrates that the Swiss employ a dignity-based approach in which the police do not misrepresent themselves to their people, which is clearly lacking in the United States. Second, the undercover agent rule's assumption of risk approach underlies the third party doctrine.[383] If courts or legislators see the weakness in the doctrine's underpinnings, they will have an easier time in granting more privacy rights in new communications technologies that rely on access to information stored by others.[384]

G. PHYSICAL OBSERVATION

1. In Switzerland

Under CrimPC, use of physical observation is a less invasive category of surveillance. While courts have not yet confirmed that surveillance by physical observation breaches privacy, scholars argue that it does,[385] at least if the observation persists. Accordingly, while CrimPC provides a legal basis for

380. CRIMPC arts. 274, 289.

381. *See* On Lee v. United States, 343 U.S. 747 (1952); United States v. White, 401 U.S. 745 (1971).

382. *See generally* LAFAVE ET AL., *supra* note 263, § 3.1(c); Ross, *supra* note 21, at 533–43.

383. *See* Bellia & Freiwald, *supra* note 108, at 153–56.

384. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (describing the third party rule as "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

385. For the different opinions among commentators, see ROBERTO ZALUNARDO-WALSER, VERDECKTE KRIMINALPOLIZE ILICHE ERMITTLUNGSMASSNAHMEN UNTER BESONDERER BERÜCKSICHTIGUNG DER OBSERVATION [UNDERCOVER LAW ENFORCEMENT INVESTIGATION WITH PARTICULAR ATTENTION TO PHYSICAL OBSERVATION] 50 (1999).

physical observation, it may proceed under a set of procedural requirements that are easier to meet.[386]

Physical observation occurs when, in the course of an investigation, a member of the public prosecutor's office or the police covertly observes people and things in places accessible to the general public and makes audio or video recordings for criminal prosecution.[387] CrimPC regulates focused, systematic physical observation, as well as observation that takes place over time. Surveillance under this category, which does not have to be recorded, is limited to physical observation in public places; CrimPC provides more oversight for surveillance in private places, which constitutes the use of the technical surveillance equipment described in Section VII.D.1, *supra.*

The Swiss Supreme Court recently decided that following a chat in an online (public) forum and focusing on some participants constitutes observation. Just following the conversation without focusing on someone in particular does not constitute surveillance but is instead comparable to when an officer patrols the street. If the observation develops to the point that the officer takes part in a conversation without identifying himself as a police officer, then it will have become an undercover investigation and be subject to further restrictions.[388]

CrimPC permits the public prosecutor or police to authorize physical observation, rather than requiring independent judicial review.[389] It may proceed so long as there are concrete reasons to assume that crimes or offenses have been committed and may be used to investigate any felony or misdemeanor.[390] The procedural hurdle is lower than the strong suspicion required of the other surveillance methods, but higher than the standard of simple suspicion used to open investigations.[391] Similar to surveillance of contacts with a bank, CrimPC provides a modified rather than a complete exclusionary remedy for targets of unauthorized physical observation.[392] Notwithstanding the lower level of oversight, lower procedural hurdles, and

386. *See* Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale [Message about Unification of Criminal Procedure Law], FF 1057, 1235 (2006).

387. *See* CRIMPC art. 282, para. 1; Conseil Fédéral, Message about Unification of Criminal Procedure Law, FF 1057, 1235.

388. Observation occurs at a distance, while undercover investigation requires an officer designated for this purpose to infiltrate a given environment. TF, June 16, 2008, 134 ATF IV 266 (Switz.).

389. Physical observation that continues for longer than one month requires the authorization of the public prosecutor. CRIMPC art. 282, para. 2. CrimPC does not require that the authorization be in writing, but that is obviously recommended.

390. CRIMPC art. 282, para. 1a.

391. *See supra* note 199.

