2007

Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead.

Allen E. Shoenberger
Loyola University Chicago, ashoen1@luc.edu

PRIVACY WARS: EU VERSUS US: SCATTERED SKIRMISHES, STORM CLOUDS AHEAD

Allen Shoenberger*

"A man in a police cell is entitled to privacy just as much as a man sitting at his fireside in his own home."[1]

Disclosure through publication of still photos from a closed-circuit television film of a person brandishing a knife while walking on a public street, "constituted a disproportionate and therefore unjustified interference with his private life."[2]

Terrorists allegedly plot to blow up ten airplanes flying from Britain to the United States. The European Court of Justice invalidates an agreement by the European Union (EU) to provide airplane passenger data to the United States government, citing privacy concerns.[3]

"The Convention protects the community of men; man in our times has a need to preserve his identity, to refuse the total transparency of society, to maintain the privacy of his personality."[4]

President Bush authorizes a domestic surveillance program without informing Congress. The New York Times discovers the program and reveals it four years later.[5]

"The money transfer company SWIFT has for years secretly supplied U.S. authorities with huge amounts of personal data for use in antiterrorism

---

* Professor of Law, Loyola University Chicago School of Law, J.D. Columbia Law School, LL.M. New York University School of Law. I would like to thank my wife, Caroline Shoenberger, J.D., M.B.A., M.A., B.A., for her many contributions toward this Article over years of discussion.

1. Wood v. United Kingdom, App. No. 23414/02, 636 Eur. Ct. H.R. (2004) (quoting British trial judge). *Contra* Hudson v. Palmer, 469 U.S. 517, 530 (1984) (prisoners have no legitimate expectation of privacy in jail cells with respect to any matter in the cell).

2. Peck v. United Kingdom, App. No. 44647/98, 36 Eur. H.R. Rep. 41, ¶ 87 (2003).

3. *See* Cases C-317/04 and C-318/04, Eur. Parliament v. Council of the Eur. Union and Comm'n of the Eur. Cmtys., 2006 E.C.R. I-4721.

4. Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 (1985) (Matscher & Farinha, JJ., partially dissenting) (referring to the European Convention on Human Rights and Fundamental Freedoms).

5. Scott Shane, *Spying Debate Interrupts Senate Session on Security*, N.Y. TIMES, Feb. 3, 2006, at A16. In February 2006, the ABA House of Delegates took a position in opposition to the program. In particular, the ABA stated that it "opposes any future electronic surveillance inside the United States by any U.S. government agency for foreign intelligence purposes that doesn't comply with the 1978 Foreign Intelligence Surveillance Act." *Quick Work on Policy Opposing Surveillance*, 5 A.B.A. J. E-REP., Feb. 17, 2006.

investigations, violating EU privacy rules. . . ."[6]

As a result of a May 30, 2006, decision of the European Court of Justice (ECJ), each passenger airplane coming from Europe to the United States faced the possibility of multi-million dollar fines for failure to divulge passenger data to the U.S. government prior to arrival.[7] Fortunately for the busy summer travel season, the court effectively stayed its decision until September 30, 2006.[8] The decision in *European Parliament v. Council of the European Union and Commission of the European Communities* reflects the sharp differences between European and American privacy law. While it is widely assumed that the impact of the decision can be dealt with by the deadline, the narrow decision of the ECJ leaves several fundamental questions of European privacy law unresolved, which may only be settled by the European Court of Human Rights.[9]

The September 27, 2006, opinion by the Commission for the Protection of Private Life of Belgium regarding SWIFT's failure to comply with EU and Belgian privacy law in providing massive amounts of financial data transfer information to the U.S. government suggests that many more areas of conflict remain to be resolved between the United States and EU regarding privacy matters.[10]

This is significant for several reasons. First, the United States exists today in an interdependent, global economy. The actions of the United States affect the rest of the world, and the United States is also affected by actions of other states.[11] For example, American firms that market products and services

---

6. *Transfer of Bank Data to U.S. Rebuked*, CHI. TRIB., Sept. 15, 2006, at C20.

7. *See* Cases C-317/04 and C-318/04, Eur. Parliament v. Council of the Eur. Union and Comm'n of the Eur. Cmtys., 2006 E.C.R. I-4721, ¶¶ 65-66.

8. *Id.* at ¶ 74.

9. In an article dated October 6, 2006, the New York Times indicated that a revised agreement had been reached. Various changes in the previous agreement indicated that the United States would have more latitude in sharing data among law enforcement authorities but that the data would not be automatically shared; transfers would only happen upon request. One explanation was that the data could no longer be pulled by the United States; it had to be pushed by the EU. The agreement remains subject to approval by the EU member nations, a matter that may have happened within the following week, according to the article. *Europe and U.S. Agree on Air Passenger Data*, N.Y. TIMES, Oct. 6, 2006, at 8, *available at* http://www.nytimes.com/2006/10/06/world/europe/07aircnd.html.

10. Commission de la Protection de la vie Privee, *Opinion on the Transfer of Personal Data by SCRL SWIFT Following the UST (OFAC) Subpoenas*, *available at* http://www.privacycommission.be/communiqu%E9s/summary_opinion_swift_%2028_09_2006.pdf. SWIFT has approximately 7800 financial institutions as clients. The Belgian investigation indicated that 2.5 billion records "could have been the subject of subpoenas" during the year 2005. *Belgians Say Banking Group Broke European Rules in Giving Data to U.S.*, N.Y. TIMES, Sept. 29, 2006, at 10. *See also EC Vows No Cover-Up on SWIFT Scandal*, BUS. WK., July 7, 2006, http://www.businessweek.com/print/global12/content/jul2006/gb20060707_22460.htm.

11. "In 1995, EC companies owned about 58% of all foreign direct investment in the United States, and US companies held about 44 percent of foreign direct investment in the EC According to one study, European investment supported 12 percent of US manufacturing jobs in

in Europe, and thus their employees, are directly impacted by European privacy law. Privacy law can be used as a trade barrier, negatively impacting the U.S. economy. Lawyers, businessmen, and citizens should therefore have an understanding of the contours of those laws.

Second, in important Constitutional opinions, the U.S. Supreme Court has cited European Court decisions as well as European laws and treaties.[12] There is every indication that this will continue, as it is a simple reflection of global interrelationships at both an economic and jurisprudential level. Moreover, United States Supreme Court Justices, as well as the Justices of European courts, talk to each other on a routine basis. Several years ago, a group of my law students were seated in Luxembourg to hear oral arguments before the European Court of Justice. Four United States Supreme Court Justices then walked into the courtroom and sat in the front spectator row to hear the arguments.[13] Additionally, amicus briefs are now routinely filed in the United States Supreme Court by attorneys for the European Union.[14]

1995." Mark Pollack & Gregory Shaffer, *Transatlantic Governance in Historical and Theoretical Perspectives*, *in* TRANSATLANTIC GOVERNANCE IN THE GLOBAL ECONOMY 13-14 (Pollack & Shaffer eds., 2001) (citation omitted). "The US and EU . . . remain the world's most important economic powers and each other's primary economic partners." Mark Pollack & Gregory Shaffer, *Who Governs*, *in* TRANSATLANTIC GOVERNANCE IN THE GLOBAL ECONOMY 287, 291 (Pollack & Shaffer eds., 2001).

> The European Union and the United States are the two largest economies in the world. They account together for about half the entire world economy. The EU and the US have also the biggest bilateral trading and investment relationship. Transatlantic flows of trade and investment amount to around $1 billion a day, and, jointly, our global trade accounts for almost 40% of world trade. By working together, the US and the EU can promote their common goals and interests in the world much more effectively.

European Union - United States Facts and Figures - Statistics, http://www.eurunion.org/profile/facts.htm (last visited Mar. 28, 2007).

12. Lawrence v. Texas, 539 U.S. 558, 578 (2003) (citing Dudgeon v. United Kingdom, 45 Eur. Ct. H.R. (ser. A) para. 13 (1981); Roper v. Simmons, 543 U.S. 551, 575-578 (2005) (noting the abolition of the death penalty for children by "other nations that share our Anglo-American heritage, and by the leading members of the Western European community," citing the 1948 abolition of the death penalty for children in Great Britain, and the eventual complete abolition of the death penalty in Great Britain).

13. This exemplifies the cross-fertilization between judges of the supreme courts of many countries that has become frequent. *See* ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER 65, 103 (2004) (discussing both the frequent meetings of supreme court judges from different countries, as well as the practice of such courts citing cases decided by courts of other countries).

14. For example, in *Roper v. Simmons*, 543 U.S. 551 (2005), an amicus brief was filed on behalf of the European Union and Members of the International Community. In *Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004), an amicus brief was filed on behalf of the European Commission. In *Crosby v. National Foreign Trade Council*, 530 U.S. 363 (2000), an amicus brief was filed on behalf of the European Communities and their member States. In *Sanchez-Llamas v. Oregon*, 126 S. Ct. 2669 (2006), an amicus brief was filed on behalf of the European Union and Members of the International Community, as well as amicus briefs by the Republic of Honduras and the Government of the United Mexican States. In *Medellin v. Dretke*, 544 U.S. 660 (2005), an amicus brief was filed on behalf of the European Union and Members of the International Community. Moreover, in *Intel Corp. v. Advanced Micro Devices, Inc.*, 124 S. Ct.

Third, European courts, particularly the European Court of Human Rights, routinely confront privacy issues and have in some areas developed extensive analysis of various constitutional rights in the context of a myriad of factual situations.[15] Accordingly, it is worthwhile to become familiarized with those decisions. Whether the United States Supreme Court accepts or rejects them, the value of a body of precedent governing over 800 million persons cannot be overlooked.

Constitutionally-derived privacy law in the United States primarily deals with privacy claims against the government.[16] European law deals far more extensively with privacy claims between individuals and/or business entities (sometimes referred to as undertakings) at a supra-national level—that of the European Union or the European Convention on Human Rights.

However, it is by no means universal that more protection is afforded to private information in the European legal systems than in the United States. For example, transcripts of telephone conversations obtained by police wire taps involving significant public figures, such as former Italian President Craxi and Prince Victor Emmanuel III, son of the last king of Italy, are routinely published in newspapers long before any trial has commenced and regardless of their relevance to particular criminal allegations.[17]

2466 (2003), not only was an amicus brief filed on behalf of the European Communities, a motion was made and granted to permit an attorney to present oral argument before the United States Supreme Court as amicus curiae, a privilege ordinarily only accorded to the Solicitor General of the United States. In *F. Hoffman-LaRoche Ltd. v. Empagran*, 524 U.S. 155 (2004), separate amicus briefs were filed on behalf of The Federal Republics of Germany and Belgium, Canada, Japan, the United Kingdom, Northern Ireland and Ireland, and the Kingdom of the Netherlands. In *Hamdan v. Rumsfeld*, 126 S.Ct. 2749 (2006), separate amicus briefs were filed on behalf of 422 current and former members of the United Kingdom and European Parliaments and on behalf of 304 United Kingdom and European Parliamentarians. In *Kansas v. Marsh*, 126 S. Ct. 2516, 2533 n.3 (2006), Justice Scalia concurred, but while doing so cited a website of the Delegation of the European Commission to the U.S.A. Justice Scalia also noted that the Supreme Court cited a brief filed for the European Union as amicus curiae in a previous case. *See Atkins v. Virginia*, 536 U.S. 304, 316 n.21 (2002).

15. In a previous article, I argue the United States should acknowledge the European Court of Human Rights case law, partly because it is the highest volume human rights court currently deciding cases in the world. Conversely, the United States Supreme Court decides only a tenth of the number of cases decided by the ECHR. Of course, most of the decisions by the Supreme Court are not human rights decisions in the ordinary sense of the term. *See*, Allen E. Shoenberger, *Messages from Strasbourg: Lessons for American Courts from the Highest Volume Human Rights Court in the World – The European Court of Human Rights*, 27 WHITTIER L. REV. 357 (2005).

16. The right to be let alone dates back to the seminal article by Warren and Brandeis, which concerned actions by the government invading and individual's privacy. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L.REV. 193 (1890). *See* Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U.L. REV. 479 (1990).

17. Craxi v. Italy, App. No. 25337/94, 38 Eur. H.R. Rep. 47, 1025 (2004) (section 30 of the decision includes extracts of wiretap conversations published in the press); Peter Popham, *The Prince and the Prostitutes*, THE INDEPENDENT, June 22, 2006, at 1 *available at* (describing that transcripts of wiretaps of Prince Victor Emmanuel had been filling Italy's daily papers about this key figure at the center of a squalid tangle of vice and greed)

Because of the importance of privacy issues to U.S. citizens and businesses, exemplified by the possibility of $2 million to $4 million dollar fines for a single airplane flight, understanding the sharp differences as well as agreements between European and U.S. privacy law is vitally important to American lawyers and businesses.

