Simply More Privacy Protective: Law Enforcement Surveillance in Switzerland as compared to the U.S.

Susan Freiwald[*]

Sylvain Métille[†]

 Both authors appreciate the comments of the participants at the Privacy Law Scholars' Conference in June 2012, and particularly _____, who moderated the panel devoted to our paper.

[*] Susan Freiwald, Professor of Law, University of San Francisco School of Law. I thank research librarian John Shafer and research assistants David Reichbach and Everett Monroe for their valuable help. ____ also contributed significantly to our thinking about this paper.

[†] Sylvain Métille, Doctor of Law, University of Neuchâtel; currently Attorney at Law at id est avocats, Lausanne and Professor at the University of Applied Sciences Western Switzerland, Lausanne. This article was mainly written during my time as a visiting scholar at the Berkeley Center for Law and Technology (UC Berkeley). I thank research librarian Jean Perrenoud for his valuable help.

I. Introduction

Calls for reform of the American laws governing electronic surveillance have heightened as the principal federal law, the Electronic Communications Privacy Act ("ECPA"),[3] recently celebrated its twenty-fifth birthday.[4] Passed in 1986 to bring government surveillance into the electronic age, ECPA has not been meaningfully updated since the advent of the World Wide Web.[5] ECPA's age raises many questions about what it covers. For example, courts currently disagree over whether the statute even applies to surveillance of mobile communications, years after cell phones have become ubiquitous in Americans' lives.[6]

Switzerland, by contrast, has recently updated its laws to cover new surveillance technologies. In January of 2011, the Swiss enacted an entirely new statute, the Swiss Criminal Procedure Code (CrimPC).[7] Substantively, CrimPC imposes similar procedural requirements on law enforcement agents' use of a variety of investigatory techniques. That nearly uniform treatment stands in stark contrast to ECPA, which uses a complicated set of categories and rules to make surveillance law in the United States exceedingly difficult to understand and apply. More importantly, Swiss law precludes the use of surveillance techniques not authorized and regulated by CrimPC, while in the United States, a tremendous amount of what the Swiss

[3] 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.). Commentators tend to refer to the Act by its acronym, ECPA, pronounced eck-pah, and to drop the definite article when doing so.

[4] *See, e.g.*, Press Release, *Leahy Marks 25th Anniversary of ECPA, Announces Plan to Markup Reform Bill*, October 21, 2011, *available at* http://www.leahy.senate.gov/press/press_releases/release/?id=56C35200-EFDC-497A-9EAF-A75B498515B8; Center for Democracy and Technology, *It's Time for a Privacy Upgrade*, Oct. 21, 2011, *available at* https://www.cdt.org/blogs/2010ecpas-25th-anniversary-time-change.

[5] *See infra* Part V for a discussion of the evolution of surveillance law in the United States.

[6] *See generally* ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 81-85 & n.14 (2010) (statement of Stephen Wm. Smith, U.S. Mag. J.) (summarizing inconsistent judicial opinions), *available at* http:// judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf.

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

consider to be surveillance takes place outside the confines of the applicable electronic surveillance laws.[8]

Enacting the new Swiss CrimPC was a long process, because the extension of federal authority that it accomplished required a change in the Federal Constitution of the Swiss Confederation (Swiss Constitution or Federal Constitution).[9] The United States, by contrast, would not require a constitutional change to update its surveillance laws. Bills currently pending in Congress would amend the federal surveillance laws to clarify their treatment of mobile communications and to strengthen and simplify the restrictions on the surveillance of other communications media.[10] Pending reform, American courts currently disagree over whether ECPA provisions even satisfy the Fourth Amendment requirements of judicial oversight and entertain different views of how the Fourth Amendment protects communications subject to surveillance.[11]

This paper describes the passage of CrimPC and its key provisions, which govern the surveillance of mail and telecommunications, collection of user identification data, use of technical surveillance devices, the surveillance of contacts with a bank, use of undercover agents, and the surveillance through physical observation of people and places accessible to the general

[8] Patricia Bellia helpfully distinguishes between electronic surveillance and communications surveillance in a recent paper. Because stored communications may be retrieved through compelled disclosure without a device, she defines communications surveillance as "techniques for acquiring the content of communications and related information." See Patricia L. Bellia, *Designing Surveillance Laws*, 43 ARIZ. L. J. 293, 294 n.1 (2011) (defining "electronic surveillance" as "the use of an electronic or mechanical device to acquire in real-time wire, oral, or electronic communications and related source and destination information.").

[9] It is much easier to change the Swiss Constitution than the United States Constitution. Any 100,000 persons eligible to vote may request a partial revision of the Swiss Federal Constitution. CONSTITUTION FÉDÉRALE [CST] [CONSTITUTION] Apr. 18, 1999, RO 101, art. 139 (Switz.). A partial revision of the Constitution can be requested by the People or decreed by the Federal Assembly. A revision needs to be adopted only by a majority of the Cantons and a majority of the eligible voters to be effective. CST art. 195. In the United States, either two-thirds of the members of both houses of Congress, or two thirds of the legislatures of the states may propose amendment to the Constitution. Such amendment must be ratified by three-fourths of the states, either by their legislatures or in state conventions. U.S. CONST. Art. 5. *See generally*, SANFORD LEVINSON, OUR UNDEMOCRATIC CONSTITUTION: WHERE THE CONSTITUTION GOES WRONG (AND HOW WE THE PEOPLE CAN CORRECT IT) 160 (2006) ("[N]o other country … makes it so difficult to amend its constitution.... Article V has made it nearly impossible….").

[10] *See, e.g.*, Electronic Communications Privacy Act Amendments Act of 2011, S.2011 (112th Cong.); Geolocational Privacy and Surveillance Act, S. 1212 (112th Cong.).

[11] *See infra* Part VIII.B.2.e (Acquisition of Stored Electronic Communications Content) and Part VIII.C.2.e. (Cell Site Location Data Acquisition).

public. It contrasts those provisions with current U.S. law. The discussion puts the proposals for U.S. law reform in perspective by showing how far our laws would have to go to match the protections the Swiss provide to their people from overreaching law enforcement surveillance. Even if Congress were to amend ECPA by passing the most restrictive of the current bills proposed, resulting U.S. law would not achieve all the privacy-protective features of CrimPC or its uniformity of treatment.

This paper shows that three features of United States law, as compared to Swiss law, contribute to a dramatically lower set of restrictions here on law enforcement surveillance. One is the failure of United States jurisprudence to find a large proportion of surveillance practices within the scope of the Fourth Amendment, as compared to the more comprehensive coverage of comparable practices under the European Convention on Human Rights (ECHR) and constitutional law in Switzerland. The second is that in the absence of constitutional regulation, United States law enforcement agents act without any authorizing statute, while in Switzerland, surveillance without statutory authorization violates the rule of law. Lastly, even when the United States does provide an authorizing statute, its provisions often fall far short of guaranteeing the meaningful remedies provided by Swiss law. Most notably, U.S. law often fails to provide notice to targets, real remedies for abuses, and neglects to impose the comprehensive judicial oversight that CrimPC mandates for all techniques it covers. In short, this paper sheds light on a radically different approach to regulating law enforcement surveillance that should open up greater possibilities for reform in this country.

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." The Swiss Confederation (also known as Switzerland or Confederatio Helvetica) has 7.9 million inhabitants[12] and is divided into 26 Cantons. Each Canton may exercise the power over its own institutions given to it by the terms

[12] 5.1 million people are eligible to vote in Switzerland.

of the Federal Constitution.[13] Until the Federal Constitution was amended to provide federal power over all aspects of criminal and civil procedure, criminal law procedure, including surveillance for criminal law enforcement, was solely within the legislative competence of the Cantons.[14]

As in most European countries, constitutional protection limits public activities. The principle of legality requires that all activities of the State, including surveillance by state authorities, shall be based on and limited by enacted law.[15] Because everyone must abide by public regulations whether or not they have individually consented to them, rights and obligations can be imposed only if they arise from a statute, the legitimacy of which derives from the consent of the people expressed through the democratic adoption of the law. CrimPC provides the specific legislative enactment required for law enforcement surveillance.

Written law, enacted by the legislature, is by far the most important source of law in Switzerland. In fact, the Swiss do not have judge-made common law as we do in the U.S. 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[16] or administrative authorities.[17] Both the Swiss Constitution and the ECHR provide significant privacy rights which the legislature must consider

[13] JEAN-FRANÇOIS AUBERT & ETIENNE GRISEL, THE SWISS FEDERAL CONSTITUTION 15-25 (2004); THOMAS FLEINER, ALEXANDER MISIC & NICOLE TÖPPERWIEN, SWISS CONSTITUTIONAL LAW 122 (2005).

[14] 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 13, at 122-126; RENÉ A. RHINOW & MARKUS SCHEFER, SCHWEIZERISCHES VERFASSUNGSRECHT (SWISS CONSTITUTIONAL LAW) 141-151 (2009).

[15] *See* CST art. 5; AUBERT & MAHON, *supra* note 14, at 39-50 (2003); THOMAS FLEINER, CANTONAL AND FEDERAL ADMINISTRATIVE LAW OF SWITZERLAND 35-37 (2004).

[16] In Europe and particularly in Switzerland, the term "government" describes the executive branch, while in the United States "government" covers the executive, legislative and judicial branches. The Swiss Government is the Federal Council, composed by seven members. Each member is the head of one of the seven departments that together form the federal administration.

[17] ANDREAS AUER, GIORGIO MALINVERNI & MICHEL HOTTELIER, DROIT CONSTITUTIONNEL SUISSE I (2006) 491-517.

when enacting a law and which courts must consider when evaluating the application of a surveillance law to a particular person. 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 mostly from article 13 of the Swiss Constitution, which says 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." The first sentence protects privacy in general and emphasizes the protection of the person and of his or her living quarters and work space 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."[18] This informational self-determination right gives every person the basic right to decide what information about his private life should be communicated to others and to what extent.[19] As a fundamental right, the right to privacy limits the power of the State but cannot be invoked against other private persons.[20]

The Swiss Supreme Court has refused to define the right to privacy, but it definitely covers every piece of personal data that is not publicly accessible.[21] On the European continent, the right to privacy relates to the dignity and autonomy of the person.[22] Article 7 of the Swiss

[18] *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).

[19] TRIBUNAL FÉDÉRAL [TF] [Federal Supreme Court] July 9, 2003, 129 ARRÊTS DU TRIBUNAL FÉDÉRAL SUISSE [BGE] I 232, 245-46 (Switz.); TF, May 29, 2002, 128 BGE II 259, 268 (Switz.).

[20] Article 8, Paragraph 3 (equality between men and women) is the exception. AUBERT & MAHON, *supra* note 14, at 62-63 and 311-17 (2003).

[21] Some examples of personal data are: identification data (TF, Apr. 23, 1998, 124 BGE I 85, 87 (Switz.); medical data; data about sexual identity and orientation (TF, Mar. 3 1993, 119 BGE II 264, 268 (Switz.); data about relationships with other human beings; and files of judicial proceedings (TF, Mar. 17, 1993, 199 BGE Ia 99, 101 (Switz.).

[22] For comparisons of the American and European notions of privacy see, e.g., 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. (2010); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. (2004); Francesca E. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. (2007). For a comparison of the German and American

Constitution also provides that human dignity must be respected and protected.[23] The right to personal freedom also protects human dignity.[24]

Fundamental rights and liberties (like the right to privacy) are not absolute and can be subject to limitations. According to article 36 of the Swiss Constitution, a restriction on the right of privacy, such as a statute that permits surveillance, must respect four conditions: it must have a legal basis, it must be justified in the public interest or for the protection of the fundamental rights of others, it must meet the standard of proportionality of means and ends,[25] and there can be no violation of the essence of the fundamental right at stake.[26] When possible, courts endeavor to interpret laws consistently with the Constitution.[27]

In sum, the Swiss Constitution requires a federal law, a public interest, and the respect of proportionality and the essence of the right. CrimPC is the federal law that authorizes the restriction of fundamental rights during a criminal investigation.

---

protection of privacy in case of surveillance, see, e.g., Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L. J. (2002); Paul M. Schwartz, *Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study*, 72 GEO. WASH. L. REV. (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. (2007).

[23] AUBERT & MAHON, *supra* note 14, at 164-178; PHILIPPE MASTRONARDI, *Kommentar zu Art. 7 BV (Commentary to article 7 Constitution)*, IN DIE SCHWEIZERISCHE BUNDESVERFASSUNG KOMMENTAR (COMMENTARY TO THE SWISS CONSTITUTION) 77-90, (2008); 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 UN COVENANTS) 1-4 (2008).

[24] Article 10 of the Swiss Constitution provides: "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."

[25] The principle of proportionality is mentioned in art. 5 Cst as well and governs all activity of the State. *See* FLEINER, *supra* note 15, at 39-40 (2004).

[26] According to the Swiss Constitution, the essence of fundamental rights is sacrosanct (art. 36). ANDREAS AUER, GIORGIO MALINVERNI & MICHEL HOTTELIER, DROIT CONSTITUTIONNEL SUISSE II 79-119 (2006); ULRICH HÄFELIN, WALTER HALLER & HELEN KELLER, SCHWEIZERISCHES BUNDESSTAATSRECHT (*SWISS FEDERAL STATE LAW*) 90-101 (2008); WALTER HALLER, THE SWISS CONSTITUTION IN A COMPARATIVE CONTEXT 157-62 (2009).

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

C. Rights to Privacy under the European Convention on Human Rights

As a member of the Council of Europe,[28] Switzerland enacted the European Convention on Human Rights[29] (ECHR) in 1974 at which time it became directly binding in the Swiss legal system.[30] 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. The Court's judgments bind the defendant country and influence law making in the other signatory countries that are not immediately involved in an action. The Court's case law spans more than fifty years.

Like the Swiss Constitution, the ECHR establishes a right to privacy and provides similar protections, even though it uses different words. Article 8 of the ECHR states: "Everyone has the right to respect for his private and family life, his home and his correspondence." The ECtHR has applied a broadly purposive approach to its interpretation of the Convention. For example, the Court views any State that chooses to employ new surveillance technologies as bearing a special responsibility for striking the right balance between the potential benefits of the extensive use of such surveillance techniques and the interference with private life they pose.[31]

[28] It is important to stress that the Council of Europe is an international organization in Strasbourg which comprises forty seven countries of Europe and was set up to promote democracy and protect human rights and the rule of law in Europe (http://www.coe.int). This organization is sometimes confused with the European Council (sometimes called the Council of the European Union, http://www.consilium.europa.eu). The European Council is not an international organization but a body of the EU, and more precisely a regular meeting of the heads of state or executive from the member states of the European Union for the purpose of planning Union policy. Forty seven States are actually Members of the Council of Europe, while twenty seven States are members of the European Union.

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

[30] Since Switzerland is a monist State, international treaties like ECHR are an integral part of the national legal system and do not need to be translated into national law. The act of ratifying an international law immediately incorporates that law into national law. *See* FLEINER, MISIC & TÖPPERWIEN, *supra* note 13, at 43-45 (2005).

[31] S. and Marper v. The United Kingdom, App. No. 30562/04 and 30566/04, § 112, European Court of Human Rights [ECtHR] (2008) *available at* http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en. (enter the full App. No. into the Application Number field, and then click Search) (finding that the retention of DNA profiles, samples, and fingerprints of persons not convicted of a crime violates Article 8 of the ECHR).

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. It also protects a right to identity and personal development, such as the right to establish relationships with other human beings and the outside world. It may also include activities of a professional or business nature. There is, therefore, a zone of interaction people have with others, even in public, which may fall within the scope of a "private life." A person's reasonable expectations of privacy may be a significant, though not necessarily conclusive, factor in determining whether he has a right to privacy.[32]

A number of elements determine whether surveillance conducted outside a person's home or private property implicates that person's private life. The Court has not enumerated those elements but rather has engaged in a fact-specific inquiry based on common norms and has considered the case as a whole. For example, in *Niemitz v Germany*, the ECtHR held that the notion of "private life" is not restricted to an inner circle in which the individual may live his own personal life as he chooses that entirely excludes the outside world. Acknowledging that the right to a private life must also comprise the right to establish and develop relationships with other human beings, the court found a warrant for the search and seizure of any documents found in the applicant's office to impinge on professional secrecy to an extent that was disproportionate under the circumstances.[33]

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."[34] Accordingly, any governmental interference in private lives

[32] *See, e.g., id*. at § 66 (finding that retention of DNA profiles, samples, and fingerprints of persons not convicted of a crime violates Article 8); Gillian and Quinton v. The United Kingdom, App. No. 4158/05, § 61, ECtHR (2010) (finding that UK 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).