392. *See supra* Section VI.E.1.

modified exclusionary remedy, CrimPC still requires that those targeted by physical observation receive notice.[393]

2. In the United States

While CrimPC provides reduced regulation for surveillance in public, U.S. law has traditionally provided no regulation at all. The understanding has been that one has no privacy from government surveillance in public. As Christopher Slobogin has written, "[t]he advent of sophisticated technology that allows the government to watch, zoom in on, track, and record the activities of anyone, anywhere in public, twenty-four hours a day, demands regulation. Yet to date no meaningful constraints on this type of surveillance exist."[394] According to Orin Kerr, "[t]he distinction between government surveillance outside and government surveillance inside is probably the foundational distinction in Fourth Amendment law . . . . According to this distinction, the government does not need any cause or order to conduct surveillance outside."[395] Although some have criticized the notion that people assume the risk of unobserved surveillance when they venture outside,[396] courts have largely accepted it.

The Supreme Court's decision in *United States v. Jones*[397] may indicate a shift. The *Jones* case found the use of a specialized GPS device attached to a car to be a search under the Fourth Amendment, but the case has broader implications. The Court could have disposed of the defendant's constitutional claim on the ground that law enforcement agents observed him while he was outside. The Court's failure to do so paves the way for future cases to revisit the assumption that movements out of doors cannot be subject to Fourth Amendment protection.[398]

---

393. But the public prosecutor may decide to postpone or omit giving notice. Defendants may challenge the surveillance when they learn of it by submitting an objection to the decision of the public prosecutor or to a cantonal court. CRIMPC art. 393, para. 1a.

394. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 79 (2007).

395. *See* Kerr, *Applying the Fourth Amendment*, *supra* note 334, at 1010 (citing cases); Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate, 519 F.2d 1335 (3d Cir. 1975) (finding that no privacy right was violated by police observations of public meetings and activities).

396. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 113–26 (2011); SLOBOGIN, *supra* note 394, at 79–136.

397. United States v. Jones, 132 S. Ct. 945 (2012).

398. *See, e.g.*, Montana State Fund v. Simms, 2012 MT 22 (Mont. 2012) (Nelson, J., specially concurring) (asserting that "Montanans do retain expectations of privacy while in public" particularly in light of the Justice's statements in *Jones*), *available at* http://goo.gl/GSL1f.

H. NEW TECHNIQUES

1. In Switzerland

It seems likely that as new techniques are developed, Swiss law will consider them to be covered under rules pertaining to technical surveillance devices. Indeed the legislature drafted the Technical Surveillance Equipment category to cover techniques used to listen, record, observe, or locate, but those categories are considered illustrative rather than exhaustive.[399]

If a new surveillance technique appears to have fundamentally different means or goals, however, a specific new rule or amendment would be needed. The federal Constitution and the ECHR require that a law be clear and foreseeable as to its effects,[400] which prohibits interpreting CrimPC to permit surveillance techniques that could not have been imagined when the law was passed. A new rule would also be needed for any techniques that the legislature considered when drafting CrimPC and specifically decided not to cover.

When law enforcement agents want to use a new surveillance technique, they have to discern if the legislature deliberately excluded that technique from CrimPC, even without explicitly saying so. If so, the technique could be used only after CrimPC had been modified to address it. On the other hand, if the legislature merely forgot to mention a technique in the explanatory reports or hearings and if the technique fits a specific category of CrimPC by analogy, the technique may be usable.[401]

For example, surreptitious installation of a government monitoring software, though not mentioned explicitly in CrimPC, may be covered under the rules pertaining to Post and Telecommunications when it targets electronic communications content, the rules pertaining to User Identification Data when it targets communication attributes, and rules pertaining to Technical Surveillance Equipment when it is used to control a webcam or microphone.[402] However, the Federal Council decided a court

399. CRIMPC art. 280; Tribunal administratif fédéral [TAF] [Federal Administrative Court], June, 23, 2011, RECUEIL OFFICIEL DES ARRÊTS DU TRIBUNAL FÉDÉRAL ADMINISTRATIF SUISSE [ATAF] A-8267/2010, § 3.2.

400. *See supra* note 61.