This Article will explore those differences and similarities, emphasizing the jurisprudence of the highest European courts having jurisdiction over privacy disputes, the ECJ and the European Court of Human Rights (ECHR), and the applicable statutory and treaty law of the European Union and Council of Europe. Particular attention will be paid to the privacy of telephones, homes, offices, computers, and data protection. A number of these differences may suggest or require legislative solutions in the United States, as well as a re-analysis of the U.S. approach to the protection of private data and privacy in a general sense.

THE PASSENGER DATA PROTECTION CASE

The dispute reflected in *European Parliament v. Council of the European Union* relates to measures taken by the United States subsequent to and as a result of the tragic events of September 11, 2001.[18] In November 2001, the United States enacted legislation requiring air carriers operating flights to, from, or across U.S. territory to provide U.S. customs authorities with electronic access to data contained in their automated reservation and departure control systems, referred to as Passenger Name Records (PNR).[19] The data consists of between thirty and sixty fields of information, including simple data such as names.[20] Additionally, certain fields could be used to reveal information about a passenger's religious affiliation, such as those fields indicating whether a passenger has ordered a kosher or halal meal.[21]

The Commission of the European Union negotiated with the United States regarding the disclosure of PNR data and eventually reached an agreement approved on May 14, 2004. The agreement was also approved by the European Union Council of Ministers on May 17, 2004.[22] However, the European Parliament declined to accept this decision and commenced litigation before the European Court of Justice, alleging a number of deficiencies, including:

1. The Commission decision was ultra vires because the subject matter

---

http://news.independent.co.uk/europe/article1094703.ece.

18. Cases C-317/04 and C-318/04, Eur. Parliament v. Council of the Eur. Union and the Comm'n of the Eur. Cmtys., 2006 E.C.R. I-4721, ¶ 33. This was a grand chamber decision, comprised of the Presidents of all the Chambers of the Court and six additional judges.

19. *Id.*

20. Henry Farrell, *Airline Passenger Data Dispute Is Merely "An Internal EU Dust-Up,"* June 7, 2006 http://www.cfr.org/pulication/10895/.

21. *Id.* Thus, whether a passenger is Jewish or Muslim may be detected.

22. *Eur. Parliament*, 2006 E.C.R. I-4721, ¶ 43.

was outside the competence of European Community law;[23]

2. It did not matter that the data was to be transferred by private airline carriers, which are covered by the provisions of the European Directive on the Protection of Individuals with regard to the Processing of Personal Data;[24]
3. Violation of Article 8 of the European Convention on Human Rights;[25] and
4. Other claims, including the principle of proportionality, the requirement to state reasons, and the principle of cooperation in good faith.[26]

The ECJ held, in short, that the entire area subsumed by the agreement between the United States and the Commission of the European Union was beyond the competence of the Commission and Council.[27] The Court noted that, although airlines were sharing the data, and not European governments, the airlines remained subject to European law.[28] The remaining issues were left to future litigation.

The Court reasoned, that the directive forming the base of European Union privacy law excludes data concerning "public security, defense, State security, and the activities of the States in areas of criminal law" from its coverage.[29] Presumably, the reason for these exclusions relates to the limited transfer to central EU institutions of sovereign power by the twenty-seven states that collectively form the EU. The justification for sharing PNR data was explicitly for state security; more particularly, for "preventing and combating terrorism and related crimes, other serious crimes, including organized crime, that are transnational in nature, as well as flight from warrants or custody for these crimes."[30]

In theory, it is possible for the twenty-seven members of the EU to negotiate separate agreements with the United States to "solve" this competence problem.[31] All of the other issues raised by the European Parliament, however, remain unresolved. In particular, two serious issues remain undecided. First is whether the essence of the PNR agreement violates Article 8 of the European

23. *Id.* ¶ 51.
24. *Id.* ¶¶ 57-58.
25. *Id.* ¶ 62.
26. *Id.*
27. *Id.* ¶¶ 60-61.
28. *Id.* ¶ 58. The fact that the "PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country . . . The transfer falls within a framework established by the public authorities that relates to public security." *Id.*
29. *Id.* ¶ 54 (citing Council and Parliament Directive 95/46, art. 3(2), 1995 O.J. (L281) (EC)) (concerning the protection of individuals with regard to the processing of personal data and the free movement of such data and its subsequent amendments).
30. *Id.* ¶¶ 55-56.
31. Henry Farrell made precisely this suggestion and characterized the dispute as "an internal EU dust-up." *See* Farrell, *supra* note 21.

Declaration of Human Rights. Separate agreements with the current governments of twenty-seven countries cannot resolve this issue. The ECHR stands above the constitutions of these countries and reflects the agreement of forty sovereign nations, including many of whom are not EU member states.[32] Second, assuming agreements are made with the United States, would the agreements themselves violate the scheme of protection established for personal data by the EU Directive protecting such data? If the agreements do violate that scheme, what are the consequences? Would the ECJ or the ECHR find such violations sufficient to vitiate any agreement, which is not completely consistent with the requirements of the EU directive on personal data protection?

The complex structure of the EU Directive on personal data must be examined before any of these questions can be answered. For purposes of the Directive, "personal data" means any information relating to an identified or identifiable natural person.[33] Personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and up to date; and (e) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which they are further processed.[34]

Processing of personal data is subjected to a series of conditions: (a) the data subject must have unambiguously given his consent; (b) processing must be necessary for performance of a contract to which the data subject is party; (c) processing must be necessary for compliance to which the controller is subject; (d) processing must be necessary to protect the vital interests of the data subject; (e) processing must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the person controlling the data or a third party to whom the data is disclosed; or (f) processing must be necessary for the purposes of the legitimate interests pursued by the controller or third party to whom the data is disclosed, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject requiring protection under Article 1.[35]

---

32. Russia and Turkey, for example, are members of the Council of Europe but not the EU. *See* The Council of Europe's Member States, http://www.coe.int/T/E/Com/About_Coe//Member_states/default.asp (last visited Mar. 28, 2007); European Countries, http://europa.eu/abc/european_countries/index_en.htm (last visited Mar. 28, 2007).

33. Council & Parliament Directive 95/46, art. 2(a) 1995 O.J. (L281) (EC) An identifiable person is one who can be identified directly or indirectly by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. *Id.*

34. *Id.* art. 6.

35. *Id.* art. 7. Article 1 provides:

1. In accordance with this Directive, Member States shall protect the

Certain types of data generally may not be processed, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or an individual's sex life.[36] Several exceptions apply, such as when the data subject gives explicit consent to the processing of the data, unless the state's laws provide such consent is invalid.[37] The most significant exception for PNR data purposes is contained in Article 8, Section 4: "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down by Article 8(2)."[38]

It is further required that the data subject be provided information, including: (a) the name of the person controlling the data; (b) the purpose of processing the data; and (c) recipients or categories of recipients of the data, whether replies to questions are voluntary and the consequences of failing to reply, as well as the existence of a right to access the data and to rectify errors concerning the data subject.[39]

Article 13 of the Directive permits EU Member States to adopt legislative measures to restrict the scope of obligations under the Directive, including disclosure obligations, when such a restriction constitutes a measure necessary to safeguard: (a) national security; (b) defense; (c) public security; (d) prevention and prosecution of criminal offenses or ethical breaches for regulated professions; and (e) enumerated important economic or financial interests of the Member States.[40]

This scheme of data protection suggests that the degree of governmental limitation placed on the processing, collection, and use of personal data in the EU is both considerably more detailed and based on a different approach from that prevalent in the United States. In particular, the EU system requires that a data subject give specific approval prior to the collection and/or processing of personal data. The approach within the United States is quite different;, individuals have the ability to opt out of the data collection system, however, if they choose not to consent is implied. The approaches are referred to as "opt in" versus "opt out" systems.[41]

A second way in which the EU scheme differs from the United States is that the use of private data is seriously curtailed. Information divulged by a data subject is to be employed solely for the purpose for which the data subject

---

fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

36. *Id.* art. 8.

37. *Id.* art. 8(2)(a).

38. *Id.* art. 8(4).

39. *Id.* art. 10.

40. *Id.* art. 13. These enumerated measures include monetary, budgetary, and taxation matters. *Id.*

41. *See* Caroline O. Shoenberger, *Consumer Myths v. Legal Realities: How Can Businesses Cope?*, 16 LOY. CONSUMER L. REV. 189, 198-99 (2004).

provides the information, in the absence of explicit permission stating otherwise.[42] It is quite common in the United States for personal information to be employed for purposes beyond the immediate transaction. For example, a purchaser of an expensive car might have themselves identified as a "Rodeo Drive Chic"[43] consumer to other businesses also interested in marketing high-end value merchandise.[44] Such disclosures are prohibited by the EU Directive.

Moreover, the EU Directive mandates that personal data be retained only for the period of time necessary for the purpose for which the data was shared.[45] For example, once an airline ticket is used, with the exception of a period of time for possible financial disputes, maintaining the associated personal data on file would likely be impermissible. No such temporal limitation exists in the United States.

What are the implications of these requirements for any revised PNR agreement on a country-by-country basis with the United States? Can they be complied with, or do they present a serious obstacle to any further agreement? Presumably, no airline passenger willingly gives the airline personal data possibly subjecting them to criminal prosecution. Nor do they unambiguously give their consent to such use as required by Article 7 of the Directive.[46] It is unclear whether Article 7's alternative grounds for permission of processing data grant blanket permission for such disclosures.[47] Consideration of decisions by the ECHR relating to privacy rights is necessary before these questions may be answered. Accordingly, we will turn to the jurisprudence of that court.

PRIVACY OF TELEPHONE COMMUNICATIONS: CASE LAW

The privacy of telephone conversations[48] is analyzed under Article 8 of

42. *See* Council & Parliament Directive 95/46, art. 7, 1995 O.J. (L281) (EC).

43. This is a term employed by American Express Company to categorize its customers. *See* Dwyer v. American Express, 652 N.E.2d 1351, 1353 (Ill. App. Ct. 1995).

44. *See id. See also* Shoenberger, *supra* note 41 at 196 (not tortious appropriation to sell or rent personal data broken down by economic strata).

45. *See* Council & Parliament Directive 95/46, art. 6, 1995 O.J. (L281) (EC).

46. *See id.* art. 7(a).

47. It is unclear, for example, whether processing the data by transmission to the United States is necessary for a legal obligation to which the data controller is subjected within the meaning of Article 7(b). The European Parliament presented various pleas for invalidation of the agreement that were not reached by the ECJ. These pleas included allegations that the agreement with the United States violated fundamental principles of the Directive, breached fundamental rights, including those covered by Article 8 of the European Convention on Human Rights, and breached the principle of proportionality. Cases C-317/04 and C-318/04, Eur. Parliament, v. Council of the Eur. Union and Comm'n, 2006 E.C.R. I-4721, ¶¶ 50, 62.

48. Telephone calls made from or to business premises, as well as to and from the home, are covered by the notions of "private life" and "correspondence" within the meaning of art. 8(1). *See* Huvig v. France, 12 Eur. H.R. Rep. 528 (1990) (warrant covered both business and personal telephone calls); Kopp v. Switzerland, App. No. 23223/94, 27 Eur.H.R.Rep. 91(1999) (private and professional telephone lines tapped); Halford v. United Kingdom, App. No. 20605/92, 24 Eur.H.R.Rep. 523 (1997) (home and office telephones tapped); MM v.

the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention).[49] Article 8, entitled "Right to Respect for Private and Family Life," provides:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as 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.[50]

At first glance the guarantee of respect in Article 8, Section 1, appears to be vitiated by the broad exceptions of Section 2. ECHR case law, however, demonstrates that the opposite is correct. Only after intense scrutiny is surveillance of telephone conversations by a government or private individual permissible under the European Convention.[51]

The ECHR analyzes privacy cases in a five step process. First, the Court determines if there is an interference with private life. Second, the Court determines if the interference was by a public authority. Third, the Court determines if the interference was justified, in that it must be in accordance with the law, the law must be accessible to the individual, there must be protections against arbitrary interference by public authorities, and the law must be sufficiently precise. Fourth, the Court determines whether the interference occurred for a proper public purpose. Finally, the Court determines that the purpose is necessary in a democratic society. [52]

Application of Article 8

The ECHR has established that telephone calls made from or to business premises or the home are covered by the notions of "private life" and "correspondence" within the meaning of Article 8(1).[53] Indeed, a police cell is also considered a private place for purposes of the European Convention.[54]

Netherlands, App. No. 39339/98, 39 Eur. H.R. Rep. 19 (2004) (police encouraged woman to record conversations on her phone to corroborate allegations that sexual advances were being made towards her via telephone).

49. European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Sept. 3, 1953, 213 U.N.T.S. 222 [hereinafter European Convention].

50. *Id.*

51. See infra notes 53 – 125 and accompanying text.

52. *See, e.g., Halford*, 24 Eur. H.R. Rep. at 523.

53. *Huvig*, 12 Eur. H.R. Rep. at 528; Miailhe v. France, App. No. 12661/87, 16 Eur. H.R. Rep. 332, 332 (1993) (offices and house searched for documents; 15,000 documents seized).