[33] Niemitz v. Germany, App. No. 13710/88, § 29, ECtHR (1992) (interpreting the words "private life" and "home" in Article 8 to include certain professional or business activities or premises).

[34] ECHR art. 8.2., *supra* note 29.

must, among other things have some basis in domestic law, have a legitimate aim and 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 (law enforcement benefits).

Under the ECtHR's jurisprudence, surveillance constitutes an intrusion into private life. When it considered several cases involving surveillance laws,[35] the Court emphasized the following seven requirements for any law authorizing government surveillance: First, exploratory surveillance for preventive monitoring is prohibited. 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. Third, data may only be used for the specific purposes for which it was collected. Fourth, surveillance should be authorized by an independent body, preferably a judicial body, which is not in any way associated with the executive power.[36] In a latter decision, the ECtHR elaborated that an independent judicial authority should authorize surveillance either before or after it takes place.[37]

Fifth, the ECtHR requires such effective remedies as notification to the individual that surveillance measures were applied to him or her at a reasonable point after the grounds necessitating the surveillance have ceased, and recourse to an independent judicial authority to contest the surveillance or its effects on protected rights,[38] and the ability to bring a civil claim for any damage suffered as a result of the surveillance. Sixth, the defendant should have access to data that could be used in a trial at the latest at the end of the investigation; the defendant should have access to the original recordings until the end of the trial. The person concerned

[35] The recent cases of Kvasnica v. Slovakia, App. No 72094/01, ECtHR (2009), Calmanovici v. Romania, App. No.42250/02, ECtHR (2008) and Dumitru Popescu v. Romania (No. 2), App. No.71525/01, ECtHR (2007), have confirmed the previous jurisprudence initiated in cases such as Klass v Germany, App. No. 5029/71, ECtHR (1978), Malone v. The United Kingdom, App. No. 8691/79, ECtHR (1984), Kruslin v. France, App. No. 11801/85, ECtHR (1990) and Huvig v. France, App. No. 11105/84, ECtHR (1990).

[36] Klass v Germany, App. No. 5029/71, § 56, ECtHR (1978),

[37] Dumitru Popescu v. Roumanie (No. 2), App. No. 71525/01, ECtHR (2007). The Swiss Federal Supreme Court requires a judicial body for the authorization (control before surveillance by the Compulsory Measures Court) and the objection (control after surveillance by an appellate cantonal court) when the surveillance is about communication. TF, Dec. 27, 1994, 120 BGE Ia 314, 318 (Switz.).

[38] Kruslin v. France, App. No. 11801/85, § 34, ECtHR (1990); Dumitru Popescu v. Roumanie (No. 2), App. No. 71525/01, §§ 73, 77, ECtHR (2007).

should also be able to obtain review by a public or private expert of the authenticity or accuracy of the recording or associated transcript.[39] Seventh, the law should indicate when and how data collected by surveillance shall be destroyed.

To summarize, as 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 that law must require that any surveillance be authorized by an independent body not associated with the executive. During that review, the independent body will also check to see that the means of surveillance is proportional to the ends to be attained by it. As for the target of surveillance, she must be notified of the surveillance, provided access to the results of it, be able to have those results reviewed by an expert, be able to challenge[40] the surveillance in court, and provided damages if successful in that challenge. As we shall see, comparable restrictions and rights do not underlie much of the "surveillance" that occurs in the United States.

The ECHR has played and continues to play an important role in shaping surveillance law in many countries, including Switzerland. The ECtHR develops its own case law and interprets the Convention so as to keep it current. The Court both addresses new situations and updates its prior interpretations when appropriate.[41] As a superior international body, the ECtHR governs how national courts apply the ECHR. Swiss courts have to apply international law, and, in cases of a conflict, international law prevails over national law.[42] Swiss Courts cannot invalidate Swiss statutes on the grounds that they violate the Swiss Constitution. However, if a statute violates the same provision contained in the ECHR, the ECHR prevails and the provision of the statute that

[39] Dumitru Popescu v. Roumanie (No. 2), App. No. 71525/01, §§ 80-81, ECtHR (2007).

[40] Objection (art. 393ss CrimPC).

[41] The Court considers ECHR to be a living instrument that must be interpreted in a dynamic and evolutionary way, that must meet present day conditions, that must be interpreted according to the purpose of the Convention, and that must be interpreted so as to make the rights practical and effective. In addition, the Court must elucidate, safeguard and develop the rules instituted by the Convention. *See* Golder v. The United Kingdom, App. No. 4451/70, ECtHR (1975).

[42] CST art. 190.

cannot be interpreted in accordance with ECHR will not be applied to the case reviewed by the court.[43]

Surveillance conducted according to CrimPC, therefore, is subject to challenge on the grounds that CrimPC does not respect the ECHR.[44] It seems likely that such a challenge would currently fail, as the Swiss legislature drafted CrimPC's provisions specifically to conform to ECtHR decisions as well as other precedents. Thus, in theory, the ECHR plays a role in Swiss law like the Fourth Amendment plays in U.S. law. In practice, the former has arguably shaped current Swiss law much more, because the Swiss drafted their law to comply with its mandates, and because all law enforcement surveillance in Switzerland may proceed only according to that law.

In the United States, by contrast, the Fourth Amendment stands as a protection against excessive surveillance much more in theory than in practice. As the next section will discuss, the U.S. Supreme Court has interpreted the Fourth Amendment to apply to only a small subset of surveillance practices. Litigators for the Department of Justice have endeavored to limit as much as possible the scope of the surveillance practices subject to the Fourth Amendment in the lower courts. Until recently, they have generally achieved success. That has left a lot of what the Swiss consider to be surveillance, and which they accordingly restrict significantly, subject to Congress' weak restrictions, if they are subject to any restrictions at all.

III. The U.S. Framework for Surveillance - Compared

A. United States Legal Structure

The structure of United States 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. As discussed, in Switzerland, legislation is required to give law enforcement agents the power to conduct surveillance, and without such authorizing legislation, law enforcement

[43] AUBERT & MAHON, *supra* note 14, at 1453-62 (2003).

[44] If a court finds that a surveillance technique goes beyond the mandates of CrimPC, it could render the results of the surveillance unusable. In such a case the legislature would soon or later complete the law to add this technique.

may not act. In the United States, by contrast, law enforcement agents generally feel empowered to use any investigative method that is not specifically restricted by either legislation or the Fourth Amendment.[45] Use of undercover agents and informants, for example, is not regulated by the Fourth Amendment and therefore not considered to be surveillance.[46] Thus, law enforcement agents in America generally conduct surveillance until either Congress or the courts tell them not to do so.[47]

In the United States, 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 and different rules apply depending on the purpose of the surveillance.[48] Although federal legislation trumps inconsistent state legislation and provides a single law for government actors all over the United States,[49] the actual rules can vary by federal circuit as federal appellate courts differ in how they interpret the federal surveillance statutes.[50] The federal rules themselves break surveillance

[45] *Compare* Orin Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 N.W. LAW 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 Ac*t, 54 ALAB. 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). As a principle author of an early version of the federal prosecutor's training manual, Professor Kerr's view has generally prevailed. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 5 (2d ed. 2002), *available at* http://www.justice.gov/criminal/cybercrime/searching.html#searchmanual.

[46] *See infra* Part VIII.F.2.

[47] *See, e.g.*, Kevin Johnson, "FBI Cuts Back on GPS Surveillance After Supreme Court Ruling," USA TODAY, Feb. 7th, 2012, *available at* http://www.usatoday.com/news/washington/story/2012-02-03/fbi-gps-surveillance-supreme-court-ruling/52992842/1 (reporting that 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. 25th, 2012, *available at* http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/tab/print/.

[48] Other than a short discussion infra Part V.C., this paper will not cover surveillance for foreign intelligence gathering.

[49] 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.

[50] *See, e.g.*, Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1538-1542 (2010) (describing the Ninth Circuit's rejection of Department of Justice's view that

practices down into many subcategories that add considerable complexity.[51] Moreover, many modern practices that some, including the Swiss, would view as surveillance are not even covered by federal surveillance law. Finally, states may pass their own laws to regulate the surveillance practices of state and local law enforcement agents as well as private actors.[52] Those laws may not be more permissive than federal law.[53] To avoid undue complexity, this paper will focus on federal statutes and federal constitutional law.[54]

The Fourth Amendment stands behind all statutes, whether state or federal, ready to invalidate any provisions that do not conform to its requirement that, in America, we not be subject to unreasonable search or seizure. Unlike the ECHR, however, the Fourth Amendment has not motivated a comprehensive re-writing of surveillance laws. Instead, it has been brought to bear on only a small subset of cases. Recent years have seen more judicial opinions in which the courts have applied the Fourth Amendment to invalidate modern surveillance practices. If that continues and accelerates, United States law may slowly begin to approach the privacy-protectiveness of Swiss CrimPC. If not, however, the Fourth Amendment will be limited largely to constraining traditional wiretapping and it will continue to leave much of modern surveillance untouched.

---

opened and accessed e-mail may be acquired without a warrant based on its differing interpretation of the applicable statute).

[51] *See infra* Part VIII.C.

[52] *See, e.g.*, Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L. J. 971 (2003). State statutes are subject to judicial review in either state or federal courts to ensure their compliance with both the federal and applicable state constitution.

[53] *See* Lane v. CBS Broadcasting, 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 base-line of protection above which states could legislate).

[54] *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its States Analogues to Protect Third Party Information from Unreasonable Seizure*, 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).

B. Rights to Privacy under the United States Constitution

Under the principle of judicial review, judges ensure that federal and state statutes conform to the United States Constitution, and may overturn provisions that do not.[55] Historically, judges have used the Fourth Amendment to set the standard when evaluating law enforcement surveillance practices.[56] The Fourth Amendment requires that "the right of the people to be secure in their persons, houses, places and effects, against unreasonable searches and seizures, shall not be violated, and no warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[57] Concerns about First Amendment rights to speech have also animated courts' reasoning in some surveillance cases,[58] but not yet provided an independent basis for review.[59]

The Fourth Amendment governs electronic surveillance efforts much more in theory than in practice. Courts have required challengers to surveillance practices to surmount such hurdles as the requirement that they have standing to sue[60] and that the controversy be ripe for review.[61]

---

[55] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (finding federal surveillance statute unconstitutional to the extent it permits law enforcement access to stored e-mail without a warrant); In re Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. 2010), *affm'd,* Nov. 11, 2011 (finding federal surveillance statute unconstitutional to the extent it permits law enforcement access to stored e-mail without a warrant).

[56] *See, e.g.*, Berger v. New York, 388 U.S. 41 (1967); *Warshak,* 631 F.3d at 283-88.

[57] U.S. CONST. amend. IV.

[58] *See, e.g.*, United States v. United States District Court, 407 U.S. 297, 315 (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.")

[59] *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).

[60] *See, e.g.*, Jewel v. National Security Agency, 2011 WL 6848406 (9th Cir. Dec. 29, 2011) (reversing lower court decision that plaintiffs lacked standing to challenge widespread warrantless surveillance of their communications phone calls and e-mails as part of terrorist surveillance program); Am. Civil Liberties Union v. National Security Agency, 493 F.3d 644 (6th Cir. 2007) (finding that plaintiffs lacked standing under Fourth Amendment to challenge the same practices).

[61] *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). Also, judges will construe a statute to avoid a constitutional ruling if possible, under the principle of constitutional avoidance. *See supra* note **Error! ookmark not defined.**; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question*

In addition, because many people who are targeted for surveillance by law enforcement never learn about that surveillance, they cannot challenge practices of which they are unaware. Finally, because the United States Supreme Court takes only a limited number of cases each year, it has issued very few cases that pertain to surveillance. One decision the Supreme Court issued in 2010 refused to make a definitive ruling on the privacy of text messages, because the Court did not want to opine prematurely on such a new method of communication.[62]

The Court recently issued a decision in *United States v. Jones*, a Fourth Amendment case addressing law enforcement use of a GPS tracker attached to a car for an extended period.[63] Although all nine Justices agreed that the practice constituted a search, they provided a fractured opinion that yielded scant insight on how to interpret the precedents or the constitutional tests.[64] The case certainly affirmed that the Supreme Court would not approve of surveillance practices it views as unreasonable, but the narrowness of the Court's holding reduces the impact it might otherwise have had. A more expansive decision might have required Congress to dramatically revamp the federal surveillance electronic surveillance statute; the *Jones* decision did not.[65] Because the more expansive Supreme Court cases concern surveillance practices that are several decades old, litigants and academics debate the extent to which relatively old cases furnish rules for modern surveillance methods.[66]

---

of Law, Not Fact, 70 MARYLAND L. REV. 681, 695 (2001) (discussing successful arguments in recent case that courts should avoid constitutional ruling).

[62] *See* City of Ontario v. Quon, 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.")

[63] United States v. Jones, 132 S. Ct. 945 (2012).

[64] *See, e.g.*, Jones, 132 S. Ct. at 954 (noting that a later case may require "resort to" a reasonable expectation of privacy but that this one could be resolved on the basis of trespass); Paul Ohm, *United States v. Jones Is a Near-Optimal Result*, Jan. 23, 2011, (describing it as positive that Court issued a narrow decision and avoided the debate over "reinventing Katz"), *available at* https://freedom-to-tinker.com/blog/paul/united-states-v-jones-near-optimal-result. For further discussion, see infra Part VIII.C.2.e.

[65] For example, Justice Sotomayor's concurrence, if it had been the majority decision, would presumably have made any use of GPS tracking a search, *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring), and it would have dramatically undermined ECPA's lesser protection for electronic communications held by third parties. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[66] *See, e.g.*, Brief for the Defendant-Appellant United States of America, In Re: Application of the United States of America for Historical Cell Site Location Data, No. 11-20884, at *16-26 (5th Cir. filed February 15, 2012)

The older Supreme Court precedents do make some things clear.[67] In *Berger vs. New York*,[68] the Supreme Court found unconstitutional a New York statute that regulated electronic surveillance because the state law did not impose sufficient procedural hurdles on law enforcement agents or limit the scope of surveillance sufficiently to satisfy the Fourth Amendment.[69] In *Katz v. United States*, [70] the court formulated the reasonable expectation of privacy test and announced that surveillance practices that intrude upon such expectations must comply with the types of restrictions the Court set out in *Berger*.[71]

In a series of cases in the late 1980's and early 1990's, 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.[72] The appellate courts reasoned that video surveillance shares the features of wiretapping that make it particularly prone to abuse. In particular, the courts found that like wiretapping, silent video surveillance is hidden, indiscriminate, intrusive, and continuous and therefore must be subject to the same restrictions as wiretapping.[73]

The crucial question for surveillance law in the United States is whether or not the law enforcement practice at issue constitutes a "search" under the Fourth Amendment. The cases just

---

[hereinafter Government Brief 5th Circuit] (arguing that Supreme Court cases from the 1970's and 1980's determine the outcome in a brief filed after the Supreme Court's decision in United States v. Jones).

[67] *See* Freiwald, *supra* note *45*, at 35-41 (2004) (providing history of constitutional regulation of electronic surveillance).

[68] Berger v. New York, 388 U.S. 41 (1967).

[69] *Berger*, 388 U.S. at 60 (emphasizing the need for "adequate judicial supervision or protective procedures").

[70] Katz v. United States, 389 U.S. 347 (1967).

[71] *See Katz*, 389 U.S. at 357-58.

[72] See Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, P53-56, http:// stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

[73] *See id*.; *see also* Freiwald, *supra* note 61 , at 748-48 *(*arguing that these four factors should be used to find cell site location data protected by the Fourth Amendment*);* Brief for the Amici Curiae, Yale Law School Information Society Project Scholars and Other Experts in the Law of Privacy and Technology in Support of the Respondent, United States v. Jones, No. 10-1259, at *34-35 (S. Ct. filed Oct. 11, 2011) (arguing that the four factors should be used to find GPS tracking data protected by the Fourth Amendment).

described established that wiretapping, bugging, and some types of silent video surveillance are constitutional searches. The legal analysis under United States law proceeds quite differently from that under Swiss law. Rather than having a set of privacy protective principles that apply to all surveillance practices and that trump inadequate legislation, constitutional privacy principles apply only to that subset of practices that are considered to be constitutional searches. Moreover, rather than requiring legislation before any surveillance is authorized, as in Switzerland, all surveillance is effectively authorized until successfully challenged in court as violating the Fourth Amendment.

