Singapore Journal of Legal Studies
[2002] 214 - 270

ELECTRONIC SURVEILLANCE AND PRIVACY IN THE UNITED STATES AFTER SEPTEMBER 11 2001: THE USA PATRIOT ACT

MARY WS **WONG** *

Electronic surveillance by the US Government and the corresponding implications for privacy protection have come under increased public scrutiny after the terrorist attacks of September 11, 2001. The USA PATRIOT Act, passed in response to the attacks and containing sweeping changes in this area, has alarmed many civil liberties groups. This article examines the nature of these changes in light of increased concerns over national security, and attempts to articulate the arguments advanced by both the US Government and privacy advocates with respect to the need and appropriateness of the legal response to the growing threat of terrorism.

I. INTRODUCTION

On 26 October 2001, US President George W Bush signed into law the anti-terrorism statute titled Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism,[1] more commonly known as the USA PATRIOT Act (the "PATRIOT Act"). Among other things, the PATRIOT Act expands the wiretapping and electronic surveillance powers of federal law enforcement authorities, increases the information-sharing powers of investigative agencies (particularly in relation to foreign intelligence matters) and tightens government controls over money laundering activity and illegal immigration. The PATRIOT Act is a dense and complex piece of legislation, and an exhaustive analysis of its breadth is beyond the scope of this essay. Instead, the focus of this essay will be on those provisions of the Act concerning the US Government's electronic surveillance powers, which, in light of the Act's relatively easy passage through both Houses of

---

* LLB (NUS), LLM (Cantab); Senior Lecturer, Faculty of Law, National University of Singapore and Special Attorney, Morrison & Foerster LLP. I am grateful to my colleagues, Associate Professor Michael Hor and Dr Lim Chin Leng, for their encouragement, suggestions and helpful comments during the writing of this article. Any mistakes and omissions, however, remain entirely my own.

1 HR 3162, incorporating elements from several earlier anti-terrorism bills; passed by the House of Representatives on 24 October 2001 and the Senate on 25 October 2001, becoming Public Law No 107-56 upon the President's signature the following day.

Congress, illustrate the shift in legislative[2] and public thinking[3] in the United States since the terrorist attacks of September 11, as to the proper balance to be struck between national security[4] and civil liberties[5] in terms of electronic privacy protection.

The tension and interaction between certain technological developments (*eg*, in computer, communications and surveillance technology) and the appropriate legal response to such changes have been brought into very sharp focus by the PATRIOT Act. New technology is not only useful to, and used by, lawbreakers and terrorists, but law enforcement authorities have also increasingly begun to employ such technology (primarily in the form of surveillance technology) in their investigative and enforcement efforts. In this respect, the "Carnivore" suite of software programs developed and used by the US Federal Bureau of Investigation ("FBI") is of particular interest, given the alleged features of Carnivore in enhancing electronic surveillance ability.[6] This article will therefore also examine the

---

2 The vote in the House of Representatives was 356-to-66, and in the Senate the vote was 98-to-1.

3 In November 2001, in a survey conducted by National Public Radio ("NPR") News, the Kaiser Family Foundation and the Kennedy School of Government at Harvard University, a majority favoured giving law enforcement broader powers in the following areas: (1) wiretapping of telephones (69%); (2) interception of mail (57%) and email (72%); (3) examining a person's Internet activity (82%); (4) tracking credit card purchases (75%); and (5) examining banking records (79%). Interestingly, 58% of those surveyed believe they will have to give up some of their own rights and liberties, while 44% thought that such expanded authority is likely to be used on someone they know and respect (source: the NPR/Kaiser/Kennedy School Poll on Security and Civil Liberties; results and followup available online at http://www.npr.org/news/specials/civillibertiespoll/011130.poll.html) (last accessed: 5 April 2002).

4 The term "national security" is often used interchangeably with the term "domestic security". It would appear that the former term is more often used by the intelligence and law enforcement community and the latter by commentators and lawyers: see William C Banks and ME Bowman, "Executive Authority for National Security Surveillance" Am U L Rev 2 (2000). In this essay, no attempt is made to distinguish between the two terms.

5 Contrast, for example, the passage of the Privacy Act of 1974, and the Foreign Intelligence Surveillance Act of 1978; both statutes were proposed and enacted in a post-Watergate era, during which evidence of intelligence-gathering abuses by law enforcement powers and government was obtained, resulting in (among other things) a strict division of the powers of the FBI, between its largely domestic law enforcement function (in terms of detecting and solving crimes) and its intelligence-gathering function (against foreign spies and international terrorists).

6 Carnivore is said to be a "diagnostic tool" of the FBI, utilized to intercept information and electronic communications so as to enable the FBI to combat "acts of terrorism, espionage, information warfare, hacking, and other serious and violent crimes occurring over the Internet". As will be discussed more fully below, the relative secrecy which the FBI has employed in not making public the full technical functionalities of Carnivore, and the corresponding concern that the FBI's unchecked use of Carnivore may result in the FBI obtaining far more information about a person than if it were to utilize a conventional wiretap, have led to policy debates and legal issues similar to those raised by the PATRIOT Act.

legal and privacy implications of the US Government's continued use of Carnivore.

Terrorism can be said to achieve three effects: (1) the "immediate effect" of killing or injuring the targets of the act of terrorism; (2) the "intermediate effect" of intimidating (and influencing) the population at large; and (3) the "aggregate effect" of undermining public order generally.[7] Effective responses to terrorism must therefore focus on arrest, prevention and deterrence,[8] and in the context of technology and electronic media, the FBI has stated publicly that one of the reasons for the development and deployment of Carnivore is to combat the increasing use by terrorist groups of new technology (such as the Internet) for recruiting, communications and propaganda purposes.[9]

In March 2001, the House Subcommittee on National Security, Veterans Affairs and International Relations heard testimony to the effect that the US continued to suffer from "a conspicuous absence of an overarching [counter-terrorism] strategy … [and] the multiplicity of Federal agencies and programs concerned with combating terrorism were inevitably fragmented and uncoordinated". Studies and reports showed that the sarin gas attacks in Tokyo and the Oklahoma City bombings in the mid-nineties were "unmistakable harbingers of a profound and potentially catastrophic change in the nature of terrorism … pointing to a new era of terrorism far more lethal and bloody than before". While the number and level of terrorist attacks in America were still few in number at the date of that hearing, it was stated that "ongoing comprehensive re-assessments" of terrorist threats are necessary, in order for the US to ensure that the "range of policies, countermeasures and defenses … are the most relevant and appropriate ones".[10]

---

7 W Michael Reisman, "International Legal Responses to Terrorism" 22 Hous J Int'l L 3 (1999), as cited in Seth R Merl, "Internet Communications Standards for the 21st Century: International Terrorism Must Force the U.S. to Adopt "Carnivore" and New Electronic Surveillance Standards" 27 Brooklyn J Int'l L 245 (2001).

8 See Merl, *ibid.*

9 See *Congressional Statement of the FBI on the Carnivore Diagnostic Tool*, delivered by the Assistant Director of the Laboratory Division of the FBI, Mr Donald Kerr, before the Senate Judiciary Committee on 6 September 2000. The Statement is available online at http://www.fbi.gov/congress/congress00/kerr090600.htm (last accessed: 2 May 2002). In the Statement, the FBI also proffered several examples of "cyber crimes" for which investigation Carnivore was developed, *viz*, (1) terrorist groups are turning to the Internet to communicate, raise funds and spread propaganda; (2) foreign intelligence services have also begun to use electronic communications for espionage; (3) there is an increasing risk of "information warfare", *ie*, the possibility of critical attacks on national communications infrastructure; (4) child pornography is increasingly being distributed online and children are being enticed through the same medium to participate in such activity; and (5) incidents of serious fraud being committed via the Internet are increasing.

10 See the written testimony of Dr Bruce Hoffman, Director of the Washington DC office of the RAND organization, before the House Subcommittee on "Combating Terrorism: In Search of a National Strategy", 27 March 2001, testimony available online at http://www.rand.org/publications/CT/CT175/CT175.pdf (last accessed: 16 May 2002).

The main question therefore, in light of the terrorist attacks of September 11 and the US Government's legislative response in the form of the PATRIOT Act, is whether the Act constitutes the "most relevant and appropriate" response to the present threat of terrorism. In an attempt to evaluate this issue, the rest of this essay is divided into four Parts. Part II provides an overview of, and background to, the PATRIOT Act, and summarizes those of its provisions that raise privacy concerns in the context of electronic surveillance by the US Government. Part III examines the relationship between these provisions with the Fourth Amendment to the US Constitution and other US statutes relating to Government electronic surveillance. Part IV focuses on the FBI's use of Carnivore surveillance technology in a post-September 11 world. Part V describes, briefly, several post-PATRIOT Act developments and initiatives that could potentially affect the policy debate in the area of privacy, surveillance and anti-terrorism. What will likely emerge from this analysis is the determination of the US Government to update and enhance its law enforcement powers and tools (including utilizing surveillance technology) in order to detect as well as prevent terrorism; some of the updates and enhancements in the PATRIOT Act, however, are so vague and extensive as to raise some very serious concerns over the nature and effectiveness of privacy protection.