54. Wood v. United Kingdom, 636 Eur.Ct.H.R. (2004) 12, 33 (audio taping).

Similarly, Community Cable Television (CCTV) films of a person on a public street[55] also implicate privacy interests, at least insofar as the videotapes or still pictures therefrom are published in newspapers or television news programs (including in one instance national British Broadcasting Corporation coverage).[56] Even telephone calls on an internal police department phone network are protected as private.[57] Similarly, intercepting phone numbers sent to a pager may violate Article 8,[58] as can the accidental recording of a conversation on someone else's telephone.[59] In short, virtually any conversation on any telephone system is covered by the Article.

Interference by a Public Authority

Private persons who record telephone conversations at the request of the police implicate the Convention; such recording "engage[s] the responsibility of the state."[60] To allow private parties to conduct such investigations would "be tantamount to allowing investigating authorities to evade their responsibilities under the Convention by the use of private agents."[61]

Such treatment mirrors the development of the "state action" doctrine in the United States.[62] The appearance of public authority may be sufficient to implicate the protection of the Fourteenth Amendment's Equal Protection clause. For example, in *Burton v. Wilmington Parking Authority*,[63] the United

---

55. The person was contemplating suicide, and within a few moments attempted to cut his wrists. Peck v. United Kingdom, App. No. 44647/98, 36 Eur. Ct. H.R. 41, ¶ 10 (2003).

56. *Id.* ¶¶ 13-20.

57. *Halford*, 24 Eur.H.R.Rep. at 524.

58. Taylor-Sabori v. United Kingdom, App. No. 47114/99, 36 Eur.H.R. Rep. 17, ¶¶ 16-19 (2003).

59. Kruslin v. France, App. No. 11801/85, 12 Eur. Comm'n H.R. Dec. & Rep. 547, 455-59 (1990). In *Kruslin*, an individual was staying with a criminal suspect whose calls were being tapped as part of a police investigation into a murder. The person being recorded talked about a separate murder. *Id.* ¶¶ 9-10. The individual was charged with murder, aggravated theft, and attempted aggravated theft. *See also* Lambert v. France, App. No. 23618/94, 30 Eur. Ct. H.R. 346, 351 (2000) (target of investigation entitled to complain about tapping a third party's telephone line).

60. MM v. Netherlands, App. No. 39339/98, 39 Eur. Ct. H.R. 19, at ¶¶ 41-42. Although initial suggestion of recording the conversation was made by private party, "the police superintendent made a crucial contribution to executing the scheme by making available for a short time his office, his telephone, and his tape recorder." *Id.* ¶ 38 (quoting A v. France, App. No. 14838/89, 17 Eur. H.R. Rep. 462, 477 (1994)).

61. *MM*, 39 Eur. H.R. Rep. at 422.

62. State action is normally required to find the Due Process and Equal Protection clauses of the Fourteenth Amendment applicable. *See* Shelly v. Kraemer, 334 U.S. 1 (1948); United States v. Stanley, 109 U.S. 3 (1883). *Contra* Marsh v. Alabama, 326 U.S. 501 (1946) (First Amendment applies to town completely owned by a private company; distribution of religious literature could not be criminalized).

63. 365 U.S. 715 (1961) (acknowledging that state and national flags were flying on the building and rent from the coffee shop was necessary to make the public garage a viable economic enterprise for the Wilmington Parking Authority were factors in making the coffee shop a state actor). In *Burton*, the Court articulated a test for state action that requires that facts

States Supreme Court held that a private coffee shop located in a public garage was subject to the limitations of the Fourteenth Amendment when it refused to serve black customers.

JUSTIFICATION IN ACCORDANCE WITH THE LAW

The scrutiny with which courts review an interference with privacy is quite strict. Ordinarily, explicit textual authorization is required by the applicable domestic legal system, however, the ECHR has recognized that adequate policy strictures may suffice. For example, at the time when *MM v. Netherlands* was decided, Dutch law presupposed that a preliminary judicial investigation and order by an investigating judge was necessary to authorize tapping or interception of "telecommunications" traffic. In *MM*, police suggested to a woman that she record telephone conversations with her husband's lawyer in order to prove allegations that the lawyer was making sexual advances toward her. Because no judicial oversight had been exercised in *MM*, these conditions failed. The Court held private tapping of telephone calls between the lawyer and his client's wife violated the lawyer's privacy rights even though the lawyer made sexual advances.[64]

In *Kruslin v. France*, the ECHR required that a law authorizing tapping had to be particularly precise, with clear, detailed standards.[65] In that context, however, enactments, which rank lower than statutes, and unwritten law may suffice as justifications.[66] But, even France admitted that seventeen safeguards implemented in French law and practice were inadequate and not "particularly precise enough."[67] While some of these safeguards were established in both written and case law, not all were so established. In some instances only a practice lacking the necessary control was established.[68] The system did not have adequate protections against possible abuse. For example, categories of those people able to have telephones tapped by judicial order were not specified, nor were the nature of offenses that could justify such an order.[69]

Also unspecified were the procedures for drawing up summary reports containing intercepted conversations, the precautions taken to communicate the recordings accurately and completely for judicial inspection, the circumstances in which tapes could be erased or destroyed (particularly when an accused has been discharged or acquitted by the court), or any limitation upon the duration

---

and circumstances be sifted and weighed to determine if there is an adequate connection between the private and public actors to hold the private action tantamount to state action. *Id.* at 723.

64. *MM*, 39 Eur. H.R. Rep. at 422. Press reports of the case induced two other women to complain of rape or sexual assaults. *Id.* at 416.

65. Kruslin v. France, App. No. 11801/85, 12 Eur. Comm'n H.R. Dec. & Rep. 451, 458 (1990).

66. *Id.* at 457. In particular, case law may be adequate. *Id.*

67. *Id.* at 456.

68. *Id.* at 458.

69. *Id.*

of the tapping.[70] The court concluded that French law did not indicate with reasonable clarity the scope and manner of relevant discretion conferred on the relevant public authorities.[71]

In contrast to French law, the United Kingdom applied no statutory system regulating interception of pager messages.[72] That practice was held violative of Article 8 of the European Convention for the Protection of Human Rights.[73] Similarly, in *Halford v. United Kingdom*, interception of private telephone calls on a private telephone network was violative of Article 8, since there was no domestic regulation providing for public scrutiny or limitation of abuse of discretion by public authorities.[74]

Domestic law must be sufficiently clear to provide an individual adequate notice of the circumstances in which public authorities may listen to calls.[75] In particular, an individual must be able to understand the law so as to enable them to regulate their own conduct.[76] In *Malone*, the government contended that the applicant, "a suspected receiver of stolen goods was a member of a class of persons against whom measures of postal or telephone interception was liable to be employed."[77] However, the court determined that the entire regulatory scheme of interception in the United Kingdom did not indicate with reasonable clarity the scope and manner of exercise of relevant discretion by public authorities.[78] Thus, the minimum degree of legal protection a citizen was entitled to was lacking and therefore, constituted a violation of Article 8 of the Convention.[79]

The Court was clearly concerned with narrowing the ambit of discretion given to relevant officials, particularly with regard to interceptions that are secret, either when conducted or subsequent to the activity.[80] The Court was terse in its treatment of "metering."[81] Metering records the time and duration of phone calls as well as the numbers called; it was designed by the Post Office, as the responsible entity for the provision of telephone services.[82] The United Kingdom government argued that such metering did not entail interference with

---

70. *Id.*

71. *Id.*

72. Taylor-Sabori v. United Kingdom, App. No. 47114/99, 36 Eur.H.R. Rep. 17, ¶¶ 16-19 (2003).

73. *Id.* ¶ 19.

74. Halford v. United Kingdom, App. No. 20605/92, 24 Eur. H.R. Rep. 523, 536 (1997).

75. Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14, 40 (1985).

76. *Id.*

77. *Id.* at 39.

78. *Id.* at 44.

79. *Id.* at 45. U.K. law was described as "somewhat obscure and open to differing interpretations." *Id.* at 44. The court found a violation even though published statistics indicated that the number of warrants granting authority to intercept was relatively low, while the number of indictable crimes committed and telephones installed was rising. *Id.*

80. *Id.* at 32-33. At no point is a person informed that his communications had been intercepted.

81. *See id.* at 34-35.

82. *Id.* at 45.

any right guaranteed by Article 8, because the supplier of telephone service necessarily obtains this data to enable it to properly charge (or bill) the subscriber.[83] No U.K. law regulated the disclosure of such data, and thus no warrant was required to obtain it.[84] The Post Office does, on occasion, make such information available to the police when requested.[85]

The Court, however, determined that such data did implicate private information, and thus the unregulated provision of such information constituted a violation of Article 8, because no regulation of the exercise of discretion by public authorities existed.[86] One judge posits in a concurring opinion that he would have gone even further:

> The danger threatening democratic societies in the years 1980-1990 stems from the temptation facing public authorities to "see into" the life of the citizen. In order to answer the needs of planning and of social and tax policy, the State is obliged to amplify the scale of its interferences. In its administrative systems, the State is being led to proliferate and then to computerize its personal data-files. Already in several of the members States of the Council of Europe each citizen is entered on 200 to 400 data-files.
>
> . . . .
>
> Telephone tapping has during the last thirty years benefited from many "improvements" which have aggravated the dangers of interference in private life. The product of the interception can be stored on magnetic tapes and processed in postal or other centres equipped with the most sophisticated material. The amateurish tapping effected by police offices or post office employees now exists only as a memory of pre-war novels. The encoding of programmes and tapes, their decoding, and computer processing make it possible for interceptions to be multiplied a hundredfold and to be analysed in shorter and shorter time-spans, if need be by computer. Through use of the "mosaic" technique, a complete picture can be assembled of the life-style of even the "model" citizen.
>
> . . . .
>
> . . . Police interception for the prevention of crime is only one of the practices employed; to this should be added political interceptions, interceptions of communications of journalists and leading figures, not to mention interceptions required by

83. *Id.* at 46.
84. *See id.* at 18.
85. *Id.* at 32.
86. *Id.* at 47.

> national defence and State security, which are included in the "top-secret" category and not dealt with in the Court's judgment or the present opinion.
>
> . . . .
>
> . . . The designation of the collective institutions responsible for ensuring the ex post facto control of the manner of implementation of the measures of interception; the determination of the dates of cancellation of the tapping and monitoring measures, the means of destruction of the product of interceptions, the inclusion in the code of criminal procedure of all measures applying to such matters in order to afford protection of words uttered in a private context or in a private place, verification that the measures do not constitute an unfair stratagem or a violation of the rights of the defence – all this panoply of requirements must be taken into consideration to judge whether or not the system satisfies the provisions of Article 8.[87]

Other countries, such as Switzerland, also failed to adequately protect privacy interests in telephone conversations. In *Kopp v. Switzerland*, the ECHR found that tapping the telephone calls of a lawyer to seek information regarding the lawyer's wife was not regulated by laws with adequate "quality" to protect the privacy interests of the attorney and his clients.[88] Even though Swiss law protected the legal privilege, the actual administration of a wire tap involved a Post Office official listening to all conversations on various telephone lines at the lawyer's office, without independent judicial supervision of the listening. "In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter."[89] The Court further noted that "it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients."[90]

Warning that an interception might occur is part of the requirement of legal regularity. For example, in *Halford v. United Kingdom*, failure to notify a police officer that a telephone call on an internal telecommunications system was intercepted violated the reasonable expectation of privacy otherwise

87. *Id.* at 49-53 (Pettiti, J., concurring). Considering the mute tone of most ECHR opinions, this concurring opinion stands out in sharp contrast. It may, someday, play a role in ECHR jurisprudence similar to that of the classic dissents by Justices Brandeis and Holmes in American Constitutional Law.

88. Kopp.v. Switzerland, App. No. 23223/94, 27 Eur. H.R. Rep. 91, 117 (1999).

89. *Id.* at 94.

90. *Id.* at 117.

applicable.[91] In the absence of any domestic law regulating interception of calls made on systems outside the public network, the government accepted that it had violated the requirement that any interference be in accordance with the law.[92] Without specific proof that her home telephone had actually been tapped, however, the Court was unable to conclude that Article 8 had been violated by intercepting calls on her home telephone.[93]

SURVEILLANCE AGAINST TERRORISM AND OTHER SERIOUS CRIME

In *Klass v. Germany*, the ECHR considered a secret government surveillance program of written and telephone communications that dated back to the Allied occupation of Germany after World War II.[94] The Court considered sequentially whether the program was an interference with private life (it was),[95] whether the program was in accordance with the law (it was),[96] whether the program was "necessary in a democratic society" (it was),[97] and most importantly, whether the system of surveillance adopted included adequate safeguards against abuse.[98] With regard to the inquiry concerning adequate safeguards, the court indicated "[it was] aware of the danger such a law pose[d] of undermining or even destroying democracy on the ground of defending it, [and] affirm[ed] that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[99]

The most rigorous portion of the ECHR analysis considered the details of the oversight of the surveillance program to determine whether adequate safeguards were in place. The surveillance program required a written application listing the applicable reasons why surveillance was proper. The program required that a set of limiting conditions be met before surveillance could be permitted. The program was confined to cases in which there were factual indications to suspect a person of planning, committing, or having committed certain serious criminal acts; measures could only be ordered if the establishment of facts by another method was without prospects of success or considerably more difficult, and even then the surveillance could cover only the

91. Halford v. United Kingdom, App. No. 20605/92, 24 Eur. H.R. Rep. 523, 524 (1997). The Assistant Chief Constable had sole use of her office telephones, one of which was designated for her private use. She had also been explicitly told she could use the phone in connection with her sex-discrimination case. *Id.* at 524.

