A BROADENED VIEW OF PRIVACY AS A CHECK AGAINST GOVERNMENT ACCESS TO E-MAIL IN THE UNITED STATES AND THE UNITED KINGDOM

ALEXANDER DÍAZ MORGAN*

* Law Clerk to the Honorable Samuel H. Mays, Jr., United States District Court for the Western District of Tennessee. J.D., 2007, New York University School of Law; B.A., 2004, Emory University. I would like to thank Professor Mitchell Lasser for his comments when this Note was in its infancy, the staff at the *New York University Journal of International Law and Politics* for much-needed editing assistance (especially Ayana Free, Rebecca Bers, and Alexis Blane), and Sofie Rahman for her feedback throughout. Finally, I would like to thank my Dad for his review of this Note, as well as most every writing assignment I have had since grade school.

I. Introduction

In a 1928 decision penned by Chief Justice William Howard Taft, the Supreme Court held that the Constitution of the United States did not proscribe warrantless wiretapping because no "material things" were searched.[1] Though the wiretap at issue concededly provided access to private conversations, the communications themselves were intangible and thus outside the purview of constitutional protection. In an impassioned dissent, Justice Louis Brandeis warned that "[w]ays may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose . . . the most intimate occurrences."[2] The words of Justice Brandeis have proven prophetic. Electronic mail has emerged as the preeminent form of communication in the Internet Age.

1. Olmstead v. United States, 277 U.S. 438, 464 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

2. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

Unfortunately, the ease with which we may now communicate via e-mail is matched only by the ease with which the government may surreptitiously peer at our private messages.[3]

With the terrorist attacks of September 11, 2001 and July 7, 2005 fresh in the memory of Americans and Britons alike, the incentive for the government to gather information has seldom been so pronounced. In spite of this grim reality, both the United States and the United Kingdom attempt to balance security and privacy interests by maintaining statutory and constitutional protections against unfettered government surveillance of e-mail. Protections that purportedly limit government access in the United States and the United Kingdom are nonetheless incomplete, recognizing only individual privacy interests while ignoring their societal analogues. Until e-mail surveillance law incorporates a societal conception of privacy, decisionmakers will underemphasize privacy when making and enforcing such laws and harms to societal interests in privacy may go undetected.

Part II of this Note describes the workings of e-mail and the methods by which governments may trace and/or intercept messages. Part III summarizes the differences between the United States' and United Kingdom's regimes of protection. In particular, this Part reviews the statutory bases for government interception, the constitutional limits thereupon, and the methods of oversight in each country. In Part IV, I argue for a broadened conception of privacy that expressly recognizes both individual and societal privacy interests. Part V addresses the shortcomings of the United States' and the United Kingdom's protective regimes in view of this broadened conception of privacy. Finally, in Part VI, I propose a Model Regime to address the weaknesses of the current systems in the United States and the United Kingdom.

II. E-mail and Government Surveillance Techniques

E-mail communication is made possible by "packet switching," a process that splits messages into minute fragments, each of which navigates the internet and makes its way to its recipient via a slightly different path (thus maximizing use of

3. Text messaging and instant messaging may also be subjected to surveillance. They each raise interesting questions which warrant further examination. However, this Note addresses e-mail alone.

available bandwidth and speeding delivery).[4] Along the way, an e-mail travels through the servers of the Internet Service Provider (ISP) and Internet Mail Provider (IMP) of the message's sender and recipient. Its final destination is the server of the recipient's IMP.[5]

An e-mail may be divided conceptually between two distinct parts: content and envelope data. The former is the message itself, and the latter consists of the subject field, source field (sender e-mail address), destination field (recipient address), date, time, and size of message.[6] Under existing regimes, the distinction between the two is critical. Legal standards provide for easier access to envelope data than to content, based on the belief that envelope data is less revealing and therefore raises fewer privacy concerns.[7]

---

4. *See* E. Parker Lowe, *Emailer Beware: The Fourth Amendment and Electronic Mail*, 2 OKLA. J. L. & TECH. 28, 5 (Feb. 2005), http://www.okjolt.org/pdf/2005okjoltrev28.pdf. In addition to a particular piece of the original message, every "packet" contains general routing information including the electronic mail addresses of the sender and recipient and the subject of the message. Peter J. Young, Note, *The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy*, 35 IND. L. REV. 303, 307 (2001). E-mail travels in either plain text or encrypted fashion. Encrypted messages require a "key" to be viewed in an intelligible form. Seth R. Merl, Note, *Internet Communication Standards For the 21st Century: International Terrorism Must Force the U.S. to Adopt "Carnivore" and New Electronic Surveillance Standards*, 27 BROOK. J. INT'L L. 245, 276 (2001). Encryption frustrates general packet sniffing, but does not affect targeted surveillance, as messages are intercepted through unencrypted envelope data.

5. *See* Lowe, *supra* note 4, at 5-6. Post Office Protocol (POP) e-mail programs download e-mail to the user's hard drive, while at the same time deleting it from the IMP server. University of Pennsylvania Information Systems & Computing, POP vs. IMAP (2004), http://www.upenn.edu/computing/eval/2004/csemail/pop_vs_imap.html (last visited Mar. 3, 2008). In contrast, Internet Message Access Protocol (IMAP) programs store e-mail on the IMP server indefinitely until the user manually deletes it. *Id.*

6. *See* Griffin S. Dunham, *Carnivore, the FBI's E-mail Surveillance System: Devouring Criminals, Not Privacy*, 54 FED. COMM. L.J. 543, 554 (2002).

7. DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 283-84 (2d ed. 2006) [hereinafter SOLOVE, INFORMATION PRIVACY]. This distinction originated in the context of telephone communication, where the Supreme Court held that telephone conversations receive Fourth Amendment protection, but numbers dialed to make the call do not. Smith v. Maryland, 442 U.S. 735, 743-44 (1979). Critics bemoan the extension of this logic to e-mail, arguing that e-mail envelope data (which includes the subject field) reveals more information than phone records. *See, e.g.*, Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287-88 (2004)

Most concede that some measure of e-mail surveillance is integral to national security, law enforcement, and criminal investigation.[8] In this vein, American agencies such as the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and National Security Agency (NSA)[9] and British groups such as MI5 (Security Service) and MI6 (Secret Intelligence Service) perform surveillance.[10] These agencies monitor e-mail in a variety of ways. They may retrieve stored e-mail by accessing IMP servers or use "packet sniffing" programs attached directly to IMP or ISP servers to catch messages in real time.[11]

A packet sniffing program "eavesdrops on . . . packets . . . then saves a copy of the packets it is interested in" and may perform either general or targeted surveillance.[12] General surveillance involves scanning *all* messages passing by but saving only those with preordained words or phrases (e.g., "dirty bomb"), whereas targeted surveillance saves only those messages going to or from a particular e-mail or internet protocol (IP) address.[13] Programmers direct packet sniffers engaged in targeted surveillance to retrieve either entire e-mail messages or envelope data alone.[14] Yet, because "even the ISP

[hereinafter Solove, *Electronic Surveillance*]; *see also* Peter J. Georgiton, Note, *The FBI's Carnivore: How Federal Agents May be Viewing Your Personal E-Mail and Why There is Nothing You Can Do About It*, 62 OHIO ST. L.J., 1831, 1841-47 (2001).

8. *See, e.g.*, Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 818 (1989).

9. Carmel Sileo, *Lawsuits Aim to Curb Warrantless Domestic Surveillance*, TRIAL, Apr. 2006, at 12.

10. Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1167-70 (2006).

11. *See* Young, *supra* note 4, at 306; Lowe, *supra* note 4, at 6.

12. Aaron Kendal, *Carnivore: Does the Sweeping Sniff Violate the Fourth Amendment?*, 18 T.M. COOLEY L. REV. 183, 191 (2001).

13. *Id.* An IP address is a unique number which identifies a particular computer, network, or server. It is similar to a telephone number in that it typically corresponds to a particular location.

14. A packet sniffer that targets a particular e-mail or IP address and only retrieves envelope data is referred to as a "trap and trace" device. *See* John Schwartz, *Wiretapping System Works on Internet, Review Finds*, N.Y. TIMES, Nov. 22, 2000, at A19. In the United States, government agencies have yet to reveal the source code for their packet sniffing programs; it is therefore unknown whether the programs have capabilities beyond those described. Ted Bridis, *FBI Refuses to Release Carnivore Details*, ZDNET NEWS, Aug. 9,

[or IMP] to whose equipment [the packet sniffer] is connected will not know what it is doing, there can be no means of verifying that surveillance is being limited to what is legally allowed."[15] The power to secretly retrieve e-mail information is thus coupled with the risk that the government will exercise it in an over-expansive fashion.

III. Government Access to E-mail in the United States and the United Kingdom

In the United States and the United Kingdom, the government's power to access e-mail is conferred by statute and indirectly limited by those same statutes as well as by privacy-related constitutional protections.

A. *E-mail in the United States*

In the United States, the Electronic Communications Privacy Act of 1986 (ECPA) and Foreign Intelligence Surveillance Act (FISA) regulate government access to e-mail. The text of the Constitution does not contain an explicit privacy protection. The Fourth Amendment may provide implicit protection, however, as might a "penumbral" right to privacy that the Supreme Court has, in certain instances, found to arise out of other enumerated provisions in the Bill of Rights.[16]

1. *Statutory Authorization of Government Access to E-mail in the United States*

The ECPA regulates government access to oral, wire, and electronic communication.[17] It has three subparts, which provide differing standards of review for each form of surveillance.[18] The Wiretap Act[19] regulates real-time e-mail intercep-

---

2000, http://www.zdnet.com.au/news/soa/FBI-refuses-to-release-Carnivore-details-/0,139023165,120103210,00.htm (last visited Mar. 3, 2008).

15. Duncan Campbell, *The Spy in Your Server*, The Guardian (London), Aug.10, 2000, http://www.guardian.co.uk/technology/2000/aug/10/news.onlinesupplement (last visited Mar. 3, 2008).

16. *See infra* notes 45-49 and accompanying text.

17. The Electronic Communications Privacy Act (ECPA) includes three subparts: the Wiretap Act, 18 U.S.C. §§ 2510-22 (2006); the Stored Communications Act, 18 U.S.C. §§ 2701-11 (2006); and the Pen Register Act, 18 U.S.C. §§ 3121-27 (2006). *See* Solove, Information Privacy, *supra* note 7, at 265-66.

18. Solove, Information Privacy, *supra* note 7, at 265-66.

tion, the Stored Communications Act[20] covers e-mail on servers, and, finally, the Pen Register Act[21] controls access to envelope data.

The Wiretap Act provides stringent requirements for real-time interception. Authorization requires a court to find "probable cause"[22] to believe each of the following: (1) that the surveillance target is committing a crime; (2) that communication relating to the crime will be uncovered by surveillance; (3) that the computer and/or e-mail searched is being used in connection with the crime; and (4) that traditional investigative techniques have failed or will fail.[23] When a court grants authorization, surveillance must occur "as soon as practicable,"[24] and the government must notify targeted individuals upon completion.[25]

The Stored Communications Act regulates access to e-mail stored on servers. Under the Act, access to e-mail differs based on the period of time it has been stored. Access to e-mail stored for 180 days or less requires a court order issued upon probable cause that a crime has been or is being committed.[26] For e-mail stored more than 180 days, the government need only show "reasonable grounds to believe" that the e-mail is "relevant and material to an ongoing criminal investigation" and give prior notice to the target.[27] If the government prefers not to give prior notice, it may decline to do so provided it meets the probable cause standard that applies to e-mail stored for fewer than 180 days.[28] If prior notice is withheld, the government must give notice to the target upon completion of surveillance unless it shows that doing so may harm

19. 18 U.S.C. §§ 2510-22.

20. *Id.* §§ 2701-11.

21. *Id.* §§ 3121-27.

22. Probable cause requires "reasonably trustworthy information" which "warrant[s] a man of reasonable caution" to believe that each precondition is met. Brinegar v. United States, 338 U.S. 160, 175-76 (1949).

23. Katherine Vogele, *Electronic Surveillance*, 90 GEO. L.J. 1209, 1216-17 (2002).

24. SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 268-69.

25. Vogele, *supra* note 23, at 1220-24.

26. 18 U.S.C. § 2703(a).