In two important cases, the Supreme Court significantly limited what surveillance-type practices count as a constitutional search. In *United States v. Miller*,[74] the Court declined to find a Fourth Amendment search when law enforcement agents compelled a bank to produce its records pertaining to the defendant such as deposit slips and account statements. The Court stated "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[75] The government and some academics have argued that the *Miller* case implies a lack of constitutional protection for any information obtained from a third party, which could include records of electronic communications stored with service providers.[76] Others have argued that the *Miller* case should be narrowly construed.[77] Under one such narrow construction, customers would not forfeit privacy by sharing their information with

[74] 425 U.S. 435 (1976).

[75] 425 U.S. at 443.

[76] *See, e.g.*, Brief for the Defendant-Appellant United States of America, Warshak v. United States, No. 06-4092, at *38 (6th Cir. filed Oct. 13, 2006) (arguing that "the government may compel a third party to disclose anything that the third party can access").

[77] *See, e.g.*, Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375 (2004); 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 stores the records in the ordinary course of its business. *See, e.g.*, In re Application of the United States for an Order Directing a Provider of Electronic Communications Services to Disclose Records to the Government, 620 F.3d 304, 317-18 (3d. Cir. 2010) (rejecting applicability of *Miller* and *Smith* and finding that acquisition of cell site location may be constitutional protected, and leaving it to the discretion of the magistrate judge to determine whether a warrant is required).

intermediaries, such as phone companies and electronic communication providers.[78] Whatever the proper application of *Miller* to new technologies, there is no doubt that it influenced Congress to provide only limited restrictions on law enforcement access to stored electronic records in the Electronic Communications Privacy Act ("ECPA").[79]

The Supreme Court extended the *Miller* holding to the communications context in 1979 when it found that law enforcement acquisition of dialed telephone numbers was not a Fourth Amendment search in *Smith v. Maryland*.[80] Law enforcement agents used a device known as a "pen register" to obtain the telephone numbers dialed on a telephone. Pen registers 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.[81] 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.[82] As with the *Miller* case, some have argued that the *Smith* decision should be limited to its facts and not read to imply a lack of constitutional protection for modern electronic communications information.[83] Justice Department officials have maintained that *Smith* establishes that all "non-content" information lacks Fourth Amendment protection.[84] Whatever the appropriate reading of the case, it inspired

[78] *See* Patricia L. Bellia and Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. L. FORUM 122, 158-69. In *Miller*, government agents acquired Miller's records from his bank, which was considered a party to his bank records.

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

[80] 442 U.S. 735 (1979).

[81] 442 U.S. at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)). *See also* S. Rep. No. 99-541, at 49 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3603 (stating that pen registers "record only the telephone numbers dialed"). *See generally* Susan Freiwald, *Uncertain Privacy: Communications Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 982-89 (1996) (reviewing the "Evolution of the Pen Register From Mechanical Device to Computer System").

[82] 442 U.S. at 741-44.

[83] *See, e.g.*, Freiwald, *supra* note 72, at P46-49; *cf.* 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 a third party… .") (citing *Smith* and *Miller*).

[84] *See, e.g.*, Government Reply Brief, In re Application of the United States for an Order Directing a Provider of Electronic Communications Services to Disclose Records to the Government, No. 08-4227, at *2-3 (3rd Cir. filed

Congress to provide in ECPA relatively little restriction on law enforcement access to communication attributes, those features of communications other than their content.[85]

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 constitutional searches that intruded upon reasonable expectations of privacy. Some United States courts have been expansive in their reading of *Miller* and *Smith*, and have accordingly found many modern surveillance practices to be outside the protection of the Fourth Amendment.[86] Recently, some courts have rejected such broad readings, and found new practices to be constitutionally protected because they differ significantly from the practices considered in the precedent cases.[87]

Congress retains complete discretion over how to regulate those practices that do not intrude upon reasonable expectations of privacy. It can restrict law enforcement use of such surveillance practices, and any others that it does not see as implicating the Fourth Amendment, as little as it wishes. Unlike in Switzerland, Congress has not produced a comprehensive surveillance law that covers all types of surveillance used during investigations. . Instead, restrictions derive from piecemeal legislation such as ECPA, which has fallen out-of-date in the twenty-five years since its passage. As we will discuss, ECPA provides dramatically fewer restrictions than CrimPC for those techniques it covers. In addition, because ECPA does not cover a host of practices that it views as falling outside of the ambit of the Fourth Amendment

---

Apr. 6, 2009), *available at* 2009 WL 3866620 (arguing that "non-content" cell-site location records are not subject to Fourth Amendment protection).

[85] *See infra* Part VIII.C.2; Freiwald, *supra* note 81, at 969-75, 993-1007 (describing how Congress accorded weak protections to communications attributes in the federal surveillance statutes).

[86] *See, e.g.*, United States v. Forrester, 512 F.3d 500 (9th Cir. 2008) (finding real-time collection of IP addresses by law enforcement unprotected by the Fourth Amendment); Government Brief 5th Circuit, *supra* note 66, 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.").

[87] *See* cases cited *infra* note 55; *see also* In re Application of the United States for an Order Directing a Provider of Electronic Communications Services to Disclose Records to the Government, 620 F.3d 304 (3d. Cir. 2010) (rejecting applicability of *Miller* and *Smith* and finding that acquisition of cell site location may be constitutional protected, and leaving it to the discretion of the magistrate judge to determine whether a warrant is required).

protection, law enforcement in the United States conducts many surveillance practices entirely free of constraints that are highly restricted in Switzerland under CrimPC.[88]

C. Rights to Privacy under International Law

The United States is not a signatory to the European Convention on Human Rights, as it is not a member of the Council of Europe. In addition, the United States is not a party to an international treaty that would purport to directly regulate its national law enforcement practices 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."[89] However, individual state parties may determine which specific safeguards to impose, and the treaty imposes no specific due process requirements on the United States, nor an international enforcement body.[90]

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[91] that part of the treaty that protected against unlawful interference with a person's privacy, family, home, or correspondence.[92] Without additional legislation, then, a U.S. citizen cannot challenge surveillance on the basis of the 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.[93] Therefore, no United States citizens can use its dispute resolution mechanisms to challenge domestic law enforcement surveillance.

---

[88] State surveillance laws may provide greater limits than ECPA on state law enforcement actors but do not constrain federal actors. *See, e.g.*, Henderson, *supra* note 54; Kennedy & Swire, *supra* note 52.

[89] Council of Europe Convention on Cybercrime art. 15, *done* Nov. 23, 2001, T.I.A.S. No. 13174.

[90] Miriam Miquelon-Weisman, *The Convention on Cybercrime: A harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, J. MARSHALL J. COMP. & INFO. L., Winter 2005, 329, 340.

[91] *Id*.

[92] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171, S. Exec. Doc. E, 95-2 (1978)§

[93] International Court of Justice, *How the Court Works*, http://icj-cij.org/court/index.php?p1=1&p2=6 (last visited Sep. 2, 2011).

The absence of a higher order treaty like the ECHR has permitted law surveillance in the United States to operate without several of the safeguards against abuse found in the Swiss system. That is particularly true given that the United States' Fourth Amendment fails to protect several types of surveillance practices that the Swiss system significantly restricts.

IV. Switzerland: Applicable 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 mails and telephone networks. In 1889, the federal Act on Telephones made the content of telephone calls secret.[94] This first law protected all users because the law treated all phone calls as private matters. Thirty years later, the federal Act on Telegraph and Telephone Traffic[95] and the federal Postal Service Act[96] both provided law enforcement authorities the right to access the content of telephone calls, telegraph messages and mail. These later laws gave a lot of power to the State. Decades later, 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).[97]

Viewing private life as insufficiently protected by the law, the federal Parliament decided at the end of 1968 to add new articles in the Criminal Code that created offenses for breach of privacy or secrecy.[98] 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

[94] Loi fédérale sur les téléphones.

[95] Loi fédérale du 14 octobre 1922 réglant la correspondance télégraphique et téléphonique.

[96] Loi fédérale du 2 octobre 1924 sur le Service des postes.

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

[98] CP art. 179bis-179septies.

conducted surveillance activities in violation of the Criminal Code was not guilty because he was doing his official duty.[99] This case spurred reform proposals in the Swiss Parliament.

As mentioned, Switzerland enacted the European Convention on Human Rights (ECHR) in 1974.[100] In 1978, the ECtHR held that any interference with an article 8 privacy right needed to have some basis in domestic law.[101] Despite the recent changes to its Criminal Code, Switzerland could not claim at that time to have a clear rule of law for surveillance and particularly not one that satisfied the requirement of the proportionality of means and end. To conform to the requirements of ECHR, Switzerland needed to update its surveillance law.

Parliament finally enacted the federal Act on Privacy Protection in 1979,[102] which amended the federal Act on Telegraph and Telephone Traffic and the federal Postal Service Act. The Act endeavored to regulate secret surveillance using the same principles that regulate the search of a house or the conduct of an arrest. It enumerated the conditions for surveillance and provided legal protection to the individual subject. 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 the surveillance. Parliament also amended the Criminal Code to make a breach of privacy caused by an individual or public official an offense, unless specifically authorized by a law and conducted in accordance with it.[103] That precluded the court from excusing official surveillance merely on the grounds that the breach was conducted as part of official duties.

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

[100] *See supra* note 29.

[101] Klass v. Germany, App. No. 5029/71, ECtHR (1978).

[102] Loi fédérale sur la protection de la vie privée du 23 mars 1979 (modifications de lois fédérales).

[103] CP art. 179octies. This addressed the holding in *Ligue marxiste révolutionaire*, discussed *supra* note 99.

The Federal Act of October 6, 2000 on the Surveillance of Post and Telecommunications (SPTA)[104] was enacted in 2002 and brought all provisions pertaining to the surveillance of post and telecommunications together in the same act.[105] The Federal Council decided not to have SPTA cover the use of such technical surveillance devices as 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.[106] Parliament designed SPTA to be as uniform as possible and to protect every kind of letter and parcel and telecommunication from surveillance.[107] It covered the content and attributes of letters and parcels,[108] phone calls (including Voice over IP), e-mail, text messages, and fax and pager transmissions. It did not

[104] Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), RS 780.1.

[105] While CrimPC establishes the rights of the target and imposes conditions on law enforcement authorities, SPTA establishes the technical requirements and obligations of the communication and postal services providers. "Communication Service Provider" is the new term in CrimPC covering both Internet Service Providers (ISP) and Telecommunication Service Providers (TSP).

[106] About the situation prior to the Federal Act on the Surveillance of Post and Telecommunications (SPTA) and SPTA in general: 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); ASTRID VON BENTIVEGNI, LES MESURES OFFICIELLES DE SURVEILLANCE EN PROCÉDURE PÉNALE (OFFICIAL SURVEILLANCE MEASURES IN CRIMINAL PROCEDURE) (1986).

[107] 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 1st, 1998) FF IV 3689, 3703-9 (1998). The rules for monitoring of post and telecommunication were applied by cross-reference to other technical surveillance devices for federal investigations. Some Cantons did the same, some had other rules, and some did not have a single rule.

[108] 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).

cover communications made in Internet public forums or chat rooms.[109] SPTA inspired the new CrimPC.[110]

CrimPC applies to all entities, so whether or not they are subject to SPTA, all entities have to permit lawful surveillance on their systems.[111] The next section describes the passage of CrimPC.

B. CrimPC

At the request of the Federal Council, a committee of experts, created in 1994 to work on the unification of criminal procedure, together with the Federal Council, submitted a draft CrimPC in 2001 to the legislative process. On March 12, 2000, all Cantons and 86.4% of the people eligible to vote approved the constitutional amendment needed.[112] In October 2007, both chambers of Parliament had accepted the bill and the referendum period had passed without a referendum having been initiated. CrimPC replaced twenty-seven different codes of criminal procedure (twenty-six cantonal and one federal).[113]

While SPTA and previous cantonal codes largely inspired CrimPC, the latter required many changes for some Cantons, especially those in the French part of Switzerland. Such

[109] While public conversations are not covered, police officer interventions in such conversations would be covered under rules pertaining to undercover agents: Beat Rhyner & Dieter Stüssi, *Kommentar zu Art. 269-279 StPO (Commentary to article 269-279 CrimPC)*, in VSKC-HANDBUCH (VSCK HANDBOOK) 443, (Gianfranco Albertini, et al. eds., 2008) [hereinafter Rhyner & Stüssi, *Kommentar zu Art. 269-279 StPO*]; Beat Rhyner & Dieter Stüssi, *Kommentar zu Art. 286-298 StPO (Commentary to article 286-298 CrimPC*), in VSKC-HANDBUCH (VSCK HANDBOOK) 498-499, (Gianfranco Albertini, et al. eds., 2008) [hereinafter Rhyner & Stüssi, *Kommentar zu Art. 286-298 StPO]*.

[110] Parliament passed the Federal Law on Undercover Investigation on June 20, 2003 and CrimPC now includes important rules from that law as well.

[111] 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, Rapport explicatif relatif à la modification de la Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) (Explanatory report about the modification of the Surveillance of Post and Telecommunications Act of October 6, 2000)).

[112] Arrêté du Conseil fédéral du 17 mai 2000 constatant le résultat de la votation populaire du 12 mars 2000, FF 2814-2820, (2000).

[113] Now, cantonal bodies enforce substantive federal criminal law and also comply with the federal CrimPC. Swiss (federal) Criminal Code was adopted in 1937. 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.

Cantons, who 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. Because some Cantons had to make extensive administrative changes to conform to CrimPC, the legislature decided to delay the new law's introduction until January 1, 2011.[114]

CrimPC provides for the public prosecutor to lead preliminary proceedings, conduct the examination of witnesses and others, bring charges and represent its case before the courts. Newly created Compulsory Measures Courts offset the public prosecutor's power. In addition to overseeing surveillance activities, the new courts approve pretrial and security detentions and authorize the deployment of undercover investigators.[115]

CrimPC provides the legal basis for all surveillance in criminal investigations. When an official wants to use any surveillance measure, he needs to satisfy the requirements of CrimPC; private parties cannot use any surveillance measures that require authorization under CrimPC. [116] The Criminal Code prohibits surveillance conducted without authorization information gathered by such surveillance would be considered illegally obtained and subject to the exclusionary rule when challenged by the subject.[117] In addition, officials who conduct surveillance in violation of CrimPC risk the imposition of disciplinary measures and prosecution.[118] Swiss law thus significantly deters violations of CrimPC.

---

[114] The federal Civil Procedure Code (CivPC) and the federal Juvenile Criminal Law Act also came into force on that day.

[115] The Compulsory Measures Court is a regular court (art. 18 CrimPC). About the others competences of the Compulsory Measures Court and the distinction to others courts: ANDRÉ KUHN, PROCÉDURE PÉNALE UNIFIÉE: REFORMATIO IN PEJUS AUT IN MELIUS? (UNIFIED CRIMINAL PROCEDURE: REFORMATIO 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 PRAXIS) 63-64 (2009).

[116] Proposed modifications of the SPTA could introduce new provisions in CrimPC: Government-Software (270bis) and IMSI-Catcher (270ter). Article 270bis would authorize the use of Governmental-Software and the decryption of data. *See* Conseil Fédéral, Rapport explicatif relatif à la modification de la Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT); Conseil Fédéral, Avant-projet de révision de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT).

[117] For more on the remedies for unlawful surveillance, see *infra* Part VI.D.

[118] The provisions contained in the Criminal Code aim to avoid private surveillance and official surveillance without authorization, or "wild surveillance." [the authors will update with any prosecutions brought at press time]

C. Other Acts Pertinent to Law Enforcement Surveillance

The Internal Security Act (ISA),[119] which is the short name for the Federal Act on Measures to Safeguard Internal Security of March 21, 1997, aims to detect and address dangers relating to terrorism, illegal intelligence, violent extremism, illegal arms and radioactive material trade and hooliganism.[120] The ISA is used for all civil (non-military) surveillance conducted inside the country, whether or not the target is a Swiss citizen. The intelligence agencies do not conduct surveillance regulated by CrimPC, but instead operate according to the ISA rules. Because intelligence agencies conduct surveillance to prevent the occurrence of offenses proactively, persons targeted by such surveillance are sometimes not even suspected of having committed or intending to commit a criminal offence. For that reason, ISA permits only physical observation of public and freely accessible places as well as video and audio recording of those places. [121] It does not permit surveillance of post and telecommunications, contacts with a bank or use of technical surveillance devices to observe private places. Because the ISA limits surveillance to publicly available information, the privacy harm is limited and the Constitution does not require prior judicial authorization for intelligence surveillance.[122]

The Swiss Criminal Code,[123] the Swiss Civil Code[124] and the Federal Act on Data Protection contain other rules relevant for surveillance. But since the enactment of CrimPC,

---

[119] The Federal Act on Measures to Safeguard Internal Security. Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120).