92. *Id.* at 533-34.

93. *Id.* at 536-37. The Court awarded petitioner 10,000 British pounds as just satisfaction for the serious interference with her privacy, along with 600 pounds for attending the proceedings in Strasbourg, and costs of 25,000 pounds. *Id.* at 523.

94. Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214, 220 (1980).

95. *Id.* at 229.

96. *Id.* at 231 (as modified by a (German) Federal Constitutional Court decision).

97. *Id.*

98. *Id.* at 232.

99. *Id.*

specific suspect or his presumed "contact-persons."[100] Exploratory or general surveillance was not permitted.[101] Further, only certain named officials could approve such surveillance, including Federal Ministers designated by the Chancellor, or where appropriate, the supreme Land authority.[102] Additionally, although not required by law, the competent Minister in practice, except in urgent cases, could seek the prior consent of the G 10 Commission.[103]

The G 10 Commission has provided strict limitations on the implementation of surveillance measures and the use of gathered information. Permission lasts a maximum of three months, after which a new application is necessary.[104] Once the conditions for the surveillance terminate, so must the surveillance.[105] Knowledge and documents obtained through surveillance may not be used for any purpose other than the original reasons listed in the application, and documents must be destroyed once they are no longer needed for their original purpose.[106] During implementation of surveillance, a person qualified for judicial office must exercise initial control, which includes examination of the information before it is transmitted to the requesting service The receiver of the information must destroy any superfluous data.[107] Recourse to the courts is precluded during implementation as well as execution of surveillance itself; however, the option for subsequent direction is provided.[108]

During surveillance, the competent Minister reports every six months to a Board consisting of five members of Parliament. The Minister reports any measures taken to the G 10 Commission on a monthly basis. In practice, the Minister seeks prior authorization from the G 10 commission.[109] The members of the Commission are appointed for the term of the parliament, "are completely independent . . . and cannot be made the subject of instructions."[110] The Court concluded that the review system implemented before and throughout the surveillance process did not exceed what is necessary in a democratic society.[111]

After surveillance has ended, judicial control is possible under the requirement of the German Federal Constitutional Court's judgment of

100. *Id.* at 233.
101. *Id.*
102. *Id.* at 243.
103. *Id.* at 233. The G 10 Commission is a parliamentary oversight commission appointed in proportion to parliamentary representation, but it always includes a member of the opposition party. *Id.* at 222.
104. *Id.* at 214.
105. *Id.* at 221.
106. *Id.* at 233.
107. *Id.*
108. *Id.*
109. *Id.* at 221.
110. *Id.* at 222.
111. *Id.* at 235.

December 15, 1970.[112] That decision requires that the subject of the surveillance be notified as soon as notification can be made without jeopardizing the purpose of the surveillance.[113] The Minister must consider such communication immediately after surveillance has been terminated, and, if necessary, at regular intervals thereafter, reporting his decisions to the G 10 Commission on a regular basis.[114] The G 10 Commission may then order the Minister to inform the subject.[115]

The ECHR considered these measures. In the absence of evidence to the contrary, the ECHR assumed that the relevant authorities were "properly applying the legislation in issue."[116] The Court agreed with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention.[117] The Court then balanced the legislation against the individual right to privacy and concluded that the provisions were appropriate in a democratic society to further the interests of national security and prevention of crime.[118]

The Court next considered whether there were adequate remedies in German law for dealing with secret surveillance. The Court held that although "there can be no recourse to the courts in respect to the ordering and implementation of restrictive measures, certain other remedies are nevertheless open to the individual believing himself to be under surveillance."[119] After notification, various legal remedies are available before the courts, including civil damages and remedies for destruction of documents, as well as resort to the Constitutional Court.[120] The Court concluded, "in the particular circumstances of this case, the aggregate of remedies provided for under German law satisfies the requirements of Article 13 [of the Convention]."[121]

It is clear from *Klass* that the ECHR considered each and every restriction under German law in making its decision, including, in particular, the subsequent notification requirement, Ministerial supervision, and the supervision on a regular basis of the G 10 Commission. It is impossible to say whether the absence of one or more of the procedures would have resulted in a different outcome, but it is reasonable to assume most of the requirements were absolutely necessary.

Accordingly, it is necessary to consider the short, separate opinion of

---

112. *Id.* at 221.
113. *Id.*
114. *Id.* at 214.
115. *Id.*
116. *Id.* at 237.
117. *Id.*
118. *Id.*
119. *Id.* at 240. These include complaining to the G 10 Commission and to the Constitutional Court. Although these were limited remedies, the Court opined, "it is hard to conceive of more effective remedies being possible." *Id.*
120. *Id.* at 240-41.
121. *Id.* at 241. Article 13 requires that domestic law provide a remedy for violation of a right under the European Convention. *Id.*

Judge Pinheiro Farinha. Judge Farinha declared the entire scheme, including its mere existence, is a "real threat" to private and family life.[122] He expressed difficulty accepting that such surveillance measures can be ordered by political authority itself.[123] The oversight of the G 10 Commission, as well as the supervision of an independent judge (as contemplated by the German law), were essential protections.[124] In this case, however, because there were representations by the Government that none of the applicants had been the subject of surveillance or had surveillance ordered, it does not disclose a violation of the Convention.[125]

The surveillance program conducted in the United States by the Bush administration stands in sharp contrast to the intense review of the German surveillance program by the ECHR, with its repeated noting that politics not be involved in the German surveillance. This program has been employed by the Bush administration as a political wedge against the Democrats.[126] It has been reported that a Justice Department official refused to approve the program because of doubts about its legal and constitutional basis and whether adequate oversight existed.[127]

---

122. *Id.* at 242 (Farinha, J., separate opinion).

123. *Id.*

124. *Id.*

125. *Id.*

126. *See* Adam Nagourney, *Seeking Edge in Spy Debate*, N.Y. TIMES, Jan. 23, 2006, at A1.

> [T]he White House . . . views its controversial secret surveillance program not as a political liability but as . . . a way to attack Democrats and re-establish President Bush's standing after difficult year.
>
> . . . .
>
> Democrats—and . . . some Republicans, too—have indeed challenged the administration for eavesdropping without obtaining warrants. They argue, among other points, that the White House is bypassing legal mechanisms established in 1978 that already allow law enforcement agencies to move rapidly to monitor communications that might involve terrorists.

Id. See also Shane, *supra* note 5:

> Senate Democrats on Thursday angrily accused the Bush administration of mounting a public relations campaign to defend the National Security Agency's domestic surveillance program while withholding details of the secret eavesdropping from Congressional oversight committees.
>
> . . . .
>
> President Bush approved the eavesdropping without warrants shortly after the 2001 terrorist attacks, but since the program's existence was revealed in December [2005] by The New York Times, some legal experts and members of Congress have asserted that it violates the Foreign Intelligence Surveillance Act.

Id.; David Cole & Martin S. Lederman, *The National Security Agency's Domestic Spying Program: Framing the Debate*, 81 IND. L.J. 1355, 1355 (2005). The *New York Times* broke the story on December 16, 2005, reporting that it had delayed publication of the story for more than a year. *Id.*

127. Eric Lichtblau & James Risen, *Justice Deputy Resisted Parts of Spy Program*, N.Y. TIMES, Jan. 1, 2006, at 1. Attorney General Ashcroft, from his hospital bed, also was reluctant to approve the program, although it remained unclear whether he ultimately approved the program or whether the administration went forward without his approval. *See id. See also*

There is, in fact, a federal statute, the Foreign Intelligence Surveillance Act (FISA),[128] that provides for "extensive review and fixed accountability."[129] The process for obtaining a warrant "required, first, that the head of the relevant intelligence agency and the Attorney General 'certify personally' that the purpose of the FISC application was to collect foreign intelligence, and second, that a judge sign the order authorizing the surveillance."[130] It appears that FISA, as originally framed, would satisfy the ECHR through its inclusion of judicial oversight, although no provision for notice of surveillance targets similar to that required by the German Constitutional Court is included.[131]

Broad standing rules in both the United States and European Union allow challenges by an individual whose phone has been tapped based upon policies of strict regulation and monitoring of such programs. According to the ECHR, each person recorded by a wiretap has standing to contest its legality.[132] In *Lambert v. France*, the complaint originally rejected by French courts had been raised by a person whose phone was not being tapped.[133] The ECHR's broad view of standing brought French law into alignment with U.S. law. In *Alderman v. United States*, the Supreme Court recognized the standing of a defendant to challenge if either he is a party to the conversation or the conversation took place on his premises.[134]

Programmatic challenges, however, are treated differently in the

---

Sanford Levinson, *The Deepening Crisis of American Constitutionalism*, 40 GA. L. REV. 877, 888 (2006) ("[T]he National Security Agency (NSA) surveillance of phone calls of American citizens, undertaken without a scintilla of judicial approval, and by the Bush Administration's defense of the surveillance in spite of legislation, the [FISA], that seems quite clearly to make it illegal.") (footnote omitted); *see generally* Katherine Wong, *The NSA Terrorist Surveillance Program*, 43 HARV. J. ON LEGIS. 517 (2006).

128. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62).

129. Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 460 (2006).

130. *Id.* at 460.

131. *See id.* at 486.

> FISA was a compromise forged in the fires of controversy created by Watergate, COINTELPRO, and the fifty-year litany of abuses meticulously documented in the Church Committee Report. FISA was a compromise designed to protect the American people from an overreaching, over-intrusive, and unchecked government while still allowing the government to conduct vital surveillance for foreign intelligence purposes with judicial oversight. . . . [I]t is clear that the privacy concerns of American citizens and Congress then are just as valid today.

Id.

132. Lambert v. France, (2000) 30 Eur. H.R. Rep. 346, 349.

133. *Id.* at 354. The complaint alleged that an extension of wiretap authorization was obtained by standard form written instructions without particularized justifications. *Id.* Even though the complainant was charged with handling the proceeds of aggravated theft, held in custody over 6 months, and released subject to judicial supervision, the ECHR awarded him 10,000 francs in non-pecuniary damage, along with costs of 15,000 francs. *Id.*

134. Alderman v. United States, 394 U.S. 165, 197 (1969) (Fortas, J., concurring in part and dissenting in part).

European Union than the United States. In Klass, the Court held that the mere possibility one could have been tapped permitted one to challenge the surveillance program itself.135 No allegation that surveillance measures had been applied was required.

Conversely, the U.S. Supreme Court has applied a more restrictive standing test in denying the right of citizens to challenge the infamous COINTELPRO surveillance program, which requires that actual injury be demonstrated by a litigant.136 Thus, the allegation that one had their own phone tapped does not suffice for a systemic challenge in the United States.137 Actual harm in some concrete form must be demonstrated, not merely the possibility that one's free speech might be chilled by a surveillance system.138

PROTECTION OF PLACES AGAINST SURVEILLANCE

Although most of the aforementioned cases and discussion focused on ECHR decisions involving telephone and/or postal interceptions, many cases have also dealt with the privacy of particular places, including the home, a prison cell, and an office. The ECHR's general approach is similar to that sketched out above; interferences with the rights to privacy are only permissible if in accordance with the law.

For example, in *Elahi v. United Kingdom*,[139] the Court considered the installation of a listening device in a subject's home for purposes of detecting heroin traffic. The subject was prosecuted with the recordings of detailed discussions between the applicant and his co-accused, demonstrating involvement in conspiracies to import and distribute drugs, including heroin.[140] The defendant absconded during trial, was convicted in absentia, and was sentenced to twelve years imprisonment.[141] When re-arrested several years later, he appealed the original conviction and was rejected.[142]

The Government, however, admitted before the ECHR that Home Office Guidelines for such surveillance were neither legally binding nor publicly accessible. Hence, the ECHR found there had been a violation of Article 8.[143]

In *Wood v. United Kingdom*, the Court considered audio tapes made in a

---

135. Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214, 227 (1980). One is not even required to allege surveillance measures were applied against him. *Id.*

136. Laird v. Tatum, 408 U.S. 1, 14 (1972).

137. Of course, a defendant in a criminal case ordinarily does have standing. *See* Peters v. Kiff, 407 U.S. 493 (1972) (criminal defendant has standing to challenge exclusion of jurors of different race).