27. *Id.* § 2703(d).

28. *Id.* § 2703(b).

the investigation or later prosecution, in which case notice may be delayed.[29]

The Pen Register Act governs interception of e-mail envelope data. The statute presumes that envelope data is less revealing and thus permits the government easier access to this information than the Stored Communications Act does for e-mail on servers.[30] Authorization under the Act requires only that the information sought be "relevant to an ongoing investigation."[31] To protect the integrity of the surveillance, the Act prohibits under penalty of law disclosure of "the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber."[32]

If gathering foreign intelligence is "a significant purpose" of surveillance, FISA[33] supersedes the ECPA. FISA applications are generally submitted to the Foreign Intelligence Surveillance Court (FISC), which reviews them in secret *ex parte* proceedings subject to considerably lower standards than applications under the ECPA.[34] FISA applications need only demonstrate probable cause to believe that a surveillance target is "a foreign power" or agent thereof—the statute requires no suspicion of wrongdoing.[35] If the intended surveillance target is an American citizen or permanent resident alien, however, there must be probable cause to believe that "the party's activities 'may' or 'are about to' involve criminal activity."[36]

The FISA amendments contained in the Protect America Act of 2007 significantly alter this process when foreign intelligence surveillance targets "a person reasonably believed to be located outside of the United States."[37] In such cases, the At-

29. *Id.* § 2705(a)(1)-(2).

30. *See supra* note 7 and accompanying text.

31. 18 U.S.C. § 3123(a)(1).

32. *Id.* § 3123(d)(2). A "trap and trace" device is a packet sniffer that records only envelope data. Schwartz, *supra* note 14.

33. Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-11 (2006).

34. *Id.* § 1801; SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 289.

35. 50 U.S.C. § 1801.

36. *Id.* (quoting 18 U.S.C. § 1801(b)(2)(A)).

37. Protect America Act of 2007, Pub. L. No. 110-55, sec. 2, § 105A, 121 Stat. 522 (2007). This was achieved by amending the definition of electronic surveillance so that, "[n]othing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." *Id.*

torney General and Director of National Intelligence (DNI) may personally authorize surveillance operations for up to one year without FISC approval provided certain ancillary requirements are met.[38] Should a third-party ISP/IMP refuse to comply with government surveillance efforts, either party may seek review by the FISC, which may in turn compel assistance or deem the surveillance authorization improper.[39] The FISC's lone additional oversight role is to certify that internal procedures for determining whether a target is outside the United States are "not clearly erroneous."[40] Finally, the Protect America Act also requires the Attorney General to provide biannual reports to Congress on the number of authorizations issued as well as on any instances of non-compliance.[41]

There is no emergency exception under the ECPA—courts must always give prior authorization for surveillance. In stark contrast, FISA permits two forms of temporary "emergency" authorization. When the Attorney General believes that a target is inside the United States, he or she can independently authorize surveillance if: (1) "an emergency situation exists . . . to obtain foreign intelligence information," and (2) the standards normally applied by the FISC under the Act are met.[42] After such authorization, FISA requires formal applications to the FISC within 72 hours.[43] When the government believes that a target is outside the United States and that "immediate action . . . is required," it can bypass authorization by the Attorney General and DNI, provided that the Attorney General and DNI grant formal certification within 72 hours.[44]

38. *Id.* § 105B(a). The Attorney General and DNI must certify in writing that: (1) reasonable internal procedures determine whether targets are indeed outside the United States, (2) surveillance does not constitute "electronic surveillance," (3) the information is obtained with the help of an ISP or IMP, (4) a "significant purpose" is to obtain "foreign intelligence information," and (5) minimization procedures are in place. *Id.*

39. *Id.* §105B(e)-(h).

40. *Id.* §105C(a)-(d).

41. *Id.* sec. 4.

42. 50 U.S.C. § 1805(f).

43. *Id.*

44. Protect America Act, § 105B(a).

2. *Constitutional Limitations on Government Surveillance in the United States*

The word "privacy" is nowhere in the Constitution of the United States, yet a limited privacy rights jurisprudence[45] has emerged in recognition of the idea that the "enumeration of certain guarantees in the [Bill of Rights] creates penumbras, or shadows . . . for certain fundamental rights."[46] Though penumbral privacy rights originated in the context of interspousal relations,[47] the Supreme Court has hinted that they may extend to informational privacy.[48] Still, "only a handful of scholars believe that the Supreme Court will strengthen that argument any further."[49] Most constitutional challenges to surveillance rely on the Fourth Amendment, which guarantees freedom from "unreasonable searches and seizures."[50] The Fourth Amendment's protection of reasonableness only extends to investigatory acts that qualify as a "search" or "seizure." As a result, Fourth Amendment challenges often turn upon this threshold question.

Katz v. United States[51] defines a "search" under the Fourth Amendment. A search occurs when the government infringes upon a target's "actual (subjective) expectation of privacy" that "society is prepared to recognize as 'reasonable.'"[52] The reasonable expectation of privacy standard establishes that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[53]

---

45. *See* Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (discussing penumbral privacy rights); *see also* Roe v. Wade, 410 U.S. 113, 152-53 (1973) (discussing "zones of privacy" recognized by the Court and the development of law, and citing cases); Whalen v. Roe, 429 U.S. 589, 599 (1977) (same).

46. Marsha Cope Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 435 (2002).

47. *Griswold*, 381 U.S. at 484-86.

48. *Whalen*, 429 U.S. at 599-600.

49. Alice Kao, Note, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, 19 BERKELEY TECH. L.J. 405, 420 (2004).

50. U.S. CONST. amend. IV.

51. Katz v. United States, 389 U.S. 347 (1967).

52. *Id.* at 361 (Harlan, J., concurring).

53. *Id.* at 351 (citations omitted).

The effect of *Katz* is double-edged: While it extends Fourth Amendment protection beyond the traditional locus of the home, it requires an ambiguous "reasonable expectation of privacy" to trigger that protection. To combat ambiguity, a formalistic third-party rule has emerged: "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[54] This rule is potentially devastating to e-mail protection, as it has been suggested that passage through ISP/IMP servers—although purely incidental to the function of e-mail—may constitute voluntary transfer sufficient to destroy one's reasonable expectation of privacy.[55]

To be reasonable under the Fourth Amendment,[56] a search generally[57] requires a warrant obtained ex ante from a neutral and detached judge upon a showing of probable cause.[58] The administrative exception doctrine permits warrantless searches for "special needs" beyond ordinary law enforcement, provided that they are not conducted arbitrarily.[59]

---

54. Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (finding no reasonable expectation in phone records because numbers dialed are exposed to phone company); *see also* United States v. Miller, 425 U.S. 435, 442-43 (1976) (finding no reasonable expectation in bank records because transactions are disclosed to bank personnel); California v. Greenwood, 486 U.S. 35, 39-44 (1988) (quoting *Smith*, 442 U.S. at 743-44) (finding no reasonable expectation in trash put in curbside bin for garbage collection).

55. *See* Owin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 365-67 (2003).

56. U.S. CONST. amend. IV.

57. The Supreme Court has recognized a number of situations in which warrantless searches are permissible. *See, e.g.*, United States v. Robinson, 414 U.S. 218, 235 (1973) (finding that warrantless searches incident to arrest are permissible); Payton v. New York, 445 U.S. 573, 583 (1980) (noting that exigent circumstances can justify warrantless searches); United States v. Ross, 456 U.S. 798, 825 (1982) (finding that once probable cause justifies an automobile search, the entire automobile and its contents can be searched); Arizona v. Hicks, 480 U.S. 321, 326-27 (1987) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (plurality opinion)) (finding that police do not need a warrant to seize evidence in plain view); Illinois v. Lafayette, 462 U.S. 640, 648 (1983) (finding searches following "established inventory procedures" reasonable); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (noting that consent searches do not require a warrant or a showing of probable cause).

58. SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 210.

59. Administrative exceptions are currently limited to areas such as sobriety checkpoints, border searches, and drug tests. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 452-53 (1990) (sobriety checkpoints); United

Some fear that this exception may erode traditional Fourth Amendment protection by allowing "increasingly aggressive government intrusions" into areas such as e-mail.[60]

3. *Oversight*

In this Note, I use "oversight" to refer to any form of review, be it internal or external, judicial or nonjudicial, that accompanies e-mail surveillance either before (ex ante) or after (ex post) its use. The American regime includes both ex ante and ex post oversight of e-mail surveillance. Ex ante oversight includes departmental protocols, as well as the judicial authorization requirements under the ECPA and FISA. Departmental protocols that require senior agency officials to approve applications to courts provide an administrative hurdle that informally limits the number of surveillance applications and ensures a good-faith basis for their submission.[61] Though these protocols provide initial limits on e-mail surveillance, the judiciary remains the most important, as judges provide an extrinsic check that agency officials cannot. Judges are less likely than prosecutors or executive agents to have a vested interest in an investigation's success and are therefore better suited to oversee compliance with surveillance requirements.[62]

States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (border searches); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 620-21 (1989) (drug testing).

60. Shauna Curphey, United States v. Lifshitz*: Warrantless Computer Monitoring and the Fourth Amendment*, 38 LOY. L.A. L. REV. 2249, 2268 (2005); *see also* George M. Dery III, *Are Politicians More Deserving of Privacy than Schoolchildren?: How Chandler v. Miller Exposed the Absurdities of Fourth Amendment "Special Needs" Balancing*, 40 ARIZ. L. REV. 73, 74 (1998) (claiming that special needs exceptions create a slippery slope).

61. *See* 18 U.S.C. § 2516(1); U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-7.100 (2006) ("[Agents must] clearly understand when Departmental review and approval are required, and what such a process entails.").

62. *See* Rotaru v. Romania, 8 B.H.R.C. 449, ¶ 59 (Eur. Ct. H.R. 2000) ("[J]udicial control affords the best guarantees of independence, impartiality and a proper procedure."); *cf.* Donohue, *supra* note 10, at 1079 (quoting United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 317 (1972)) (indicating that executive agents have a duty "to enforce the laws, to investigate, and to prosecute" and therefore "should not be the sole judges of when to utilize constitutionally sensitive means"). Formal recognition of the problems posed by conflicts of interest is perhaps best documented in the field of legal ethics. *See, e.g.*, MODEL R. PROF'L CONDUCT 1.7-1.12 (1983).

Courts are the only forum for ex post oversight in the United States. Where the government conducts surveillance in violation of statute, courts may impose penalties on the persons guilty of unauthorized surveillance and, in some cases, they may exclude the evidence from trial.[63] Suppression of evidence obtained in violation of the ECPA is available for wire or oral communications, but is inexplicably absent for e-mail.[64] Legal commentators denounce this distinction as "baseless"[65] and further argue that, without a statutory hook, criminal defendants have a lesser "incentive to raise challenges to the government's internet surveillance practices."[66]

When government surveillance abridges constitutional rights, there are two avenues of redress.[67] At trial, criminal defendants may seek to suppress evidence obtained through unconstitutional means, as well as evidence derived therefrom (deemed "fruit of the poisonous tree").[68] Victims of unconstitutional searches may also bring civil actions seeking damages for deprivation of rights under color of law.[69]

B. *E-mail in the United Kingdom*

A single statute regulates government access to e-mail in the United Kingdom. The statute itself provides remedies for aggrieved surveillance targets, as does a European human rights convention, incorporated into the British Constitution, which expressly recognizes a qualified right to privacy.

---

63. *See, e.g.*, 50 U.S.C. § 1809; 18 U.S.C. §§ 2511, 2520, 2701, 3121.

64. 18 U.S.C. § 2518(10)(a).

65. Solove, *Electronic Surveillance*, *supra* note 7, at 1282 (stating that because "e-mail has become a central mode of communication, this discrepancy is baseless").

66. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824 (2003).

67. SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 213.

68. *See* Weeks v. United States, 232 U.S. 383, 398 (1914); *see also* Segura v. United States, 468 U.S. 796, 804 (1984).

69. 42 U.S.C. § 1983 (2006) (stating that anyone who subjects another "to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law"); *see, e.g.*, Zinermon v. Burch, 494 U.S. 113, 125 (1990) ("A plaintiff may bring suit under § 1983 for . . . violation[s] of his rights to, e.g., freedom of speech or freedom from unreasonable searches and seizures.").