II. THE PATRIOT ACT: BACKGROUND TO ENACTMENT AND SELECTED PROVISIONS

A. *Overview of the PATRIOT Act*

The PATRIOT Act, in furthering its aim of anti-terrorism, increases the ability of US Government agencies to use electronic surveillance tools in order to gather information and evidence. It does this by expanding the scope of existing US surveillance legislation while simultaneously reducing the level of judicial scrutiny over surveillance activity by the US Government. In this respect, pro-privacy groups and civil liberties advocates have publicly attacked the broad powers conferred on the US Government and its various agencies by the PATRIOT Act.[11]

---

[11] For example, the American Civil Liberties Union (the "ACLU") has stated that the Act is "based on the faulty assumption that safety must come at the expense of civil liberties [and] gives law enforcement agencies nationwide extraordinary new powers unchecked by meaningful judicial review." Specifically, some of the issues which the ACLU raised in relation to the Act include those provisions that (1) minimize judicial review to ensure that wiretapping is conducted legally and with proper justification; and (2) allow for investigative authority used for intelligence purposes to bypass normal criminal procedures that protect privacy (for example, in lowering the standard of proof that law enforcement authorities are required to show in order to gain access to the information "content" of an Internet communication, as opposed to merely getting the telephone numbers dialled on a telephone, which under pre-PATRIOT Act law carried a lower threshold of proof than access to the contents of a communication); under the PATRIOT Act, access to "content

The short title of the PATRIOT Act states its objectives to be, among other purposes, to "deter and punish terrorist acts in the United States and around the world [and] to enhance law enforcement investigatory tools"; a view publicly echoed by US Attorney General John Ashcroft, who stated that "new tools and resources [were] necessary to disrupt, weaken, and eliminate the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish the perpetrators of terrorist acts". Mr Ashcroft took care, however, to add that such tools would not detract from the protection afforded to civil liberties by the US Constitution.[12] Similarly, Senator Patrick Leahy, the Chairman of the Senate Judiciary Committee, also expressed Congress' awareness, during the debate on the PATRIOT Act, of the need to strike a reasonable balance between combating the threat of terrorism and protecting constitutional freedom.[13] Senator Leahy added that the Act "has raised serious and legitimate concerns about the expansion of authorities for government surveillance and intelligence gathering within this country. Indeed, this bill will change surveillance and intelligence procedures for all types of criminal and foreign intelligence investigations, not just for terrorism cases".

The Act comprises ten Titles (including several provisions classified as Miscellaneous, under Title X). A glance at the subtitles of each Title will

---

information" would require a standard of proof far lower than the pre-existing need to show "probable cause": see the ACLU's legislative analysis of the PATRIOT Act, titled *USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances*, available online at http://www.aclu.org/congress/l110101a.html (last accessed: 4 April 2002). Other civil liberties groups have also criticised the PATRIOT Act and its (substantially similar) precursors (such as the Anti-Terrorism Act ("ATA"), the Uniting and Strengthening America Act and the Intelligence to Prevent Terrorism Act) that were introduced in the brief period between 11 September 2001 and 24 October 2001. See, for example, the 3 October 2001 testimony of Jerry Berman (from the Center for Democracy and Technology) before the Senate Judiciary Committee on "Protecting Constitutional Freedoms in the Face of Terrorism", stating that "measures hastily taken in times of peril – particularly measures that weaken controls of government exercise of coercive or intrusive powers – often infringe civil liberties without enhancing security", and commenting that the ATA and the original PATRIOT Act do at least two things that infringe on civil liberties: (1) that they "eviscerate the division" between the government's powers of conducting "counter-intelligence surveillance" of suspected foreign terrorists, and its powers of domestic law enforcement and criminal investigation of Americans; and (2) that they "broadly expand the government's ability to conduct surveillance and diminish the rights of Americans online". For a full list of all Congressional bills and legislation related to the September 11 incident, see http://thomas.loc.gov/home/terrorleg.htm (a database compiled by the US Library of Congress; last accessed: 5 April 2002).

[12] See the press release from the US Department of Justice dated 26 October 2001, titled *Attorney General Ashcroft Directs Law Enforcement Officials to Implement New Anti-Terrorism Act*, available online at http://www.usdoj.gov/opa/pr/2001/October/01_ag_558.htm (last accessed: 4 April 2002).

[13] See Statement of Senator Patrick Leahy, Chairman of the Senate Judiciary Committee and Democratic Manager of the Senate, Debate on the Anti-Terrorism Bill, 25 October 2001, available online at http://www.senate.gov/~leahy/press/200110/102501.html (last accessed: 22 May 2002).

leave even the casual reader with no doubt about the specific objectives of, and major themes underlying, the Act. For instance, Title I is subtitled "Enhancing Domestic Security Against Terrorism"; Title II deals with "Enhanced Surveillance Procedures", Title V with "Removing Obstacles to Investigating Terrorism", Title VII provides for "Increased Information Sharing For Critical Infrastructure Protection", Title VIII "[Strengthens] the Criminal Laws Against Terrorism", and Title IX allows for "Improved Intelligence".[14]

The PATRIOT Act uses the terms "terrorism" and "terrorist acts" in its short title and the statement of its objectives. The phrase "national security" (or "domestic security") appears nowhere in these two provisions.[15] Although it seems clear that where there exists a real threat of terrorism – in the form, for instance, of either additional terrorist incidents or the risk of other attacks carrying even more devastating consequences than the events of September 11 – national security is necessarily threatened, it is also possible to distinguish between the threat of terrorism, and a more general threat to national security. In other words, while terrorism constitutes a threat to national security, the concept of "national security" is wider than terrorism. Privacy law has developed through legislators and judges balancing the need to ensure national security against the need to protect individual privacy, and a popular post-September 11 argument is that the individual citizen must be prepared to give up some of the latter in the interests of the former. Where the wider concept of "national security" is utilized to justify expanding Government powers and/or curtailing individual rights, the concern is that the imprecision of this wider concept can render the necessary balancing exercise not only more difficult, but possibly even unworkable.[16]

The term "terrorism" is not necessarily precise or easy to define.[17] None of the United Nations conventions dealing with terrorism define the term; various US statutes have attempted to define concepts and activities relating to terrorism in terms largely similar to one another.[18] The PATRIOT Act

---

[14] The other Titles (in addition to Title X: Miscellaneous) are: Title III, dealing with "International Money Laundering Abatement …", Title IV concerning "Protecting the Border" (including provisions dealing with immigration law violations), while Title VI contains provisions for compensation to victims of terrorist attacks (including aid for families of public safety officers)

[15] Although Title I does expressly deal with enhancing "domestic security against terrorism", and the phrases "domestic security" and "national security" do appear in specific provisions of the Act.

[16] For a variant on this point with respect to the current US test of privacy under the Fourth Amendment, see Massucci, *infra*, n 50.

[17] *Infra*, n 18, 19, 22, 23 and 32.

[18] For example, 22 USC § 2656(f) (which requires the Secretary of State to provide Congress with an annual country report on terrorism) includes the following definition: "(1) 'international terrorism' means terrorism involving citizens or the territory of more than 1 country; (2) the term 'terrorism' means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents; and

added "domestic terrorism" to existing definitions and criminal acts of terrorism under US law, including international terrorism[19] and terrorism transcending national borders. It defined "domestic terrorism" to mean activities occurring primarily within the US that constitute violations of US criminal laws and that involve the endangering of human lives, where those activities appear intended to either intimidate or coerce the civilian population, or to influence government policy by intimidation or coercion, or to affect the workings of government by mass destruction, assassination or kidnapping.[20] The PATRIOT Act also makes the harbouring or concealing of a person whom one knows (or has reasonable grounds to believe) has committed or is about to commit a terrorist act a crime as well.[21]

With this plethora of definitions in US law covering various aspects of terrorism and the lack of international consensus on what, exactly, constitutes terrorism,[22] it would seem therefore equally imprecise whether the word "terrorism" or the phrase "national security" is used to justify making laws that increase Government powers. The word "terrorism" is ostensibly more specific, while the concept of "national security" seems wider and more general in nature, but neither term can be defined with precision. At the same time, as will be seen, the concept of privacy, and the scope of protection therefor, is also not necessarily a matter capable of clarity and precision in definition. The necessary "balancing exercise" of weighing security against privacy is thus made all the more difficult by the imprecise nature and uncertain scope of the two (opposing) interests it seeks to balance.

For the purposes of this essay, the provisions of the PATRIOT Act that will be summarized and examined are those in Title II (regarding enhanced surveillance procedures), with respect to the changes made thereby to

---

(3) the term 'terrorist group' means any group practicing, or which has significant subgroups which practice, international terrorism".

19 "International terrorism" is defined along similar terms, except that the activities would have to occur primarily outside the territorial jurisdiction of the US: see 18 USC § 2331. See also 22 USC § 2656(f), *ibid*. Acts of terrorism transcending national boundaries are described in 18 USC § 2332(b) (amended by Sec 808 of the PATRIOT Act to include a "federal crime of terrorism").

20 Sec 802, PATRIOT Act.

21 Sec 803, PATRIOT Act. See also *infra*, n 23, outlining the new federal crimes created by the PATRIOT Act.

22 It has been suggested that several fundamental elements go to make up most legal or working definitions of terrorism: (1) the victims (generally civilians as opposed to military targets), (2) the intended targets (being the "secondary", or non-direct but real targets of the act), (3) the intent behind the act (generally of intimidation, coercion or manipulation), (4) the means (generally violent), and (5) the motivation for the act (generally political in nature). These elements were taken from an online article written by Professor Donna Arzt, Director of the Center for Global Law and Practice at Syracuse University, for the "Terrorism Law & Policy" section of the JURIST Legal Network hosted by the University of Pittsburgh: see http://jurist.law.pitt.edu/terrorism/terrorism1a.htm#1 (last accessed: 22 May 2002).

existing federal laws on electronic surveillance.[23] What follows is a brief description of these provisions; where appropriate, certain of the legal effects of these provisions will be examined in greater detail in the subsequent discussions regarding the federal wiretap and foreign intelligence surveillance laws.