138. *Id.* at 14.

139. Elahi v. United Kingdom,_App.No. 30034/04, 2006 WL 1994706. The listening devices had been installed while the police executed a search warrant in connection with a car theft case. *Id.*

140. *Id.* ¶ 8.

141. *Id.* ¶ 10.

142. *Id.* ¶ 11.

143. *Id.* ¶ 20.

police cell while suspects were being held together in hopes that they might reveal criminal activity.[144] No statutes existed either permitting or prohibiting such taping.[145] The applicant was convicted largely through the use of these tapes and sentenced to eight years imprisonment.[146] The court of appeals found there had been a violation of Article 8 of the Convention, but dismissed the appeal because the recording could still be relied upon as evidence.[147] The court reasoned that as long as there was no unfairness or suggestion the confessions were oppressively obtained or otherwise unreliable, they were usable as evidence.[148] Because the Government had conceded there had been no legal basis for the surveillance and that no effective remedy existed under British law,[149] the Court held the Convention was violated.[150] Earlier decisions by the ECHR, including *Khan v. United Kingdom*[151] and *Allan v. United Kingdom*,[152] reached similar results regarding police taping because no statutory system existed to regulate the use of covert recording devices by the police.[153]

In *Miailhe v. France*, the court considered customs officers' seizure of more than 15,000 documents from premises housing governmental head offices and the Philippines consulate.[154] The Court held the wholesale seizures made on the applicants' premises were indiscriminate, to such an extent that several thousand documents seized had no relevance to the inquiries.[155] The Court reasoned that granting customs authorities exclusive competence to assess the expediency, number, length, and scale of inspections in the absence of a judicial warrant did not afford adequate protections against abuse.[156]

---

144. Wood v. United Kingdom, App.No. 23414/02, [2004] Eur. Ct. H.R. 636.

145. *Id.* ¶ 12.

146. *Id.* ¶ 15.

147. *Id.* ¶ 17.

148. *Id.* ¶¶ 20-21. The House of Lords refused to consider the case. *Id.* ¶ 22.

149. *Id.* ¶ 32.

150. *Id.* ¶ 33.

151. Khan v. United Kingdom, App. No. 35394/97, 31 Eur. H.R. Rep. 45 (2001). The police had installed listening devices in the premises of a friend of the applicant. In audio recordings, the applicant admitted that he had been involved in the illegal importation of drugs by his cousin, who had arrived in the U.K. on the same plane as the applicant. *Id.* ¶ 10. The applicant was convicted and sentenced to three years imprisonment. *Id.* ¶ 12. His appeal was dismissed by the House of Lords, even though Lord Nolan, giving the opinion of the majority of the House, stated:

> The sole cause of this case coming to your Lordship's House is the lack of a statutory system regulating the use of surveillance devices by the police. The absence of such a system seems astonishing, even more so in view of the statutory framework which has governed the use of such devices by the Security Service since 1989, and the interception of communications by the police as well as by other agencies since 1985.

Id. ¶ 14.

152. Allan v. United Kingdom, App. No. 48539/99, 36 Eur. H.R. Rep. 12 (2003).

153. *Id.* ¶ 36.

154. Miailhe v. France, App. No. 12661/87, 16 Eur. H.R. Rep. 332, 334 (1993).

155. *Id.* at 343.

156. *Id.*

Ultimately, the initial prosecution was aborted because of subsequent changes in the criminal law.[157] In a similar customs search case, *Funke v. France*,[158] a seizure of documents in a private home was deemed violative of Article 8 because the restrictions and conditions provided for by law "appear[ed] too lax and full of loopholes for the interferences . . . to have been strictly proportionate to the legitimate aim pursued."[159]

The ECHR has considered many cases involving searches and seizures of homes. In *Soini v. Finland*,[160] the Court considered the legality of searching the homes of anti-fur demonstrators who were forcibly removed from a sit-in demonstration at a department store.[161] The demonstrators' homes were searched; eventually, they were charged with criminal violations, including, in several cases, defamation of a department store.[162] After convictions of various offenses and sentences of forty, fifty, or sixty days, many convictions were reversed on appeal and the remaining sentences were reduced to fines.[163] Upon review, the ECHR held that Article 8 had not been violated by the searches of the demonstrators' homes, or by the brief seizure of a diary of one demonstrator.[164] The searches were adequately justified under domestic law and thus regarded as necessary in a democratic society.[165] The seizure, however, of multiple copies of a pamphlet for evidentiary use was held not adequately prescribed by law and hence a violation of Article 10 of the Convention, which pertains to freedom of expression.[166]

---

157. *Id.* at 335.

158. Funke v. France, App. No. 10828/84, 16 Eur. H.R. Rep. 297, 312 (1993).

159. *Id. Accord* Cremieux v. France, App. No. 11471/85, 16 Eur. H.R. Rep 357 (1993) (concerning searches and seizures in homes and office).

160. Soini v. Finland, App. No. 36404/97, 2006 Eur. Ct. H.R.48.

161. *Id.* ¶ 7.

162. *Id.* ¶ 15.

163. *Id.* ¶ 23.

164. *Id.* ¶ 46. The diaries were seized on June 13, 1996; two were returned on June 26, 1996, the other September 9, 1996. *Id.* ¶13.

165. *Id.*

166. *Id.* ¶ 57. The applicants had contended that the police could have simply photocopied the pamphlets and that seizure was unneeded. *Id.* Article 10 provides:

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

European Convention, *supra* note 49, art. 10.

In a more serious case, *Elci v. Turkey*, sixteen Turkish lawyers were arrested, detained for varying periods, and subjected to torture.[167] During their detention, five attorneys' homes and offices were searched and privileged material taken.[168] The Court found no Government records existed limiting the scope of the searches and seizures, and "the search and seizure measures were implemented without any, or any proper, authorization or safeguards."[169] No search warrants had been issued by a prosecutor or judge, and no judicial authority before or after the searches described the scope or purpose of the searches.[170] Thus, the Court held that Article 8 had been violated.[171]

In one rather peculiar case, *Chappell v. United Kingdom*, a private search authorized by an ex parte judicial order was challenged in the ECHR.[172] In order to be granted such an order, the petitioner must have clearly demonstrated to the court that his claim would succeed on the merits. In granting the order, the Court noted "the potential damage is very serious for [the petitioner/defendant], and there is clear evidence that the defendant has in his possession incriminating documents or things, and that there is a real possibility that, if he is forewarned, he may destroy such material."[173] The petitioner was then authorized to search the defendant's premises.[174]

Similarly, in *Chappell* (which originated as a copyright action)[175] the police obtained a search warrant for pornographic video films.[176] The warrant on behalf of the copyright plaintiff and the police warrant were served together, and the plaintiff and several policemen in plain clothes conducted the search.[177] Despite allegations that the simultaneous searches by the police and the plaintiff were distracting, the Court did not find the searches disproportionate to the legitimate aims pursued.[178]

Although the petitioner's claims of invasion of privacy were rejected in *Chappell*, it is important to note that the case was framed as a potential violation of the Convention.[179] Rarely can individuals in the United States successfully claim that purely private action constitutes a constitutional violation.[180]

---

167. Elci v. Turkey, App. Nos. 23145/93 and 25091/94, Eur. Ct. H.R. 588 (2003).

168. *Id.* at 687.

169. *Id.* at 698-99.

170. *Id.* at 697.

171. *Id.* at 700. The Court also concluded that there had been torture of several of the lawyers while in custody and ill-treatment of others that was sufficiently serious as to render it inhuman and degrading within the meaning of Article 3 of the Convention. *Id.* at 646-47.

172. Chappell v. United Kingdom, App.No. 10461/83, 12 Eur. H.R. Rep. 1 (1989).

173. *Id.* at 5.

174. *Id.*

175. *Id.* at 8.

176. *Id.* at 8-9.

177. *Id.* at 10-12.

178. Chappell v. United Kingdom, App. No. 10461/83, 12 Eur. H.R. Rep. 22.

179. *Id.* at 17.

180. The state action requirement often arises as a constitutional impediment to actions

Forcible police entry into a premises, even with a search warrant, has been held to be a violation of the Convention. In *Keegan v. United Kingdom*,[181] the police failed to make inquiries to discover that the target family had moved out over six months previously.[182] Although the police acted without malice, the action was nevertheless an abuse of power. The Court reasoned that the Convention protected against any abuse of power, however it was motivated or caused.[183] Domestic law that conditioned recovery of damages upon such malice[184] was rejected as inadequate.[185]

U.S. law regarding liability contrasts quite sharply with such holdings. A combination of good faith defenses available to police officers,[186] along with the restrictive implications of *Monell v. Department of Social Services*,[187] frequently results in exculpating both individual officers as well as units of local government from liability.[188] Thus, execution of search warrants in the wrong house or apartment unit rarely creates liability unless the police officers demonstrate some improper mental element, such as knowingly or recklessly

---

regarding equality or due process. *See* Shelley v. Kraemer, 334 U.S. 1 (1948); Moose Lodge No. 107 v. Irvis, 407 U.S. 163 (1972); Jackson v. Metro. Edison Co., 419 U.S. 345 (1974).

181. Keegan v. United Kingdom, App. No. 28867/03, Eur. Ct. H.R. (2006).

182. *Id.* ¶ 33.

183. *Id.* ¶ 34.

184. *Id.* ¶ 19. Lord Justice Ward of the Court of Appeals in the United Kingdom stated, while rejecting the appeal:

> "That an Englishman's home is said to be his castle reveals an important public interest, but there is another public interest n the detection of crime and the bringing to justice of those who commit it. These interests are in conflict in a case like this and on the law as it stood when these events occurred, which is before the coming into force of the Human Rights Act of 1998, which may be said to have elevated the right to respect for one's home, a finding of malice on the part of the police is the proper balancing safeguard."

Id.

185. *Id.* ¶ 34.

186. Hope v. Pelzer, 536 U.S. 730, 736 (2002). Government officials performing discretionary functions are entitled to qualified immunity so long as "their actions could reasonably have been thought consistent with the rights they are alleged to have violated." Anderson v. Creighton, 483 U.S. 635, 638 (1987). "Qualified immunity protects all but the plainly incompetent or those who knowingly violate the law." Malley v. Briggs, 475 U.S. 335, 344-45 (1986). *See generally* Harlow v. Fitzgerald, 457 U.S. 800 (1982) (objective reasonableness of official's conduct by reference to clearly established law provides immunity); Wilson v. Layne, 526 U.S. 603 (1999) (Qualified immunity allowed police to bring media observers into defendant's home while executing arrest warrant, for although it was unconstitutional to do so, that rule had not been clearly established at the time of the entry into the house).

187. Monell v. Dept. of Soc. Servs. of the City of N.Y., 436 U.S. 658 (1978). *Monell* exonerates a unit of local government from liability unless a policy or custom of the local government unit was implicated in the violation of inhabitants' constitutional rights. *Id.* at 694-95. Improper action by a law enforcement official alone is insufficient to create municipal liability. *Id.*

188. "The offending official, so long as he conducts himself in good faith, may go about his business secure in the knowledge that a qualified immunity will protect him from personal liability for damages that are more appropriately chargeable to the populace as a whole." Owen v. City of Independence, 445 U.S. 622, 657 (1980) (quoting *Monell* , 436 U.S. at 694).

employing false statements to obtain the warrant.[189] Mere mistake is insufficient if the "officer's conduct was consistent with a reasonable effort to ascertain and identify the place intended to be searched."[190] A mistaken search of a house on a different street and of a different color from the one to be searched, however, might not be "objectively reasonable."[191]

Damage claims against federal officers ordinarily founder on similar impediments when suits are brought under the Federal Torts Claims Act.[192] In theory, *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*[193] permits recovery from Federal agents for violations of certain constitutional rights, such as the Fourth Amendment prohibition of unreasonable search and seizure. Such actions, however, are unavailable in a number of situations.[194] For example, pat-down searches are entitled to qualified immunity, but strip searches, done willfully and wantonly, are not so protected.[195] Moreover, the evidence obtained by improper searches may still be used in criminal prosecutions.[196]

---

189. Hill v. McIntyre, 884 F.2d 271, 273-74 (6th Cir. 1989). A seventeen-year-old girl was handcuffed and forced to stand wearing only a sheer nightshirt until, after some delay, a female officer provided more clothing. Dry goods and food were spilled onto the floor and the front door was broken open. Approximately $3000 in damages was claimed. *Id.*

190. Maryland v. Garrison, 480 U.S. 79, 88-89 (1987).

191. Dawkins v. Graham, 50 F.3d 532, 535 (8th Cir. 1995). *Compare* Pray v. City of Sandusky, 49 F.3d 1154 (6th Cir 1995) (officers' entry of wrong downstairs door in duplex unit reasonable under circumstances since raid was at night on the premises of a suspected drug dealer), *with* Richardson v. Oldham, 12 F.3d 1373 (5th Cir. 1994) (objectively reasonable to execute search warrant against either of two houses which fit search warrant description since it was not demonstrated that officer knew two houses fit description).