1. *Statutory Authorization of Government Access to E-mail in the United Kingdom*

The Regulation of Investigatory Powers Act of 2000 (RIPA) controls government surveillance powers.[70] Part I of RIPA covers e-mail and is divided into two subchapters: Chapter I for interception of content and Chapter II for interception of envelope data.[71]

Access to content requires a warrant from the Home Secretary,[72] who as head of the Home Office also oversees law enforcement and national security.[73] The Home Secretary may issue a warrant upon a showing that interception is "necessary" and "proportionate" to that which is sought.[74] The Home Secretary exercises discretion over proportionality determinations, while interests that may render interception "necessary" are specifically limited to national security, "preventing or detecting serious crime," or "safeguarding the economic well-being of the United Kingdom."[75]

Access to envelope data is more easily obtained, as the Home Secretary may authorize others to approve access.[76] The Home Secretary or her designee enjoys the same level of discretion to determine proportionality when reviewing applications for access to envelope data as with regard to content. Nevertheless, the statute extends the interests that render envelope surveillance "necessary" beyond those recognized for access to content to include public safety, public health, tax collection, or any other reason specified by order of the Home Secretary.[77]

---

70. Regulation of Investigatory Powers Act (RIPA), 2000, c. 29 (Eng.).

71. RIPA §§ 1-20, 21-25.

72. *Id.* § 5. The role of the Home Secretary is akin to that of the Secretary of State in the United States.

73. Home Office, http://www.homeoffice.gov.uk/about-us/ (last visited Feb. 3, 2008).

74. RIPA § 5. This language tracks article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, *infra* note 83.

75. RIPA § 5(3)(a)-(c).

76. Yaman Akdeniz, *Regulation of Investigatory Powers Act 2000: Part I: Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights*, CRIM. L. REV., Feb. 2001, 73, 81.

77. RIPA §22.

The Anti-Terrorism, Crime, and Security Act of 2001[78] (ATCSA) collaterally enhanced government surveillance powers under RIPA. The ATCSA requires ISPs and IMPs to retain all envelope data passing through their servers for a period set by the Home Secretary.[79] Although compulsory retention is premised upon national security, the government may later access the data under RIPA for any number of less compelling reasons, as outlined above.[80]

2. *Constitutional Limitations on Government Surveillance in the United Kingdom*

The United Kingdom does not have a formal, written constitution. Rather, its Constitution is amorphous and includes "the whole body of public law, customary as well as statutory, which is continually being modified by custom, judgment in the courts as well as by [Parliament]."[81] In this system, fundamental freedoms are largely protected by the 1998 Human Rights Act[82] (HRA), which formally incorporates the European Convention on Human Rights[83] (ECHR) into domestic constitutional law. Article 8 of the ECHR establishes privacy in one's communications as a qualified, fundamental right:

> 1. Everyone has the right to respect for . . . his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[84]

---

78. Anti-Terrorism, Crime and Security Act (ATCSA), 2001, c. 24 (Eng.).

79. *See id.* § 102.

80. Donohue, *supra* note 10, at 1182.

81. United Kingdom Parliament, http://www.explore.parliament.uk/Parliament.aspx?id=10152&glossary=true (last visited Mar. 4, 2008).

82. Human Rights Act (HRA), 1998, c. 42 (Eng.).

83. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, 230 [hereinafter ECHR].

84. *Id.* art. 8.

Article 8 decisions of the European Court of Human Rights (ECtHR) at Strasbourg, France, influence domestic privacy rights jurisprudence.[85] Under the HRA, claimants bring domestic actions for violations of rights under the ECHR. If claimants exhaust domestic remedies without satisfaction, they may apply to Strasbourg for relief.[86] Though decisions of the ECtHR only bind the member state(s) party to a particular case, British courts do "not adopt a protection for rights that is below the 'floor' of protection afforded by [ECtHR] jurisprudence" for fear of later being held accountable on similar grounds.[87]

Under ECtHR jurisprudence, interception of e-mail content and envelope data triggers article 8 protection.[88] Article 8 permits interception only if it is (1) "in accordance with law" and (2) "necessary in a democratic society"[89] pursuant to a limited set of interests.[90] The Strasbourg Court interprets "in accordance with law" to "require[ ] that an interference . . . have some basis in national law" and that the law "be accessible and precise": that is, "publicly available and foreseeable in its consequences."[91] Determinations of necessity turn on "pro-

85. *See, e.g.*, R (B) v Responsible Medical Officer, Broadmoor Hospital & Ors, [2005] EWHC (Admin) 1936 [48] (citing Klass v. Federal Republic of Germany, 2 Eur. Ct. H.R. 214 (1978), for the proposition that exceptions to article 8 are to be interpreted narrowly); R (Kent Pharmaceuticals Ltd) v Serious Fraud Office & Ors, [2004] EWCA Civ 1494 [19] (citing *Klass* for the proposition that government surveillance regimes must contain "adequate and effective guarantees against abuse"); Secretary of State for Work and Pensions v M, [2004] EWCA Civ 1343 [74] (citing *Klass* for the proposition that a claimant cannot merely allege that a law violates rights under the ECHR, but must show that the law was actually applied to the claimant's particular detriment).

86. SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 878-79.

87. David Bonner, *Judicial Approaches to the Human Rights Act*, 52 INT'L & COMP. L.Q. 549, 552-53 (2003).

88. Nick Taylor, *Policing, Privacy and Proportionality*, 3 EUR. HUM. RTS. L. REV. 86, 90 (2003 Supp.) (U.K.).

89. ECHR, *supra* note 83, art. 8(2).

90. *See* RIPA §§ 5(3)(a)-(c), 22; ECHR, *supra* note 83, art. 8.

91. Ben Emmerson and Helen Mountfield, Privacy International, U.K. Info Commissioner Challenges Legality of Data Retention, ¶ 16, http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=X-347-62148 (last visited Mar. 4, 2008); *see, e.g.*, McLeod v. United Kingdom, 27 Eur. Ct. H.R. 493, 506 (1999) ("[T]he expression 'in accordance with the law' requires firstly that the impugned measure should have some basis in national law; it also refers to the quality of the law in question, requiring that it

portionality" and consider (1) the degree of intrusion relative to its justification and (2) "an assessment of the adequacy of the safeguards in place to prevent abuse."[92]

Interference with privacy must also relate to interests that make surveillance "necessary," such as national security, crime prevention/detection, and economic well-being. Although none of these interests is easily defined, national security stands out as perhaps the least susceptible to precise characterization. Reliance on such terms therefore poses a potential threat to privacy.[93]

3. *Oversight*

Part IV of RIPA structures the oversight of e-mail surveillance. Under the Act, ex ante oversight is constrained because the same body responsible for law enforcement—the Home Secretary—is charged with judging surveillance applications. RIPA does require the Home Secretary to issue Codes of Practice to provide public guidance to authorities affected by the Act[94] that may create "additional [internal] safeguards" akin to departmental protocols in the United States.[95] The codes are

---

should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law.").

92. Emmerson & Mountfield, *supra* note 91, ¶ 16; *see also* Leander v. Sweden, 7 Eur. Ct. H.R. 557, 569 (1985) ("[A]n interference with a Convention right cannot be regarded as 'necessary in a democratic society' unless it is proportionate to the legitimate aim pursued."); G. v. Germany, 6 Eur. Ct. H.R. 499, 508 (1984) ("[T]he Convention requires a clearly established need for any interference with the rights it guarantees, before such interference can be justified on that basis."); Chappell v. United Kingdom, 11 Eur. Ct. H.R. 543, 554 (1989) ("In deciding whether the interference was necessary in a democratic society the Commission must examine whether the interference was proportionate to this legitimate aim. This question involves an assessment, in particular of the way in which the interference arose in practice, and hence of the way in which the order was executed in the light of the safeguards which it contained.").

93. RIPA enumerates interests sufficient to justify access to e-mail content and data information. *See supra* notes 75 and 77 and accompanying text.

94. RIPA § 71; Gillian Ferguson, *Privacy and Surveillance: A Review of the Regulation of Investigatory Powers Act 2000*, 3 EUR. HUM. RTS. L. REV. 100, 107 (2003) (U.K.).

95. Ferguson, *supra* note 94, at 107.

of little effect, however, because they are not binding on agencies and are unenforceable in court.[96]

Under RIPA, ex post oversight is more robust. Section 57 creates an Interception of Communications Commissioner who reviews surveillance authorizations[97] and reports to Parliament.[98] Section 65 creates an Investigatory Powers Tribunal (the "Tribunal") with sole jurisdiction over HRA complaints regarding the "exercise of powers under RIPA."[99] Finally, if claimants find domestic resolution of complaints unsatisfactory, they may seek redress at Strasbourg. Though judicial oversight of the Tribunal is theoretically buttressed by the Strasbourg Court, the effectiveness of this outlet is limited both because the likelihood of review is slight and because the Court is slow to respond to petitions.[100]

IV. A Broadened Conception of Privacy

Privacy is an amorphous concept. In this Part, I set out the elements of privacy and briefly address the individual interests most commonly associated with the concept. I then compare privacy rights with property rights, which, although an imperfect analogue, provide an example of rights which have come to be viewed as serving both individual and societal interests.[101] Building on this comparison, I argue that the similarities between privacy and property interests show that privacy should be treated with some of the same considerations. In particular, the dual nature of privacy rights suggests that policymakers should pay more attention to the costs of e-mail surveillance, particularly those felt at the societal level. This realization informs my critique of the American and British regimes and, ultimately, the Model Regime which proposes a more desirable balance between privacy and security.

---

96. *Id.* However, note that those guilty of unauthorized surveillance may be subject to criminal sanction. RIPA § 1.

97. Ferguson, *supra* note 94, at 105.

98. Akdeniz, *supra* note 76, at 89.

99. Ferguson, *supra* note 94, at 106.

100. *See* Solove, Information Privacy, *supra* note 7, at 879. On average five years elapse between application to the Strasbourg Court and final judgment. *Id.*

101. The analogue is imperfect because the societal interests related to property rights do not align with those related to privacy rights.

A. *Traditional Individualized Elements of Privacy*

Privacy is traditionally understood as an individual right and is therefore conceptualized in individualized terms. Conceived in this way, privacy possesses "three independent and irreducible elements: secrecy, anonymity, and solicitude."[102] Secrecy is "the control we have over information about ourselves."[103] Anonymity is limited access to self.[104] And solicitude is the "autonomy of the intimacies of personal identity," or simply intimacy.[105]

Unfettered third-party access to e-mail offends each of these interests. Secrecy is upset when the distinction blurs between information revealed in private correspondence and public discourse. The anonymity we rely upon when, for example, we communicate under an internet pseudonym is frustrated by access to e-mail which reveals one's true identity. Finally, the intimacy of one's religious, political, personal, and social affiliations may all be revealed by access to e-mail.[106]

For most, these elements of privacy and the fears to which they relate create a demand for the protection of e-mail communication. These interests are not, however, all-encompassing. Privacy also relates to broader societal interests, susceptible to different harms which are often ignored if one takes a myopic view of privacy centered on the individual alone.

B. *Individual v. Societal Conceptions of Property Rights*

Beyond individual interests in privacy, some assert the existence of concomitant societal interests that policymakers must recognize to protect privacy fully.[107] An example of such dual recognition is seen in modern understandings of property rights, which recognize both personal and societal interests.

---

102. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 433 (1980).

103. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

104. Gavison, *supra* note 102, at 433 n.40.

105. *See* Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 281 (1977).

106. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 66, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

107. *See infra* notes 120-124 and accompanying text.

Our understanding of property rights has evolved over the centuries from focusing on the individual to encompassing societal interests. William Blackstone characterized property rights as the "sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual."[108] In the twentieth century, however, "a social, or relational, conception of ownership" emerged, and "social interference with one person's ownership interest was deemed inevitable."[109]

The societal interest in property rights extends beyond exclusive possessory ownership to encompass a collective interest in property that stems from the overarching needs of the people. Theorists now "imbue[ ] property with a social purpose."[110] For example, some argue that "through ownership of property a citizen gains values necessary to participate meaningfully in government,"[111] while others assert that property rights facilitate the "creation of social order."[112] Conceptualized as such, "property serves two masters: the individual and society."[113] It is therefore idle to speak of one interest in the absence of the other[114] because "the social aspect [is not] an exception, but rather an *essential* part of the institution of property."[115] Legal and policy analyses of laws affecting property rights must in turn conceive of the right in *both* individual and societal terms to prevent unforeseen and undesired consequences.