In summary, the main changes made by Title II of the PATRIOT Act to in relation to Government surveillance powers and related laws are:

(i) Wiretap or interception orders can be obtained for a larger number of suspected crimes, including acts relating to terrorism and computer abuse.[24]

(ii) An additional exception to the general prohibition against wiretapping has been created. This exception allows for the interception of

---

[23] For a much more complete and comprehensive look at all the legislative changes introduced by the PATRIOT Act, see Charles Doyle, *The USA PATRIOT Act: A Legal Analysis*, a report prepared by the Congressional Research Service, 15 April 2002, Order Code RL 31377, available online at http://www.fas.org/irp/crs/RL31377.pdf (last accessed: 28 May 2002). Mr Doyle also prepared an earlier report, *Terrorism: Sec. by Sec. Analysis of the USA PATRIOT Act*, Order Code RL 31200, updated 10 December 2001, available online at http://www.cdt.org/security/usapatriot/011210crs.pdf (last accessed: 28 May 2002). On 31 October 2002, the Electronic Frontier Foundation ("EFF") released its own report, focusing on those aspects of the Act relating to online activities. The report is available online at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (last accessed: 28 May 2002). On the related point that the PATRIOT Act expands government interference in the private sphere of individual activity, it must be noted that the Act creates several new domestic crimes. Sec 802 creates a new federal crime of "domestic terrorism" that broadly extends to "acts dangerous to human life that are a violation of the criminal laws" if they "appear to be intended…to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping" where those acts "occur primarily within the territorial jurisdiction of the United States". The vagueness of some of the terms used and the potentially subjective nature of certain determinations that need to be made, *eg*, as to whether an act "appears to be intended" to achieve the ends described or what constitutes intimidation or coercion, has led to fears that this new crime will permit investigators to justify the investigation and surveillance of political activists, anti-governmental organizations and other persons or groups critical of government policies. Sec 805 of the PATRIOT Act expands the crime of providing terrorists with "material support and resources" by, first, doing away with the previous requirement that the act in question had to take place within the United States; secondly, by increasing the number and types of criminal violations for which providing material support would be an offense; and thirdly, by adding to the definition of "material support or resources". The definition of "material support or resources" is fairly broad, meaning the provision of "currency or monetary instruments or financial securities, financial services, lodging, training, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials". Providing such support or resources, or "concealing or disguising the nature, location, source or ownership of such support or resources, with the knowledge or intention that they would be used in preparation for or carrying out the listed crimes, is a federal offense". See the Doyle analysis for a more detailed description of the expanded list of crimes and the enhanced penalties for certain offenses.

[24] Sec 201 and 202, PATRIOT Act.

communications to or from a "computer trespasser" on a "protected computer".[25]

(iii) Roving (or multipoint) wiretaps[26] are now available under the Foreign Intelligence Surveillance Act ("FISA").[27]

(iv) In an investigation of domestic or international terrorism, a nationwide search warrant can now be obtained. The warrant must be authorized by a judge "in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district."[28]

(v) For electronic evidence (*ie*, wire, oral or electronic communications in "electronic storage" or stored in a "remote computing service" as described in the federal wiretap law), nationwide authorizations may now also be obtained. Either a warrant is issued by any court "with jurisdiction over the offense under investigation", or a court order for disclosure of such evidence can be granted by any "court of competent jurisdiction" (meaning a court having jurisdiction over the offense being investigated, "without geographic limitation").[29]

(vi) While notice of a search warrant was generally and previously accepted as necessary in order to permit the subject of the search to invoke her Fourth Amendment rights (*eg*, by pointing out deficiencies in the warrant), the PATRIOT Act expressly allows for such notice to be delayed. These so-called "sneak and peek" search warrants would be permissible where the court has "reasonable cause to believe" that notification may have an "adverse result"[30] on the investigation, provided that tangible property may not be seized unless the court finds "reasonable necessity" for such seizure, and notice is ultimately given within a "reasonable period" of the warrant's execution (such period being extendable only if "good cause" is shown to the court).[31]

(vii) It is now easier for Government agencies to share information with one another. A Government attorney, investigator or law enforcement officer with "knowledge of the contents of a wire, oral or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents

---

25 Sec 217.

26 *Ie*, a wiretap of a person who switches and/or uses various communication devices and different locations; a "roving wiretap" order means it would no longer be necessary to specify the identity of the surveillance target, or the location or nature of the communications system being tapped.

27 Sec 206.

28 Sec 219.

29 Sec 220 and 216(c).

30 Meaning "endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial" (§ 2705, Title18 USC).

31 Sec 213.

include foreign intelligence or counterintelligence … or foreign intelligence information". The disclosure is made to assist the recipient officer "in the performance of his official duties" and he may use the information "only as necessary".[32]

(viii) Several provisions can be seen as positive developments for Internet Service Providers ("ISPs"), *eg*, the Act provides for immunity and "good faith" defenses (and in some cases, compensation) when ISPs comply with surveillance and disclosure orders, enables the Government to intercept communications of "computer trespassers" (such as hackers) if so authorized by the ISP (being the owner or operator of the "protected computer"), and does not impose design restrictions or any additional obligations of technical assistance beyond the current law and what it takes to implement the various surveillance orders.[33] However, the PATRIOT Act also expands the type and amount of information the Government can obtain from an ISP, *eg*, ISPs may voluntarily provide "non-content" information to law enforcement without the need for a court order, and the Government can obtain information such as records of session times and their duration, payment methods (including credit card or bank account numbers) and temporary Internet Protocol addresses.[34]

(ix) Voicemails may be seized via search warrant (instead of, as previously was the case, requiring a wiretap order), thereby harmonizing the treatment of voicemail and email messages in this context.[35]

(x) One important aspect of the PATRIOT Act is the "sunset" provisions in Sec 224. These provide that most of the changes introduced by Title II of the PATRIOT Act, *viz*, as regards (1) the expanded list of offenses for which a wiretap order can be obtained; (2) the sharing of intercepted information among government agencies and their officials; (3) the use of roving wiretaps under FISA and the extended duration of FISA surveillance; (4) the voluntary emergency disclosure of the contents of subscriber communications and records by a computer/communications service provider; (5) the mandatory disclosure of stored communications pursuant to a court order or warrant; (6) the use of pen/trap orders under FISA and access to "tangible things" during a FISA investigation; (7) the permitted interception of communications of "computer trespassers" on a "protected computer"; (8) the nationwide effect of criminal search warrants;

---

[32] Sec 203(b) and (d). "Foreign intelligence" and "counterintelligence" is defined in Sec 3 of the National Security Act, while "foreign intelligence information" is defined in § 2510(19) of Title 18. Note that Sec 203(a) permits the disclosure of matters occurring before a grand jury when "the matters involve foreign intelligence or counterintelligence … or foreign intelligence information"; the disclosure may be to similar officials, and for similar limited purposes, as intercepted information disclosures under Sec 203(b). Similarly, the definitions of the various forms of intelligence information are identical. Note, however, that Sec 203(a) does not "sunset" with Sec 203(b).

[33] Sec 215, 225, 202 and 222.

[34] Sec 210-212.

[35] Sec 209.

and (9) the possibility of civil liability for Government violations of the wiretap provisions. However, it should be noted that some other significant changes made by the PATRIOT Act through Title II are not subject to the "sunset" provisions. These include those sections governing the use of "sneak and peek" warrants and the inclusion of non-content information from electronic communications within the Pen/Trap statute.[36]

The main criticism of the legislative changes made by Title II is that they are too broad, *viz*, the provisions expand Government powers beyond what is necessary to fight terrorism (*eg*, being aimed also at domestic, non-violent crimes such as computer offenses). It is also not clear if or how these expanded powers would have allowed the Government to detect and prevent the September 11 (or any other) terrorist attacks.[37]

The above-stated provisions of the PATRIOT Act illustrate the concerns over the breadth and vastness of their application. First, the nationwide application of warrants and court orders could mean that the judges issuing those authorizations will have difficulty in conducting any meaningful monitoring of their execution. Secondly, the issue of "sneak and peek" warrants has also raised concerns among privacy advocates, largely because of the fact that the PATRIOT Act does not limit their use to anti-terrorism cases. Rather, § 41(b) of the Federal Rules of Criminal Procedure (which Sec 203 of the PATRIOT Act amends to permit "sneak and peek" warrants) covers search warrants for evidence of criminal offenses generally.[38]

Where greater information sharing is concerned, it is arguable that better and more coordinated information sharing between and among various government agencies (*eg*, the FBI with the CIA) prior to September 11 could have helped alert the Government to potential suspects and planned terrorist activities. To the extent that the US Government and its various agencies lack sufficient coordination and mutual assistance that would enable them to better perform their duties and detect and prevent crimes and terrorism, allowing for such information sharing should, in principle, be unobjectionable. Further, it has been argued that information sharing between the intelligence and law enforcement communities is "especially critical in the new fight against terrorism", largely because the tactics involved in detecting terrorists and their activities would resemble those used in criminal investigations and arrests.[39] Further, given information that was released about the movements, activities and legal status of various of

---

[36] See discussion *infra*, n 89-94 and accompanying main text.

[37] See the EFF report, *supra* n 23.

[38] US courts have also not been entirely consistent in their decisions as to the constitutionality and lawfulness of "sneak and peek" warrants: see, *eg*, *US v Freitas*, 800 F2d 1451 (9th Cir 1986), and *US v Villegas*, 899 F2d 1324 (2nd Cir 1990).

[39] See Brian Hook, Margaret Peterlin and Peter Welsh, *Intelligence and the New Threat: The USA PATRIOT Act and Information Sharing Between the Intelligence and Law Enforcement Communities*, a White Paper prepared for the Federalist Society for Law and Public Policy Studies, December 2001, available online at http://www.fed-soc.org/Publications/Terrorism/Intelligencepdf.pdf (last accessed: 28 May 2002).

the September 11 hijackers before that fateful day, it is arguable – although this is impossible to determine, even in hindsight – that better information sharing amongst government agencies could have contributed to a better, more serious and comprehensive warning of the potential plans of the terrorists.[40]

However, one fear that arises in this context is that extensive information sharing in this manner would erode, possibly even remove, the barrier between domestic law enforcement and foreign intelligence operations. Given the historical context that necessitated the setting up of such a barrier in the first place,[41] this fear cannot be taken lightly. The problem, therefore, is of finding the appropriate balance between assisting the Government (as far as possible) to perform its function of protecting national security, while ensuring that such assistance does not lead to a lack of accountability on the part of Government agencies, or to the legitimisation of over-zealous investigative efforts on the part of Government agents, such that abuses of information-sharing powers are condoned or shielded from public knowledge. The PATRIOT Act attempts to strike this balance, and limit the potential for abuse of these powers, by subjecting a large portion of the information sharing provisions to the "sunset" clause.