401. *See* SYLVAIN MÉTILLE, MESURES TECHNIQUES DE SURVEILLANCE ET RESPECT DES DROITS FONDAMENTAUX EN PARTICULIER DANS LE CADRE DE L'INSTRUCTION PÉNALE ET DU RENSEIGNEMENT [SURVEILLANCE MEASURES AND FUNDAMENTAL RIGHTS, WITH PARTICULAR ATTENTION TO CRIMINAL AND INTELLIGENCE INVESTIGATIONS] 220–24 (2011).

402. *See* Sylvain Métille, *Les mesures de surveillance prévues par le CPP*, WEBLAW JUSLETTER (Dec. 19, 2011), *available at* http://jusletter.weblaw.ch/_645.

may not consider the legal basis for such use to be sufficiently clear and foreseeable and proposed that Parliament amend CrimPC to permit government monitoring software to monitor communications.[403] Any other use of government monitoring software (e.g., distant search and seizure, monitoring of the environment of the computer, etc.) is deemed illegal.[404]

Similarly, IMSI-Catchers, which mimic cell towers to acquire cell site location data,[405] have never been mentioned by courts or legislators, but they are sometimes used to intercept communications and communications attributes by using communications infrastructures.[406] As such, courts should treat IMSI-Catchers under the rules pertaining to Post and Telecommunications and Acquisition of User Identification Data when they collect electronic communications and their attributes.[407] For the sake of clarity and foreseeability of the law, the Federal Council also proposed that Parliament amend CrimPC to explicitly allow the use of IMSI-Cacthers.[408]

2. In the United States

Because law in the United States generally provides negative rights (restrictions on government behavior) rather than positive rights (rules that must be in place to authorize government behavior), law enforcement agents have generally used new surveillance methods during the period before their treatment under existing statutes or the Fourth Amendment was clear.

---

403. *See* Conseil Fédéral, Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication [LSCPT] [Message About the Modification of the Surveillance of Post and Telecommunications Act] FF 2013 2379, 2464–74 (2013), *available at* www.admin.ch/opc/fr/federal-gazette/2013/2379.pdf.

404. *Id.*

405. *See EPIC v. FBI—Stingray / Cell Site Simulator*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/foia/fbi/stingray/ ("A StingRay is a device that can triangulate the source of a cellular signal by acting 'like a fake cell phone tower' and measuring the signal strength of an identified device from several locations. With StingRays and other similar 'cell site simulator' technologies, Government investigators and private individuals can locate, interfere with, and even intercept communications from cell phones and other wireless devices."); *see, e.g.*, United States v. Rigmaiden, No. CR08-0814, 2012 WL 1038817 (D. Ariz. Mar. 28, 2012) (involving the government's use of StingRay to locate defendant).

406. *See* Sophie de Saussure, *Le IMSI-Catcher: fonctions, applications pratiques et légalité*, WEBLAW JUSLETTER (Nov. 30, 2009), *available at* http://jusletter.weblaw.ch/_547.

407. New articles may be added to CrimPC to authorize the use of Government-Software (Trojans) and IMSI-Catchers and to extend to twelve months from six the obligation for service providers to keep logs of user identification data. *See* Conseil Fédéral, Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication [LSCPT] [Message About the Modification of the Surveillance of Post and Telecommunications Act], FF 2379, 2393-4, 2397-8, 2426-7, 2436-7, 2464-72 (2013).

408. *Id.*

For example, some courts have found that acquisition of cell phone location data falls outside the scope of ECPA.[409] But if so, it remains unclear whether the technique is covered by the Fourth Amendment, and if not, whether there are any constraints at all upon the use of that method of surveillance.[410] As another example, some law enforcement agencies have started the widespread use of license plate readers to match captured data from parked cars with state databases of stolen vehicles and wanted criminals. Because no regulation currently addresses what can be done with the information or how long it can be retained, one privacy advocate complained, "the infrastructure to protect individuals' privacies and rights doesn't exist, particularly on the legislative and the judicial side."[411]