---

108. 2 WILLIAM BLACKSTONE, COMMENTARIES *2.

109. Vincenzo Vinciguerra, Note, *The Dialectic Relationship Between Different Concepts of Property Rights and Its Significance On Intellectual Property Rights*, 10 J. TECH. L. & POL'Y 155, 162 (2005). Some modern readings of Blackstone now urge that he too realized that "potential restraints exist and these restraints on individual use of property may be propelled by the social aspect of property." Marla Mansfield, *When "Private" Rights Meet "Public" Rights: The Problems of Labeling and Regulatory Takings*, 65 U. COLO. L. REV. 193, 205 (1994).

110. *See* Mansfield, *supra* note 109, at 205.

111. *Id.*

112. Craig Anthony, *The Reconstitution of Property as a Web of Interests*, 26 HARV. ENVTL. L. REV. 281, 286 n.29 (2002) (citing GREGORY S. ALEXANDER, COMMODITY & PROPERTY: COMPETING VISIONS OF PROPERTY IN AMERICAN LEGAL THOUGHT, 1776-1970, 319-23, 381-82 (1997)).

113. Mansfield, *supra* note 109, at 194.

114. *Id.* at 201 (indicating that "it may be a conceptual error to separate the 'public' from the individuals within it," and vice versa).

115. Vinciguerra, *supra* note 109, at 163 (emphasis added).

C. *The Societal Interest in Privacy Rights*

American and British e-mail regimes recognize the traditional, individual components of privacy but ignore its social importance.[116] Recognition of privacy as a penumbral right arising from enumerated protections in the Bill of Rights betrays a link to other fundamental social rights and, moreover, a causal relation.[117] The current regimes ignore this link by casting privacy as a mere individual right.[118] So limited, privacy is "put on the defensive" because policymakers and courts weigh an *individual* right against *societal* interests in which it is "assumed that the individual has a stake."[119] But the inverse is equally true. Society has a vested interest in individual privacy just as individuals have a vested interest in national security.

To protect the full spectrum of privacy concerns, privacy's "societal value . . . in the public interest" must be recognized "with less emphasis on individual self-policing."[120] Individualized notions of privacy permit citizens to assert rights at a *per-*

---

116. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 213 (1995).

117. *See, e.g.*, Huie, *supra* note 46, at 434. Huie summarizes the scholarship on the issue in writing that:

> This right to personal privacy vis-à-vis the government exists in the penumbra of the following enumerated rights:
>
> - the right of privacy from governmental intrusion exists in the penumbra of the First Amendment's guaranties of freedom of speech and of the press, and of freedom of association;
> - in the Third Amendment's prohibition on the peacetime quartering of troops in private homes;
> - in the Fourth Amendment's prohibition on unreasonable searches and seizures;
> - in the Fifth Amendment's guaranty against compelled self-incrimination;
> - in the Ninth Amendment's reservation to the people of rights not specifically enumerated in the Constitution;
> - and perhaps in the liberty which the Fourteenth Amendment's Due Process of Laws Clause protects.

Id. at 435.

118. REGAN, *supra* note 116, at 213, 225; James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 33-35 (2003). *See generally* EDWARD J. BLOUSTEIN, INDIVIDUAL & GROUP PRIVACY (2d ed. 2003); Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 367 (1974).

119. REGAN, *supra* note 116, at 213.

120. Nehf, *supra* note 118, at 7.

sonal level in demanding, for example, reasonable searches (under the Fourth Amendment of the Constitution) and privacy in communication (under article 8 of the ECHR). Professor Anthony Amsterdam characterizes this individualized view of privacy as protecting "atomistic spheres of interest" like "*my* person and *your* house."[121] Apart from the atomistic interpretation, Amsterdam argues that privacy protections may likewise be viewed as "a regulation of government conduct."[122] In this regard, privacy protections operate like a "regulatory cannon" which "keeps us collectively secure."[123] Reliance upon an atomistic understanding limits privacy to its traditional role as a *personal* right justified by *personal* interests. Yet if privacy rights, like property rights, serve both individual and societal interests, they require expanded legal protections.

When viewed in societal terms, privacy touches upon a broad spectrum of interests not cognizable at a personal level. Principal among these are the "psychological, social, and political dimensions."[124] The psychological dimension exists in primarily developmental terms:

> The man . . . whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. . . . His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient . . . is not an individual.[125]

Understood in these terms, "[p]rivacy is the basis of individuality," without which "character [is] formed by uncontrolled external stimulations" resulting in a "homogenized" person.[126] The homogenization of society obviates the protec-

---

121. Amsterdam, *supra* note 118, at 367 (emphasis in original) (referring specifically to the Fourth Amendment).

122. *Id.*

123. *Id.*

124. BLOUSTEIN, *supra* note 118, at 2.

125. *Id.* at 42.

126. United States v. White, 401 U.S. 745, 763 (1971) (Douglas, J., dissenting) (quoting RAMSEY CLARK, CRIME IN AMERICA 287 (1970)).

tion of diversity of thought fostered by free speech and free association.[127] To the extent that Americans and Britons place value on uncompromised psychological development and diversity of thought, they should recognize a societal interest in privacy.

The social dimension of privacy arises from the nature of surveillance which renders it "difficult for any of us to have privacy unless we all have privacy at a similar level."[128] Unlike a disease against which some are vaccinated and others are not, if the government fails to respect certain forms of privacy *everyone* is likely to suffer.[129] This dimension of privacy counsels against exclusive reliance on individual, case-by-case resolution of privacy abuses.[130]

The political dimension of privacy relates to a "distrust of powerful institutions"[131] and embraces a regulatory view of privacy that is "profoundly anti-government" in that it limits the scope of acceptable action.[132] The political interest also ties privacy to the preservation of free thought and speech—factors central to maintenance of a "democratic political system."[133] In support of the link, commentators point to the privacy protections traditionally afforded in jury deliberations and voting.[134] In each case, Americans and Britons presume that a juror's views on a trial or a voter's political persuasions will be unduly influenced if subjected to public scrutiny.[135]

---

127. The right to free speech and association receives protection in the United States and the United Kingdom. *See* U.S. CONST. amend. I; ECHR, *supra* note 83, arts. 9-11; HRA § 1 (incorporating ECHR protections).

128. Nehf, *supra* note 118, at 69.

129. Even targeted surveillance of a suspect's e-mail requires access to servers containing numerous other e-mails. Kendal, *supra* note 12, at 191; *see also infra* note 224. General surveillance poses a more immediate threat as messages are scanned indiscriminately. *See* Kendal, *supra* note 12, at 191-92.

130. *Id.*

131. Nehf, *supra* note 118, at 71.

132. Amsterdam, *supra* note 118, at 353, 369; *see also* REGAN, *supra* note 116, at 225 ("A public value of privacy derives not only from its protection of the individual as an individual but also from its usefulness as a restraint on the government or on the use of power.").

133. Nehf, *supra* note 118, at 69.

134. BLOUSTEIN, *supra* note 118, at 152-54.

135. As in the United States, jury deliberation and voting in the United Kingdom are conducted in secret. Peter Johnstone, *International Controls of Corruption: Recent Responses from the U.S. and U.K.*, 11 J. FIN. CRIME 217, 225 (2004); Rory O'Connell, *Towards a Stronger Concept of Democracy in the Stras-*

Privacy-related laws like those in the regimes at issue do not *define* privacy but rather identify those situations in which it receives legal protection.[136] In designing a protective regime, policymakers must therefore competently identify the full range of privacy interests they wish to protect. Without this static, normative baseline of interests, courts can only measure government encroachments against "current expectations of privacy," which continuously shrink due to "increasing surveillance in the modern world."[137] Adding to the problem, if courts conceive of current expectations of privacy in individual terms alone, protections will remain incomplete and harms at the societal level may proceed undetected. Whereas societal privacy interests may suffer due to the mere threat of abusive surveillance if it chills certain behavior, individual interests in privacy are necessarily offended only by actual abuse. Accordingly, reliance upon protections that conceive of privacy in a limited, individual sense alone may prove inadequate.[138]

Framed as both an individual and societal concern, privacy protections have "a broader public purpose."[139] Once the societal or "public value" of privacy gains recognition, one may weigh *societal* interests in privacy against *societal* interests in surveillance, like national security, law enforcement, and crime prevention.[140] The result is a more complete balancing of in-

---

bourg Convention, 3 EUR. RTS. L. REV. 281, 283 (2006) (noting that voting in secret is tied to "an effective political democracy" and protected by the ECHR). The link between privacy and free society has received mention by the Supreme Court. In dissent Justice Douglas quoted Ramsey Clark in saying that "secret electronic surveillance" is "incompatible with a free society." United States v. White, 401 U.S. 745, 764 (1971) (Douglas, J., dissenting) (quoting CLARK, *supra* note 126, at 287). A year later, the majority acknowledged the "potential danger posed by unreasonable surveillance on individual privacy and free expression." United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 315 (1972).

136. Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 36 (1967).

137. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1142 (2002).

138. The traditional individualized elements are discussed earlier and include secrecy, anonymity, and intimacy. *See supra* notes 102-105 and accompanying text. While the threat that they may be offended may chill behavior, the particular interests themselves—anonymity, for example—are violated by actual exposure alone.

139. Nehf, *supra* note 118, at 73-74.

140. REGAN, *supra* note 116, at 213.

terests and a reduced likelihood that policy determinations will exact unforeseen social costs.

V. A Critique of Existing Regimes Through the Lens of Privacy

Review of the above regimes uncovers several problems that jeopardize privacy interests. First, American constitutional protections are too formal and their British equivalents under the ECHR too amorphous. Second, the methods of oversight in each country are incomplete. And third, expansions of government surveillance powers made in response to terrorism have spread to general law enforcement. These failures raise the question of whether current policies protect privacy adequately, especially in view of an expanded concept of privacy which accounts for both individual and societal interests.

A. *Fourth Amendment Formalism*

U.S. case law interpreting the Fourth Amendment provides a lesson in formalism.[141] Formalistic rules are easy to apply and give ample notice to the public, allowing people to conform behavior. Unfortunately, the inflexibility of formalistic rules poses a risk that cases may turn on arbitrary distinctions which ultimately produce counter-intuitive results.

The Fourth Amendment test for a "reasonable expectation of privacy" originally produced results that squared with intuition. The test required both that the party claiming a privacy interest harbor an actual (subjective) expectation of privacy and an objective determination by the court that society would deem that expectation reasonable.[142] This permitted consideration of the nuanced facts of each case. In *Katz*, the test brought telephone conversations within the ambit of the Fourth Amendment because the men speaking thought their exchange was private and society recognized the belief as "reasonable."[143]

---

141. *See supra* notes 54-55 and accompanying text.

142. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

143. *Id.*

More recently, the reasonable expectation of privacy test has fallen prey to formal distinctions that are blind to nuanced considerations of reasonableness. For example, the third-party rule deems expectations of privacy necessarily unreasonable when communication is voluntarily exposed to third parties.[144] Professor Laurence Tribe observes that the current rule conceives of privacy "as if it were a 'discrete commodity, possessed absolutely or not at all.'"[145] Given the absence of a statutory remedy for illegal e-mail surveillance under the ECPA, the third-party rule could preclude constitutional protection and thus sound the death knell for protection of e-mail privacy rights.[146]

The applicability of the third-party rule to e-mail turns on whether one views e-mail in practical or technical terms; or, as Professor Owen Kerr explains, whether one takes an "internal" or "external" view of the internet.[147] The internal, or practical, perspective analogizes the internet to real space and conceives of e-mail as equivalent to postal mail, the interception of which would constitute a search.[148] The external, or technical, perspective counters that "when [person] A sent the e-mail to [person] B, A was instructing his computer to send a message to his Internet Service Provider (ISP) directing the ISP to forward a text message to B's ISP."[149] Under this perspective, by disclosing the message to the third-party ISP, both A and B lose any reasonable expectation of privacy.[150]

The third-party rule has an abstract, logical appeal: In transferring information to a third party, we voluntarily assume the risk that it will be exposed, thus negating any expectation of privacy.[151] However, when the purported voluntary

144. *See supra* notes 54-55 and accompanying text.