In examining the privacy debate concentrated around the PATRIOT Act, it is necessary to recall the history behind much of the surveillance legislation in the US, and the past activities of law enforcement agencies in attempting to obtain information about individuals under investigation. A notable incident was the FBI's electronic surveillance of Dr Martin Luther King Jr in 1963, authorized by then-FBI Director, J Edgar Hoover. Another significant and prominent incident was the 1969 order by President Nixon, to conduct illegal wiretaps on government officials and journalists, in order to discover the source of "leaks" of sensitive government information. In the mid-1970s, the extent of government abuse of surveillance in the name of intelligence-gathering began to be exposed, through such means as the Watergate hearings and various investigative Congressional committees

---

[40] See Shane Ham and Robert Atkinson, *Using Technology to Detect and Prevent Terrorism*, a policy brief prepared for the Progessive Policy Institute, January 2002, available online at http://www.ppionline.org/documents/IT_terrorism.pdf (last accessed: 30 May 2002). The authors point out the fact that Mohamad Atta (one of the September 11 terrorists and allegedly the ringleader of those attacks) had been the subject of a criminal warrant of arrest in Broward County, Florida, in May 2001, but that two months later, an officer who pulled Atta over for speeding in Palm Beach County (also in Florida) had found no outstanding warrants on record. Atta had also rented cars and piloted small planes in the US before, transactions and activities that would have left a paper trail. Ham and Atkinson argue for improved data sharing (including better data entry procedures and the creation of more comprehensive databases) and caution that abuses of any powerful technological system is traceable not to the technology itself, but rather to the persons charged with overseeing and utilizing such technology. This point bolsters the argument that the law needs to ensure that proper procedures, transparency, sufficient oversight and some level of public disclosure exist concurrently with the expansion of technological powers and tools.

[41] See discussion, *infra*, n 42-45 and accompanying main text.

(such as the Church Committee), representing a reversal of the 1950s-60s trend, where "anti-Communist" sentiments prevailed in support of firm Government action, thus resulting in a lack of Congressional scrutiny over surveillance and information-gathering activities by executive branch agencies, and a lack of public disclosure of such processes and procedures.[42]

Even up to the late 1990s, the FBI's track record in successful prosecutions of internal security and terrorism-related cases has been poor. Between 1992 and 1996, only 22% of these cases ended with a conviction of the accused, meaning that over three-quarters of the cases were either dismissed by the judges, declined by prosecutors or resulted in acquittals.[43] At the same time, various Administrations have either increased FBI funding (in some cases, specifically with respect to counterintelligence and counter-terrorism operations, *eg*, in response to the Oklahoma City bombings) or otherwise supported FBI investigative and surveillance-related initiatives (*eg*, with respect to the Digital Telephony Law, or "CALEA"[44]).[45] The somewhat lacklustre and chequered history of the US Government's conduct in terms of its surveillance activities can be said to lend strength to privacy advocates' fears that greater Government power in this area – even in a time of national and international crisis – is likely to be abused.

B. *Development of Privacy Protection Laws in the United States*

Pre-September 11 US federal statutes may provide some useful background to the passage of the PATRIOT Act. Several of these US statutes relating to electronic privacy (*viz*, the federal wiretap statute and the Electronic Communications Privacy Act) and the US Constitution (insofar as it offers and affects privacy rights) will be examined in greater detail in Part III. It should be noted at the outset that the question whether or not a right of privacy exists in the US has been examined exhaustively, both judicially and academically. For the purpose of the present essay, therefore, only a

---

[42] See Morton Halperin, Jerry Berman, Robert Borosage and Christine Marwick, *The Lawless State: The Crimes of the U.S. Intelligence Agencies* (New York: Penguin Books, 1976), and "Intelligence Activities and the Rights of Americans", the Final Report of the US Senate's Select Committee to Study Governmental Operations with Respect to Intelligence Activities (or the Church Committee Report), 26 April 1976, available online at http://www.thirdworldtraveler.com/FBI/Church_Committee_Report.html (last accessed: 28 May 2002).

[43] See David Burnham, "The FBI: A Special Report" in The Nation magazine, 11-18 August 1997, available online at http://past.thenation.com/issue/970811/0811burn.htm (last accessed: 28 May 2002).

[44] *Infra*, n 62.

[45] See, *eg*, the Clinton Administration Counter-terrorism Initiative of 1995, available online at http://www.epic.org/privacy/terrorism/clinton_terrorism_proposal.txt (last accessed: 28 May 2002).

brief outline of privacy law developments that are relevant to electronic communications and technology will be discussed.

In 1890, in a seminal article in the Harvard Law Review, Warren and Brandeis called for a right to privacy in the form of a new tort, protecting a personal (not property) "right to be let alone", in response to what they viewed as journalistic overstepping in pursuit of details of a family's domestic and social affairs.[46] In 1928, the US Supreme Court in *Olmstead v US* grappled with balancing the interests of the government in obtaining evidence of illegal activity through telephone wiretapping, against the Constitutional protection of individuals against unreasonable search and seizure (afforded by the Fourth Amendment).[47] The Court held that the wiretapping did not amount to an unreasonable search and seizure in violation of the Fourth Amendment since "[t]he evidence was secured by the use of the sense of hearing and … [t]here was no entry of the houses or offices of the defendants"; to apply the Fourth Amendment to telephone wiretapping would be to afford it an "enlarged and unusual meaning". In a vigorous dissent, Justice Brandeis (as he had then become) argued energetically against a overly literal construction of the language of the Constitution, pointing out in a prescient passage that "[s]ubtler and more far-reaching means of invading privacy have become available to the government … The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day 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 to a jury the most intimate occurrences of the home".

A Constitutional right of privacy was first judicially recognized in 1965, in a case that did not concern wiretapping or surveillance; rather, *Griswold v Connecticut* was about privacy in the context of reproductive rights,[48] and it was in this case that the famous "penumbra" right to privacy (based on the concept that certain "penumbra", or zones, of protection, emanated from each of the guarantees outlined in the Constitution and its various Amendments) was first discussed by the Court.

It was not, however, till 1967 that the "physical trespass" doctrine espoused by the majority in *Olmstead* was finally overturned by the Supreme Court, in the case of *Katz v US*.[49] In *Katz*, the FBI had obtained evidence of the illegal transmission of wagering information across state

---

46 SD Warren and LD Brandeis, "The Right to Privacy" 4 Harvard LR 193 (1890). Note that the phrase "to be let alone" was not coined by Warren and Brandeis, but had been in use prior to their work; see, *eg*, TM Cooley, *A Treatise on the Law of Torts* 2nd ed (Chicago: Callaghan & Co, 1888).

47 277 US 438 (1928). The court also had to consider whether or not the Fifth Amendment had been violated in this case. The Fifth Amendment states, in part, that "[n]o person … shall be compelled in any criminal case to be a witness against himself".

48 381 US 479 (1965).

49 389 US 347 (1967).

lines through installing a listening and recording device to a telephone booth, without first obtaining the necessary warrant authorization. The Court held that this constituted an unreasonable search and seizure in violation of the Fourth Amendment, which protects "people, not places" and which application thus did not depend upon there having been a physical intrusion into a particular place.

In place of the *Olmstead* "trespass doctine", the *Katz* Court articulated a test that balanced the Government's interests in obtaining information with the affected individual's expectations of privacy in a particular situation. The *Katz* test was a two-pronged test that asked (1) whether a person had an actual personal expectation that he/she would be left alone from government intrusion ("subjective" privacy); and (2) whether such a personal expectation was one that society would be prepared to recognize as reasonable ("objective" privacy). The previous "hyper-literal, spatial" interpretation of the US Constitution to restrain unreasonable government intrusion thus gave way to a more "subjective" test of a person's privacy expectations that turned on "a nominally objective, societal validation of the reasonableness of those expectations".[50]

Since *Katz*, the US courts have continued to apply and explain the *Katz* test to a variety of situations.[51] Most recently, the Supreme Court has had to consider First and Fourth Amendment privacy issues specifically in relation to the use of surveillance technology, in the cases of *Bartnicki v Voepper*[52] and *Kyllo v US*.[53] In the *Nicodemo Scarfo* case,[54] the US District Court of

---

[50] See, *eg*, T Massucci, "Judges Without Chests or Rules Without Traces? The State, Technology and the Law of 'Warrantless Searches'" (1995) 21 Rutgers Computer & Tech L J 519.

[51] *Ibid*, including the references cited at note 2. Massucci considered the *Katz* test to be inherently inconsistent and to have become "weakened if not meaningless". He also pointed out that one of the most significant factors contributing to the "continued and accelerated erosion of the legal protections citizens may assert against technologically-aided state intrusions into their homes and personal affairs are not technological per se, but rather are ideological", meaning the "passivity and general pessimism regarding the state and state action … and a growingly privatised collective self-conception" that have "dovetailed with the American public's fundamental belief in the essentially progressive and absolutely inevitable nature of technology and technological change". Note that various aspects of personal privacy are also protected under US law under tort law; these were first comprehensively outlined by Professor Prosser in his famous article entitled "Privacy" 48 Cal L Rev 383-423 (1960) and in the "Restatement (Second) of Torts" at §§652A-652I (1977). In addition, at the federal level, many statutes protect specific forms and aspects of personal privacy, generally in relation to personal data, *eg*, the Fair Credit Reporting Act of 1970, the Privacy Act of 1974, the Cable Communications Privacy Act of 1984, the Video Privacy Act of 1988, and several industry- specific statutes enacted or implemented in the past three years, *viz*, the Children's Online Privacy Protection Act (regulating the information collecting practices of websites directed at children or that knowingly collect information from children), the Gramm-Leach-Bliley Act (regulating the data privacy practices of financial institutions), and the regulations made under the Health Insurance Portability and Accountability Act.

[52] 200 F 3d 109.

[53] 190 F 3d 1041.