192. Qualified immunity is an affirmative defense. Harlow, v. Fitzgerald, 457 U.S. 800, 815; Gomez v. Toledo, 446 U.S. 635, 640 (1980). There is also immunity for discretionary acts under the Federal Tort Claims Act. *See* Berkovitz v. United States, 486 U.S. 531, 539 (1988).

193. Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (warrantless entry into an apartment).

194. Carlson v. Green, 446 U.S. 14, 18-19 (1980). When Congress provides an alternative remedy viewed as equally effective or when, even absent legislative remedial action, there are "special factors counseling hesitation." *Id.* at 18. The Supreme Court has refused to imply a cause of action under the Fifth Amendment for military personnel who were the victims of alleged racial discrimination by superior officers. *See* Chappel v. Wallace, 462 U.S. 296 (1983); Soldiers were severely injured when deceptively subjected to LSD experimentation by the Army. United States v. Stanley, 483 U.S. 669 (1987). Disability recipients whose procedural due process rights were violated in benefit termination decision. Schweiker v. Chilickey, 487 U.S. 412 (1988). All situations in which an alternative remedy was completely unavailable or significantly limited. PETER L. STRAUSS ET AL., GELLHORN AND BYSE'S ADMINISTRATIVE LAW CASES AND COMMENTS 1268-69 (10th ed. 2003).

195. Anderson v. Cornejo, 284 F.Supp. 2d 1008, 1031-36 (N.D. Ill. 2003), *rev'd* in part, *vacated* in part and *remanded,* 355 F.3d 1021 (2004).

196. Hudson v. Michigan, 126 S.Ct. 2159, 2185 (2006) (evidence usable when there is forcible entry into premises in violation of knock-and-announce rules).

REMEDIES FOR VIOLATIONS OF FUNDAMENTAL RIGHTS

Remedies provided by the ECHR for privacy violations range from a statement that there was a violation (the finding being just satisfaction), the ordering of financial compensation for pecuniary or non-pecuniary damage, or the ordering of payment for substantial costs and expenses for litigation.

Just Satisfaction from the Finding of Violation

The finding of a violation of Article 8 in a case involving customs officers invading head offices and homes, and seizing documents with no relationship to the investigation, was held to be adequate just satisfaction.[197] It should be noted that the Court so held even though it believed non-pecuniary damage had been suffered.[198]

The Court reached a similar "just satisfaction finding" decision in a case in which no domestic remedies existed with which to raise an arguable Article 8 issue.[199] Curiously, the Court found no direct violation of Article 8 but nevertheless reached the decision after extensive consideration of arguments about the alleged violation.[200] Notably, the petitioner had only requested a symbolic sum of 100 Swiss francs.[201]

Such a "just satisfaction finding" was also issued in the far more serious home invasion case of *Chalkley v. United Kingdom*.[202] The police in *Chalkley* arrested the petitioner and his partner and removed them and their children, taking them to the police station in order to plant a listening device in their home.[203] The police reentered the premises several months later to renew the battery.[204] The petitioner was charged with conspiracy to commit robbery and burglary. The Court allowed the tape-recorded evidence to be used at trial; eventually, the petitioner and his co-defendant entered guilty pleas and received ten year imprisonment sentences.[205]

In another example of surreptitious installation, police officers installed a

---

197. Cremieux v. France, App. No. 11471/85, 16 Eur. H.R. Rep. 357, 366 (1993).

198. *Id.* at 368.

199. Camenzind v. Switzerland, App. No. 21353/93, 28 Eur. H.R. Rep. 458 (1998).

200. *Id.* at 467. The search was for an allegedly illegal cordless telephone. *Id.* at 461. The target of the search admitted that he had used such a telephone, but stated it was no longer in his possession. *Id.*

201. *Id.* at 471. Costs of 8000 Swiss francs were awarded, less legal aid already paid. *Id.* at 471.

202. Chalkley v. United Kingdom, App. No. 63831/00, 37 Eur. H.R. Rep. 30 (2003).

203. *Id.* at 681. The arrest regarded a separate credit card offense whose investigation had lapsed, but was revived to give a pretext for the removal. *Id.* at 682. The police had a copy of the house key cut to enable them to reenter the house later. *Id.* No prosecution ensued on the credit card matter. *Id.*

204. *Id.*

205. *Id.* at 683. After serving approximately five years, the applicant was released on license. *Id.* Costs of 4800 Euros were awarded. *Id.* at 686.

listening device in the apartment of a friend of the defendant. The Court found that action constituted a violation of Article 8. The finding of a violation was held to be just satisfaction, despite the fact that the defendant had received a sentence of three years imprisonment.[206] Costs of 11,500 British pounds were awarded.[207] In most cases of this type, the petitioner had already been released from confinement, in part because of the length of time it took to take their cases up through the domestic legal system and then over to the ECHR in Strasbourg.[208]

The Court has considered the possibility that an objection to confinement itself might be addressed; in at least one case the Court required direct causation between the material obtained in violation of Article 8 and the conviction.[209]

In particular, the ECHR has held the admissibility of an illegal recording of a telephone call does not necessarily vitiate a Swiss criminal conviction for hiring an assassin to kill one's wife.[210] In that case, the tape-recorded telephone call was played in court before two lay judges and six jurors.[211] The defendant was found guilty of attempted incitement to murder and sentenced to ten years imprisonment.[212] Because the defendant had failed to exhaust available domestic remedies regarding the tape recording, the Court could not consider an Article 8 challenge.[213] Accordingly, the Court considered the use of the recording under Article 6 of the Convention, which provides for a fair trial.[214] The Court found there was sufficient evidence other than the tape recording to sustain the conviction, including the testimony of the "strong arm" man hired to

---

206. Khan v. United Kingdom, App. No. 35394/97, 31 Eur. H.R. Rep. 45, 1019 (2000). The applicant had been released on license after serving a part of his sentence on August 11, 1994. *Id.*

207. *Id.*; *see also* Wood v. United Kingdom, App. No. 23414/02,2006 WL 1994706 (costs above that already supplied by legal aid of 550 euros awarded); Elahi v. United Kingdom, App. No. 30034/04, 2006 WL 1994706 (costs of 6000 euros awarded. It may be that this petitioner was still in custody at the time of the ECHR decision. The sentence pronounced in 1999 was a twelve year sentence, but the defendant had absconded and was rearrested years later); Taylor-Sabori v. United Kingdom, App. No.47114/99, 36 Eur H.R. Rep. 17 (2002) (costs of 4800 euros awarded); Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur.H.R.Rep. 483, 508 (1998).

208. This is the author's impression from review of many European Court of Human Rights cases involving domestic criminal convictions and violations of Article 8. One contributing factor, to be sure, is the relatively shorter sentences awarded by European Courts by comparison to American sentences. Such shorter sentences when combined with the length of time necessary to bring and litigate a case before the ECHR likely explains the situation. See *infra* note 212.

209. Schenk v. Switzerland, App. No. 10862/84, 13 Eur. H.R. Rep. 242, ¶ 48 (1988)

210. *Id.*

211. *Id.* at 247.

212. *Id.* at 248. He actually served approximately two years, for he was given a partial pardon because of health reasons. *Id.* at 261. The decision was rendered about 3.5 years after his release. *Id.* at 246, 261.

213. *Id.* at 263.

214. *Id.*

kill the wife.[215]

In a case involving bankruptcy, a lawyer was permitted to inspect the petitioner's mail in a manner not in accordance with law.[216] The Court rejected a claim for non-pecuniary damage, stating the finding of a violation was itself sufficient.[217] Additionally, in a similar case, the search of a lawyer's office pursuant to a search warrant was deemed unlawful and unjustified, and such finding was deemed just satisfaction.[218]

Pecuniary and Non-pecuniary Damage Awards

The ECHR has, in many other cases, awarded damages to petitioners who allege violations of their rights to privacy under Article 8 of the Convention: either as non-pecuniary damages, emotional distress, or pecuniary damage. For example, a case involving a person taped on another's tapped phone resulted in an award of 10,000 francs.[219] In addition, an award of 11,800 euros was granted for non-pecuniary emotional damages in a case involving the closed circuit television taping and subsequent broadcast of an individual brandishing a knife on a public street.[220]

In a case involving covert surveillance of a police holding cell, the Court awarded 1,642 euros in non-pecuniary damages for violation of the petitioner's right to respect for private life and because of the lack of an effective remedy under domestic law.[221] The petitioner was convicted of murder and given a life sentence because of the taped evidence.[222]

Another case, involving customs officers violating Article 8 by searches and seizures in a home, resulted in an award of 50,000 francs for non-pecuniary

---

215. *Id.* at 266. The Court briefly stated it could not directly reach the Article 8 issue, but in dicta it indicated it would have reached a similar result under Article 8. *Id.* at 268. *See also* Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur. H.R. Rep. 483, 508 (1998) (costs of 1,5000,000 pesetas were awarded); Elahi v. United Kingdom, App. No. 30034/04, 2006 WL 1994706 (costs of 6000 euros awarded).

216. Narinen v. Finland, App. No. 45027/98, 4 Eur. H.R. Rep. 241, ¶ 37 (2004).

217. *Id.* ¶¶ 46, 49. App. No. 45027/98, 4 Eur. H.R. Rep. 241, 257 (2004) (costs and expenses of 5043 euros were awarded).

218. Niemietz v. Germany, App. No. 13710/88, 16 Eur. H.R. Rep. 97, 103 (1993). *Accord* Kruslin v. France, App .No. 11801/85, 12 Eur. Comm'n H.R. Dec. & Rep. 451, 454 (1990).

219. Lambert v. France, App. No. 23618/94, Eur. H.R. Rep. 346, 348, 355 (1998) (costs of 15,000 francs were also awarded).

220. Peck v. United Kingdom, App. No. 44647/98, 36 Eur. H.R. Rep. 41,753 (2003) (costs of 18,075 euros were also awarded).

221. Allan v. United Kingdom, App. No. 48539/99, 36 Eur. H.R. Rep..12 (2003). Costs of 12,800 euros were also awarded. *Id.* at 161. The Court had also found a violation of an Article 6 right, the right to a fair trial, partly through the police placing an informant in the jail cell with the defendant, gaining information in defiance of the will of the defendant, and thereby impinging upon the defendant's right to silence and privilege against self-incrimination. *Id.* at 159. The applicant's request for violation of his right to privacy was for a "reasonable sum." *Id.* at 160.

222. *Id.* at 148. The murder conviction was obtained on a ten to two jury vote. *Id.*

damages.[223] In a forcible entry case, where the police broke down the door of a private home with a battering ram, the Court awarded 3,000 euros each to the husband, wife, and fourteen year old child, and 2,000 Euros each to the parties' young children even though the suspect had moved more than seven months prior to entry, .[224] The Court noted the "violent and shocking nature of the police entry of the applicants' home" as well as the undoubted distress caused and medical reports indicating they would benefit from therapeutic intervention.[225] Similarly, in another case the improper publication of private telephone conversations of the former prime minister of Italy, Benedetto Craxi, resulted in an award of 2,000 euros to each member of the prime minister's family in non-pecuniary damages.[226]

In *Michta v. Poland*, the improper opening of prison correspondence resulted in an award of 1,500 euros in non-pecuniary damages.[227] Further, in a case involving interception of private telephone calls of an applicant who was at the time an Assistant Chief Constable, the Court awarded 10,000 British pounds in non-pecuniary damages.[228] The Court noted the interception of calls was conducted for the primary purpose of collecting material to be used against the applicant in sex discrimination proceedings that she herself had initiated.[229] This was considered a serious infringement of her rights.[230]

In a sequence of cases from Turkey, the ECHR consistently held Article 8 was violated, along with other Articles of the European Convention, when security forces destroyed the houses of various people. Deliberate destruction of houses and property constituted grave and unjustified interference with the rights to private and family life.[231] For example, pecuniary damages of 25,000 euros and non-pecuniary damages of 14,500 euros were awarded in a case involving the burning of a house.[232] In a similar case, each of five applicants were awarded over 8,000 euros in pecuniary damages for the physical damage to their houses and outbuilding, 6,000 euros for other property, 6,000 euros for lost income, 6,000 euros for rent for alternative housing, and 14,500 euros in

223. Funke v. France, App. No. 10828/84, 16 Eur. H.R. Rep. 297, 313 (2003). The amount requested was 300,000 francs. Costs of 70,000 francs were also awarded. *Id.* at 312. One factor used in reaching the conclusion that Article 8 was violated was the fact that the prosecution was not related to the original reason cited for the search. One might surmise that the unregulated discretion of the customs officers to conduct a search was viewed as particularly suspect, since the search failed to turn up the anticipated evidence of criminal conduct.