[120] 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).

[121] Intelligence agents may gather information through sources open to the public and official documents, and cantonal and federal authorities may transmit information to intelligence agencies. Art. 14 ISA.

[122] There is an indirect right to access information (art. 18 ISA) and a general political and administrative control by the Federal Data Protection and Information Commissioner (FDPIC) and by the Control Delegation of the Federal Chambers (CD).

[123] The Swiss Criminal Code penalizes unlawful entry (CP art. 186) and breach of postal or telecommunications secrecy as a misdemeanor (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 LAW",

those rules do not generally govern surveillance by law enforcement.[125] Officials who carry out an interception in accordance with CrimPC do not commit an offense under these laws.

V. USA: Applicable Acts

A. The Wiretap Act

Congress passed the Wiretap Act[126] in 1968 and codified the strict requirements that the Supreme Court had established in *Berger* the year before.[127] The Wiretap Act significantly restricts the use of surveillance by law enforcement agents in criminal investigations. Under the Wiretap Act, law enforcement agents may not wiretap without exhausting other remedies, minimizing the acquisition of non-incriminating communications, and establishing both probable cause to believe a crime has been committed by the target and significant reason to believe that the wiretapping will yield evidence of that criminality.[128] The Wiretap Act also provides for mandatory notice to targets, substantial remedies to victims of improper investigations, and detailed requirements for reporting to Congress.[129] The Wiretap Act's standards are the closest to

---

INTERFERENCES AND INTERDEPENDENCES BETWEEN PRIVATE LAW AND PUBLIC LAW) (JEAN-PHILIPPE DUNAND & PASCAL MAHON eds., 2009).

[124] 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 all those causing the infringement. 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. REGINA E. AEBI-MÜLLER, PERSONENBEZOGENE INFORMATIONEN IM SYSTEM DES ZIVILRECHTLICHEN PERSÖNLICHKEITSSCHUTZES UNTER BESONDER BERÜCKSICHTIGUNG DER RECHTSLAGE IN DER SCHWEIZ UND IN DEUTSCHLAND (PERSONAL RELATED INFORMATION IN THE SYSTEM OF PROTECTION OF PERSONALITY BY CIVIL LAW WITH PARTICULAR ATTENTION TO THE LEGAL FRAMEWORK IN SWITZERLAND AND IN GERMANY) 1-180 (2005); STÉPHANE BONDALLAZ, LA PROTECTION DES PERSONNES ET DE LEURS DONNÉES DANS LES TÉLÉCOMMUNICATIONS (PROTECTION OF PERSONS AND THEIR DATA IN TELECOMMUNICATIONS) 146-56 (2007).

[125] They do pertain to surveillance by private actors (*e.g*. monitoring at the workplace or on private property).

[126] 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 (2002)). Commentators refer to the law as either "Title III" or the more intuitive "Wiretap Act".

[127] Berger v. New York, 388 U.S. 41 (1967). *See supra* Part III.B.

[128] 18 U.S.C. § 2518; JAMES G. CARR AND PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE §4.17-4.48 (Aug. 2011 ed.)

[129] *See* Freiwald, *supra* note *45* (arguing that surveillance of online communications should adhere to the Wiretap Act's procedural safeguards).

those provided by CrimPC, and offer the highest level of judicial and congressional oversight of any of the other surveillance methods in the United States.

The depth of Wiretap Act protections may be great, but their breadth is not. The Wiretap Act applies by its terms only to the use of wiretaps to obtain the contents of wire conversations (telephone calls) and the use of electronic surveillance (bugs) to record oral conversations in places where those conversations are subject to reasonable expectations of privacy.[130] As mentioned earlier, the substantive provisions of the Wiretap Act have been applied, by analogy, by federal courts of appeal to govern use of video surveillance in places where the subject has a reasonable expectation of privacy.[131] All other types of surveillance proceed either according to other statutes, such as ECPA, or are unregulated by federal statutory law.

B. The Electronic Communications Privacy Act ("ECPA")

In 1986, Congress endeavored to bring the law into the electronic age by amending the Wiretap Act to cover surveillance of modern communications technologies. The Electronic Communications Privacy Act ("ECPA")[132] it passed that year extended some but not all of the Wiretap Act's protections to electronic communications' content; it also includes entirely new provisions to govern some new surveillance practices Congress viewed as less intrusive than traditional wiretapping. ECPA's complexity has led to considerable controversy about exactly what it provides.[133]

ECPA contains three titles. The first title amends the 1968 Wiretap Act provisions to extend their protection to the acquisition in real-time of electronic communications such as e-mail.[134] As we will discuss in more detail, it is easier for agents to obtain approval for such

[130] 18 U.S.C. § 2511.

[131] *See supra* text accompanying notes 72 to 73.

[132] 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.).

[133] *See, e.g.*, Mink v. Salazar, 344 F. Supp. 2d 1231 (D. Colo. 2004) ("As several courts have noted, the [ECPA] is 'famous (if not infamous) for its lack of clarity.'") (citations omitted); Freiwald, *supra* note *45*, at 42-74 (describing and critiquing the online surveillance provisions).

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

surveillance than for a traditional wiretap.[135] More significantly, no information obtained in violation of ECPA is subject to a statutory exclusionary remedy, which significantly reduces the deterrent effect of the statute.[136] ECPA's second title, the "Stored Communications Act," address access to stored electronic information.[137] It has significantly fewer protections for such information than the first title and distinguishes between the contents of electronic communications and information associated with such communications that are not-contents, or "communication attributes."[138] The third title, known as the "Pen Register Act"[139], covers law enforcement use of pen registers and "trap and trace devices" to obtain dialing and addressing information for both wire and electronic communications.[140] The Pen Register provisions restrict law enforcement agents significantly less than do the analogous Wiretap Act provisions.

C. The USA PATRIOT Act and other amendments

Congress passed the USA PATRIOT Act in 2001 ("Patriot Act"),[141] just six weeks after the terrorist attacks of September 11.[142] While many of the Patriot Act's provisions have nothing

[135] *See infra* Part VIII.B.2.d.

[136] It also reduces the number of cases brought to contest surveillance conducted according to its authority. *See* Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L. J. 805 (2003); *see also* Freiwald, *supra* note 72 (arguing that difficulties in determining constitutional questions have also inhibited their resolution).

[137] Title II, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701-11 (2010)).

[138] *See* Freiwald, *supra* note 81, at 951 (introducing and explaining use of the term "communication attributes"). The statute creates different categories of attributes for different treatment, which the next Part covers in more detail.

[139] Title III, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1873 (1986) (codified as amended at 18 U.S.C. §§ 3121-27 (2010)).

[140] Historically, pen registers acquired the telephone number dialed by the target's phone. Trap and trace Devices, which the Pen Register Act also covers, acquired the telephone number of the calling party, revealing the same information as does caller id. Modern pen registers acquire more detailed information.

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

[142] For an insightful description of the legislative process that produced the Patriot Act, see Beryl A. Howell, *Seven Weeks: The Making of the USA Patriot Act*, 72 GEO. WASH. L. REV. 1145 (2004). Ms. Howell was senior democratic

to do with surveillance, a few of them did clarify or alter some surveillance rules.[143] For example, the Patriot Act amended ECPA so that acquisition of voicemail would receive the same (lesser) protection as stored electronic messages instead of the stronger protections accorded to telephone calls by the Wiretap Act.[144] In another example, the Patriot Act clarified 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.[145]

Other than the Patriot Act, which had a limited impact on surveillance regulations, Congress has not significantly altered the statutory scheme just described. In 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA"),[146] to ensure that providers of telecommunications service maintain the accessibility of their systems to wiretapping notwithstanding the introduction of digital communications technologies.[147]

Although a thorough discussion lies beyond the scope of this paper, it is worth noting that, unlike terrorism-motivated surveillance in Switzerland,[148] surveillance for foreign intelligence gathering and to prevent terrorism may be conducted with significantly fewer rather than more constraints.[149] Agents who conduct such surveillance operate under the Foreign

---

staffer at the time, and she argues that several democrats valiantly resisted, sometimes successfully, some of the Administration's demands. *See id.*

[143] *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 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 provisions' impact on electronic privacy rights).

[144] *See* Patriot Act § 209, 115 Stat. 272, 283 (2001); *DOJ Field Guidance*, *supra* note 143, at 1232-33.

[145] *See* Patriot Act §§ 216, 115 Stat. 272, 288-90 (2001) (amending 18 U.S.C. § 3127(3)); *DOJ Field Guidance*, *supra* note 143, at 1233-34; *supra* note 45.

[146] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001-10 (2000) and in scattered sections of 18 U.S.C.)

[147] *See generally* Freiwald, *supra* note 81 (describing the debates that accompanied the passage of CALEA).

[148] *See infra* text accompanying notes 119 –122.

[149] *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);

Intelligence Surveillance Act,[150] which provides considerably more discretion to agents, permits even traditional wiretapping to proceed without notice to targets, and permits review by a secretly impaneled court whose proceedings are not public.[151] In response to controversial large-scale monitoring programs conducted in the wake of the September 11 attacks, Congress amended FISA to provide immunity to service providers who aided such monitoring.[152]

Returning to law enforcement surveillance, recent years have seen growing recognition that the current statutory framework for regulation of the surveillance of new technologies needs updating both to conform to the case law and as a matter of public policy.[153] Reform bills have been introduced to simplify and strengthen rules regulating surveillance of new electronic communications.[154] Passage of such bills is surely inhibited by the Congress' current inability to overcome a partisan divide. Perhaps Congress will be spurred to act by an increasing number of decisions finding ECPA to be unconstitutional as well as the recent Supreme Court case finding law enforcement use of GPS tracking to be a search under the Fourth Amendment.[155]

VI. Surveillance Procedure According to Swiss CrimPC

Before detailing the specific protections afforded to each type of surveillance in Switzerland, the following sections describe the types of limits that the law provides. That overview is designed to give the reader a sense of the range of options from which the legislature

---

Peter Swire, *The System of Foreign Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004) (reviewing the history of foreign surveillance laws and practices).

[150] Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801-62, covers the use of electronic surveillance and other investigatory techniques to pursue foreign intelligence.

[151] *See* KRIS & WILSON, *supra* note 149, at § 27; William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1 ,89 (2000).

[152] See FISA Amendments Act of 2007, § 802, Pub. L. No. 110-261, 122 Stat. 2435, codified at 50 U.S.C. § 1885a (granting retroactive immunity to service providers); In Re National Security Agency Telecommunications Records Litigation, 2011 WL 6823154 (9th Cir. Dec. 29th, 2011) (upholding the constitutionality of the immunity provision).

[153] *See, e.g.*, Digital Due Process Coalition, *About the Issue*, 2010, *available* at http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

[154] *See* sources cited *supra* note 10.

[155] *See infra* text accompanying notes 63 - 65.

chooses when it imposes restrictions on law enforcement's use of a particular surveillance method.

A. Levels of Oversight

CrimPC divides surveillance methods into six main categories[156] subject to one of three different authorization processes which vary according to the intrusiveness of the method. More invasive categories need to be approved by more independent bodies, not the police.[157] As mentioned, CrimPC established independent Compulsory Measures Courts to oversee law enforcement surveillance requests, among other duties.[158]

Under the most restricted category, the Compulsory Measures Court must confirm the propriety of the public prosecutor's order that the police conduct surveillance. If the Court does not confirm the order, the surveillance must terminate, and the results obtained from it cannot be used. Under the middle category, the police may conduct surveillance only when the public prosecutor authorizes them to do so. Under the least restricted category, the police are free to act up to a month without any prior judicial authorization from the Compulsory Measures Court and without authorization from the public prosecutor.[159] This last category includes only surveillance measures where the harm is low and where it is unclear if there is a breach of privacy.

B. Conditions

1. Procedural Hurdles

Surveillance measures aim to discover the perpetrator or gather evidence related to a committed offence. Surveillance may not be undertaken unless a criminal offense has already

[156] They are: the monitoring of post and telecommunications, use of technical surveillance devices, surveillance of contacts with a bank, undercover operations, the collection of user identification data, and physical observation. *See* i*nfra* Part VIII.

[157] The police and the public prosecutor are law enforcement authorities (art. 15 and 16 CrimPC).

[158] *See infra* note 115.

[159] After one month, the continuation of the observation requires authorization by the public prosecutor.

been committed; it may not be conducted to prevent crimes from occurring in the first place.[160] Some ongoing offenses like drug trafficking are considered committed offences; acts in preparation for the commission of some particularly serious offenses are themselves independent offenses.[161] Surveillance may not take place unless there is the strong suspicion that an offense has been committed, or, for physical observation only, an intermediate standard which is less than strong suspicion but more than simple suspicion.[162] Surveillance itself cannot be used to create suspicion, which means that preventive monitoring and fishing expeditions are strictly prohibited.[163]

2. Predicate Offenses

Surveillance is appropriate only for serious criminal offenses. Different categories of surveillance require different levels of seriousness. Some categories of surveillance can proceed for a wide range of crimes, and others may proceed only to investigate a specific list of serious crimes. Decisions about which offenses to include have often reflected politics rather than legal analysis.[164]

3. Other Limits

All surveillance practices must respect the subsidiarity principle and the need for proportionality between means and end. Subsidiarity means that surveillance must not be the

[160] *But see* text accompanying notes 118- 121 for a discussion of surveillance under ISA, which may proceed preventatively.

[161] Those offenses are explicitly listed in Swiss Criminal Code article 260bis as: 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).

[162] Note that only simple suspicion is required to open an investigation that does not use surveillance. CRIMPC art. 309.

[163] 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 106, at 145.

[164] Several scholars have criticized the lists of offenses for that reason. *See, e.g.*, Conseil Fédéral, Analyse de la situation et des menaces pour la Suisse à la suite des attentats terroristes du 11 septembre 2001, rapport du Conseil fédéral à l'intention du Parlement (Analysis of the situation and the threats for Switzerland after the Terrorist Attacks of September 11, 2001, Report of the Federal Council to the Parliament) FF 1674 (2003) 1732; Sträuli, *supra* note 108, at 124-127; HANSJAKOB, *supra* note 106, at 154-76 (2006).

first investigatory activity; other investigatory activities already conducted have not been successful or have no prospect of success.[165] Proportionality depends on the seriousness of the offense, the invasion of privacy, the likelihood of success, the length of the surveillance and its type. Proportionality requires that the scope and duration of surveillance be as limited as possible. Proportionality review means that less invasive surveillance techniques will more easily pass muster than more invasive techniques.[166]

C. Notice

Surveillance notice provides a crucial means for the target to defend her rights.[167] Notice provides the only official way to know about surveillance and opens the way to an objection by the notified target.[168] To comply with the effectiveness of remedies granted by the article 13 ECHR targets need to receive notice.[169] CrimPC calls notice "communication" and requires it for all types of surveillance.[170]

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,

[165] Surveillance can be undertaken without having first tried all possible alternatives if such other investigatoryactivities would be made disproportionately more complicated. HANSJAKOB, *supra* note 106, at 152-154 (2006); NIKLAUS SCHMID, SCHWEIZERISCHE STRAFPROZESSORDNUNG, PRAXISKOMMENTAR (SWISS CRIMINAL PROCEDURE CODE: PRAXISCOMMENTARY) 505-06 (2009).

[166] Other limits restrict surveillance to those set out in the order, see CRIMPC art. 278, and protect professional secrets. *See* CRIMPC art. 271 CrimPC; 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 131-7 (2011).

[167] 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).

[168] CRIMPC art. 279, para. 3; CRIMPC art. 298, para. 3.

[169] HANSJAKOB, *supra* note 106, at 310 (2006); PIQUEREZ, *supra* note 108, at 627. The Federal Council says the duty to provide notice is a matter of Constitution: 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 2007 4773) 4838.