New Jersey had to grapple with a Fourth Amendment challenge to the FBI's search and seizure of computer evidence utilizing a "key logging" technique authorized by a warrant. Analysis of the courts' rulings in these recent surveillance technology cases may prove interesting in light of the changes wrought by the PATRIOT Act.

C. *The Risks to Privacy of Electronic Surveillance by the Government*

In comparison with electronic surveillance employing new technology, earlier forms of government surveillance involved a tremendous commitment of time and labour, ranging from the need to physically track a person using human agents, to round-the-clock monitoring of a suspect or his/her telephone conversations and the co-opting and use of "informers". The costs of mounting such labour-intensive operations functioned as a form of economic deterrent to engaging in widespread wiretapping.[55] Furthermore, information gathered from such activities, even if filed systematically, could not be checked and cross-referenced easily. The development of powerful computers, an increasing range of surveillance technology (from facial recognition software and biometrics to electronic surveillance devices) and large electronic databases can safely be said to have revolutionized, and made easier, the task of surveillance.

With the increasing use of such sophisticated technology, a great deal of personal information (*eg*, in the form of electronic mail, Internet and "listserv" postings, cached information or data stored on computers) can be and is transmitted and distributed electronically. Technology is also making it easier to find, track, intercept and store such information and communications; this makes possible the compilation of more and more information about people, their habits, preferences and other information, the creation of larger and more detailed databases, and the ability to match the electronic data with other kinds of information – all much more quickly and to an extent wider than was previously possible in "real space". The decrease in the ability to guard one's privacy is thus both quantitative and

---

[54] *US v Nicodemo Scarfo and Frank Paolercio, Criminal Case No 00-404* (United States District Court of New Jersey). The court's ruling on the pre-trial motions concerning Fourth Amendment issues was handed down on 26 December 2001: see discussion *infra*. On 1 March 2002, Nicodemo Scarfo entered a guilty plea to a bookmaking charge, thereby ending a plea bargaining process that also resulted in a more serious charge (of conspiracy to commit extortion) being dropped; see "Scarfo's High Tech Case Ends With Plea" in *The Philadelphia Inquirer* of 1 March 2002, available online at http://www.philly.com/mld/inquirer/news/local/2769774.htm (last accessed: 21 May 2002), and "PC Surveillance Tool Helps Win Conviction" in *PC World.com*, 1 March 2002, report available online at http://www.pcworld.com/news/article/0,aid,87084,00.asp (last accessed: 23 May 2002).

[55] See, *eg*, *Big Brother in the Wires: Wiretapping in the Digital Age*, a White Paper issued by the ACLU in March 1998, available online at http://www.aclu.org/issues/cyber/wiretap_brother.html (last accessed: 2 May 2002).

qualitative.[56] It follows that (1) it is becoming more difficult to ensure privacy in online and electronic communications; (2) it is also becoming more difficult to know who can and is intercepting such information, how this is being done, and how much is being intercepted and used; and (3) as people become more accustomed to new technology (and the fact that electronic surveillance may be more likely), their "reasonable expectations of privacy" will decrease, and hence legal protection based on such a standard could become more limited and increasingly meaningless.[57]

At the same time, legislation permitting the use of electronic surveillance[58] has been gradually passed and amended in the US, culminating (at present) in the PATRIOT Act. Concerns over whether, how and to what extent a person's privacy should be protected by law, in such a legislative and technologically advanced environment, are timely and important. However, in light of increasing terrorist activities (including the events of September 11, 2001), legislators, judges and governments have also to resolve the conflict between such "individual interest" (in protecting one's privacy), and the national interest in fighting terrorism and ensuring national security.

With respect, specifically, to the use of electronic surveillance technology and the risks this poses to privacy protection, the arguments can be summarized thus:[59] first, those based on the fear of the consequences surveillance can have on a person's public persona or behaviour. These include the concern that information collected about a person through surveillance can be judged out of context or be misleading, as it would require an extremely sophisticated system to gather, compile and portray – intelligently – the whole person being tracked (as opposed to a mere

---

[56] See Christiane Wilke, *Privacy Meets Free Speech Online*, a paper prepared for the Critical Themes in Media Studies Conference 2001, organized by the New School University and held on 21 April 2001. The paper is available online at http://www.newschool.edu/mediastudies/conference/internet_ethics/christiane_wilke.htm (last accessed: 15 April 2002).

[57] For an overview of the development of information privacy laws in the US and the legal issues raised by the Internet and other electronic media, see Susan E Gindin, *Lost and Found in Cyberspace: Information Privacy in the Age of the Internet*, 34 San Diego Law Review 1153 (1997). The issue of information privacy, and invasion thereof, is obviously not limited to government intrusions into a person's privacy; a person's electronic communications can be read and used by other individuals and commercial entities, *eg*, Internet service providers, online advertisers and data profilers. The use of Internet-related technology such as "cookies" and "web bugs" has spawned privacy concerns of its own, *viz*, the "hidden" collection, compilation and commercial use (through sale, sharing or leasing of the resulting database) of a person's online history (*eg*, types, duration and numbers of Websites visited or online purchases made). This issue is of particular concern as such "profiling" is often done without the knowledge of the online user: see, *eg*, *In Re Doubleclick Inc Privacy Litigation*, No 00 CIV 0641 NRB, 2001 WL 303744 at *1 (SDNY 28 March 2001).

[58] See the discussion of Title III and the Electronic Communications Privacy Act, *infra*.

[59] See, *eg*, Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2001).

compilation of separate facts and unrelated packets of information). In addition, if the increasing use of surveillance means the gradual public acceptance of surveillance as a risk of everyday life, a person could thereby be "dehumanised", becoming instead a mere object or collection of impersonal bits of information. Furthermore, the availability of "private space" and the enjoyment of such a space (whether consciously or unconsciously) allow a person to build relationships in confidence and to act freely; in contrast, a person under observation may have to rationalize his/her actions, or runs the risk of having such actions justified or explained away by the observer, possibly erroneously.[60]

The second argument is based on the fear that the nature of modern communications is inherently insecure (*eg*, the open and interconnected nature of the Internet) and cannot be counted on to guard privacy.[61] In this context, electronic surveillance is viewed as an even greater threat to privacy (as compared with a physical search of premises), due to several factors. First, how much information is captured by an act of surveillance depends in large part on the nature and sophistication of the technology and techniques employed in the surveillance; not every kind of technology will be able to filter out "irrelevant" information and capture only the specific pieces of information required by that particular investigation. Even if technology could provide some means of filtering, it may be easier (and therefore more tempting) to simply capture all communications of a suspect, and perform any necessary filtering only "after the fact". In order to prevent such indiscriminate collection, the law needs to ensure that sufficient safeguards and sanctions exist to limit information collection only to what is necessary for that specific purpose (within the limits of known technology). However, besides this problem, the nature of electronic communications also means that surveillance of these is generally and necessarily of an

---

[60] It is possible to divide privacy concerns in this context into "informational privacy" and "autonomy privacy" concerns; however, these two categories are essentially and closely intertwined in relation to the Internet and also in relation to surveillance. As such, they are not treated as different classes, or as necessitating different legal treatment, in this essay. For more on the two categories and their specific relevance to the Internet, see D Glancy, "At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet" 16 Computer & High Tech LJ 357 (May 2000). "Informational privacy" is commonly used to mean the "ability to control the acquisition or release of information about oneself", while the wider, more general concept of privacy "encompasses ideas of bodily and social autonomy, of self-determination, and of the ability to create zones of intimacy and inclusion that define and shape our relationships with each other", of which control over our own personal information is a "key aspect of some of these ideas of privacy, and is alien to none of them": see A Michael Froomkin, "The Death of Privacy" in 52 Stan L Rev 1461. See also Banks and Bowman, *supra*, n 4 at 36, discussing Alan Westin's "classic taxonomy of privacy" in the context of national security law and electronic surveillance.

[61] See, *eg*, James Dempsey, "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy" in the Albany Journal of Science and Technology, Volume 8, Number 1, 1997.

ongoing nature. Where a search warrant (authorizing a physical search) is limited to a single act of entry to particular premises in order to perform the search, it is not possible to require the same limitations in the "virtual space" of electronic surveillance and communications. Again, the law must ensure that the necessary safeguards and sanctions exist in order to minimize the overly broad exercise of surveillance powers.

This second argument has important ramifications for the US law on electronic surveillance (meaning, in this context, the interception and monitoring of wired or electronic communications and their contents),[62] and the resulting impact on privacy protection. The various US statutes governing the US Government's ability to conduct surveillance, and the interpretations given to these statutes by US courts, disclose different legal standards for obtaining proper authorization for different methods of information gathering. The different standards correspond generally to the different methods that can be employed in surveillance, *viz*, a wiretap, a search warrant, or a subpoena or other court order.[63] There are also statutes governing surveillance by means of devices such as pen registers and trap and trace devices[64] ("pen/trap devices"), for which orders a lower standard is generally required, compared to that for a wiretap or a search warrant.

For a wiretap (*ie*, the interception of the contents of a "wire, electronic or oral communication"), the relevant statute (known as Title III, first enacted in 1968[65] and subsequently amended) requires that: (1) a court order based on a finding of probable cause be obtained; (2) it be used only for specific, limited crimes; (3) it be granted only as a last resort, *ie*, only where normal

---

[62] This essay focuses largely on the following US federal statutes (in addition to the relevant Constitutional provisions and protections): the federal wiretap law (or Title III), the Electronic Communications Privacy Act (amending Title III), and to a limited extent, the Pen/Trap statute and the Foreign Intelligence Surveillance Act. It should be noted that, as regards interception of communications, the Communications and Law Enforcement Act ("CALEA") was enacted in 1994 in response to the numerous types of voice and data communications technology that had been developed and were increasingly being used commercially following the breakup of the telephone monopoly that hitherto had been held by Bell Telephone and AT & T. CALEA is a law relating to digital telephony requiring that telecommunications carriers "cooperate in the interception of communications for law enforcement purposes" by designing their systems so as to facilitate government access. For a brief critique of CALEA in relation both to its implementation and impact on privacy protection, see the materials provided by the Center for Democracy and Technology at http://www.cdt.org/digi_tele, and the Electronic Frontier Foundation at http://www.eff.org/Privacy/Digital_Telephony_FBI/ (last accessed: 13 May 2002). For a discussion of how CALEA may be relevant to determining the deployment of Carnivore, see J Lewis, *infra*, n 139, at 347-348.