VIII. CONCLUSION

In the United States, traditional wiretapping (of wire, oral, and electronic communications) and some video surveillance is subject to most of the restrictions imposed by CrimPC in Switzerland: notice, a remedy, subsidiarity, and proportionality.[412] The rest of what CrimPC treats as surveillance is subject to significantly less protection. Law enforcement agents in the United States may use undercover agents, collect stored communications contents and attributes, intercept communication attributes in real time, track location data, and use other modern surveillance techniques subject either to no regulation at all or to the anemic protections afforded by ECPA and a few related statutes.[413]

CrimPC, which brought unity and comprehensive treatment to Swiss surveillance law, dramatically contrasts with the incomplete, confusing, and ineffective laws that regulate surveillance in the United States. It seems clear that the substantive requirements in both the European Convention on Human Rights and the Swiss constitution have yielded significantly stronger

409. *See In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc"ns Servs. to Disclose Records to the Gov"t, 534 F. Supp. 2d. 585, 602 n.44 (W.D. Pa. 2008) (collecting cases), *aff"d*, No-524M, 2008 WL 4191511 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

410. *See supra* Section VII.C.2.e.

411. Eric Roper, *Police Cameras Quietly Capture License Plates, Collect Data,* STAR TRIBUNE, Aug. 10, 2012, www.startribune.com/local/minneapolis/165680946.html.

412. The significant exception is that the unlawful interceptions of electronic communications are not subject to a statutory suppression remedy.

413. This Article has not covered a few minor surveillance statutes, such as the Video Privacy Protection Act. 18 U.S.C. § 2710 (2012), *amended by* Video Privacy Protection Act Amendments Act of 2012, 18 U.S.C.A. § 2710, Pub. L. No. 112-258, 126 Stat. 2414 (amended 2013).

restrictions on law enforcement surveillance. The limited coverage of the Fourth Amendment, and the fact that it exerts no real influence absent a ruling, shifts the default rule in the United States in favor of using new surveillance methods that the legislature has not yet regulated. The opposite rule applies in Switzerland, where techniques that CrimPC does not cover, either explicitly or by analogy, cannot be used. It would represent a significant and likely unattainable shift in our jurisprudence to prohibit law enforcement agents from using new surveillance techniques until Congress explicitly authorizes those techniques. It should be possible, however, for Congress to design a set of surveillance rules that abandon arbitrary distinctions, provide sufficient procedural hurdles and oversight to constrain invasive practices, furnish meaningful remedies to deter abuse, and provide notice and transparency to ensure that the system works as designed. In drafting such an overhaul, American legislators should look to CrimPC for guidance.

APPENDIX

Table 1.

Comparison of U.S. and Swiss Laws for Interception/Acquisition of Communications Content

	Notice Requirement		Suppression Remedy		Level of Judicial Review	
	Switz.	U.S.	Switz.	U.S.	Switz.	U.S.
Mail	Yes	Yes	Yes	Yes	Strong suspicion**	Probable cause
Wire and Phone Communications	Yes	Yes	Yes	Yes	Strong suspicion**	Probable cause with add'l requirements
Electronic Communications	Yes	Yes	Yes	No	Strong suspicion**	Probable cause
Communications Stored ≤ 180 days	Yes	*	Yes	No	Strong suspicion**	Probable cause
Communications Stored > 180 days	Yes	*	Yes	No	Strong suspicion**	Relevant and material to an ongoing investigation

* Notice requirement varies depending on the procedures used and where the data is stored.

** of any enumerated felony

Table 2.

Comparison of U.S. and Swiss Laws Regarding Acquisition of User Identification/Non-Content Data

	Notice Requirement		Suppression Remedy		Level of Judicial Review	
	Switz.	U.S.	Switz.	U.S.	Switz.	U.S.
Mail	Yes	No	Yes	No	Strong suspicion*	None
Real Time Interception of Electronic and Phone Data	Yes	No	Yes	No	Strong suspicion*	Relevant to an ongoing criminal investigation
Stored Electronic Data	Yes	No	Yes	No	Strong suspicion*	Relevant and material to an ongoing investigation
Cell Site Location Data	Yes	No	Yes	No	Strong suspicion*	Varies by Jurisdiction

* of any felony or misdemeanor