224. Keegan v. United Kingdom, App. No. 28867/03. Costs and expenses of 9500 euros were also awarded. *Id.* ¶ 53.

225. *Id.* ¶ 48.

226. Craxi v. Italy, App. No. 25337/94, 38 Eur. H.R. Rep. 47, 1025 (2004). No costs were requested. *Id.*

227. Michta v. Poland, App. No. 13425/02 Eur .Ct. H.R. 537 (2006),

228. Halford v. United Kingdom, 24 Eur. H.R. Rep. 523, 550 (1997).

229. *Id.*

230. *Id.* 600 British pounds were awarded for pecuniary damages and 25,000 British pounds for costs. *Id.* at 552.

231. Yoyler v. Turkey, App. No. 26973/95 Eur. Ct. H.R. 398 (2003).

232. *Id.*

non-pecuniary damages.[233]

Conversely, in a Turkish case authorities had detained sixteen Turkish lawyers, five of whom had their houses and offices searched during the detention. The lawyers were awarded various sums, ranging from 1,510 to 1,660 euros each in pecuniary damages and from 12,000 to 25,500 euros each in non-pecuniary damages.[234] However, none of the lawyers made a specific claim for just satisfaction in relationship to violations of Article 8 of the Convention.[235] The higher non-pecuniary damage awards relate to torture, ill-treatment, and unlawful detention by the authorities, with the awards increasing as the length of detention increased.[236]

Conclusion Regarding Remedies

In a high proportion of cases involving invasion of privacy, when the basis for state intervention was suspected criminality, the finding of violation as "just satisfaction" is often the major remedy provided.[237] Court costs, including attorneys' fees, are rdinarily awarded as well.[238] In none of these reviewed

233. Ayder v. Turkey, App. No. 23656/94, Eur. Ct. H.R. 3 (2004), *available at* http://worldlii.org/eu/cases/ECHR/2004/3.html. Costs of 40,000 euros were also awarded less 725 euros in legal aid already paid. *Id.*; *accord* Ozkan v. Turkey, App. No. 21689/93 Eur. Ct. H.R. (2004), *available at* http://worldlii.org/eu/cases/ECHR/2004/133.html (non-pecuniary damages of 1500 euros to 49,800 euros awarded to thirty-two different families); Akdivar v. Turkey, App. No. 21893/93, 23 Eur.H.R.Rep. 143, 194 (1997); Mentes v. Turkey, App. No. 23186/94, 26 Eur. H.R. Rep. 9 (1998); Selguk v. Turkey, App. Nos. 23184/94 and 23185/94, 26 Eur. H.R. Rep. 447 (1998) (awards given of 1,000,000,000 dinars to two applicants for destroyed buildings, 4,000,000,000 dinars in pecuniary damages, and 10,000 in British pounds for non-pecuniary damages); Bilgin v. Turkey, App. No. 23819/94, 36 Eur. H.R. Rep. 50 (2003) (pecuniary damages of 12,000 British pounds and non-pecuniary damages of 10,000 British pounds awarded for burning of house and property).

234. Elci v. Turkey, App.No. 23145/93; 25091/94 Eur. Ct. H.R. (2003), *available at* http://worldlii.org/eu/cases/ECHR/2003/588.html.

235. *Id.* However, only three of the remaining lawyers were awarded non-pecuniary damages above those of any of the five lawyers whose Article 8 rights were violated, respectively one award of 14,400 euros, and two of 36,000 euros. It appears these awards are largely proportional to the time of unlawful detention. Also, the awards of pecuniary damages appear to relate to lost earnings for the period of detention. *Id.*

236. *Id.*

237. *See* Wood v. United Kingdom, App. No. 23414/02, 636 Eur. Ct. H.R. (2004); Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur.H.R.Rep. 483, 508 (1998); Kruslin v. France, App. No. 11801/85, 12 Eur. Comm'n H.R. Dec. & Rep. 547, 455-59 (1990); Taylor-Sabori v. United Kingdom, App. No. 47114/99, 36 Eur.H.R. Rep. 17, ¶¶ 16-19 (2003); Niemietz v. Germany, App. No. 13710/88, 16 Eur. H.R. Rep. 97, 103 (1993); Narinen v. Finland, App. No. 45027/98, 4 Eur. H.R. Rep. 241, ¶ 37 (2004); Elahi v. United Kingdom, App.No. 30034/04, 2006 WL 1994706; Kopp v. Switzerland, App. No. 23223/94, 27 Eur.H.R.Rep. 91(1999).

238. *See* Soini v. Finland, App. No. 36404/97, 2006 Eur. Ct. H.R.48 (each applicant awarded 1,000 euro, as well as 425.9 euro for costs and expenses); *Contreras*, App. No. 27671/95, 28 Eur.H.R.Rep. at 508 (no award for pecuniary damage, but 1,500,000 pesetas for expenses and lawyers' fees awarded); MM v. Netherlands, App. No. 39339/98, 39 Eur. H.R.

cases did courts order criminal convictions overturned because of improper privacy invasions.

In cases where criminal activity was not the basis for surveillance, modest damage awards (by American standards) of both a pecuniary and non-pecuniary nature were ordinarily awarded. In some cases involving criminal conduct, such damage awards also occurred. Since damage awards are ordinarily paid by the states in the Council of Europe, one may assume that these awards were paid as well, providing some tangible recognition of the violation plus the intangible value of a finding that the government violated the fundamental right to privacy.

When serious property destruction accompanies the privacy invasion, the ECHR is quite willing to order far more substantial pecuniary damage awards, such as in numerous cases from Turkey involving the destruction of homes and property.[239] Noticeably absent, however, from ECHR damage awards is any rule indicating that where no actual damages are awarded, costs (legal fees and expenses) may not be awarded. The two types of awards, damages and costs, appear to remain disconnected in the ECHR.

Significantly, the ECHR is on course to carve out a system of human rights protection for over 800 million people from the more than forty-five states currently forming the Council of Europe.[240] Thus, any decision that solidifies a rule of law either curtailing or defining the power of government or liberties of fellow citizens has significant value. To award legal costs encourages people to bring such cases and courts to define such rights. Therefore, such cases have significant societal value.

Additionally, conspicuously missing from the privacy decisions of the ECHR are orders of injunctive relief. No case or statute requires a state to conform its legislative and administrative statutes and regulations to the ECHR commands. Except for awards of damages and costs, there is no direct confrontation with the sovereign nature of states. But, many cases do mention that legislative changes have occurred, often subsequent to the operative facts of the case at bar.[241]

Rep. 19 (2004) (10,000 euros awarded for costs and expenses); *Kruslin*, App. No. 11801/85, 12 Eur. Comm'n H.R. Dec. & Rep. at 455 (20,000 francs for costs and expenses); Halford v. United Kingdom, App. No. 20605/92, 24 Eur.H.R.Rep. 523 (1997) (25,000 pounds awarded for costs and expenses); Keegan v. United Kingdom, App. No. 28867/03, Eur. Ct. H.R. (2006) (9,500 euros for costs and expenses); Narinen v. Finland, App. No. 45027/98, 4 Eur. H.R. Rep. 241, ¶ 37 (2004) (6843 euros for costs and expenses); *Elahi*, App.No. 30034/04, 2006 WL 1994706 (6000 euro for costs and expenses); Allan v. United Kingdom, App. No. 48539/99, 36 Eur. H.R. Rep. 12 (2003) (12,800 euros for costs and expenses); Peck v. United Kingdom, App. No. 44647/98, 36 Eur. H.R. Rep. 41 (2003) (18,075 euros for costs and expenses); Khan v. United Kingdom, App. No. 35394/97, 31 Eur. H.R. Rep. 45 (2001) (11,500 pounds for costs and expenses); *Kopp*, App. No. 23223/94, 27 Eur.H.R.Rep. at 91 (15,000 francs for costs and expenses).

239. *See, e.g.*, Selguk v. Turkey, App. Nos. 23184/94 and 23185/94, 26 Eur. H.R. Rep. 447 (1998).

240. *See supra* note 32.

241. *See, e.g.*, Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214, 231 (1980).

Clearly, the decisions of the ECHR have encouraged states to change their domestic law in order to avoid future legal problems. The United Kingdom's adoption of the Human Rights Act of 1998, which made the European Convention on Human Rights domestically applicable within the country, is one example.[242] By not ordering statutory changes, the ECHR avoids the type of conflict with sovereign power exemplified by United States Supreme Court decisions, such as *Martin v. Hunter's Lessee*.[243] Accordingly, one may credit the ECHR with adopting a wise policy to minimize conflicts with states.

By awarding costs even when a prisoner's confinement resulted from evidence of criminality gained from an invasion of privacy, the ECHR sets a standard for the states of the Council of Europe to aspire. When the evidence of criminality relates to some other offense other than the original reason for surveillance, significant non-pecuniary damages have been awarded.[244] According to the ECHR, invasions of privacy must be narrowly and strictly authorized for appropriate and proportionate reasons.[245] Thus, broad administrative or police discretion is antithetical to the legal order the ECHR finds embodied in the European Convention on Human Rights.

Moreover, in contrast to the general practice in the United States in which an improper search generates (at best) the preclusion of the use of the evidence or its fruits in a criminal case, the ECHR may award non-pecuniary damages. Likewise, the ECHR approach rejects the U.S. approach, which ordinarily rejects the award of attorneys' fees unless something beyond nominal damages are awarded.[246] The U.S. approach permits an award of nominal damages in cases involving the deprivation of constitutional rights unless actual injury can be demonstrated.[247] In cases involving improper searches the United States Supreme Court suppresses the improperly gathered evidence, but does not apply any other remedy.[248]

---

242. Human Rights Act 1998, ch. 42 (Eng.).

243. 14 U.S. 304 (1816) (conflict between the Virginia Court of Appeals decisions and decisions by the United States Supreme Court). *See also* Roe v. Wade, 410 U.S. 113 (1973) (effectively invalidating all state abortion legislation); Furman v. Georgia, 408 U.S. 238 (1972) (effectively invalidating all existent state capital punishment legislation).

244. *See, e.g.*, Funke v. France, App. No. 10828/84, 16 Eur. H.R. Rep. 297, 312 (1993) (seizures related to alleged financial dealings gave rise to parallel proceedings for disclosure of documents resulted in 50,000 francs for non-pecuniary damage plus 70,000 francs for costs and expenses);

245. *See, e.g. Funke*, App. No. 10828/84, 16 Eur. H.R. Rep. at ¶ 57 ("strictly proportionate to the legitimate aim pursued"); Kopp v. Switzerland, App. No. 23223/94, 27 Eur.H.R.Rep. 91, ¶ 72 (1999) ("law must be particularly precise"); Huvig v. France, 12 Eur. H.R. Rep. 528, ¶ 34 (1990) (law must "afford adequate safeguards against various possible abuses").

246. Farar v. Hobby, 506 U.S. 103, 111-12 (1992) (actual relief, either monetary damages or a judgment or order affecting the "behavior of the defendant towards the plaintiff"). *Id.* at 110.

247. Carey v. Piphus, 435 U.S. 247 (1978).

248. Hudson v. Michigan, 126 S. Ct. 2159, 2165 (2006) (violation of knock and announce

Similarly, in a decision involving statutory interpretation, the Supreme Court required proof of actual damages from a privacy violation under the Privacy Act[249] before the plaintiff could recover the statutory minimum damages of $1,000.[250] Privacy concerns, however, are inherently intangible. How does one value the solitude of seclusion in the midst of a Redwood forest, or the value of some degree of seclusion in the midst of a busy, urban neighborhood or building?

THE EU PRIVACY DIRECTIVE: CONTRAST WITH U.S. PRIVACY LAW

In addition to the effects the European Convention on Human Rights has on privacy, an entirely separate but interrelated regime exists in Europe regarding privacy law: the regime regulated by the European Privacy Directive of the European Parliament and the Council of Europe of October 24, 1995.[251] That directive requires the member states of the European Union[252] to develop domestic laws regarding privacy under the Directive's guidance.[253] Such domestic law must include very specific elements and mandate personal information be:

> Processed fairly and lawfully;
> Collected for specified and legitimate purposes only;
> Accurate and up-to-date;
> Steps must be taken to rectify or erase incorrect data;
> Nontransferable to third parties without permission;
> Nontransferable to countries which lack adequate privacy protection;
> Protected by a corporate data controller (equivalent to the U.S. chief privacy officer responsible for ensuring that data practices are followed;
> Processed only in cases where the subject has given clear consent.[254]

At first glance, the sharpest difference between European and American privacy law is the adoption of an "opt in" versus "opt out" system of approving

---

rule no justification for application of exclusionary rule for evidence).

249. 5 U.S.C. § 552A(g)(4)(A)(2004).

250. Doe v. Chao, 540 U.S. 614, 621 (2004) (citing the general tort rule that actual damage is required for recovery). *Accord* Memphis Cmty Sch. Dist. v. Stachura, 477 U.S. 299 (1986) (damage based upon abstract value or importance of constitutional rights held not a permissible element of compensatory damages in cases under 42 U.S.C. § 1983).