[63] Essentially, a subpoena is an order requiring a person to surrender tangible evidence (*eg*, telephone records), a warrant authorizes a search to be conducted (*eg*, of premises) and the seizure of (generally tangible) evidence, and a wiretap order authorizes the interception of communications (and hence the obtaining of the contents thereof).

[64] See discussion *infra*, n 89-93 and accompanying main text.

[65] A more detailed discussion on Title III, its application and impact on privacy protection can be found *infra*, n 72-87 and accompanying main text.

investigative procedures have failed or are likely to fail, or may be too dangerous; (4) the wiretap be carried out in such a way so as to minimize the risk of interception of innocent communications; and (5) notice be provided after the investigation is concluded, and an opportunity to challenge both the finding of probable cause and the conduct of the wiretap given, prior to the introduction at trial of the evidence obtained through the wiretap. Wiretapping for national security purposes in the conduct of foreign or counterintelligence was authorized with the enactment of FISA in 1978. In general terms, FISA also contains requirements and procedures that must be satisfied in order for a FISA court to authorize a wiretap.

For a search warrant to be granted by a magistrate, probable cause that a crime has been or is about to be committed has to be shown (*eg*, by describing with some specificity the object of the search), and certain procedures (including notice to the suspect) have also to be observed.[66] Because the rules governing the issuance of the warrant are designed for use largely in criminal proceedings and investigations, they could in some cases be unsuitable to, and possibly even jeopardize, a situation where intelligence information is sought, *eg*, in investigations where information is gathered for national security purposes.[67] It has been said that the Fourth Amendment does not provide "even handed guidance" for criminal investigations and those involving national security; and, further, that the US Government does not treat the Fourth Amendment as applying equally to both types of investigations.[68]

For pen/trap devices, the procedure for obtaining the requisite installation and use order is the "least demanding and perhaps least intrusive".[69] In the general statute governing pen/trap devices, the court has little discretion; it has to make the order upon the government certifying that the information to be obtained is relevant to an ongoing criminal investigation.

Notwithstanding the existence of the various legal standards governing the scope of government surveillance, however, recent annual reports issued by the Administrative Office of the United States Courts and covering the wiretapping activities of federal, state and local police indicate that judges do not generally turn down applications for wiretap orders.[70] For example, in 2000, the number of domestic wiretapping requests approved was 1,190 but no request was denied. An additional 1,012 surveillance applications under FISA were granted by the FISA court during the year 2000;

---

66 See, generally, Rule 41 of the Federal Rules of Criminal Procedure.

67 See, generally, Banks and Bowman, *supra* n 4.

68 *Ibid*, at 9.

69 See Doyle, *supra* n 23.

70 See, *eg*, the 2000 Wiretap Report from the Administrative Office of the United States Courts, available online at http://www.uscourts.gov/wiretap00/contents.html (last accessed: 2 May 2002), in particular, Table 7 which shows a ten-year chart of such approvals dating from 1990.

according to the Center for Democracy and Technology ("CDT"), the FISA court has denied a government request for FISA surveillance only once since 1978.[71]

III. The Relationship Between the PATRIOT Act and Other US Laws on Electronic Surveillance and Privacy

A. *The PATRIOT Act, the Federal Wiretap Law and the Electronic Communications Privacy Act*

(i) *Title III and ECPA Prior to the PATRIOT Act*

The Omnibus Crime Control and Safe Streets Act was passed in 1968. The federal wiretap law that was enacted as Title III of the Act (as amended by the Electronic Communications Privacy Act ("ECPA") in 1986)[72] provides for authorization of the interception of " wire, electronic and oral"[73] communications by law enforcement officials in their investigation of specified criminal offences.[74] Its provisions therefore do not apply to non-

---

[71] See the study and report issued by the CDT on *The Nature and Scope of Government Electronic Surveillance Activity* (September 2001), available online at http://www.cdt.org/wiretap/wiretap_overview.html (last accessed: 2 May 2002).

[72] Codified at 18 USC § 2501-2521. ECPA and the amendments it made to Title III were necessary in light of *US v Seidleitz*, 589 F 2d 152 (4th Cir 1978), *cert denied*, 441 US 992, which had held that interception of a computer transmission was not an "aural" acquisition and hence fell outside the federal wiretap law.

[73] A "wire communication" is defined as an "aural transfer … by the aid of wire, cable or other like connection" and (prior to the PATRIOT Act) included the "electronic storage of such communication". An "oral communication" must be uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation" but does not include an "electronic communication". An "electronic communication" means a "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature … by a wire, radio, electromagnetic, photoelectronic or photooptical system" but excluding a wire or an oral communication, among other exclusions. See 18 USC § 2510(1), (2) & (12).

[74] ECPA also created the Stored Communications Act, governing the access to and disclosure of stored wire or electronic communications, *ie*, unauthorized access to a facility that is used to provide an "electronic communications service" is prohibited where access is used to obtain communications that are "in electronic storage". For a judicial analysis of the differences between "storage" and "transmission" of an "electronic communication", see *In Re Doubleclick, Inc Privacy Litigation*, *supra* n 57. The *Doubleclick* case (and its application in subsequent cases such as *Dane Chance v Avenue A, Inc*, 2001 US Dist LEXIS 17503 (WD Wash. 2001) and *In Re Toys R Us, Inc Privacy Litigation*, 2001, US Dist LEXIS 16947, decided 9 October 2001) affirmed the complex structure, technical difficulties and consequent limitations of Title III and ECPA. For example, an "interception" under ECPA occurs when the act of acquiring the information is contemporaneous with the transmission of the communication containing that information. It follows that once the communication has been received by the recipient (or, perhaps, when it enters or is received by his/her network or computer system), any acquisition of the same information would not constitute an "interception", but may possibly then fall under the Stored Communications Act. See discussion *infra* for more on this point.

criminal investigations. Title III does not "limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government".[75] Furthermore, surveillance for foreign and counterintelligence purposes is outside the ambit of these provisions, *eg*, § 2511, which generally prohibits the interception and disclosure of wire, oral and electronic communications, is stated expressly not to apply to electronic surveillance activity authorized under FISA.[76]

Authorization to conduct a wiretap under Title III is obtained by means of a Federal Court order,[77] which requires the submission of an affidavit containing detailed information, including the following: (1) the respective identities of the applicant law enforcement official and the high-level government attorney authorizing the application; (2) relevant facts justifying the order, including details of the alleged criminal offence, the identity of the suspect, the nature of the communication to be obtained and the location of the communications facilities; (3) whether or not other investigative procedures have been utilized and have failed, or if not, why these would fail or be too dangerous; and (4) the period of the interception (up to a maximum of thirty days). In addition to these requirements, law enforcement agencies (the FBI as well as the state police) have imposed additional internal procedures (including additional levels of internal review and approval) that further restrict the ability to obtain a wiretap order.[78] Electronic surveillance is therefore generally to be viewed as a matter of last resort, and where detailed procedures involving minute executive and judicial review have been followed.

The wiretap order will be granted only if the court has determined that, among other requirements, there is "probable cause for belief" that (1) an individual is committing, has committed, or is about to commit a specific criminal offence listed in the statute;[79] (2) "particular communications concerning that offence" will be obtained through the requested

---

[75] However, the exercise of such powers by the President (generally through the Attorney General) may still be subject to Fourth Amendment limitations: see the discussion of the *Keith* case, *infra*, n 96-99 and accompanying main text.

[76] § 2511(2)(e).

[77] Note, however, that there are express provisions covering "emergency situations" involving "immediate danger of death or serious physical injury" to a person, or "conspiratorial activities" that threaten national security or that indicate organized crime, where interception of wire, oral or electronic communications is required before the necessary court order can be obtained. In such "emergency situations", a forty-eight hour period to apply to the court, and running from the time the interception occurred, is provided for in the statute: see § 2518(7).

[78] See "Wiretap Orders and Procedures: What Happens When the US Government Taps a Line", an article from Computer Professionals for Social Responsibility, dated 23 September 1993, available online at http://www.cpsr.org/cpsr/privacy/wiretap/wiretap.procedure.html (last accessed: 13 April 2002).

[79] See § 2516.

interception; and (3) "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by" the target.[80] The court order must specify, among other things, the identity of the surveillance target, the "nature and location of the communications facilities as to which, or the place where, authority to intercept is granted", a "particular description of the type of communication sought to be intercepted" and the duration of such interception. In addition, upon request of the applicant for the order, a "provider of wire or electronic communication service" is to render "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services" provided. Finally, the interception cannot be approved for any period longer than necessary to accomplish the stated purposes, up to a maximum period of thirty days (an extension of which requires another application to the court). Periodic reports on the progress of the interception may also need to be presented to the court; and notice of the interception must be provided to the target within ninety days of the termination of the order.[81]

Critics of Title III and its workings draw attention to the fact that the list of specified crimes for which a wiretap may be obtained has gradually increased (from the original list of twenty-six to ninety-five by 1996), and the type of crimes included on the list has expanded to include crimes of a different nature from those than the original list, which targeted mostly violent and serious crimes, espionage, treason and organized crime. Judicial denials of applications for wiretap orders are also extremely rare.[82] The definitions and scope of, and the relationships between, different sections of Title III are also fairly complex and cumbersome to discern. Unfortunately, few of these criticisms are dispelled by the changes spelt out in the PATRIOT Act to the federal wiretap law.