145. LAURENCE TRIBE, AMERICAN CONSTITUTIONAL LAW 1391 (2d ed. 1988) (quoting Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)), *quoted in* SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 237 n.11.

146. *See supra* text accompanying note 55.

147. Kerr, *supra* note 55, at 361-62, 365-67.

148. *Id.*

149. *Id.* at 366.

150. Because e-mail is so easily "sniffed" en route to its destination, some suggest "e-mail may be akin to a postcard, with each postal worker on the route being able to read about the great time you are having on your vacation." Kendal, *supra* note 12, at 186.

151. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

assumption of the risk ignores real world considerations—as in the externalist view—it becomes unmoored from common sense and warrants reconsideration.[152] As Justice Marshall explained, "[i]mplicit in the concept of assumption of the risk is some notion of choice . . . [but] [i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[153]

Justice Marshall's view exposes assumption of the risk as legal fiction and supports Kerr's internal perspective of e-mail as akin to postal mail. But this argument is easily met: Despite similarities between e-mail and postal mail, an inanimate packet-sniffing program is hardly the functional equivalent of a postal worker reading letters. Although an inanimate "sniff" may eventually trigger human inspection, one might counter that the prevalence of hackers on the internet militates against a "reasonable" belief that e-mail is secure. Still, the potential for *illegal* access to e-mail is not necessarily dispositive. That a criminal may break into a locked car does not render one's expectation of privacy in personal effects left in the car unreasonable. But this distinction is not absolute, as the Supreme Court has found unreasonable one's expectation of privacy in sealed garbage bags put out for trash even though it was illegal for others to sift through them.[154]

A formalistic Fourth Amendment exception for canine sniffs may also weaken e-mail privacy rights by analogy. Though they reveal hidden information about items sniffed, canine sniffs are not a "search" because they "disclose[ ] only the presence or absence of . . . contraband."[155] This assertion provoked strong disagreement on the Supreme Court, and dissenting justices argued that the "infallible dog . . . is a creature

---

152. For example, the following are not protected by the Fourth Amendment: sealed garbage bags, California v. Greenwood, 486 U.S. 35, 39-44 (1988) (transferred to garbage man); confidential bank records, United States v. Miller, 425 U.S. 435, 442-44 (1976) (transferred to bank personnel); and phone numbers dialed, Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (transferred to phone company). While legitimate reasons for government to access such information may exist, the question remains whether it should be able to do so absent ex ante judicial approval.

153. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

154. *Greenwood*, 486 U.S. at 39-44.

155. United States v. Place, 462 U.S. 696, 707 (1983).

of legal fiction."[156] Legal fiction or not, the exception may extend to packet sniffers if one assumes that they too may be programmed to detect only criminal communication. Though computer programs are doubtless more easily controlled than dogs, it is unlikely that even the most sophisticated programming can effectively winnow out the truly criminal communication from the non-criminal in view of the sarcasm, slang, and otherwise coded language which pervades everyday e-mail.

In addition to formalistic exceptions to the reasonable expectation of privacy test, some contend that the original test is vulnerable to formalism in its own right.[157] As explained by Justice Marshall, "to make risk analysis dispositive . . . allow[s] the government to define the scope of Fourth Amendment protections."[158] As proof, he offered the example of a government announcement that it will randomly monitor mail and telephone calls.[159] Strict adherence to the test holds that the announcement put everyone on notice and therefore defeats any subjective expectations of privacy. Farfetched as this example may be, it confirms the risk of strict adherence to formalism and teaches that even seemingly logical rules must not be applied blindly, without reference to their real world implications.[160]

B. *Amorphous Standards Under RIPA, the HRA, and the ECHR*

In comparison to American formalism, Britain's standards languish at the other extreme, mired in ambiguity. RIPA and

---

156. Illinois v. Caballes, 543 U.S. 405, 411 (2005) (Souter, J. dissenting).

157. An additional offshoot of the reasonable expectation of privacy test emerged in *Kyllo v. United States*, 533 U.S. 27 (2001), where the Court held a "search" occurs where "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unavailable without physical intrusion." *Id.* at 40. Although some suggest e-mail is protected under this rule, the argument fails for two reasons. *See* Lowe, *supra* note 4, at 16-19. First, to argue e-mail is analogous to "details of the home" stretches the rule. Second, access to e-mail does not otherwise require "physical intrusion"; rather, e-mail content is obtained by attaching a device to a third-party ISP or IMP device, a place to which the target of surveillance has no proprietary claim. *Id.*

158. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

159. *Id.*

160. Along similar lines, a formalistic view of the internet holds that its susceptibility to hackers may also defeat reasonable expectations of privacy. *See* Lowe, *supra* note 4, at 6-7.

HRA standards are modeled after article 8 of the ECHR and are grounded in sound logic: Privacy is a valued right in a free democratic society; hence government interference therewith is permissible only to the limited extent *necessary* to maintain the existence of that very society.[161] Lest the concept of necessity be manipulated, article 8 circumscribes its use by providing an exhaustive list of interests which alone render surveillance "necessary."[162] In spite of this deliberate limitation, several questions persist. How necessary is necessary? What exactly *is* national security? These questions create a vacuum of uncertainty vulnerable to exploitation at the hands of an overzealous government.

Against the statutory backdrop of RIPA, most government surveillance has a basis in law. Therefore, "the crux of a case will often be the proportionality of the action."[163] Proportionality determinations require consideration of necessity, underlying interests (most notably national security), and oversight. The Strasbourg Court interprets necessity to mean more than "ordinary, useful, reasonable or desirable" but less than "indispensable,"[164] and further requires that it address a "pressing social need."[165] In addressing government access to postal mail, the Court elaborated that "secret surveillance" is tolerable "only insofar as *strictly* necessary for safeguarding democratic institutions."[166] Beyond this generalized language, the Court offers little guidance for domestic courts charged with reviewing surveillance applications.[167]

Defining the subjects that justify surveillance is a difficult task in its own right. The broadest interest is national security. "When placed against counterterrorist claims, [it] provides a

161. ECHR, *supra* note 83, art. 8(2).

162. *Id.* (listing national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health or morals, and protection of rights and freedoms of others).

163. Taylor, *supra* note 88, at 89.

164. Silver v. United Kingdom, 5 Eur. Ct. H.R. 347, 376 (1983).

165. Taylor, *supra* note 88, at 88.

166. Klass v. Federal Republic of Germany, 2 Eur. Ct. H.R. 214, 231 (1978) (emphasis added).

167. One scholar posits that where there exists a less restrictive alternative, "[i]t is unlikely that a measure could be considered to be proportionate." Taylor, *supra* note 88, at 88. Although appealing in its simplicity, the argument ignores the difficulty of proving the existence of a less restrictive alternative.

loophole that can be exploited by the state," because "what constitutes a national security concern can be molded to fit the moment."[168] This creates fear that claims of national security may someday provide carte blanche for over-aggressive regimes to justify surveillance. In spite of this apprehension, the Strasbourg Court has yet to provide a concrete definition, instead holding that for a system of surveillance justified on national security grounds to be compatible with article 8, the domestic law should "indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."[169] Nevertheless it is unfair to hold the Court accountable for this problem. To define what constitutes an amorphous concept like national security, much less those things that may somehow threaten it, is beyond the reach of a simple, easily applied judicial standard. Furthermore, those quick to allege judicial complicity in executive excesses ignore the hindsight bias to which they too are susceptible: Just as uncovering inculpatory evidence suggests that a search was justified, the failure to do so tends to the conclusion that it was not.

Strasbourg Court decisions with respect to oversight also lack clear rules. The Court has stressed that because "judicial control offer[s] the best guarantee of independence, impartiality and a proper procedure" it is "desirable to entrust [ex ante] supervisory control to a judge";[170] yet it has neglected to require it. The Court instead holds that supervision need only "normally" be vested in the judiciary.[171] The lone mandate is that lower courts examine the "grounds required for ordering [surveillance], the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by national law."[172]

---

168. Donohue, *supra* note 10, at 1155. Indeed, some legal scholars have claimed that national security admits cases ranging from terrorism to drug trafficking. *See, e.g.*, Solove, *Electronic Surveillance*, *supra* note 7, at 1301-02.

169. Rotaru v. Romania, 8 B.H.R.C. 449, ¶ 61 (Eur. Ct. H.R. 2000); *see also id.* at 472 (Wildehaber, J., concurring) ("States do not enjoy unlimited discretion . . . national security must be balanced.").

170. Klass, 2 Eur. Ct. H.R. at 235.

171. Rotaru, 8 B.H.R.C. 449, ¶ 59 ("[J]udicial control affords the best guarantees of independence, impartiality and a proper procedure.").

172. Klass, 2 Eur. Ct. H.R. at 233.

To blame the Court for the lack of definite instructions is inappropriate. As a multinational tribunal it must respect a divergent set of domestic norms regarding internationally recognized rights.[173] To this end, under a practice known as "the margin of appreciation," the ECtHR "grants varying degrees of deference to the national authorities' evaluation of how [an internationally agreed-upon] right applies in particular circumstances."[174]

Looking past the Strasbourg Court, domestic British application of existing standards via the HRA suffers in its own right. Due to British adherence to a system of parliamentary superiority, the HRA "requires only that legislation be read as far as possible in a manner compatible with the ECHR."[175] Where courts find that a practice runs afoul of the ECHR, they may only render a "declaration of incompatibility."[176] Powerless to strike legislation, British courts cannot correct problems directly and are instead limited to signaling the issue and trusting in Parliament. This limitation hampers the already difficult application of ECHR standards and casts doubt upon whether the British regime meets the article 13 requirement of a right to "an effective remedy before a national authority."[177]

C. *Failings of Oversight*

Most concede that some measure of government access to e-mail is necessary. However, because even innocuous powers may grow oppressive absent external checks, most also agree that there must be "safeguards in place to restrict potential abuse."[178] This is best achieved via ex ante judicial protection. Ex ante protection avoids many of the failings of ex post or internal protection: judgments are not clouded by the fruits of surveillance already conducted, or an overriding responsi-

---

173. Anthony J. Colangelo, *The New Universal Jurisdiction: In Abstentia Signaling Over Clearly Defined Crimes*, 36 GEO. J. INT'L L. 537, 545 n.21 (2005).

174. *Id.* (quoting Gerald L. Neuman, *The United States Constitution and International Law: The Uses of International Law in Constitutional Interpretation*, 98 AM. J. INT'L. L. 82, 87 n.29 (2004)).

175. Donohue, *supra* note 10, at 1155.

176. *Id.*

177. ECHR, *supra* note 83, art. 13.

178. Natasha Jarvie, *Control of Cybercrime—Is an End to Our Privacy on the Internet a Price Worth Paying?: Part 2*, 9 COMPUTER & TELECOMM. L. REV. 110, 114 (2003) (U.K.).

bility to catch criminals or to protect the country from terrorism. Unfortunately, American and British systems of oversight each suffer from a variety of shortcomings.

Ex ante judicial review "respect[s] . . . individual rights and the separation of powers," and is therefore the highest form of oversight.[179] Yet it is completely lacking in the United Kingdom, and absent in the United States where the Protect America Act alters FISA. Ex ante review in the United Kingdom relies entirely on a Home Secretary at once charged with enforcing the law and judging surveillance applications. The United Kingdom omits ex ante judicial oversight based on the belief that, "judges [are] inappropriate because of the need for an executive officer to deal with cases of national security and economic well-being."[180] Although a Tribunal exists to hear claims of abuse ex post, overall the system "prescribes far less judicial involvement than in most other European countries."[181] The British regime relies upon the belief that the Home Secretary is capable of disinterested review of surveillance applications. But executive agents like the Home Secretary have a duty "to enforce the laws, to investigate, and to prosecute" and therefore "should not be the sole judges of when to utilize constitutionally sensitive means."[182] For similar reasons, critics bemoan the Protect America Act amendments to FISA, which permit warrantless surveillance when the government believes the target is outside the United States and foreign intelligence is a significant purpose.[183] According to

179. Akdeniz, *supra* note 76, at 78. Separation of powers was once a distinctly American value but has since been recognized by the ECtHR. Roger Masterman, *Taking the Strasbourg Jurisprudence Into Account: Developing a "Municipal Law of Human Rights" Under the Human Rights Act*, 54 INT'L & COMP. L. Q. 907, 927 (2005) (U.K.) ("[S]eparation of powers has attained a certain prominence in the case law of the Strasbourg Court."). Although Britain still adheres to Parliamentary sovereignty, the independence of its judiciary remains a constitutional principle. Mads Andenas, *A European Perspective on Judicial Independence and Accountability*, 41 INT'L L. 1, 15 (2007).