251. Council & Parliament Directive 95/46, 1995 O.J. (L281) (EC).

252. All member states of the EU are also members of the Council of Europe, but more than a dozen members of the Council of Europe are not members of the EU, including, for example, Russia, Switzerland, and Turkey. *See supra* note 32.

253. Council & Parliament Directive 95/46, art. 32, 1995 O.J. (L281) (EC).

254. Council Directive, Daintry Duffy EU Data Privacy_Directive, CSO, Aug. 2003, http://csoonline.com/read/080103/privacy-sidebarr_1607.html.

the release and use of personal data. In the European system, each data subject (i.e. person) must give clear, explicit permission for the data to be collected, used, and/or transferred.[255] American law has generally adopted an opt out approach, in which a data subject must affirmatively inform a business entity that he or she does not want the data shared.[256]

Exceptions to the EU requirement of explicit permission do exist: if the collection of data is necessary for performing a contract with the data subject; is for compliance with a legal obligation; is necessary for protecting the vital interests of the data subject; is necessary for the performance of a task carried out in the public interest; or is necessary for legitimate purposes pursued by the controller or by a third party to whom data is disclosed, except where such interests are overridden by the interest for fundamental rights and freedoms of the data subject with protection under Article I of the Privacy Directive.[257]

The first major dispute between the U.S. and the EU pertained to the Privacy Directive and the related effort to develop a safe harbor solution to permit U.S. business enterprises to continue to operate in Europe.[258] Case law and national legislation concerning this Directive is far less developed than that of the ECHR regarding privacy rights embodied in the European Convention on Human Rights. Nevertheless, the ECJ has decided several interesting privacy cases.[259]

The Directive is not limited to commercial activity. For example, the Directive applied to church parishioners putting personal information on a web page, despite the non-commercial nature of this act.[260] The web page posting sometimes included full names, sometimes first names, and described the jobs

255. Council & Parliament Directive 95/46, art. 7(a), 1995 O.J. (L281) (EC).

256. Gramm-Leach-Bliley Act, 26 U.S.C. § 6103 (1975), *amended by* Pub. L. No. 108-173, 117 Stat. 2066 (2003).

257. Council Directive 95/46, art. 7(b)-(f) 1995 O.J. (L 281) 31 (EC).

258. Alexander Zinser, *The Safe Harbor Solution: Is It an Effective Mechanism for International Data Transfers Between the United States and the European Union?*, 1 OKLA. J.L. & TECH. 11 (2004). "[W]ith regard to data transfers from the European Union to the United States, data controllers in the United States are required to ensure an adequate level of protection in order to be in compliance with European data protection laws. However, the fulfillment of the requirement of adequacy is problematic." *Id.*; Kyle T. Sammin, Note, *Any Port in a Storm: The Safe Harbor, The Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*, 36 GEO. WASH. INT'L L. REV. 653 (2004). *See also*, Gregory Shaffer, *Globaliztion and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000).

259. *See* Case C-101/01, Lindqvist, [2003] E.C.R. I-12971; Case C-68/93, Shevill v. Presse Alliance SA, [1995] E.C.R. I-415; Case 53/84, Adams v. Comm'n, [1985] E.C.R. 3595.

260. Case C-101/01, Lindqvist, [2003] E.C.R. I-12971. "[P]rocessing of personal data such as that described . . . is not covered by the exceptions in Art. 3(2) of Directive 95/46." A fine of SEK 4000 plus SEK 300 to be paid to a Swedish fund to assist victims of crimes was assessed by the Swedish trial court. *Id.* On Jan. 29, 2007, one U.S. dollar was equal to SEK 6.9767. Currency Converter, http://finance.yahoo.com/currency/convert?amt=1&from=USD&to=SEK&submit=Convert.

held and hobbies of eighteen colleagues in the parish.[261]

The EU differs from the Council of Europe, however, because its primary focus is on economic matters rather than issues of human rights.[262] Still, personal rights litigation does sometimes implicate economic concerns, such as privacy rights protected through defamation lawsuits.

The ECJ considered the matter of jurisdiction for suits in defamation in *Shevill v. Presse Alliance SA*.[263] The Court held that the target of a defamatory publication could bring legal action in either the state in which the publisher was established or before the courts of each contracting state in which the publication was distributed.[264] If suit was brought in a contracting state of distribution, the damages recoverable were limited to the harm caused in that contracting state.[265] If the action was brought either in the state of the defendant's domicile or where the publisher was established, however, suit could be brought for all harm caused.[266] Thus, in effect the broadest scope was permitted within the contracting states of the EU for lawsuits protecting aspects of privacy through defamation suits.

In a more unusual privacy case, a whistleblower employee of a Swiss company violating EU antitrust law had his name disclosed by the employees of the EU Commission. As a result, when he subsequently went to Switzerland, he was arrested and criminally prosecuted for making the disclosures.[267] The whistleblower sued the Commission for damages as well as for an order requiring Switzerland to correctly interpret and respect international law.[268]

The subject of searches has been frequently considered by the ECJ in reported cases. The Court has repeatedly affirmed that the EU Regulations must be interpreted in ways consistent with the fundamental rights protected by the European Convention on Human Rights.[269] The Court has distinguished

---

261. *Id.* ¶ 13. In many cases family circumstances, telephone numbers, and other matters were mentioned. The defendant also stated that one colleague had injured her foot and was on half-time on medical grounds. *Id.*

262. *See* MATS LINDFELT, FUNDAMENTAL RIGHTS IN THE EUROPEAN UNION – TOWARDS HIGHER LAW OF THE LAND? 1-4, ABO Akademi University Press (2007)(discusses the limited incorporation of fundamental rights in EU jurisprudence).

263. Case C-68/93, Shevill v. Presse Alliance SA, [1995] E.C.R. I-415.

264. *Id.* ¶ 33.

265. *Id.* ¶ 30.

266. *Id.* ¶¶ 25, 32.

267. Case 53/84, Adams v. Comm'n, [1985] E.C.R. 3595. The Commission was ordered to pay half the damage suffered by Mr. Adams as a result of identifying him as the source of the information. He was held in solitary confinement in Swiss prison and convicted under Swiss law for economic espionage. While he was in prison, Mr. Adams' wife was interrogated by Swiss police officers and then she committed suicide. *See* RALPH H. FOLSOM, PRINCIPLES OF EUROPEAN UNION LAW 94 (2005); Kurt Riechenberg, *The Merger of Trading Blocks and the Creation of the European Economic Area: Legal and Judicial Issues*, 4 TUL. J. INT'L & COMP. L. 63, 75-76 (1995).

268. Case 53/84, Adams v. Comm'n, [1985] E.C.R. 3595.

269. *See* Case 85/87, Dow Benelux NV v. Comm'n, [1989] E.C.R. 3137; Case 97/87, Dow Chems. Iberica v. Comm'n, [1989] E.C.R. 3165; Case 4/73, Nold v. Comm'n, [1977] E.C.R. 7;

between the protections of the home and protections of business premises, for which "not inconsiderable divergences between the legal systems of the Member States in regard to the nature and degree of protection afforded to business premises against intervention by the public authorities."[270] In all legal systems of the member states, however, any intervention must have a legal basis. Consequently, those varied systems provide protection against arbitrary or disproportionate intervention.[271]

The broad search powers granted to the Commission include authorization to: examine books and other business records; take copies of or extracts from the books and business records; ask for oral explanations on the spot; and enter any premises, land, and means of transport of undertakings.[272] In order to conduct such examinations, prior authorization is required. With the authorization and required cooperation of the national authorities (who have a very limited ability to question the legitimacy of the search),[273] the investigation is authorized to go forward; however, they

> may not obtain access to premises or furniture by force or oblige the staff of the undertaking to give them such access, or carry out searches without the permission of the management of the undertaking, which may, however, be implied, in particular by the provision of assistance to the Commission's officials.[274]

If the undertaking expresses opposition to the investigation, however, the Commission may search for any information with the "assistance of the national authorities, which are required to afford them assistance necessary for the performance of their duties."[275] Each state has an obligation to ensure that the

---

Case 222/84, Johnston v. Chief Constable, [1986] E.C.R. 1651; Case 46/87, Hoest v. Comm'n, [1989] E.C.R. 2589.

270. Dow Benelux NV, [1989] E.C.R. at ¶ 28.

271. *Id.* The Court also noted that it has the power to determine whether measures taken by the Commission under the European Coal and Steal Community Treaty are excessive. *Id.* (citing Case 5/62, Societa Industriale Acciaiene San Michele v. Eur. Coal and Steel Cmty., [1962] E.C.R. 449).

272. *Id.* ¶ 32 (citing Treaty Establishing European Coal & Steel Community, art. 14(1), Apr. 18, 1951, 261 U.N.T.S. 140).

273. *Id.* ¶ 6.

> [The] national body, after satisfying that the decision ordering the investigation is authentic, [are] to consider whether the measures of constraint envisaged are arbitrary or excessive having regard to the subject-matter of the investigation and to ensure that the rules of national law are complied with in the application of those measures.

Id. ¶ 7. *See also* Case C-94/00, Freres v. Consommeation et de la Repression des Fraudes, [2002] E.C.R. I-9011. (Community law precluded review by the national court of the justification of measures beyond that required by the principal that coercive measures were not arbitrary or disproportionate to the subject matter of the investigation).

274. *Freres*, [2002] E.C.R. I-9011.

275. *Id.*

Commission's action is effective, but in doing so they respect the relevant procedural guarantees "laid down by national law."[276]

Attorney-client confidentiality is respected by many of the contracting states and will be respected by the Commission under case law of the ECJ.[277] The definition of "attorney" is critical. In-house lawyer communication is not protected, because such lawyers are considered employees of the enterprise.[278] Moreover, the protection afforded to communications from outside lawyers only applies to lawyers entitled to practice in one of the Member States.[279] American lawyers practicing in Europe, who are not qualified to practice in one of the member countries, enjoy no confidentiality of written communication.[280]

Remedies Under Members State Laws

As indicated above, remedies in EU member states for violation of laws relating to privacy include both criminal and civil sanctions. Under the provisions of the Privacy Directive and implementing member state statutes, what may be considered more serious penalties may be imposed upon a business entity that desires to collect and maintain personal data for business purposes. The enterprises may be banned from such activity if they fail to comply with the privacy commands and thus suffer serious hardship in their efforts to prosper as an economic enterprise.[281] This is particularly significant to banks, airlines, insurance companies, and marketing enterprises of all types, who would be unable to collect and manage data about their customers and clients.[282]

---

276. *Id.* ¶ 44.

277. *See* Case 155/79, Austl. Mining & Smelting Eur. Ltd. v. Comm'n, [1982] E.C.R. 1575, ¶ 3.

278. *Id.* ¶ 29.

279. *See id.* ¶ 25. Regardless of the member state in which the attorney is licensed, the protection of attorney-client confidentiality stems from either of two sources: recognition of the role of attorneys in a system of a rule of law or, alternatively, that the "right of defence must be respected." *Id.* ¶ 20.

280. *See id.* ¶ 25.

281. For violation of the safe harbor agreement, "[S]anctions include deletion of data obtained improperly in violation of the Safe Harbor Principles, 'suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance' and/or injunctive orders." Zinser, *supra* note 258, at 40. Furthermore, "[P]rivate sector dispute resolution bodies and self-regulatory bodies must notify failures of safe harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts." *Id.* (quoting Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000). They are also required to notify the United States Department of Commerce. *Id.*

282. See Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 HOUS. L. REV. 717, 735-38 (2001); Fred Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 IND. L. REV. 174, 227-229 (1999).

CONCLUSION

This Article, in a broad outline, sketches a number of the major European regulatory systems regarding privacy. These systems contemplate far more privacy than is typical in the United States. The idea that a jail cell inmate or a person walking down the street would enjoy privacy protections is quite absent from American law but starkly present in European law.

It would be unthinkable in the United States for a court to hold, as did the ECHR, that the eldest daughter of Prince Rainier III of Monaco, Princess Caroline, had a valid complaint that German law did not adequately protect her from paparazzi who followed her every daily movement because her private life made no contribution to a debate of general interest.[283] Similarly, one would expect that the ECHR would hold that the public has no legitimate interest in learning that the Italian King in exile, Victor Emmanuel III, had procured prostitutes for business associates or for himself (absent, that is, prosecution for soliciting). The European approach to privacy, limiting data disclosure to particular purposes with explicit consent required and prohibiting further transmission of such data without further permission, makes a great deal of sense. These principles are essentially absent in United States privacy laws.

283. Von Hannover v. Germany, App.No. 59320/00, 43 Eur. H.R.Rep. 7 (2006). Furthermore the Court considers that the public does not have a legitimate interest in knowing where the applicant [Princess Caroline and her children] is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well know to the public.

Id. ¶ 77.