(ii) *Changes to the Wiretap Law Made by the PATRIOT Act*

To the list of crimes for which a wiretap order can be sought, the PATRIOT Act added, under Sec 201, the material support of terrorists and terrorist organizations, use of weapons of mass destruction, chemical weapons offenses, financial transactions with countries that support terrorism and violent acts of terrorism transcending national borders, and under Sec 202, computer fraud and abuse. These changes are subject to the Sec 224 "sunset" provisions.

---

[80] See § 2518(1) and (3).

[81] See § 2518(4), (5) and (8).

[82] *Supra* n 70. For other criticisms of Title III, see Dempsey, *supra* n 61.

A new exception to the general prohibition against wiretapping (found in § 2511 of Title III) was added by Sec 217(2). This new exception allows for the interception of a wire or electronic communication of a "computer trespasser" transmitted to, through or from a "protected computer"[83] if (1) the owner or operator of that computer authorized the interception; (2) the interception is done while "lawfully engaged" in an investigation; (3) where there are reasonable grounds to believe that the contents of that communication are "relevant" to the investigation; and (4) provided that the interception does not acquire any other communications besides those transmitted to or from the computer trespasser. A "computer trespasser" is defined as a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in communications transmitted to, through or from that computer, although it does not include a person whom the computer owner or operator knows has an existing contractual relationship with such owner or operator, governing the person's access to all or part of the computer in question. By this definition, just about all hackers can fall within the scope of the new exception (although subscribers and other authorized users are clearly excluded). This wide definition thus means that the federal wiretap law now allows a suspected hacker's computer communications to be intercepted, based on the fact that these communications can reasonably be viewed as "relevant" to a lawful, ongoing investigation. The exception applies where the communication in question is reasonably believed to be "relevant" to an investigation, rather than requiring that probable cause that this is the case be shown. The language used to create this new exception can also be read to allow the interception of evidence that ultimately does not necessarily relate to the crime being investigated; thus it is possible for investigators to keep and use information that they, in the course of investigating a certain crime, lawfully (by virtue of this new exception) intercept, believing such information relevant to that investigation; even where it turns out that the intercepted contents point to a different crime.

It is noteworthy that the definition of "computer trespasser" presumes any unauthorized access-user would not have a "reasonable expectation of privacy" in communications transmitted to, through or from the accessed computer. Given the express exclusion of persons such as existing subscribers or customers of a network operator, this conclusion is probably correct for many instances of unauthorized access, *eg*, where someone breaks into a computer system and begins sending and receiving emails. A more difficult situation is one where the unauthorized user was, previously,

---

[83] A protected computer has the same definition as that in the Computer Fraud and Abuse Act, *viz*, either a computer used exclusively by a financial institution or the U.S. Government, or a computer that is otherwise used in interstate or foreign commerce or communication. Note that the PATRIOT Act, in Sec 814(d), expands this definition to include computers that are located outside the US but that are used in a manner that affects interstate or foreign commerce or communication of the US.

an authorized subscriber to the computer network and system, and is breaking in to, *eg*, delete or retrieve emails sent to her and stored in that computer. This latter situation is difficult in large part because US law has made a distinction between intercepting an electronic communication and acquiring that same communication while it is "in electronic storage". US courts generally require that to "intercept" a communication means acquiring it while it is being transmitted; in other words, the interception and the transmission must be contemporaneous. Where electronic communications are concerned, up to August 2001, the only instance where an appeals court had to consider this distinction was the Fifth Circuit in *Steve Jackson Games, Inc v US Secret Service*.[84] In *Steve Jackson Games*, the US Secret Service were accused of having violated Title III in that their acquisition of a computer hard drive (containing various emails) was alleged to have been an illegal interception. The Court held that, unlike wire communications, an electronic communication cannot be intercepted while it is in storage. The Court relied heavily on the literal language of the statute (where, *eg*, "electronic communication", unlike "wire communication", did not expressly include the possibility of electronic storage) and on its conclusion that in the ECPA amendments to the wiretap law, Congress had not intended to alter the meaning of the word "intercept", even where it had added the phrase "or other [means of] acquisition" to the definition thereof.

Steve Jackson Games has been heavily criticized, on grounds including the concern that the Court overlooked the very nature of an email communication, which necessarily involves electronic storage while in the process of transmission, and hence possibly explaining the lack of reference to "electronic storage" in the statutory definition of "electronic communication". Other criticisms include the fact that the Court's decision effectively causes the question of the lawful acquisition of many email messages to fall within the Stored Communications Act rather than Title III, which carries different sanctions and requirements. It would also mean that very few email messages acquired by investigators would likely constitute an interception within the scope of Title III, as the contemporaneity requirement leaves a very small window, or period of time, for any possible interception during transmission.[85]

In light, however, of the recent Ninth Circuit decision in *Robert Konop v Hawaiian Airlines*,[86] issued on 8 January 2001, and the change to the definition of "wire communication" made by the PATRIOT Act, it is possible to argue that US law will no longer distinguish between the interception and storage of electronic communications the way the Court in

---

84 36 F 3d 457 (5th Cir, 1994).

85 See, *eg*, Krista Belt, "Did Congress Really Intend to Give Investigative Officers Free Reign With Your Email?" in the South Texas Law Review online articles collection, available at http://www.stcl.edu/lawrev/Articles/Electronic_Privacy/electronic_privacy.html (last accessed: 30 May 2002).

86 236 F 3d 1035.

Steve Jackson Games did. In *Konop*, the Court had issued a written decision ruling that wire and electronic communications were to be treated similarly in determining whether or not an interception had occurred, and that the interception of an electronic communication encompassed the lesser act of acquiring such information while it is in electronic storage. The Court considered it "senseless" to treat wire and electronic communications differently. Unfortunately, the Ninth Circuit proceeded to withdraw its opinion on 28 August 2001 and as of this writing, no new opinion has been issued by the Court.

Since that first opinion in January 2001, however, the Eastern District of Pennsylvania has had occasion to consider a similar issue, where an employer was alleged to have illegally "intercepted" an employee's (Fraser's) emails that were stored on servers, thereby violating the federal and Pennsylvania wiretap laws. In deciding that no illegal interception had occurred, largely because the emails had long been in storage on the servers, the judge stated that emails necessarily were stored, in both "intermediate" and "backup" storage while being transmitted from sender to recipient (such storage being the case up to the point the recipient downloads the message from the server and thus retrieves it, thereby completing the transmission). While rightly distinguishing the facts of the case from those in *Konop*, the judge nonetheless commented that obtaining emails that were either in intermediate or backup storage would constitute an interception within the meaning of the federal wiretap laws.[87] The *Fraser* case, while certainly not going as far as *Konop*, at least allows for the possibility that US courts will not only refuse to make a distinction between different types of communication going forward, but also indicates that a more thoughtful and considered approach to the complex language and concepts of Title III will be adopted. In this way, the fragmented and confusing result of *Steve Jackson Games* may yet be avoided going forward.

This hope may be bolstered by the change made to the definition of "wire communication" in Title III by Sec 209(1) of the PATRIOT Act. The express inclusion of electronic storage of such a communication in constituting a "wire communication" has been deleted, with the result that neither the term "wire communication" nor "electronic communication" refers to the possibility of electronic storage. While one could certainly argue that this not only preserves, but underlines, the distinction to be drawn between intercepting a communication (of any sort) while it is in transmission (thus requiring contemporaneity) and accessing such communication while it is in storage (*ie*, post-transmission), the better view is probably that, in view of the nature of such communications – including the similarities as well as the differences between each type – the requirement of contemporaneity simply works differently for each type of communication. In other words, while contemporaneity for a telephone call

---

87 *Fraser v Nationwide Mutual Insurance Co*, 135 F Supp 2d 623 (ED Penn 2001).

or other wire or oral communication can be easily established, the same concept when applied to an electronic communication must take into account the fact that there will be a period where that communication is both being transmitted as well as stored in some fashion. The Pennsylvania Eastern District Court's observation on this point in *Fraser*, and the initial Ninth Circuit opinion in *Konop*, illustrate a more robust, consistent and commonsensical approach to this issue.

Another change made by the PATRIOT Act that affects the scope of Title III is found in Sec 203, which permits certain types of information intercepted in the course of a wiretap to be shared with security, immigration, intelligence, defense and other federal officials, for use in carrying out their official duties. Information falling within this category would be intelligence information relating to protecting the US from attacks or hostile action, sabotage or international terrorism by a foreign power or its agents, or clandestine foreign intelligence activities, information concerning a foreign power or territory that relates to US national defense, security or foreign policy, or foreign or counter intelligence information as defined in the National Security Act of 1947. Any such information sharing must be disclosed to a court, and information regarding US citizens or residents is subject to procedures outlined by the Attorney General. This change is subject to the "sunset" provisions.

B. *The Use of Pen Registers and Trap and Trace Devices for Surveillance*

Because interception by means of electronic surveillance technology can be of different types of information, it is necessary to clarify certain terms that are used to describe the various ways of intercepting information. In essence, electronic surveillance technology can be used to intercept either the contents of a particular communication, or simply the fact that a communication has been made. In the former case, the privacy concerns can be said to be greater because "information concerning the substance, purport or meaning"[88] of a communication is obtained; in the latter case, the contents may be unknown; rather, what is intercepted is the fact that a call was made or email sent, the time and date of the communication, or the origin and destination of the call or email. Under US law, this distinction can be illustrated by reference to the difference between the statute governing the use of "pen register" and "trap and trace" devices[89] (Chapter 205 of Title 18 of the US Code, known as the "Pen/Trap statute")[90] and Title III. Where Title III governs the interception of the contents of an electronic communication, the Pen/Trap statute deals with obtaining the

---

88 See Title III § 2310(8).

89 And as interpreted by the US courts. See, *eg*, *US v New York Telephone Company*, 434 US 159 (1977) and *Brown v Waddell*, 50 F 3d 285 (4th Cir, 1995).