180. Akendiz, *supra* note 76, at 78.

181. Andrew Ashworth & Michelle Strange, *Criminal Law and Human Rights in 2002*, 2 EUR. HUM. RTS. L. REV. 139, 141 (2002) (U.K.).

182. Donohue, *supra* note 10, at 1079 (quoting United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 317 (1972)).

183. *See supra* notes 37-38 and accompanying text.

one privacy advocate, the Protect America Act "turned the court into a spectator."[184]

When aggrieved parties seek judicial review, the American and British systems demonstrate that the value of judicial review is compromised by secrecy—a factor that plagues both the FISC and the Tribunal.[185] Proponents of secrecy defend it by reference to security, asserting that "[i]t would greatly aid the operation of agencies hostile to the state if they were able to estimate even approximately the extent of [e-mail] interceptions."[186] Others respond that the lack of transparency hinders creation of a factual record necessary to challenge surveillance in court and, moreover, provokes fear that behind closed doors courts are rubber-stamping executive excess.[187] The relevant statistics do little to quell such fears: From 1979 to 2003 the FISC denied but 3 of 16,450 FISA applications,[188] and as of 2003 the Tribunal had yet to uphold a single complaint.[189] These numbers suggest systemic failure, yet governments answer that they merely indicate that the standards are self-enforced.[190] In other words, "an application that would not pass muster would simply be stopped before reaching the court."[191] Self-enforcement is an unsatisfactory explanation in the face of overwhelming statistics; it implies that the executive's self-enforcement is near perfect. Belief in perfection is hard to credit in systems that anticipate error by specifically providing for judicial oversight in the first place.

Ex post judicial review is compromised by hindsight bias.[192] Strict reliance on ex post approaches presupposes that judges charged with determining the sufficiency of original

---

184. James Risen & Eric Lichtblau, *Concerns Raised on Wider Spying Under New Law*, N.Y. TIMES, Aug. 19, 2007, at A1 (quoting the Executive Director of the Electronic Privacy Information Center, Marc Rotenberg).

185. *See* Richard Norton-Taylor, *The Watchdogs*, THE GUARDIAN (London), Sept. 14, 2002 (U.K.); 50 U.S.C. § 1801; SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 289.

186. Donohue, *supra* note 10, at 1170.

187. Ferguson, *supra* note 94, at 106.

188. Donohue, *supra* note 10, at 1097.

189. Ferguson, *supra* note 94, at 106.

190. Donohue, *supra* note 10, at 1097.

191. *Id.*

192. "[I]t may well be easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results." Ferguson, *supra* note 94, at 105.

search justifications are capable of ignoring potentially inculpatory evidence since uncovered. As with the notion of a disinterested Home Secretary, this appears at odds with human nature.[193]

The delay or outright denial of notice to search targets minimizes the efficacy of judicial review. Without notice, "the majority of interferences with privacy will be undetected," and most will only learn that they were surveillance targets if criminal charges follow.[194] By implication, the true extent of surveillance (and any abuse) remains unknown.[195] Untimely notice also compromises the value of judicial review because the court will be privy to the fruits of a search already conducted and thus susceptible to hindsight bias. In the United Kingdom, the Home Secretary never gives notification,[196] and delayed notice is fast growing in the United States through the use of "sneak and peek" warrants.[197] Gauging the scope of surveillance in the United Kingdom is further frustrated by nonresponsive Tribunal decisions which "simply state whether the determination is favourable . . . thus, not necessarily revealing [if] there has been any interception or its details."[198]

---

193. Formal recognition of this fact is found in the United States Federal Rules of Evidence (the "Rules"). Under the Rules, courts may exclude otherwise relevant evidence for fear that "its probative value is substantially outweighed by the danger of unfair prejudice." FED. R. EVID. 403. Although courts may instruct juries to only consider evidence for a relevant purpose and to ignore its prejudicial components, the Rules acknowledge that limiting instructions are generally insufficient for highly prejudicial information like prior criminality. FED. R. EVID. 105, 609. If judges, like juries, are susceptible to such failings of human nature, the risk of ex post review is apparent: Judges cannot be trusted to limit their consideration to ex ante justifications for a search when they are at the same time privy to its fruits.

194. Ferguson, *supra* note 94, at 106.

195. Akdeniz, *supra* note 76, at 79. In the United Kingdom, 1,314 authorizations were granted in 2001, while but 102 claims were brought before the Tribunal from October 2, 2000 to December 31, 2001. Ferguson, *supra* note 94, at 106 n.35.

196. Taylor, *supra* note 88, at 93. Taylor argues that lack of notice necessitates heightened requirements for oversight as the lack of notice "decreases substantially the chances of abuse ever being uncovered, and therefore the system of authorization, accountability, and review must be particularly robust." *Id.*

197. SOLOVE, INFORMATION PRIVACY, *supra* note 7, at 295.

198. Akdeniz, *supra* note 76, at 90.

Independent monitors such as the Interception of Communications Commissioner are prone to hindsight bias and also suffer from distinct shortcomings due to their generalized function. Their general charge allows them to uncover and address (through recommendations to Parliament) systemic defects more easily, unlike courts, which are limited to case-by-case review. The converse is that monitors lack authority to remedy any specific abuses they uncover.[199] Above all, commentators characterize monitors as helpless because there are too many authorizations to oversee, such that "not all authorisations are subject to scrutiny; only those selected at random."[200] In sum, the government's power to withhold notice precludes targets from seeking judicial review, and the result is that many authorizations are never held "to any form of independent scrutiny."[201]

D. *Problematic Expansions of Power in Response to Terrorism*

Legislatures in the United States and the United Kingdom responded swiftly to the terrorist attacks of September 11, 2001. Six weeks after the Twin Towers fell, the USA PATRIOT Act (the "Patriot Act")[202] became law; shortly thereafter, the United Kingdom followed with the Anti-Terrorism, Crime, and Security Act (ATCSA).[203] The laws betrayed a belief that fighting terror required not only improved enforcement of existing surveillance laws but also their expansion. Through the Patriot Act and ATCSA, Congress and Parliament intended to change the rules for the war on terror.[204] Though expansion

---

199. Regulation of Investigatory Powers Act (RIPA), 2000, c. 29, § 57. (Eng.).

200. Ferguson, *supra* note 94, at 105.

201. *Id.*

202. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the U.S.C.).

203. Anti-Terrorism, Crime and Security Act (ATCSA), 2001, c. 24 (Eng.).

204. According to some, differing treatment is permissible. The *Katz* Court acknowledged that national security *is* different. Katz v. United States, 389 U.S. 347, 389 n.23 (1967) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."); *see also id.* at 363 (White, J., concurring) ("[T]oday's decision does not reach national security cases."). Richard Posner argues for a sliding

was made in the name of national security and counter-terrorism, it was not long before commentators realized that the windfall of newly approved surveillance measures extended to agencies responsible for general law enforcement.[205] The extension of counter-terrorism measures into the realm of general crime prevention signaled problems regarding the proportionality of the legislative response.

The Patriot Act dramatically increased the government's ability to monitor e-mail. Before the act, a "wall" separated those responsible for law enforcement from those responsible for intelligence gathering. The Patriot Act blurred the line by expanding FISA to include cases in which foreign intelligence gathering was "*a*" significant purpose (as opposed to "*the*" purpose).[206] Law enforcement officials have responded by diverting applications to the FISC where a less demanding standard of review applies, a trend which stands to obviate the ECPA—thereby reducing transparency and increasing fears of executive abuse.[207] This trend is likely to continue following the passage of the Protect America Act amendments to FISA, which eliminate ex ante judicial review altogether when the govern-

---

scale approach which permits express consideration of national security. RICHARD POSNER, LAW, PRAGMATISM, AND DEMOCRACY 303 (2003). Under Posner's reading, the Fourth Amendment's use of "'unreasonable' . . . invites a wide-ranging comparison between the benefits and costs of a search or seizure." *Id.*

205. *See, e.g.*, Jack M. Balkin, *The Process of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 530 (2006) (noting that the Patriot Act "contained a list of reforms that law enforcement officials had sought for some time, but which had been held back by a combination of legislative inertia and concerns over civil liberties"); Emmerson, *supra* note 91, ¶¶ 3-4 (stating that ATCSA's compulsory data retention was premised on national security, but would later enable government access for far lesser concerns).

206. *See* Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-11 (2006). Patriot Act amendments to FISA destroyed the "wall" between foreign intelligence and law enforcement and have led many to question its constitutionality. *See, e.g.*, Donohue, *supra* note 10, at 1104. "The way FISA previously withstood challenge was, precisely, the purpose for which it was directed [foreign intelligence]; this purpose allowed it to fall outside the warrant requirements of the Fourth Amendment. By eviscerating purpose from the equation, the appeals court eliminated the basis on which the statute passed constitutional muster." *Id.* at 1104-05 (discussing In re Sealed Case, 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev. 2002) (upholding the change)).

207. Donohue, *supra* note 10, at 1105.

ment believes a target is outside the United States.[208] As with the Patriot Act amendments, the Protect America Act produces an even greater incentive for law enforcement to justify surveillance under FISA. The Patriot Act also makes delayed notice ("sneak and peek") warrants available if there is "reasonable cause to believe that notice may cause an adverse result."[209] Denied timely notice, targets cannot challenge government access to e-mail ex ante. This allows the government to uncover inculpatory evidence in the interim, which may later tip the scales (via hindsight bias) during ex post review. This heightens the risk of judicial acceptance of otherwise unseemly investigative acts.

In response to this critique, the government contends that increased powers are necessary in the Internet Age. Addressing Congress, then-Attorney General John Ashcroft declared: "[T]hose who scare peace-loving people with phantoms of lost liberty . . . aid terrorists, for they erode our national unity and diminish our resolve . . . giv[ing] ammunition to America's enemies, and pause to America's friends."[210] Under this interpretation, "the digital environment is perceived as threatening national security and as an arena that must be governed."[211]

In the United Kingdom, ATCSA similarly broadened the scope of permissible action in the name of national security. Most important, the Act requires mandatory envelope data retention by ISPs and IMPs for a period set by the Home Secretary.[212] As one human rights organization found, "placing [ ] the onus on [ISPs and IMPs] to say no to such requests is likely

208. *See supra* notes 37-38 and accompanying text.

209. Donohue, *supra* note 10, at 1107-08.

210. *DOJ Oversight: Preserving Our Freedoms While Defending Against Terrorism: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 316 (2001) (statement of of John Ashcroft, Att'y Gen. of the United States), *available at* http://judiciary.senate.gov/testimony.cfm?id=121&wit_id=42.

211. Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, ¶ 37 (2003), http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf.