[170] CRIMPC art. 279, 284, 298.

the conditions imposed on the surveillance, and the rights of the target as a result of the surveillance.[171]

Notice is required even if 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. Typically the court will permit notice to be postponed when notice without delay will ruin another ongoing investigation, but recourse to this exception should be limited and the court should rarely permit notice to be omitted altogether. Within ten days of receiving notice, a surveillance target may contest violations of law including misuse or incorrect use of discretion and incomplete or incorrect establishment of the factual circumstances of the case. The court has complete power of review over the facts and law.[172]

D. Consequences if Illegal

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.[173] Whether or not an authorization would have been granted is irrelevant.[174]

For unauthorized surveillance, CrimPC relies on general rules about illegal evidence and subjects some data to a complete exclusionary rule and treats other types as relatively unusable. Under a complete exclusionary rule, findings may not be used and data must be destroyed immediately. When surveillance results are relatively unusable: findings can be used if they are necessary to solve serious offenses.[175] If the evidence could have been obtained legally, the court

[171] SCHMID, *supra* note 165, at 525; HANSJAKOB, *supra* note 106, at 315-16.

[172] Complaints are addressed to cantonal (trial) courts. CRIMPC 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); DANIEL JOSITSCH, GRUNDRISS DES SCHWEIZERISCHEN STRAFPROZESSRECHTS (BASICS OF SWISS CRIMINAL PROCEDURE LAW) 203-6 (2009); André Kuhn, *La procédure pénale suisse selon le futur CPP unifié*, 128 REVUE DE DROIT SUISSE 161-162 (2009).

[173] CRIMPC art. 277, art. 281, para. 4, art. 289, para. 6; TF, May 3, 2005, 131 BGE I 272, 281 (Switz.).; HANSJAKOB, *supra* note 106, at 250-53 (2006).

[174] TF, Oct. 9, 2007, 133 BGE IV 329, para. 4.4 (Switz.).

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

must weigh the competing interests of the prosecution in confirming suspicions and the accused targets in protecting their personal rights.[176]

The European Court of Human Rights (ECtHR) has expressed that it should be left to national courts to decide on the admissibility of evidence, but the ECtHR may opine on whether the proceedings as a whole, including the way in which evidence was obtained, has been fair.[177] The ECtHR has held that the exclusion at trial of evidence gained through any unlawful surveillance activity is necessary but not sufficient as a remedy for any violation of the right to private life that may have occurred.[178]

When government agents have unlawfully employed surveillance, CrimPC entitles the victim to request reasonable compensation and reparation for non-pecuniary loss. While being a victim of illegal surveillance does not automatically entitle a person to damages,[179] CrimPC provides damages for economic losses and emotional distress, but not punitive damages. CrimPC permits those other than the accused to be compensated for damages incurred by unlawful surveillance by law enforcement agents and those who aid law enforcement.[180]

E. Reporting

CrimPC does not require that any particular reports about surveillance practices be prepared. The requirement of notice to the targets of surveillance, however, adds significant transparency. In addition, information about surveillance practices may be available from the police or other bodies involved in surveillance. Apparently as a voluntary matter, some authorities released a report about the monitoring of mail and telecommunications.[181]

---

[176] TF, Sept. 7, 1983, 109 BGE Ia 244, para. 2.3 (Switz.).

[177] Schenk v. Switzerland, App. No. 10862/84, ECtHR (1988).

[178] Khan v. The United Kingdom, App. No. 35394/97, § 44, ECtHR (2010); Taylor-Sabori v. The United Kingdom, App. No. 47114/99, §§ 22-24 (2002).

[179] CRIMPC art. 431, 434; PIETH, *supra* note 115, at 221-1; SCHMID, *supra* note 165, at 837-9.

[180] CRIMPC art. 431, 434; PIETH, *supra* note 115, at 221-1; SCHMID, *supra* note 165, at 843-5 and 837-9.

[181] See the website of the federal Post and Telecommunications Surveillance Service: https://www.li.admin.ch/en/themes/stats.html.

VII. Surveillance Procedure in the United States

Just as the last Part did for the Swiss system, this Part reviews the range of choices available to regulate particular surveillance methods. Then, Part VIII describes the choices legislators have made with regard to each category of surveillance.

A. Levels of Oversight

United States law 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 some forms of surveillance.[182] Spreading responsibility for surveillance between members of the executive branch (law enforcement agents) and the judicial branch advances the United States constitutional principle of institutional checks and balances.[183] Fourth Amendment cases have noted the importance of having "a neutral magistrate" (judge) pre-approve of searches and seizures to constrain the executive's zeal for law enforcement.[184]

Various members of the executive branch must also approve some surveillance investigations before they may commence. Approval by high level officials in the executive branch is designed to inhibit unjustified investigations.[185] In some cases, the Attorney General himself must initially approve of a surveillance practice. Sometimes the applicant may obtain the approval of lower-level senior officials, and in some cases approval may be obtained from any prosecutor. In some cases, the agent wishing to conduct a particular investigation does not have to obtain approval from anyone else before commencing surveillance.

[182] 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) (permitting emergency wiretap orders which last up to 48 hours in limited circumstances).

[183] The third branch, Congress, is involved when it receives reports of surveillance that inform it on whether it needs to amend the surveillance laws using its lawmaking power. *See infra* part VII.E.

[184] *See, e.g.,* Dalia v. United States, 441 U.S. 238, 255 (1979).

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

B. Conditions

1. Procedural Hurdles

Procedural hurdles vary considerably in terms of the burden they impose on law enforcement agents and the scope of discretion they afford to reviewing judges to deny government applications for surveillance. The most demanding procedural hurdle requires that an agent 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.[186] That hurdle may be raised higher by a requirement that the communications device being surveilled has itself been used in the crime.[187]

Procedural hurdles are easier to satisfy when they relax the need to link the targeted device to criminal activity. Standards lower than probable cause remove the requirement that criminal activity itself will be revealed and instead require relevant information. For example, a procedural hurdle may require only that the information sought be relevant to an ongoing criminal investigation. Even easier to meet standards require only relevance to a law enforcement inquiry.

With more demanding hurdles, reviewing judges make factual determinations about whether the government's application satisfies the standard. When the hurdles are lower, judges are to approve applications that are complete without conducting an independent review of the facts.[188] Finally, some statutes permit agents to proceed without obtaining judicial approval at all, such as when a statute authorizes them to issue subpoenas, or demands for records.[189] In such cases, targets may challenge the subpoena only if in the limited circumstances in which it is unreasonable or oppressive, and only if she even learns of it in the first place.[190] Department of

[186] *See* 18 U.S.C. §§ 2516(1), 2518(3)(a) (requirement under the Wiretap Act).

[187] *See* 18 U.S.C. §§ 2518(3)(b) (same).

[188] 18 U.S.C. § 3122(b).

[189] *See* James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data,* 970 PLI/PAT 687, at 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).

[190] 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*

Justice lawyers have argued that one can contest a subpoena 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.[191]

2. Predicate Offenses

Some surveillance methods may be used only to investigate certain types of offenses, such as particularly serious crimes. Some statutes permit surveillance methods to be used for a wide variety of crimes, or place no limit on the types of crimes for which a surveillance method may be used.

3. Other Limits

Some surveillance methods establish a process by which a surveillance order subject to a time limit may be renewed for additional time. Some surveillance methods are not subject to time limits and orders for such investigations do not need to be renewed.

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.[192] Similarly, only the Wiretap Act requires that agents minimize the collection of non-incriminating conversations.[193] For the rest of surveillance methods in the United States, such as the vast majority of techniques that apply to modern communication methods, there is no general requirement that agents either minimize the collection of non-incriminating information or exhaust other types of surveillance first.[194]

Information in the Age of Big Data, 24 HARV. J. L. & TECH. 543, 547 (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).

[191] *See* Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-mail: The Law Professors' Brief in Warshak v. United States*, 41 U.S.F. L. REV. 559, 579-85 (2007) (describing and responding to government's argument).

[192] *See* 18 U.S.C. § 2518(3)(c). These requirements also apply to some video surveillance. *See infra* note 331.

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

[194] *See* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 463 (5th Cir. 1994) (explaining that only the interception provisions of the federal surveillance statutes have minimization requirements because agents

The United States has no general requirement of subsidiarity or proportionality. As we shall see in the next Part, the lack of the requirement that surveillance means be justified by their ends probably contributes the most to comparatively lower restrictions on government surveillance in the United States as compared to Switzerland. 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.

C. Notice

In some cases, criminal defendants may learn, through criminal discovery, of a surveillance investigation. But evidence not subject to criminal discovery rules, or obtained about those who are not prosecuted, may not come to the target's attention unless an applicable statute requires target notification.[195] Surveillance statutes vary in terms of who must receive notice, when agents must provide that notice, and the circumstances under which agents may delay providing notice. Some surveillance practices do not require any notice to targets, and, as mentioned, some surveillance proceeds without any authorizing statute. Surveillance statutes generally preclude service providers involved in surveillance from notifying targets.[196] Many orders to conduct surveillance are issued under seal (to be kept secret from the public, including the target), and remain under seal indefinitely.[197] Several commentators have recommended that the United States amend its electronic surveillance statutes to provide better notice to targets.[198]

---

can use key-word searching when going through stored communications). *But see infra* Part VIII.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.)

[195] *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, HARV. J. OF LAW AND PUB. POL. at *23, *28-29 (forthcoming 2012) (doubting that criminal defense lawyers will learn of many online surveillance orders noting that uncharged targets will not learn of much surveillance).

[196] *See* Smith, *supra* note 195, at *15-20.

[197] *See* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177 (2009); Smith, *supra* note 195, at *3 ("Ex parte sealing and non-disclosure orders combine to hide electronic surveillance not only from targeted individuals, but also from the public at large.").

[198] *See, e.g.*, Smith, *supra* note 195, at *31 ("ECPA should be amended to require notice to the target of any electronic surveillance order, including the customer, subscriber or user of a targeted hone or Internet service."); Stephanie Pell & Christopher Soghoian, *Can You See Me Now*, BERK. TECH. L. J. *52-55 (forthcoming 2012) (recommending notice when law enforcement obtains location data); Gruenspecht, *supra* note 190, at 561 (advocating for notice to be given to data creators instead of just third party intermediaries in the context of cloud computing).

D. Consequences if Illegal

Unlawful surveillance that violates the Fourth Amendment gives rise to a claim for money damages[199] and the protections of the suppression remedy.[200] The latter prohibits any evidence obtained by the unlawful surveillance and any evidence derived from that 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, and is not available in some cases.[201]

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." So far, the Supreme Court has considered only wiretapping, bugging, and the installation and use of a GPS tracking device to be surveillance practices that are constitutional searches.[202]

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, and that is not available for the interception of electronic communications.[203] Some provide monetary relief and vary in terms of the amounts they award for compensation and whether they provide for punitive damages and attorney's fees. Some provide for the possibility of criminal punishment or administrative discipline for law enforcement agents who violate the terms of the statute. The executive branch rarely prosecutes its own agents, however.

---

[199] A victim must bring a claim under 42 U.S.C. § 1983 (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*, 532 F.3d at 528, 532 (expressing disapproval of target's pursuit of injunctive relief rather than a civil damages claim).

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

[201] *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).

[202] *See supra* Part 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* Part VIII.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.

[203] 18 U.S.C. §§ 2515, 2518.

E. Reporting

Some statutes require that Congress receive periodic reports about surveillance practices. Such reporting facilitates the oversight that may constrain executive branch abuses.[204] Congress may choose to revise surveillance statutes in light of information it receives in surveillance reports. The statutes vary in how much detail must be provided to Congress, and some require no reporting at all. Compliance with the reporting requirements varies as well.[205]

VIII. Surveillance Regulation Compared

A. Introduction

In Switzerland, CrimPC regulates the surveillance law enforcement conducts during an inquiry proceeding, meaning when a criminal investigation is open and there is an accused person (sometimes unknown). CrimPC defines six categories of surveillance. They can be classified from the most invasive (and requiring the most extensive judicial oversight) to the least invasive (and not requiring judicial authorization at all). The most invasive techniques are the surveillance of post and telecommunications,[206] use of technical surveillance devices,[207] surveillance of contacts with a bank,[208] and undercover operations;[209] physical observation is the least invasive.[210] The collection of user identification data[211] is a subcategory of surveillance of post and telecommunications and considered to be a little less invasive. This paper will only briefly

[204] *See, e.g.*, In re Sealed Case, 310 F.3d 717, 742 n. 25 (FISC App. 2002) (citing senate report accompanying FISA).

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

[206] CRIMPC art. 269.

[207] CRIMPC art. 280.

[208] CRIMPC art. 284.

[209] CRIMPC art. 286.

[210] CRIMPC art. 282.

[211] CRIMPC art. 273.

mention the rules pertaining to search and seizure, which are not considered to be surveillance in Switzerland.[212]

Because the United States lacks a uniform and comprehensive surveillance law, there is no comparable definition of surveillance here. Moreover, the effective scope of "surveillance" differs in the two countries. Some of the practices the Swiss regulate as surveillance under CrimPC are virtually unregulated here. Further discussion of each regime should shed more light on the similarities and differences in treatment.

We have organized the following discussion according to the categories of CrimPC.

B. Monitoring of Post and Telecommunications

1. In Switzerland

The first category is the oldest one and consists of the monitoring of the postal address and telecommunications of the accused person.[213] It covers the acquisition of any information included in letters and parcels,[214] and communications made by phone call, fax, text (both SMS and MMS), pager, e-mail, and Voice over IP ("VoIP").[215] Surveillance of traditional letters and telecommunications generally means real-time monitoring.[216] When the police compel a service provider to produce an e-mail from its system or a letter from its facilities, however, that is also considered to be the surveillance of communications. Acquiring communications from a third

[212] *See infra* Part VIII.I.

[213] It also covers surveillance of the third party when the accused person is using the postal address or telecommunications connection of the third party or the third party is receiving specific messages for the accused person or forwarding messages from the accused to other people; CRIMPC art. 269ss.

[214] 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) 103-4 (2002); PIQUEREZ, *supra* note 108, at 615; HANSJAKOB, *supra* note 106, at 71-72; Sträuli, *supra* note 108, at 95-112.

[215] The law does not protect communications made in public forums or in online chat rooms. *See supra* note 109.

[216] There are no cases yet, but the installation of Government-Software (Trojan) should be treated like surveillance of telecommunication or user identification data when it targets electronic communications. *See* Sylvain Métille, *Les mesures de surveillance prévues par le CPP*, JUSLETTER, December 19, 2011, Weblaw.

party rather than the target herself intrudes on the secrecy of communications and is considered surveillance because it may proceed without the interested person being aware of it.[217]

The surveillance of post and telecommunications is subject to the highest procedural hurdles: it must be ordered by the public prosecutor and confirmed by the Compulsory Measures Court[218] and proceed only when the public prosecutor has a strong suspicion that an offense has been committed.[219] Under the subsidiarity principle, other investigatory activities must not have been successful or have any likelihood of success.[220] Surveillance orders 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.[221] Within 24 hours after the surveillance order is made (and the surveillance has started), the public prosecutor must submit a copy of the order to the Compulsory Measures Court and must include the reasoning supporting the surveillance and any files necessary to provide backup information.[222]

Within five days after the surveillance order has been made (and the surveillance started), the Compulsory Measures Courts shall authorize surveillance with retroactive effect for up to three months.[223] 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

[217] Police acquisition of such communications through search of a home, a computer, or a person, constitutes a form of search and seizure. *See* HANSJAKOB, KOMMENTAR ZUM BÜPF, *supra* note 106, at 81-85; Sträuli, *supra* note 108, at 99-100 and 107-8. *See infra* Part VIII.I.

[218] CRIMPC art. 274.

[219] A higher level of suspicion is required to use surveillance than to open an investigation and surveillance cannot be ordered without suspicion or to find or create suspicion.

[220] In practice, police officers first recommend that surveillance be undertaken to the public prosecutor, which 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

[221] Art. 11, 15 and 23 SPTO, RS 780.11, HANSJAKOB, KOMMENTAR ZUM BÜPF, *supra* note 106, at 403-08, 412-24 and 443-49.

[222] In practice, the public prosecutor sends a copy of the order by mail to the Compulsory Measures Court and attaches a copy of the official files. If the order is comprehensive and self-explanatory and refers to the important pieces of the file then the mailing does not need to contain a lot of further reasoning, but if the order is a simple form then the mailing shall contain additional explanations.

[223] The Court may also impose its own requirements and request further information.

limited as possible to respect the principle of proportionality. Also, as with all types of surveillance under CrimPC, notice to the target must be given unless the Compulsory Measures Court consents to notice being postponed or omitted[224].