212. Anti-Terrorism, Crime and Security Act (ATCSA), 2001, c. 24, §§ 102, 104 (Eng.).

to result in disclosure constituting a disproportionate interference with privacy rights."[213]

Although national security justifies expanded retention under ATCSA, later use of retained information is not so limited. Through RIPA, the government can access data retained pursuant to ATCSA for collateral public purposes which have no connection (direct or indirect) with national security.[214] Specifically, RIPA permits access to this data in the interest of, among others, "economic well-being," "public safety," "public health," and tax collection.[215] Access in the name of such lesser interests skews proportionality analysis and, according to the Information Commissioner,[216] may constitute a violation of proportionality under article 8 of the ECHR.[217] While expansion of the law "occurred in the name of counter-terrorism, the measures deployed often go much further into addressing areas of more general criminality."[218]

The British government responds that privacy, while valued, is not an absolute right. "In the same way our freedom is balanced against society's rules, our privacy has to be balanced against the needs of society for preventing and detecting crime."[219] That privacy interests must be balanced is but a truism. The question of *how* privacy is to be balanced is what sparks debate. The answer of the British government fails to address the underlying concern: that allowances made for ter-

---

213. INTERNATIONAL HELSINKI FEDERATION FOR HUMAN RIGHTS, ANTI-TERRORISM MEASURES, SECURITY AND HUMAN RIGHTS: DEVELOPMENTS IN EUROPE, CENTRAL ASIA, AND NORTH AMERICA IN THE AFTERMATH OF SEPTEMBER 11, at 203 (2003), *available at* http://www.ihf-hr.org/viewbinary/viewdocument.php?doc_id=6426.

214. Emmerson, *supra* note 91, ¶ 5; RIPA § 22.

215. *Id.*

216. The Information Commissioner reports directly to Parliament and is responsible for monitoring personal privacy. *See* Ferguson, *supra* note 94, at 105; Akdeniz, *supra* note 76, at 89.

217. Stuart Millar, *Snooping Laws May Be Illegal*, THE GUARDIAN (Manchester, UK), July 31, 2002, at 2 (quoting David Smith, Assistant Information Commissioner); *see also* Emmerson, *supra* note 91, ¶ 16.

218. Birnhack & Elkin-Koren, *supra* note 211, ¶ 93.

219. HOME OFFICE, ACCESS TO COMMUNICATION DATA: RESPECTING PRIVACY AND PROTECTING THE PUBLIC FROM CRIME 30 (2003), *available at* http://www.homeoffice.gov.uk/documents/comms-data-2003/consult2003.pdf?view=Binary.

rorism under ATCSA are spreading to general law enforcement.

E. *Lessons Learned and the Harm to Privacy*

Although far from exhaustive, the preceding critique underscores several major flaws in the protection of privacy in the United States and the United Kingdom. Formalistic rules may become arbitrary, while amorphous ones may be exploited. A successful regime must therefore clearly circumscribe surveillance power yet account for the unique nature of e-mail so that rules are not arbitrary in practice. Effective judicial oversight necessitates involvement by non-secretive general courts both before and after the fact. To ensure abuses are detected, the regime must require the government to notify surveillance targets. Finally, the regime must confine allowances for national security, lest restrictions applicable to general law enforcement become meaningless.

When examining current surveillance regimes in light of an expanded notion of privacy, it is difficult to ignore the harms they impose. On an individual level, the government violates personal privacy interests when accessing someone's e-mail without adequate justification. On the societal level, governmental surveillance has the potential to exact a far greater toll: It may stunt free psychological development, chill the exercise of free speech, and therefore undercut factors central to the maintenance of a truly democratic society.

VI. The Model Regime

Equipped with an understanding of the basic flaws of the American and British regimes and a broadened conception of privacy, this Note proposes a Model Regime. The goal is to provide an example of a regime which improves upon existing protections by expressly recognizing both the individual and societal interests in privacy.

A. *General Policy Considerations for the Model Regime*

To the extent that American and British regimes are premised on an incomplete conception of privacy interests, those regimes risk being non-responsive to a variety of problems posed by e-mail surveillance. For the purpose of crafting a Model Regime, I address this weakness by reexamining gen-

eral policy considerations in light of an expanded conception of privacy.

1. *Crime Prevention, Detection, and Counter-Terrorism*

The proper scope of e-mail surveillance requires a balance of two factors: efficacy and intrusiveness. Those arguing in favor of surveillance emphasize its necessity and downplay its toll on privacy, while those stressing privacy contend that surveillance is both easily abused by the government and easily avoided by knowledgeable criminals.

Those defending governmental surveillance power assert that "new technologies present powerful new tools for criminals," such that the law must respond by placing government on equal footing.[220] They contend that surveillance powers must increase in tandem with criminal advancements in technology.[221] Where technology substantially increases the threat of an underlying crime, some advocate increases in government power that outstrip criminal advancements. They argue that "technological advances in communication" like e-mail facilitate diffusion of terrorist cells and thereby intensify preexisting threats.[222] Others add that the prevalence of potential hackers on the internet decreases the public's expectations of privacy. They question: "Why should the government be barred from reading your email also?"[223]

Privacy advocates argue that e-mail surveillance poses too great a social cost to warrant expansion. As even the targeted interception of envelope data requires access to an entire ISP or IMP server, privacy advocates fear that little prevents rampant abuse of power.[224] What is more, many dispute the utility

220. *Being Watched*, ECONOMIST (London), Aug. 26, 2000, at 47.

221. Merl, *supra* note 4, at 258-59.

222. *See* Dunham, *supra* note 6, at 546; *see also* Merl, *supra* note 4, at 253 (quoting then-CIA Director George Tenet's testimony before Congress that use of internet information technology by terrorist groups posed a significant threat to national security).

223. Lowe, *supra* note 4, at 7; *see also* Manton M. Grier, Comment, *The Software Formerly Known as "Carnivore": When Does Email Surveillance Encroach Upon a Reasonable Expectation of Privacy?*, 52 S.C. L. REV. 875, 890-91 (2001).

224. Barry Steinhardt, *Cage Carnivore / Clinton Needs to Act to Tame FBI E-Mail Surveillance*, S.F. CHRON., July 21, 2000, at A21, *available at* http://www.commondreams.org/views/072100-104.htm (explaining that the use of a packet sniffer "is like the telephone company being forced to give the FBI

of surveillance on the grounds that its success is so easily frustrated: "Setting up new internet accounts and email addresses . . . takes barely a minute to do, yet can limit or defeat . . . intelligence targeting."[225]

Arguments for a diminished expectation of privacy seemingly balance out those asserting the futility of e-mail surveillance, and data tending to support or refute either argument simply do not exist. Resolution thus requires a theoretical weighing of the normative interests at play—privacy and need for surveillance.[226] Balancing the two, it follows that the degree of e-mail surveillance permitted should be directly proportional to its efficacy and inversely proportional to its intrusiveness. The power must also be sufficiently defined so as to signal norms and expectations to the government and public alike. Failing this, it is impossible to know the bounds of acceptable surveillance and monitor its use.

2. *The Specter of "Invisible Omniscience"*[227] *as a Threat to Democracy*

Concern about privacy is at root political. The mere perception that one is without privacy exacts a social cost: Under constant supervision, opposition to government is chilled for fear of reproach. Privacy is thus both a means and an end in a free democratic society.

Jeremy Bentham utilized the power of "apparent omnipresence" in creating his ideal prison, the Panopticon.[228] In the prison, inmates are isolated from one another in individual cells, each in constant view of a central tower privy to their every action.[229] In this setting, "knowing that one *could* be ob-

---

access to all the calls on its network when it only has permission to seek the calls for one subscriber").

225. Campbell, *supra* note 15; *see also* Grier, *supra* note 223, at 890-91.

226. Prominent privacy interests at the individual and societal level are set out earlier. *See supra* notes 102-105, 124 and accompanying text. A proper balance would consider these alongside government interests in e-mail surveillance such as national security, law enforcement, and crime prevention. *See* Cinquegrana, *supra* note 8, at 818.

227. This term, attributable to no single author, is commonly used to describe the mode of surveillance addressed in Bentham, Orwell, and the like.

228. Jeremy Bentham, The Panopticon Writings 45 (Miran Božovič ed., Verso 1995) (1787).

229. *Id.* at 33-48.

served, a prisoner would behave in accordance with the expected norm."[230] George Orwell expanded upon this concept in his nightmarish world of Big Brother, where one lived "in the assumption that every sound you made was overheard, and . . . every moment scrutinized."[231] For Orwell and Bentham, "continual surveillance" resulted in "conformity and discipline."[232] This follows because "openness to new . . . and unconventional ideas, requires . . . an atmosphere where [one] is not being evaluated, not being measured by some external standard."[233] Whether real *or* imagined, surveillance "constrain[s], *ex ante*, the acceptable spectrum of belief and behavior."[234] This is troubling to the extent that free speech and the exchange of ideas ensure preservation of a democratic state.[235]

Fear of e-mail surveillance may chill free exchange of information over the internet, the very purpose for which the internet was created.[236] If one justifies surveillance on the grounds of law enforcement and national security—interests which themselves uphold and maintain a stable democracy—the irony is even more pronounced. Government interests in surveillance are not trump cards; they must be balanced with interests in privacy which, although at times in tension with surveillance, likewise support democracy and therefore merit protection.[237]

---

230. Nehf, *supra* note 118, at 11 (emphasis in original).

231. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 4 (1949).

232. Nehf, *supra* note 118, at 12.

233. BLOUSTEIN, *supra* note 118, at 158.

234. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

235. This relation is both recognized and valued in the United States and the United Kingdom by the protection free speech receives. *See* U.S. CONST. amend. I; Human Rights Act (HRA), 1998, c. 42, sched. 1, art. 10 (Eng.); *see also* ECHR, *supra* note 83, art. 10.

236. Grier, *supra* note 223, at 892.

237. *See* Joyce W. Luk, Note, *Identifying Terrorists: Privacy Rights in the US and U.K.*, 25 HASTINGS INT'L & COMP. L. REV. 223, 234 (2002) (indicating that privacy preserves the "marketplace of ideals" which "gives rise to a free society").

3. *The Lure of Invisible Power:* Quis Custodiet Ipsos Custodes?

Transparency encourages self-restrained use of power.[238] Scholars have long recognized that invisible power defies extrinsic limitation and tempts abuse. In Plato's *Republic*, Glaucon tells of a humble shepherd who, upon discovering a ring of invisibility, commits adultery, kills his king, and steals the throne.[239] The moral is simple: Invisible deeds go unpunished, and where evil is unpunished, nothing separates the just man from the unjust. Centuries later, fear of such abuse led the Roman satirist Juvenal to question: *quis custodiet ipsos custodes*, or who watches the watchers?[240]

Without considerable oversight, e-mail surveillance may function like the power of invisibility. Even if the government uses the power only for legitimate interests, the risk endures because "[e]xperience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent."[241] While one instinctively "repel[s] invasion" by known enemies, "[t]he greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[242]

The risk of over-expansive surveillance is seldom greater than in the realm of national security. Here, "[t]he veil drawn over access to . . . information may become an impenetrable wall, with the Judiciary—or the Legislature—loath to second-guess those responsible for ensuring national security,"[243] leaving no one to audit the use of such power.[244] A Model Regime

---

238. Dawn E. Johnsen, *Functional Departmentalism and Nonjudicial Interpretation: Who Determines Constitutional Meaning?*, 67 LAW & CONTEMP. PROBS. 105, 115 (2004) ("The effectiveness of. . .principled self-restraint and external political checks in turn depends heavily on the traditional values of transparency and accountability.").

239. PLATO, THE REPUBLIC, Book II at 359b-360e (Allan Bloom trans., 2d ed. 1991).

240. JUVENAL, SATIRE VI 347-48, *available at* http://www.thelatinlibrary.com/juvenal/6.shtml.

241. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

242. *Id.*

243. Donohue, *supra* note 10, at 1193.

244. Dunham, *supra* note 6, at 562 (noting that the "simple click of a mouse (whether intentional or unintentional) changes . . . configuration settings from [trap-and-trace] collection to a full collection").

must therefore maintain a transparent system for the review of surveillance applications in order to avoid the dangers of blind deference. Where sensitive tools are at issue, there is no room for trust.

B. *Specific Recommendations*

To improve upon the American and British regimes, a Model Regime must create more robust standards for judicial review of e-mail surveillance and increase the consistency in which it is conducted. A new regime must balance competing *societal* interests in privacy and surveillance in order to facilitate appropriate policy choices. It must also explicitly state the privacy interests it aims to protect. Doing so tethers the regime to a static conception of privacy and avoids unforeseen changes in the law due to evolving expectations of privacy.