Surveillance is unauthorized if the authorization has been rejected, if no authorization has been requested or if the authorization has not been extended.[225] When notice has not been provided or surveillance is unauthorized, findings from the surveillance are not usable for evidentiary purposes. This is a complete exclusionary rule; documents and data storage devices must be destroyed immediately and intercepted mail should be delivered. Victims of unlawful monitoring of their post and telecommunications are entitled to damages and violators face criminal prosecution.

2. In the United States

a) Several Distinctions

For real-time surveillance like that covered by the above provisions of CrimPC, laws in the United States distinguish between the content of communications made by mail, communications made by wire, and electronic communications. In addition, United States law treats acquisition of electronic communications content in real time as a much more significant invasion of privacy than the acquisition of communications contents in electronic storage. These distinctions arise out of ECPA and reflect the Supreme Court's precedents from the 1960's and 1970's.[226] Commentators have criticized ECPA for incorporating so many distinctions that have

[224] For physical surveillance, consent to notice being postponed or omitted is given by the prosecution.

[225] CRIMPC art. 277; TF, May 3, 2005, 131 BGE I 272 (Switz.); HANSJAKOB, KOMMENTAR ZUM BÜPF, *supra* note 106, at 250-253 (2006). Whether or not an authorization would have been granted is irrelevant; TF, Oct. 9, 2007, 133 BGE IV 329 (Switz.).

[226] *See supra* section III.B. (discussing this history).

become arbitrary and even counter-intuitive.[227] In recent years, efforts to reform and simplify the statute have increased.[228]

As in Switzerland, United States law treats the acquisition of communications directly from a person's home or computer as a search or seizure.[229] As such, they 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, are treated as a form of surveillance.[230]

b) Interception of Postal Mail contents

First class mail and sealed packages in the United States have long been protected against warrantless interception. [231] As such, they are subject to a standard Fourth Amendment warrant requirement in most cases.[232] The warrant requirement does not protect fourth class mail and the information visible on the outside of envelopes.[233] Because of the Fourth Amendment regulation, victims of unlawful acquisition of their mail have a suppression remedy available to them.[234] In

[227] *See, e.g.*, Ohm, *supra* note 50, at 1551 ("First ECPA is confusing; epically confusing; grand-champion-of-the U.S. Code confusing….ECPA's complexities confuse judges who then made a mess of our understanding of the Act."); Dempsey, *supra* note 189, at 704-05, 722 (criticizing complexity of online surveillance rules and recommending one warrant standard for all stored e-mail).

[228] *See e.g.*, Digital Due Process Coalition, *News*, 2010, *available* at http://digitaldueprocess.org/index.cfm?objectid=26802940-3840-11DF-84C7000C296BA163; Ohm, *supra* note 50, at 1551 ("I agree with essentially everybody who has ever written about ECPA that the law is sorely in need of reform.").

[229] *See infra* Part VIII.I.

[230] *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* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.CCIPS SEARCH MANUAL (explaining that ECPA does not apply to e-mails that "are not stored on the server of a third-party provider" of services.).

[231] *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2000) (reviewing history of protection of mail); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1142-43 (2002) (same).

[232] *See* United States v. Jacobsen, 466 U.S. 109, 144 (describing warrantless searches of sealed packages and letters as "presumptively unreasonable"); Ex Parte Jackson, 96 U.S. 727, 733 (1877).

[233] WAYNE R. LAFAVE ET. AL., CRIMINAL PROCEDURE § 4.2(a) (3d. ed. 2007).

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

addition, a federal statute makes tampering with the mail a criminal offense.[235] No statute provides for reporting or other remedies for victims of unlawful surveillance, however.

c) Interception of Wire Communications Content

As under CrimPC, real-time interceptions of the contents of wire communications[236] in the U.S. are subject to the highest procedural hurdles, which are found in the Wiretap Act.[237] Under that Act, a member of the judiciary oversees all phases of law enforcement surveillance. Applications for approval, which may only be made by high level officials,[238] must persuade the reviewing judge of probable cause to believe the target "is committing, has committed, or is about to commit" a particular enumerated offense and that the surveillance will obtain incriminating communications about that offense.[239] As in Switzerland, applications for orders under the Wiretap Act require detailed information of facts and circumstances that support the application.[240]

Before a court may approve of a request to wiretap, the judge to whom the application is made must be convinced that the information sought may not be obtained by normal investigative methods.[241] Surveillance orders must be limited to thirty days, unless renewed, and end when the information sought is obtained.[242] Agents conducting the investigation must minimize the monitoring of non-incriminating communications and provide a full accounting of how they have

[235] 18 U.S.C. § 1703.

[236] *See* 18 U.S.C. § 2510(1) (defining "wire communication").

[237] For more on the distinguished pedigree of the Wiretap Act, see Freiwald, *supra* note 106, at 74-76. For an overview of the Wiretap Act requirements, see In re: Sealed Case, 310 F.2d 717, 739-40 (FISC App. Ct. 2002).

[238] 18 U.S.C. § 2516(1),(2).

[239] 18 U.S.C. §§ 2516(1), 2518(3).

[240] 18 U.S.C. § 2518(1). The reviewing "judge may require the applicant to furnish additional testimony or documentary evidence in support of the application." *Id.* § 2518(2).

[241] 18 U.S.C. § 2518(3)(c).

[242] Judges must make the same findings of probable cause before issuing any extensions beyond the 30 day maximum time limit. *Id* § 2518(5).

done that to the reviewing judge when the investigation ends.[243] The Wiretap Act, however, lacks the general proportionality principle that Swiss law follows.

Notice must be provided to anyone named in an application under the Wiretap Act, as well as anyone else that the reviewing judge deems appropriate.[244] 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.[245] In addition, Congress provided for detailed annual reports to Congress on the numbers of orders issued under the Wiretap Act and their efficacy in fighting crime.[246] Based on the reports to Congress, a Report on Wiretapping is supposed to be made public each year.[247]

Violations of the Wiretap Act may be punished by a significant fine and jail time.[248] In addition, any person whose communications were intercepted, disclosed or used in violation of the Act to bring civil claims for damages against those who violated their rights under the Act.[249] Under the Wiretap Act, a victim could receive attorney's fees, punitive damages, and actual damages or statutory damages if they preferred.[250]

Between the significant limitations on when wiretaps may be used, the oversight by judges of their use as they are being used, and the significant remedies for misuse, the Wiretap Act sets the high water mark for restrictions on surveillance in the United States. Judicially-

[243] *See* 18 U.S.C. § 2518(8).

[244] *See* 18 U.S.C. §§ 2518 (8)(d), (9).

[245] *See* S. Rep. No. 90-1097, at 105 (1968), *reprinted in* U.S.C.C.A.N 2112, 2194.

[246] *See* 18 U.S.C. § 2519.

[247] *See* Soghoian, *supra* note 205.

[248] 18 U.S.C. § 2511(4).

[249] *See* 18 U.S.C. §§ 2518(10).

[250] *See* 18 U.S.C. § 2520.

guaranteed notice to the target and the transparency effectuated by reporting to Congress and the public, mean that the rights and remedies the Wiretap Act provides will likely be actualized.

d) Interception of Electronic Communications Content

When ECPA amended the Wiretap Act to take account of "electronic communications" in 1986, it extended some but not all of the restrictions on the wiretapping of traditional telephone calls to the interception of electronic communications, such as e-mail and cellular phone calls.[251] In particular, all of the restrictions described above regarding probable cause, 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. It may be somewhat easier to get an order to intercept electronic communications rather than wire communications, however, because ECPA permits any "attorney for the government" to authorize the interception of electronic communications,[252] in pursuit of any felony, rather than for only certain serious crimes.[253]

The much more significant difference between the unlawful wiretapping of traditional phone calls and the unlawful interception of electronic communications is that victims of the latter do not have the benefit of the statutory suppression remedy that Congress provided for victims of the former in the Wiretap Act.[254] Although the expressed goal of Congress was to craft ECPA so as to ensure the privacy of electronic communications and extend all of the Wiretap Act's protections to the new media,[255] the Senate report reveals that the omission of a statutory suppression remedy was the "result of discussions with the Justice Department."[256] The

[251] 18 U.S.C. § 2510 (12) (defining "electronic communication").

[252] 18 U.S.C. § 2516(3). The Justice Department has nonetheless required high level approval as a matter of its own policies. CCIPS Search manual, *supra* note 230, at 167.

[253] 18 U.S.C. § 2516(3).

[254] 18 U.S.C. §§ 2515, 2518(10); *see* Steve Jackson Games, 36 F.3d 457, 461 n.6 (5th Cir. 1994) (discussing statute and legislative history).

[255] *See* H.R. Rep. No. 99-647 (1986), at 17-19; S. Rep. No. 99-541 (1986), at 20, *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3574.

[256] *See* S. Rep. No. 99-541, at 23, *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3577; 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).

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.[257]

The other reason that few cases are brought to vindicate interests under ECPA provisions pertaining to the interception of electronic communications contents, is that their application is severely limited. Government litigators have succeeded in having courts restrict application of the statutory provisions to interceptions that occur "contemporaneously with" the "transmission" of an electronic communication."[258] Agents who choose to wait and acquire electronic communications out of storage instead of in real-time may comply with the weaker provisions of the Stored Communications Act ("SCA"),[259] which the next section describes.[260]

e) Acquisition of Stored Electronic Communications Content

The Stored Communications Act (SCA), which applies when law enforcement agents obtain e-mail stored with third party providers of "electronic communications service[s]" and "remote computing service[s][261] restricts law enforcement agents much less than either the Wiretap Act or CrimPC. The SCA places no limits on who may conduct stored content acquisitions and permits them to be used to pursue any "ongoing criminal investigation," rather than just felonies or serious crimes.[262] Acquisition of stored contents does not need to be used as a last resort, nor does it need to minimize non-incriminating communications.[263] The SCA places no time limits on stored content investigations, which means that investigators can ask for

[257] *See supra* note 136.

[258] *See, e.g.*, Konop v. Hawaiian Airlines, 302 F. 3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-63 (5th Cir. 1994).

[259] *See supra* note 137; *see also* United States v. Scarfo, 180 F.3d 1051, 1058-59 (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 "engaged" was not subject to statutory regulation as a wiretap or electronic intercept).

[260] *But see* United States v. Councilman, 418 F. 3d 67 (1st Cir. 2005) (en banc) (concluding that e-mail may be "intercepted" when it is acquired out of "transient electronic storage that is intrinsic to the communication process").

[261] *See* 18 U.S.C. § 2703(a), (b).

[262] *See* 18 U.S.C. § 2703(d).

[263] *See supra* note 194.

e-mail received over a span of years.[264] The SCA does not require reports to Congress on law enforcement's acquisition of stored content.[265]

As for remedies, the SCA does not provide a statutory suppression remedy for victims. Unless they have a Fourth Amendment claim, victims of unlawful access to their stored e-mail by law enforcement agents are unable to have the acquired information suppressed from their trials. In the *Warshak*[266] case in late 2010, the Sixth Circuit found a warrantless acquisition of stored e-mail to violate the Fourth Amendment,[267] granted no suppression remedy because the investigating officers had relied in good faith on the terms of the SCA.[268] Until other federal circuits follow suit or Congress amends ECPA to provide a statutory suppression remedy, victims of unlawful stored content acquisitions outside the Sixth Circuit will continue to lack a suppression remedy. The SCA provides for civil damages in some cases, but it does not provide for punitive damages or criminal penalties against law enforcement officials who violate its provisions.[269]

The provisions just described apply to all investigations proceeding under the SCA. But the SCA provides different rules on notice and on what must be demonstrated to a judge based on different features of the stored content. The next subsections describe those different rules. The reader will no doubt find the distinctions to be confusing and hard to follow. If the *Warshak* holding is followed by the courts, and certainly if Congress amends ECPA to conform to it, then the protection of stored e-mail contents will be much more straightforward and stronger.

---

[264] *See, e.g.*, United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (government compelled the disclosure of over 27,000 e-mails); Freiwald & Bellia, *supra* note 191, at 572 (noting Warshak's claim that some of his e-mails were 9 years old).

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

[266] *Warshak*, 631 F.3d 266.

[267] *Id.* at 283–88.

[268] *Id.* at 288-92.

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

a. Subject to the Warrant Requirement

The contents of e-mail in "electronic storage" for 180 days or less may not be obtained unless the law enforcement applicant obtains a warrant based on probable cause.[270] The 180 day cutoff reflects the notion that e-mails left in storage longer than 180 days could be seen to be abandoned and therefore less worthy of protection.[271] The Justice Department interprets the statutory language so that only unopened (unretrieved) e-mails are entitled to the protection of a warrant requirement, because only those are in "electronic storage" under the statute.[272]

Although federal criminal law generally requires notice to the target when a warrant is required,[273] the Justice Department argues that when it is authorized to use a warrant under ECPA it does not have to provide notice to the target.[274] If the practice of not giving notice to the target is widespread, then those privileged with the highest protections afforded to stored contents, which is the warrant, may never learn that they have any rights under the statute. If, as the *Warshak* court held, use of a warrant is constitutionally mandated, it may be that notice is mandated as well. In the *Warshak* case, however, agents unlawfully delayed providing notice for over a year, and the Sixth Circuit made no definitive statement about the constitutional requirement of notice.

[270] *See* 18 U.S.C. § 2703(a).

[271] *See* H.R. Rep. NO. 99-647, 23 n.41 (1986) (analogizing e-mails held in long term storage to business records); *see also id*. at 67-68 (regarding e-mail in storage less than 180 days as likely protected by the Fourth Amendment). As practices have changed and many uses store their more important e-mails with their service providers for years, the rationale to treat older e-mails as less privacy protected makes no sense.

[272] The Justice Department argues that once e-mails are retrieved they are no longer in electronic storage as defined in the SCA. CCIPS SEARCH MANUAL, *supra* note 230, at 124-25, 138.

[273] *See* Smith, *supra* note 195, at *13 (citing Fed. R. Crim. Pro. 41(f)(1) (C) & (f)(3)); *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.").

[274] CCIPS SEARCH MANUAL, *supra* note 230, 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)). 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).

b. Subject to a Lesser Standard

ECPA permits law enforcement agents to acquire stored electronic communications contents that have been stored more than 180 days by using a special court order pursuant to 18 U.S.C. § 2703(d) ("D Order"). Courts may issue D Orders when the law enforcement application "offer[s] 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."[275] When agents use a D Order to obtain stored e-mail contents, they must give notice to the target, but such notice may be delayed.[276] In fact, the sample 2703(d) court order in the Justice Department's manual provides for delayed notice, until such time as the court determines.[277] Instead of obtaining a D Order, agents may obtain the stored e-mail content available without a warrant[278] using an administrative, trial, or grand jury subpoena, so long as notice is provided.[279]

Under the Justice Department's interpretation, e-mails that have been opened, accessed or read are also subject to the D Order standard, even if they are stored for fewer than 180 days,[280] so long as they are stored on services that provide e-mail to the public.[281] If the service provider furnishes e-mail services to the public, it is a statutory "remote computing service," and

[275] 18 USC § 2703(d).

[276] See 18 U.S.C. § 2705 (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.*, United States v. Warshak, 631 F.3d 266, 289 (6th Cir. 2010) (finding that law enforcement delayed giving notice of stored e-mail acquisition for over a year despite having approval to delay giving notice only for 90 days).

[277] See CCIPS SEARCH MANUAL, *supra* note 230, at 213-23 (App. B and attachment).

[278] According to the Justice Department, this includes e-mails stored more than 180 days on public systems, e-mails and unread e-mails that reside on private systems. CCIPS SEARCH MANUAL, *supra* note 230, at 44-45.

[279] 18 U.S.C. § 2703(b)(B).

[280] *See* Freiwald, *supra* note 45, at 57-59 (criticizing the DOJ's approach); Ohm, *supra* note 50, at 1538-1542 (describing the 9th Circuit's rejection of the DOJ's approach and its requirement of a warrant for access to stored e-mail) (citing Theofel v. Farey Jones, 359 F.3d 1066 (9th Cir. 2004)) .

[281] 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 ("It is a particularly remarkable achievement given that its enactment dates back to 1986. The SCA has weathered intervening technological advances surprisingly well.")

acquisition of read or accessed e-mails from it may proceed under a D Order.[282] If the service provider that stores the e-mail does not furnish e-mail to the public, for example if it is a University or corporate provider, the Justice Department considers the read e-mail to be unprotected by the SCA.[283]

c. Not Covered by the SCA

As mentioned, the DOJ argues that acquisition of e-mails that have been opened, accessed or read and stored on a system that does not provide service to the public is not covered by the SCA.[284] Disclosure of Information that falls outside of the SCA may be compelled with a simple subpoena without any judicial oversight.[285] It is subject to no statutory protections or remedies and will often proceed without notice to the subject. Because such "surveillance" is covered and protected under CrimPC, a great disparity exists between U.S. and Swiss surveillance law.

C. Collection of User Identification Data

1. In Switzerland

User identification data is sometimes called secondary data, because it does not include call content but rather includes related information ("communication attributes"). User identification data is treated similarly under CrimPC to the monitoring of communications content, but judges consider acquisition of non-content information as less intrusive than acquisition of content information when they apply the proportionality principle. Collection of user identification data is often a retroactive investigation, but can be done in real time as well.[286] User identification data includes information about when and with which people or connections

[282] *See* CCIPS SEARCH MANUAL, *supra* note 230, 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.").

[283] *See* CCIPS SEARCH MANUAL, *supra* note 230, at 126 (describing how the "SCA no longer regulates access" to an e-mail retrieved from a company provider of e-mail). The 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.

[284] *See* CCIPS SEARCH MANUAL, *supra* note 230, at 125-26, 138.

[285] See CCIPS SEARCH MANUAL, *supra* note 230, at 128 (describing this process).

[286] *See* Sträuli, *supra* note 108, at 98 - 99.

the person under surveillance is or was communicating by way of post or telecommunications. It also includes billing data and traffic data, such as information about the duration of a call, the amount of data downloaded, and the like.

A request for user identification data may be made up to six months after the data is generated, according to article 273 CrimPC. SPTA requires post and communications service providers to keep a log for six months of all communications traffic data.[287] Because they are subject only to CrimPC, and not SPTA, local couriers and those responsible for private in house telecommunication networks do not have to keep a log, but if they do, they are required to produce it upon request. The Swiss Supreme Court recently ruled that Internet hosting providers have the same obligations as access providers and therefore need to keep logs for six months.[288]

There are no cases yet, but tracking or locating someone using cell site location data or an IMSI-catcher should be treated like collection of user identification data because it requires the use of a communications installation (and involves the secrecy of telecommunications) but does not acquire the content of communications when used to locate or track someone.[289]

Under CrimPC, collection of user identification data requires approval by the Compulsory Measures Court.[290] The procedure is similar to the one for monitoring of Post and Telecommunications, except that law enforcement may collect user identification data when they have strong suspicion of the commission of any felony or misdemeanor, rather than being limited to the list of felonies specified in the statute.[291] Other than those two differences, all of the

[287] SPTA art. 12, para. 2, art. 15, para. 3. Proposed revisions to SPTA would extend from six to twelve months the obligation for service provider to keep a log of user identification data. Constitutional courts of 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.

[288] TF, Jan. 8, 2010, docket no. 6B 766/2009, para. 3.4 (Switz.).

[289] If there is access to the content of communications then this technique would be covered under the section on monitoring of Post and Telecommunications.

[290] CRIMPC art. 274, 289.

[291] As an exception and because collecting user information is the only way to investigate it, the misuse of a telecommunications installation (CP art. 179septies) is a sufficient offense for the collection of user identification data even though it is only a contravention rather than a misdemeanor or felony.

provisions that apply to the surveillance of post and telecommunications (subsidiarity, proportionality), apply to the collection of user identification data. As with the surveillance of post and telecommunications, notice to the target must be given unless the Compulsory Measures Court consents to notice being postponed or omitted.

When notice has not been provided or an investigation is otherwise unauthorized, findings from the surveillance are not usable for evidentiary purposes and must be destroyed.[292] Victims of unlawful access to their user identification data are entitled to damages and violators face criminal prosecution.

2. In the US

a) Several Distinctions

The last section introduced the different treatment American law accords to postal mail and more modern forms of communications. Our most "modern" statute, ECPA, has 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 the single category just described.

b) Collection of Postal Mail Attributes

United States courts have historically distinguished between the contents of mail that is unreadable until the envelope carrying it is opened, and information residing on the outside of the envelope and therefore observable to postal workers when they process mail.[293] 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.[294]

[292] TF, Oct. 9, 2007, 133 BGE IV 329, para. 4.4 (Switz.).

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

[294] *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);

Legislating against the backdrop of no Fourth Amendment protection, Congress has provided few procedural protections to the targets of surveillance of envelope information.[295] 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 obtain information relevant to the commission or attempted commission of a crime."[296] No judge need be involved in the investigation, no notice need be provided, and victims of improper investigations are afforded no remedies.[297]

c) Collection of Electronic Communication Attributes in Real Time

ECPA's third title governs the use of pen registers and trap and trace devices to acquire "dialing, routing, addressing and signaling information."[298] Modern pen registers also acquire the date, time, and duration of transmissions, and information in cc and bcc fields of e-mails.[299] 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 under the pen register authority.[300] 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 with a pen register order.[301]

---

[295] Kerr, *supra* note 45, at 631.

[296] 39 C.F.R. § 233.3(e)(2)(iii); Kerr, *supra* note 45, at 631.

[297] Kerr, *supra* note 45, at 631.

[298] See 18 U.S.C. § 3121(c).

[299] *See* CCIPS SEARCH MANUAL, *supra* note 230, at 230 (Appendix D). The Justice Department claims that any e-mail header information may be acquired using a pen register. *See id*. at 154.

[300] *See* CCIPS SEARCH MANUAL, *supra* note 230, at 154. The manual expresses ambivalence about whether the subject line is content or not by stating that it "*can* contain content") (emphasis added). *See id.* at 152-53. For a thorough discussion of the ambiguity here, see Freiwald, *supra* note *45*, 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 Orin Kerr, *supra* note 45 (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 1019-1037 (2010) (developing claim that there are two categories online: content and non-content information).

[301] United States v .Forrester, 512 F.3d 500 (9th Cir. 2008).

Under ECPA, 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 must certify his belief "that information likely to be obtained is relevant to an ongoing criminal investigation."[302] A judge asked to grant a pen register order "shall approve it" so long as she "finds that the application is complete."[303] Judges are not to conduct independent reviews of the factual support for the application, and the Justice Department has largely persuaded courts to view their role as "purely ministerial."[304] Several courts and commentators have criticized the weak protections afforded by the pen register provisions.[305]

Unlike CrimPC, the pen register provisions do not provide notice to the target or any remedies to the target for unlawful investigations; no statutory suppression remedy or damages are available.[306] The statute provides for the possibility of a criminal action against violators, but no known cases have been brought.[307] The statute does not provide for reports to Congress or the public.[308]

d) Collection of Electronic Communication Attributes from Electronic Storage

Congress afforded electronic communication attributes in electronic storage the lowest level of protection in ECPA. For a large set of information called "basic subscriber information," the SCA permits law enforcement agents to compel its disclosure from service providers upon presentation of an administrative subpoena or a grand jury or trial subpoena.[309]

---

[302] 18 U.S.C. § 3122(b).

[303] 18 U.S.C. § 3123(a).

[304] *See, e.g.*, United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

[305] *See, e.g.*, Ohm, *supra* note 50, 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, 1288-89 (2004);.

[306] Smith, *supra* note 195, at *13, 29. 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).

[307] 18 U.S.C. § 3121 (d) (providing for a penalty of a fine and up to one year of imprisonment). [No known prosecutions – to be confirmed at press time]

[308] 18 U.S.C. § 3123(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.

[309] 18 U.S.C. § 2703 (c)(2); CCIPS SEARCH MANUAL, *supra* note 230, at 128 .

Under this provision, law enforcement agents may acquire identifying information about a subscriber, the electronic communication service to which he subscribes, when the subscriber used the service to access the Internet and what IP address he used to do so.[310] Under that provision, 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."[311]

Service providers keep such information in electronic log files to protect themselves against hacking and fraud. Although log files vary by service provider, they can be quite revealing.[312] Service providers can often provide the entire history of one's communications and movements through the World Wide Web, down to an astonishing level of detail.[313] Currently, service providers vary in how long they retain data. However, bills currently pending in Congress would require service providers to retain data for a specified period of time.[314]

Any other records "concern[ing]" electronic communications may obtained with a D Order.[315] Information obtained in this category is subject to the weak protections of the SCA, which means that there is no minimization requirement and no subsidiary or proportionality principle applicable. Law enforcement agents are specifically excused from giving notice to

[310] For example, the information comprises the subscriber's name, address, length of service, telephone number or IP address and means and source of payment. 18 U.S.C. § 2703(c)(2)-(3). *See also* Patriot Act § 210, 115 Stat. 272, 283 (2001) (adding "records of session time and durations" and "any temporarily assigned network address").

[311] CCIPS SEARCH MANUAL, *supra* note 230, at 122.

[312] CCIPS SEARCH MANUAL, *supra* note 230, at 139 (noting that "some providers retain very complete records for a long period of time," while others retain few if any records).

[313] 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 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 e-mail or internet connections. *See* CCIPS SEARCH MANUAL, *supra* note 230, 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).

[314] *See, e.g.*, Protecting Children from Internet Pornographers Act of 2011, H.R.1981 (112th Cong.)(imposing obligation to hold identifying information for eighteen months).

[315] 18 U.S.C. § 2703(c). There are some other limited ways in which government agents may acquire access to such records. *See id.*

targets under this section,[316] 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 only and have no statutory suppression remedy.[317]

e) Cell Site Location Data Acquisition

The legal framework for acquisition of cell phone location data rivals the complexity attendant to acquisition of e-mail. In addition to being complex, the rules are contested, and they rely on categories whose dividing lines are not always bright. To be clear, recall that the content of cell phone calls and 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 Data ("GPS") associated with smart phone 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."[318] Cases have begun to reach the appellate courts raising the issue of whether cell phone location data acquisition must be protected by the Fourth Amendment, and if so, just what protections that affords.[319]

---

[316] 18 U.S.C. § 2703(c)(3).

[317] 18 U.S.C. § 2707. *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).

[318] *See, e.g.*, In Re Application of the United States for Historical Cell Site Data, 747 F. Supp.2d 827, 846 (S.D. Tx. 2010).

[319] *See* Freiwald, *supra* note 732-49 (reviewing 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's Brief 5th Circuit, *supra* note 66 (appealing district court case that affirmed Magistrate Judge's opinion cited *infra* note **Error! Bookmark not defined.**).

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.[320] For acquisition of cell phone location data in real-time, some courts require a warrant and some require the combination of a D Order and a pen register order under what is called a "hybrid theory."[321] For the acquisition of historical records, 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 which require a warrant will also require notice to the target and whether they will provide a suppression remedy to those subject to warrantless acquisition. 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

Technical surveillance equipment (sometimes called "other surveillance measures") may be used to intercept or record statements not made in public, to observe or record incidents in non-public places or places which are not accessible to the public and to establish the location of people or things (art. 280). Before the introduction of CrimPC, the law of the different Cantons regarding these practices varied considerably.[322]

Technical surveillance equipment is a residual and open category that may include currently unknown techniques. It clearly includes listening or audio recording devices, cameras, movie cameras, tracking device (GPS, RFID), etc. There may appear to be some overlap with other categories of surveillance but each technique is supposed to belong in only one category.[323]

[320] *See infra* note 6.

[321] *See, e.g.*, Steven B. Toenisketter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*,13 RICH. J.L. & TECH. (2007).

[322] GOLDSCHMID, *supra* note 163; Sträuli, *supra* note 108, at 112-117.

[323] There are no cases yet, but the installation of Government-Software (Trojan) should be treated like technical surveillance devices when the Government software is used to control a webcam or microphone in order to observe the environment of the machine. But it is clearly illegal to use such software to execute a search and seizure. *See* Métille, *supra* note 216.

For example, making audio and video recordings in places accessible to the general public to aid in a criminal prosecution is treated as physical observation because it happens in a public space.[324] Video monitoring or photographing of a telephone booth constitutes the use of technical surveillance measure and not the monitoring of telecommunications when there is no access to the content of the phone call.[325]

As discussed, CrimPC treats the use of technical surveillance devices as sufficiently invasive to be included in the most restricted category. As such, only particular offenses justify the use of technical surveillance devices and the Compulsory Measures Court must approve the surveillance submitted by the public prosecutor.[326] The subsidiarity and proportionality rules apply.

Also as in the case of surveillance of post and telecommunications, notice to the target must be given unless the Compulsory Measures Court consents to notice being postponed or omitted. Findings from the surveillance are not usable for evidentiary purposes in those cases where notice has not been provided or when use of technical surveillance devices has been unauthorized. This is a complete exclusionary rule as for an unauthorized surveillance of post and telecommunications.[327]

2. In the US

Reflecting the relative lack of simplicity of U.S. law, no comprehensive category covers technical surveillance equipment. The closest approach to CrimPC in the U.S. would be the use of bugs and video surveillance in private areas. Bugging, or the interception of spoken words in the open, is subject to the highest protections of the Wiretap Act when conducted in an area in

[324] CRIMPC art. 282. Audio and video recording of private domain is instead a case of other technical equipment and therefore subject to authorization by the Compulsory Measures Court (art. 272 and 281).

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

[326] CRIMPC art. 269, 274, 289.

[327] CRIMPC art. 281, para. 4. *See supra* Part VIII.B.1.

which the subject has a reasonable expectation of privacy.[328] As described above, the Wiretap Act provides a comprehensive set of protections such as a high level of probable cause, a statutory suppression remedy, notice, the last resort and minimization rule, and reports to Congress.[329] 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 merit those highest protections of the Fourth Amendment by analogy.[330] Because the protections do not come directly from the Wiretap Act, however, the provisions for Congressional reporting and some of the other "technical" requirements do not apply.[331]

The Supreme Court has also restricted the use of a thermal imaging device to record the heat emanating from the target's home by finding law enforcement's use of such a device to be a search under the Fourth Amendment.[332] Though the *Kyllo* case was privacy-protective in its result, its holding shows its significant limits. The Court found a search because 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."[333] The Court's emphasis both on home and on devices not in general public use strongly suggest U.S. law would not restrict many of the techniques that CrimPC would. Moreover, the device in *Kyllo* was subject only to Fourth Amendment protection of a possible suppression remedy and not the statutory protections accorded by the Wiretap Act.

[328] 18 U.S.C. § 2510(2) (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.")

[329] *See infra* VIIIB.2.c.

[330] *See infra* text accompanying notes 72-73.

[331] 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, limited duration).

[332] Kyllo v. United States, 533 U.S. 27 (2001).

[333] Kyllo, 533 U.S. at 40

E. Surveillance of Contacts with a Bank

1. In Switzerland

The surveillance of contacts between an accused person and a bank or a bank-type institution was introduced for the first time by CrimPC.[334] This rule 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. Such techniques may include orders to the bank to transmit, in real time, information about every transaction with the bank, information from physical observation, telecommunications which have been intercepted, and specific documents relating to the accused person's interactions with a bank. Banks may also be ordered to provide access to their computer systems.

Article 284 of CrimPC seems confusing because it currently seems to cover access to previously existing information, such as bank statements. But procedures for acquiring bank records are already covered by the more straightforward rules pertaining to search and seizures.[335] Article 284 should be used to obtain an order for a bank to transmit information and documents to the public prosecutor that do not exist yet but will be created soon.[336] Such surveillance is forward-looking and pertains to both financial flows and credit card usage information.

As discussed, CrimPC includes surveillance of contacts in the most restricted category of surveillance. The procedure is similar to the one pertaining to telecommunications surveillance

[334] CRIMPC art. 284.

[335] CPP art. 241ss and 263ss; STEPHANIE EYMANN, *Die strafprozessuale Kontosperre* (*The Bank Account Freeze according to Criminal Procedure*) 81-90 (2009). Rhyner and Stüssi view surveillance of contacts with a bank as retroactive and in real time. Beat Rhyner & Dieter Stüssi, *Kommentar zu Art. 284-285 StPO*, in VSKC-HANDBUCH 484 (2008).