1. *Judicial Review of E-mail Surveillance*

Successful oversight requires improved judicial review of e-mail surveillance, which in turn requires that Congress strengthen statutory protections to enhance constitutional review of privacy rights. Detailed, narrowly defined statutes avoid manipulation, give notice, and provide guidelines for decision-making by courts. In addition, courts could strengthen judicial review by reconsidering Fourth Amendment doctrine to recognize e-mail as *sui generis* rather than relying on imperfect analogies to older technologies. A Model Regime should follow the current American statutory framework in applying differing standards based upon the intrusiveness of requested surveillance.[245] Added to these standards would be an overriding proportionality requirement borrowed from the ECHR.[246] Proportionality offers an additional ground for judicial review and combats exploitation of formal rules. Slightly relaxed standards would apply to national security applications; however, the regime would not permit law enforcement to invoke national security interests, following the pattern of the pre-Pa-

245. That is, differing standards for trap/trace, access to stored communication, and real time interception as under the ECPA. *See supra* notes 22-32 and accompanying text.

246. *See supra* notes 74-77 and accompanying text.

triot Act FISA "wall."[247] Finally, exclusionary remedies would be available for *all* statutory violations to encourage strict compliance with the regime.[248]

Under a Model Regime, courts should abandon efforts to examine e-mail under outdated constitutional standards. Treating e-mail as postal mail ignores the unique potential it presents for surveillance. Treating e-mail in abstract technological terms likewise disregards its place in the modern world and potentially destroys claims to privacy because of an unavoidable—though somehow "voluntary"—transfer through third-party servers.[249] E-mail demands *sui generis* treatment which allows courts to locate a middle ground between monolithic "all-or-nothing" Fourth Amendment formalism and the amorphous, easily manipulated standards of the ECHR.[250]

2. *Improved Oversight*

The furtive nature of e-mail surveillance contributes to the threat of abuse.[251] Whether realized or not, this threat may harm the public by causing anxiety.[252] To allay public fears, a Model Regime would utilize ex ante and ex post judicial review in addition to a non-executive government surveillance monitor.

To increase transparency and mitigate fears of rubber-stamping, general courts of law rather than secretive bodies like the FISC and Tribunal should review surveillance applications.[253] Legislatures should ensure ex ante judicial oversight

---

247. This is achieved by requiring that foreign intelligence is *the* purpose of the surveillance as opposed to one among several. *See supra* notes 33, 206-207 and accompanying text.

248. A blanket exclusionary remedy for all statutory violations stands in contrast to the existing American regime under the ECPA where the remedy is unavailable for illegal e-mail surveillance. 18 U.S.C. § 2518(10)(a).

249. *See supra* notes 54-55 and 144-153 and accompanying text.

250. Amsterdam, *supra* note 118, at 388. The proper mode of constitutional interpretation raises questions with respect to the proper role of the judiciary which merit extensive treatment in their own right. Formalism suggests the judiciary as passive law-giver, whereas ambiguous standards promote an image of the court as law-maker.

251. *See supra* Part VI.A.3.

252. *See supra* Part VI.A.2.

253. Though executive representatives deride efforts at transparency as counter-productive, if one assumes a preference towards deterrence, it is wise to make the breadth of existing capabilities public. Transparency would

by requiring judicial authorization for all surveillance applications[254] and ex post judicial oversight by granting courts jurisdiction over claims brought by aggrieved targets.[255] So as not to obviate the role of ex post review, the regime must require timely notice to targets following the completion of surveillance.[256] Prima facie evidence of infringement upon individual privacy rights should shift the burden to the government to justify the intrusion,[257] and where an individual succeeds in his or her claim, evidentiary exclusion and/or financial redress should follow.[258]

A non-executive government monitor[259] or watchdog would provide a second layer of oversight in the Model Regime. Its operation would follow that of a corporate internal audit committee. Like internal audit committees review confidential financial information to assure compliance with reporting guidelines, a non-executive monitor would be privy to confidential surveillance to assure compliance with existing privacy protections.[260] Despite close interaction, monitors, akin to audit committees, would remain independent and consist of non-agency personnel so as to prevent conflicts of inter-

---

also assuage fears of abuse, increase the acceptance of existing power, and perhaps instill a willingness to confer additional power if/when necessary.

254. *See supra* notes 17-32 and accompanying text (discussing the ECPA and requirements for judicial authorization).

255. *See supra* notes 68-69 and accompanying text (discussing § 1983 actions and the exclusionary rule regarding illegally obtained evidence).

256. The importance of notice cannot be overstated as it is the lynchpin of citizen-initiated oversight.

257. Compelled justification is inspired by the ECHR which requires that all government intrusions with privacy be necessary and proportionate to the particularized government interest at stake. *See supra* notes 74-77 and accompanying text.

258. Exclusion and redress borrow largely from the American model. *See* 42 U.S.C. § 1983 (civil action for deprivation of rights under color of law); 18 U.S.C. § 2518(10)(a) (statutory suppression of evidence obtained through illegal wiretap).

259. Discussion of the specific composition and practical function of such a monitor could fill an entire note. For the moment, it is sufficient to conceive of the monitor as a government entity, separate and apart from the executive branch and beholden to distinct interests (i.e., legislative oversight and privacy concerns as opposed to law enforcement and national security), that is nonetheless exposed to the inner workings of executive surveillance actions.

260. *See* Jody K. Upham, *Audit Committees: The Policemen of Corporate Responsibility*, 39 TEX. J. BUS. L. 537, 538 (2004).

est.[261] Monitors should also make recommendations to the legislature (thereby influencing surveillance legislation).[262] Finally, the regime should grant monitors standing to sue *parens patriae* to enjoin proposed actions that may offend privacy protections.[263]

3. *Emergency and National Security Exceptions*

The ability to easily circumvent statutory safeguards on the basis of emergency or national security obviates their protective role. In the United States, the Patriot Act's amendments to FISA eliminated its hitherto narrowly circumscribed applicability, allowing those seeking surveillance an end run around the generally applicable and more rigorous standards of the ECPA.[264] In the United Kingdom, ATCSA has expanded the pool of information from which surveillance under RIPA may draw.[265] The fear of just such outcomes has historically prevented judicial acceptance of general emergency power for fear that "emergency powers would tend to kindle emergencies."[266] Said one commentator: " 'The history of liberty has largely been the history of observance of procedural safeguards.' And the history of the destruction of liberty . . . has largely been the history of the relaxation of those safeguards in the face of plausible sounding governmental claims."[267] In recognition of these fears, a Model Regime should not permit emergency powers, but should instead dif-

---

261. *See id.*

262. *See supra* notes 97-98 and 216 and accompanying text.

263. Federal antitrust law provides an example of *parens patriae* standing. In this context, Congress granted State Attorneys General the authority to sue on behalf of their residents in cases that would be difficult, if not impossible, to assert individually. 15 U.S.C. § 15c (2006). This form of standing may also be seen in § 301 of the Voting Rights Act and Title VII of the Civil Rights Act. RICHARD H. FALLON, JR. ET. AL., HART & WECHSLER'S THE FEDERAL COURTS AND THE FEDERAL SYSTEM 154 (5th ed. 2003) ("Congress has often given . . . federal officials power to bring suit for the purpose of enforcing laws. . . .").

264. *See supra* Part V.D.

265. *See supra* notes 212-218 and accompanying text.

266. *See, e.g.*, Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 650 (1952) (Jackson, J., concurring).

267. Amsterdam, *supra* note 118, at 354 (quoting in part McNabb v. United States, 318 U.S. 332, 347 (1943)).

ferentiate between national security and law enforcement surveillance.

The Model Regime would impose a rigid distinction between national security surveillance and general law enforcement akin to the pre-Patriot Act "wall."[268] The regime would limit any relaxation of standards to cases in which *the* primary objective is national security surveillance or foreign intelligence gathering, thus limiting pretextual surveillance applications.[269] This affords adequate surveillance powers to those charged with safeguarding the country at large, while combating the unwanted spillover of power to those responsible for enforcing the criminal law.

4. *Applicability of the Model Regime*

Against the backdrop of existing privacy protections in the United States and the United Kingdom, practical implementation of the Model Regime is unlikely. My goal in developing the Model Regime is to demonstrate how a society could better balance security and privacy when providing for government access to e-mail. Most importantly, an improved balance requires recognition of the dual nature of privacy and the varied interests to which it relates. Policymakers can endorse a broadened concept of privacy without jettisoning a country's statutory or constitutional underpinnings. Thus, obstacles to adopting the Model Regime are political rather than legal in nature.

VII. Conclusion: A True Balancing

E-mail surveillance poses a significant risk to privacy and, under an extremist view, represents a first step toward an Orwellian police state. Such extremist rhetoric likely exaggerates the threat and, in so doing, causes many to neglect the

268. *See supra* notes 33, 206-207 and 247 and accompanying text.

269. The original FISA requirement that intelligence gathering be *the* reason for surveillance was changed to include situations in which intelligence gathering was merely *a* significant reason for it. Donohue, *supra* note 10, at 1103. In response to the change, the "FISC expressed concern that: '[C]riminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance).'" *Id.* at 1104 (quoting in part In re All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624 (Foreign Intel. Surv. Ct. 2002)).

lesser—albeit more likely—risks posed by the mere *fear* of being watched, which inheres due to the furtive nature of e-mail surveillance. Risks of this nature are not cognizable under a limited individualized conception of privacy. Acceptance of privacy's societal component is therefore necessary. Without it, the full range of interests affected is unknown, making a true balance impossible to strike.

This Note does not intend to suggest that a true balance naturally results in increased privacy protections akin to those set out in the Model Regime. E-mail facilitates general criminality and terrorism alike, a fact which in and of itself calls for some measure of government surveillance. It is thus possible that consideration of the social interests in privacy may not dramatically alter the result of interest balancing by those in power. What may change, regardless of the outcome of this balancing, is the spirit in which e-mail surveillance is conducted.

Once the full range of interests affected by e-mail surveillance come into view, it is likely that those exercising the power will tread more lightly, and that those overseeing its operation (be it before or after the fact) will do so more stringently—thereby minimizing the negative costs of e-mail surveillance.

* * *

On February 17, 2008, shortly before this Note went to print, the Protect America Act of 2007 expired.[270] Attempts to make the Act's changes to FISA permanent have been stalled by political wrangling over the subject of telecommunications immunity.

There are nearly 40 lawsuits pending against AT&T, Verizon, and Sprint Nextel arising out of their participation in the NSA warrantless wiretapping program begun in the wake of 9/11.[271] The House of Representatives rejected a Senate bill (supported by the White House) which, in addition to making

270. *See supra* notes 37-41 and accompanying text; Carl Hulse, *House Leaves Surveillance Law to Expire*, N.Y. TIMES, Feb. 15, 2008, at A17.

271. Richard Cowan & Jeremy Pelofsky, *House Defeats Stopgap Extension of Spy Program*, REUTERS, Feb. 13, 2008, *available at* http://www.reuters.com/article/politicsNews/idUSN1335251820080213?feedType=RSS&feedName=politicsNews; *see also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Call-*

the Protect America Act's amendments to FISA permanent, grants retroactive immunity from lawsuit for these companies.[272] In its place the House has since passed a bill, denounced by supporters of the Senate bill, permanently amending FISA (though less comprehensively than the Senate-sponsored version) while denying blanket immunity.[273]

Although resolution of the immunity issue appears uncertain, the House, Senate, and White House have all demonstrated a willingness to amend FISA along the lines of the Protect America Act.[274] The problems attendant to those laws (e.g., judicial secrecy and limited ex ante oversight) are therefore likely to persist in the United States, warranting continued examination of whether we are competently balancing the need for surveillance against the dual interests in privacy.

---

ers Without Courts, N.Y. TIMES, Dec. 16, 2005, at A1 (describing NSA program).

272. Cowan & Pelofsky, *supra* note 271; FISA Amendments Act of 2007, S. 2248, 110th Cong. (2007) (returned to Senate calendar Feb. 12, 2008).

273. Eric Lichtblau, *House Votes to Reject Immunity for Phone Companies Involved in Wiretaps*, N.Y. TIMES, Mar. 15, 2008, at A14; FISA Amendments Act of 2008, H.R. 3773, 110th Cong. (2008) (House and Senate resolving differences as of Mar. 14, 2008).

274. Editorial, *Congress' First Task: FISA*, L.A. TIMES, Mar. 30, 2008, at M2.