[336] 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 (BASICS OF SWISS CRIMINAL PROCEDURE LAW) 150 (2009); SCHMID, *supra* note 165, at 538.

and requires approval by the Compulsory Measures Court.[337] The surveillance of contacts with a bank requires strong suspicion of the commission of a felony or a misdemeanor, all offenses that carry a custodial sentence or a monetary penalty.[338] In all cases, however, notice to the target must be given unless the Compulsory Measures Court consents to notice being postponed or omitted. CrimPC does not make strictly unusable the results of an unauthorized surveillance of contacts with a bank; instead they are considered to be relatively unusable: findings can be used if they are necessary to solve serious offenses.[339] For the Supreme Court, the evidence is not acceptable if there was no way to obtain it legally.[340] The more serious the committed offence, the more the interest of the prosecution in knowing the truth outweighs the private interest in not using the illegally obtained evidence, but only if the evidence could have been obtained legally.[341]

2. In the US

Undoubtedly because the United States does not share Switzerland's tradition of bank secrecy and bank records are not subject to the Fourth Amendment, no laws in the United States tailor surveillance regulation specifically to the bank context.[342]

F. Undercover Operations

1. In Switzerland

Undercover operations are treated by CrimPC as another secret surveillance measure even though they involve active police involvement with suspects.[343] The Swiss Supreme Court

[337] *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) 167-170 (2011). The bank itself primarily executes this type of surveillance by following the instructions contained in the surveillance order.

[338] *See supra* note 97 (defining various offense levels in Swiss law).

[339] *See supra* Part VI.D.

[340] TF, Nov. 4, 1970, 96 BGE I 437, 441 (Switz.).

[341] TF, May 3, 2005, 131 BGE I 272, 279 (Switz.).

[342] We have a statute providing some secrecy for bank records, but it does not regulate the surveillance of bank contacts as CrimPC does. *See* the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1978) (requiring a subpoena or warrant for the disclosure of financial information to the government).

describes undercover investigation as when a police officer, while hiding his official function, makes contact with suspected people in order to establish and collect evidence of committed offenses.[344] There is no undercover investigation out of or prior to a criminal investigation. The public prosecutor may equip undercover investigators with a cover which provides them with a fake identity.[345] Under Swiss law, undercover investigators shall not engender general readiness to commit criminal offences or direct such readiness towards more serious offences, which addresses similar concerns to the concept of entrapment in the United States. They must restrict their activities to substantiating a pre-existing intention to commit a criminal offense. Their activities must only be of secondary importance to the decision to commit a specific criminal offence, but when necessary they may carry out test purchases or establish that they have the resources to engage in illegal transactions.[346]

Under CrimPC, use of undercover operations requires approval by the Compulsory Measures Court in the same way as for monitoring of telecommunications.[347] Undercover investigations may be used to investigate a smaller number of serious offenses than surveillance of post and telecommunications or technical surveillance devices.[348] The rules of subsidiarity and proportionality apply and notice must be given to the target unless the Compulsory Measures Court consents to notice being postponed or omitted.

---

[343] CRIMPC art. 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) (2010); Laurent Moreillon & Miriam Mazou, *Commentaire ad art. 296-298 CPP (Commentary to articles 296-298 CrimPC*), in *Commentaire* ROMAND DU CODE DE PROCÉDURE PÉNALE (COMMENTARY TO CRIMINAL PROCEDURE CODE) (2010).

[344] TF, June 16, 2008, 134 BGE IV 266, 277, para 3.7 (Switz.).

[345] 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.

[346] If an undercover investigator oversteps the scope of the permissible action, then this 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. 3.

[347] CRIMPC art. 274, 289.

[348] CRIMPC art. 269, para. 2 contains the list pertaining to surveillance of post and telecommunications and use of technical surveillance equipment and art. 286 contains the second list pertaining to undercover investigations. The two lists contain contraventions, misdemeanors and felonies, but art. 269 lists more offenses than art. 286.

Findings made in the course an unauthorized undercover investigation or when notice has not been given may not be used. This is a complete exclusionary rule as for an unauthorized surveillance of post and telecommunications.[349]

2. In the US

No statute regulates law enforcement use of informants. Instead, in a series of cases that are decades old, the Supreme Court found that it did not constitute a Fourth Amendment search for agents to use undercover agents who either recorded or transmitted information divulged by a criminal suspect.[350] The use of undercover agents, per se, does not require a warrant or other judicial oversight. But if undercover agents engage in wiretapping or another surveillance method that is regulated by statute or by the Fourth Amendment, then the same rules that apply to law enforcement investigators generally apply to agents working undercover. [351]

G. Physical Observation

1. In Switzerland

Members of the public prosecutor and police officers, in the course of investigations, may covertly observe people and things in places accessible to the general public and may make audio and video recordings for criminal prosecution.[352] CrimPC regulates focused, systematic physical observation, as well as observation that takes place over time, for the first time. Physical observation is limited to public places and is treated differently from surveillance in private places, which falls under use of technical surveillance devices and is therefore subject to more oversight. While courts have not yet confirmed clearly that observation breaches privacy,

[349] CRIMPC art. 289, para. 6. *See supra* part VIII.B.1.

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

[351] *See, generally*, WAYNE R. LAFAVE ET. AL., CRIMINAL PROCEDURE § 3.1(c) (3d. ed. 2007).Ross, *supra* note 22, at 533-43.

[352] CRIMPC art. 282; Conseil Fédéral, Message relatif à l'unification du droit de la procédure pénale (Message about Unification of Criminal Procedure Law) (FF 2006-1057) 1235); SCHMID, *supra* note 165, at 533-535.

scholars argue that it does, at least if the observation persists. The Federal Council correctly decided to provide a legal basis for physical observation in CrimPC.[353]

Physical observation, which may be recorded or not, typically occurs in real time. The Swiss Supreme Court decided that following a chat in an online (public) forum and focusing on some participants constitutes observation, while just looking into the conversation without focusing on somebody or something is not surveillance but is instead comparable to officers patrolling the street. Note that it will be considered to be an undercover investigation when a police officer takes part in a conversation without identifying himself as a police officer. Observation occurs at a distance, while undercover investigation requires an officer designated for this purpose to infiltrate a given environment.[354]

Under CrimPC, use of physical observation is not treated as in the most invasive category of surveillance. Instead, it may proceed so long as there are concrete reasons to assume that crimes or offenses have been committed.[355] This is a lower standard than the strong suspicion required of the other surveillance methods. Physical observation requires that the underlying offense be any felony or misdemeanor. The police can covertly observe people and things in places accessible to the general public and make audio and video recording up to a month. After one month, the continuation of the observation requires authorization by the public prosecutor.[356]

Physical observation is authorized only by the public prosecutor or the police and not by an independent court. Because of this lack of judicial review, defendants may challenge the surveillance when they learn of it by submitting an objection to the decision of the public prosecutor or the surveillance itself to a cantonal court.[357] In addition and similarly to other categories of surveillance, defendants may challenge the surveillance after receiving notice of it.

---

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

[354] TF, June 16, 2008, 134 BGE IV 266 (Switz.).

[355] CRIMPC art. 282, para. 1a.

[356] CRIMPC art. 282. CrimPC does not require that the authorization be in writing, but that is obviously recommended.

[357] CRIMPC art. 393, para 1a.

Similar to surveillance of contacts with a bank, CrimPC does not treat as unusable the results of an unauthorized surveillance of contacts with a bank. Instead, such results can be used only if they are necessary to solve serious offenses.[358]

2. In the US

While CrimPC provides reduced regulation for surveillance in public, traditional U.S. law has provided none at all. The traditional understanding has been that there is 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 exists."[359] 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."[360] Although some criticized have the notion that people assume the risk of unobserved surveillance when they venture outside,[361] courts have not largely questioned it.

The Supreme Court's decision in *United States v. Jones*[362] may indicate a shift. The *Jones* case concerned the use of a specialized GPS device attached to a car, but it has broader implications because the Court could have disposed of the defendant's claim on the ground that he was observed outside. The Court's failure to do so opens the way for future cases to revisit

[358] *See supra* Part VIII.**Error! Reference source not found.**.1.

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

[360] *See* Kerr, *supra* note 300, at 1010 (citing cases); Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate, 519 F.2d 1335 (3rd Cir. 1975) (no privacy right violated by police observations of public meetings and activities).

[361] *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 113-126 (2011); SLOBOGIN, *supra* note **Error! Bookmark not defined.**, at 79-136.

[362] United States v. Jones, 132 S. Ct. 945 (2012).

the assumption that movements out of doors cannot be subject to Fourth Amendment protection.[363]

H. New Techniques

1. In Switzerland

CrimPC is drafted as a technology neutral law that is open to new techniques, including those not yet known.[364] No rules specifically include new techniques but at the same time no rules are specifically limited to existing techniques.

It seems likely that as new surveillance techniques are developed, Swiss law will consider them to be covered under rules pertaining to technical surveillance devices. Indeed the Technical Surveillance equipment category, article 280, has been designed for techniques used in order to listen, observe or locate, including to record, but those categories are considered illustrative rather than exhaustive.

If a new technique is fundamentally different in its means or goals, however, a specific new rule would be necessary. The federal Constitution and the ECHR require that a law be clear and foreseeable as to its effects, which prohibits adding techniques that the person concerned could not have 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, such as perhaps electronic field interceptors.

When law enforcement agents want to use a new technique, they have to discern if the legislature deliberately excluded that technique from CrimPC. If the legislature deliberately excluded a technique, even without saying so explicitly, CrimPC is not a legal basis for this technique and there is no basis to argue from analogy. The technique may be used only after

[363] *See, e.g.*, Montana State Fund v. Simms, 2012 MT 22 (MT Sup. Ct. Feb. 1, 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.

[364] Tribunal administratif fédéral [TAF] [Federal Administrative Court] June, 23, 2011, RECUEIL OFFICIAL DES ARRÊTS DU TRIBUNAL FÉDÉRAL ADMINISTRATIF SUISSE [ATAF] A-8267/2010, para. 3.2.

CrimPC has 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, the technique is usable.

In passing CrimPC, the legislators failed to mention government-software or electromagnetic field interceptor equipment that is used to collect data that is not publicly accessible. This equipment is used to monitor communications, but it may collect more than communications, and when it does so it cannot be treated as surveillance of post and telecommunications. The courts will have to decide if a new rule is needed or if use of this equipment is the use of technical surveillance devices. IMSI-Catchers have never been mentioned by courts or legislators, but they are used to intercept communications and communications attributes by using communications infrastructures. As such, courts should treat IMSI-Catchers as devices that monitor telecommunications when they collects communications and attributes.

2. In the US

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

For example, some courts have found that acquisition of cell phone location data falls outside the scope of ECPA.[365] But if so, it remains unclear whether the technique is covered by the Fourth Amendment, and if not, what the proper legal treatment of such techniques should be.[366] Ambiguity in both constitutional and statutory coverage in the United States leads to a significant amount of legal uncertainty that is not resolved when the judges who address the issues disagree.

---

[365] *See* In re Application of the United States for an Order Directing a Provider of Electronic Communications Services to Disclose Records to the Government In re Application, 534 F. Supp. 2d. 585, 602 n.44, (W.D. Pa. 20008) (collecting cases), *aff'd*, No-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010)

[366] *See infra* Part VIII.C.2.e.

I. Search and seizure Distinguished from Surveillance

1. In Switzerland

Under Swiss law, search and seizure are not treated as surveillance under CrimPC but rather as coercive measures like arrest and detention. Searches may proceed after the public prosecutor writes an order and without the subject's consent only if there are sufficient reasons to assume the presence of wanted people or if offenses are currently being committed. Searches may proceed if there is evidence, such as objects or assets, that could be legally seized. In general, personal documents and correspondence of an accused person may not be searched and seized when the protection of his or her privacy is considered as more important than the criminal investigation.[367] If a search is challenged, all documents and objects are sealed and the Compulsory Measures Court has to decide whether to unseal them.[368]

Neither the text of CrimPC nor any Supreme Court case draws a clear line between surveillance and searches. As mentioned before, it would seem to be significant whether the accused person is aware of the search and whether it happens in a place the target controls, such as his home, which would be a search, or in a place controlled by a provider, which would be surveillance.[369] Seizures and searches of computer material from the accused person's or property would be treated as a seizure rather than as surveillance.[370] Orders to a service provider to disclose an accused person's communications in storage with that provider would fall under the surveillance rules.

2. In the US

United States law shares with Swiss law a distinction between surveillance techniques and searches and seizure. Unlike in Switzerland, however, in the United States there is no comprehensive surveillance law; instead, statutory law covers many fewer categories of surveillance than does CrimPC, and provides many fewer protections than does the Swiss law.

---

[367] Certain communications may not be subject to seizure, such as correspondence between an accused person and his or her lawyers, and other privileged items and communications.

[368] CRIMPC art. 244ss and 263ss.

[369] HANSJAKOB, KOMMENTAR ZUM BÜPF, *supra* note 106, at 81-85; Sträuli, *supra* note 108, at 99-100 and 107-8.

[370] CRIMPC art. 263ss; Rhyner & Stüssi, *Kommentar zu Art. 269-279 StPO*, *supra* note 109, at 443-5.

As discussed in Part III.B, the U.S. Supreme Court and several federal courts of appeal recognized that law enforcement investigatory techniques that may be characterized as hidden, indiscriminate, intrusive, and continuous require the highest level of protection from abuse and the greatest level of judicial oversight. Since then, however, the Court has limited the types of investigations subject to the highest protections to wiretapping, eavesdropping, and silent video surveillance of places in which the subject has a reasonable expectation of privacy. In ECPA, Congress expanded the category to include real-time acquisition of e-mails, but the coverage was limited in that it did not include a statutory suppression remedy, and the use of this technique has been quite limited due to the easier route of acquiring e-mails from storage with service providers.[371] Arguments to extend the category to take account of modern analogues of wiretapping and video surveillance have not been successful.[372]

As a result, while traditional wiretapping (of wire, oral and electronic communications) and some video surveillance is subject to the type of protections provided by CrimPC: notice, a remedy, subsidiarity and proportionality, the rest of what CrimPC treats as surveillance is subject to significantly less protection. Search and seizure of documents from the target's own possession, as in Switzerland, is accorded the intermediate treatment of the requirement of a probable cause warrant, notice in most cases, and a remedy.[373] But a large number of investigative techniques are subject to considerably less protection than that afforded during ordinary search and seizure investigations. Law enforcement agents in the United States may use undercover agents, collect stored communications contents and attributes, collect attributes in real time, track location data, and use all sorts of modern techniques subject either to no regulation or to the anemic protections afforded by Congress. In the United States then, the distinction between search and seizure and surveillance is a bit schizophrenic. Either, as a result of Supreme Court precedent, a surveillance technique is subject to the highest level of regulation and considerably

[371] *See* Soghoian, *supra* note 205, at 10 (pointing out that since 1997, federal authorities had obtained only 67 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 cheaper and easier for them to do it after the fact rather than in real-time").

[372] *But see In re Application*, 534 F. Supp. 2d. at 586 n.7 (discussing factors in reference to cell site location information).

[373] *See* Fed. R. Crim. P. 41; Smith, *supra* note 195, at *13 (noting that traditional search warrants provide notice to the target unlike online surveillance orders).

more restricted than is a traditional search and seizure, or the surveillance technique is treated as outside the scope of the Fourth Amendment and subject to a confusing and complex set of rules, most of which restrict law enforcement's use of the technique dramatically less than the warrant requirement under search and seizure law.

IX. **Conclusion**

Passage of CrimPC heralds a new era in Swiss law during which the rules that pertain to the surveillance of people and their communications has been updated and made largely uniform. CrimPC dramatically contrasts with the laws that regulate surveillance in the United States, which are an incomplete and outdated set of rules that provide disuniformity and weak regulation. As discussed, three features of United States law, as compared to Swiss law, explain the weaker and less comprehensive protections it provides to the targets of law enforcement surveillance. First, United States jurisprudence finds a large proportion of surveillance practices to be outside the scope of the Fourth Amendment, as compared to the more comprehensive coverage of comparable practices under ECHR, constitutional law, and now CrimPC in Switzerland. The second is that in the absence of constitutional regulation, United States law enforcement agents proceed without any statutory regulation, while Swiss police may not conduct surveillance that CrimPC does not authorize and regulate. Lastly, United States statutory regulations, like ECPA, in addition to be incomplete are also weak and ineffectual and fall far short of guaranteeing the meaningful remedies provided by Swiss law. Most notably, under U.S. law, targets often receive no notice that they have been surveilled, and they have no real remedy for abuse. Much surveillance in the U.S. operates without meaningful oversight either by the Courts or Congress. As Americans recognize the need for change, they should turn to CrimPC for guidance.