90 18 USC §§ 3121-27.

addressing information relating to such communications. As such, the two statutes regulate access to different types of electronic information. The Pen/Trap statute would relate to telephone numbers dialled on a telephone line, or, with respect to electronic communications, addressing and routing information such as those contained in the "headers" of email messages (*eg*, the email addresses of the sender and recipient, or the time when the email was sent). However, whether or not other information that could conceivably be described as "header"-type information, such as the "Subject" line of an email, would be covered by the Pen/Trap statute was unclear before the PATRIOT Act. One point of view was that such information would not fall under the Pen/Trap statute as the nature and extent of such information (*eg*, indicating the subject matter of the communication) could be considered part of the "content" of the communication itself.[91]

(i) *The Pen/Trap Statute Prior to the PATRIOT Act*

A "trap and trace device" was defined in the Pen/Trap statute as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted". A "pen register" device was defined as a device that "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted" on the telephone line to which it is attached. Thus, a pen register device was one that recorded outgoing addressing information, and a trap and trace device was one that recorded incoming addressing information.[92] Either device can be installed upon the obtaining of a court order where a government official certifies that "the information likely to be obtained is relevant to an ongoing criminal investigation".[93] Additionally, there was no room for judicial discretion in authorizing the use of a pen register or trap and trace device, as the statute mandated that the court "shall" make such authorization upon

---

[91] In *Smith v Maryland*, 442 US 735, the Supreme Court had held that there is no Fourth Amendment protection for the numbers dialled on a telephone in order to initiate a call, thus paving the way for the different legal standards to be applied in authorizing the interception of the contents of a communication (under Title III) and the interception of the electronic impulses identifying and/or recording any telephone numbers dialled (under the Pen/Trap Statute). The reasoning in *Smith* was based on the belief that (following the *Katz* test) there is no "reasonable expectation of privacy" when dialling a telephone number using a home telephone line. Because the user is conveying information to the telephone company when he/she dials a number for a call, and that information may be collected by the telephone company for a variety of legitimate purposes, the *Katz* test cannot be satisfied. In another case concerning the disclosure of financial records by a bank to investigators, the Supreme Court had also held that the account-holder could not claim a "reasonable expectation of privacy" in those records once he had disclosed them to a bank: *US v Miller*, 425 US 435 (1975).

[92] 18 USC § 3127(3)-(4)

[93] § 3123(a)(1).

such certification by the relevant government official. Unlike a Title III wiretap, there is no requirement for minimization and little judicial oversight of the process of interception utilizing either device under the Pen/Trap statute.

(ii) *Changes to the Pen/Trap Statute Made by the PATRIOT Act*

As mentioned earlier, until the passage of the PATRIOT Act, there was some confusion over the applicability and scope of the Pen/Trap statute in relation to electronic (*ie*, non-telephonic) communications and addresses. This was due mainly to the statutory definitions of the devices in question, which were limited to telephone numbers and lines. Sec 216 of the PATRIOT Act attempts to settle this issue by providing that pen registers and trap and trace devices mean "device[s] or process[es]" which, in the former case, record or decode "dialing, routing, addressing, or signalling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted [but not including the contents of such communication]", and in the latter case, capture "the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and[94] signalling information reasonably likely to identify the source of a wire or electronic communication [but not including the contents of such communication]".

The expanded definitions make it clear that electronic communications are also subject to the Pen/Trap statute. However, the expanded definitions are not without problems. For example, "dialing, routing, addressing, and signalling information" is not further defined. The exclusion of the "contents" of a communication is indicative (particularly since Title III defines content to mean information concerning the "substance, purport, or meaning" of a communication), but not entirely helpful. The question of classifying matter such as information in the Subject line of an email (which, as displayed and shown by the interface of most email programs currently, could be described as treated as "header information", and hence similar to the To: and From: lines of the same email), is still not answered clearly by the language of the PATRIOT Act. The expanded definitions could conceivably be read to include information far more significant to an investigation than mere telephone numbers dialled on a telephone line, such as the websites visited by an Internet user.

These problems arise because Internet and other electronic communications are simply different, by their very nature, from telephone calls. For telephone calls, the numbers dialled and received are easily separable from the content of the call itself; except for, *eg*, the To:, From:,

---

[94] It is assumed that the use of the word "and" in the definition of a trap and trace device, as opposed to the use of the word "or" in a similar context in the definition of a pen register, is not significant.

time and date designations of an email, the same division cannot easily be applied to Internet and other electronic communications. Further, information over the Internet is delivered in packets, and the technology used to divide and deliver these packets does not distinguish between various types of information, as the design emphasis and mode of delivery concentrates exclusively on utilizing the quickest and most efficient route of transmission, largely regardless of the content, length, origin or destination of the communication.

The PATRIOT Act also expands the Pen/Trap statute by allowing a court to authorize the installation and use of a pen register or trap and trace device "anywhere in the United States", where previously the order had to be "within the jurisdiction of the court". A court order is also stated to "apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order". As with the nationwide application of search warrants in criminal investigations (provided for by Sec 220 of the PATRIOT Act), the nationwide applicability of a pen/trap order could make it difficult for smaller or localized Internet service providers to challenge or query such orders.

To militate against abuses of these expanded pen/trap powers where the devices are installed on a service provider's network, Sec 216 provides for records to be kept, regarding the identities of those officers installing the device or obtaining information thereby, the date and time of installation, access (each time) and uninstallation, the configuration of the device installed and any later modifications thereof, and information collected thereby. This provision acts as an important safeguard in light, particularly, of the FBI's deployment of Carnivore (discussed *infra*). The records mandated to be kept by Sec 216 have to be provided under seal to the court that issued the original authorization within thirty days of the termination of the order.

In addition, Sec 216(a) of the PATRIOT Act clarifies that the Government agency using the relevant pen/trap device or process is also to use technology reasonably available to it that restricts the information recorded or decoded, "so as not to include the contents of any wire or electronic communications". This is clearly intended to serve as a kind of safeguard, in the form largely of a general guideline. However, it is not clear, and probably extremely difficult, to determine how and whether this can and has been done in individual cases.

A final point about the expansion of the Pen/Trap statute due to the PATRIOT Act is that these changes do not "sunset" in December 2005. Sec 216 of the PATRIOT Act therefore makes significant changes to US law regarding the installation and use of pen register and trap and trace devices.

C. *The PATRIOT Act and the US Constitution*

In April 2000, US Deputy Assistant Attorney General Kevin Gregory testified[95] before the House of Representatives' Subcommittee on the Constitution, to the effect that the Fourth Amendment to the US Constitution has long been the "cornerstone of protecting individual privacy from unwarranted government intrusion" and that such protection extends to an individual's online activities as well. These Constitutional limitations work in combination with "statutory restrictions on government access" (such as those provided for in Title III and the ECPA) and with the courts, which have a role in ascertaining that law enforcement authorities have met the proper legal standards for such access (which standards may differ depending on whether a wiretap order, search warrant or subpoena is being sought). The combination attempts to strike the appropriate balance between the need for the government to obtain information about an individual's activities (through the exercise of powers to investigate and obtain evidence of crimes and suspected criminal activity) and the need to ensure that access to such information is reasonable and not unduly intrusive of an individual's privacy.

The Fourth Amendment provides for the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures … and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".[96] As has been discussed earlier, the test applied by US courts to determine whether or not a search violates the Fourth Amendment dates back to the *Katz* case, and essentially depends on whether or not the subject of the search had an actual expectation of privacy that society is prepared to accept as being a reasonable one. The Supreme Court in *Katz*, however, expressly excluded cases involving national security from its ruling.[97]

The issue of national security weighed against a US citizen's individual right to privacy (as protected by the Fourth Amendment) came before the Supreme Court in 1972, in *US v US District Court for the Eastern District of Michigan* (commonly referred to as the *Keith* case). In *Keith*, a wiretap

---

[95] Testimony available online at http://www.cybercrime.gov/inter4th.htm (last accessed: 5 April 2002).

[96] For an excellent overview of the scope of application of the Fourth Amendment to searches and seizures of evidence in relation to computer crime (including issues relating to what constitutes public/private space, workplace searches, "sneak and peek" warrants and the permissible exceptions to the requisite search warrant, *eg*, in the case where the subject has given his/her consent), see *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, a manual issued by the Computer Crime and Intellectual Property Sec of the US Department of Justice (Criminal Division), January 2001. The manual is available online at http://www.cybercrime.gov/searchmanual.htm#Ib (last accessed: 4 May 2002).

[97] *Katz v US*, 389 US 347 at 353.

had been conducted on persons suspected of conspiracy to destroy government property (including, in one case, a bombing) but no court order had been sought for its authorization. The US Government attempted to rely on the express exclusion in Title III regarding non-limitation of the President's Constitutional powers to act in cases of national security. The Supreme Court held that the potential for abuse if the executive branch freely conducted wiretaps without prior judicial scrutiny outweighed any justification for an exception. The protections afforded by the Fourth Amendment therefore applied to the defendants in this case. The Court commented that:

> Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

The Court considered that the role of the judiciary was essential to ensure a proper separation of powers and protect individual privacy and freedom:

> Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates … The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy …

Another noteworthy aspect of the *Keith* case is the Court's statement that its decision was limited to cases involving domestic security; as such, the *Keith* reasoning would not necessarily apply to issues surrounding intelligence information gathering in cases involving foreign powers. Further, the Court recognized that surveillance for intelligence information gathering purposes could be different (*eg*, in intent, scope and the use of the information gathered) from surveillance for information gathering as evidence in criminal investigations. However, it elected not to elaborate on whether and how the law would differ in these two types of cases.

There have been only a handful of cases where the US courts have had to consider the legality of warrantless searches of suspected foreign agents.

In *United States v Truong*,[98] the Fourth Circuit held that these searches are justified where the "primary purpose" of the search was foreign intelligence gathering. These cases are relevant to FISA searches, in that they can be seen to exemplify a distinction between conducting a search for foreign or counterintelligence purposes, and a search for criminal investigation purposes. The former may leave some room for a warrantless search, but the latter must comply with Fourth Amendment requirements; where the former is conducted under FISA, then presumably FISA warrant/search requirements would apply.[99]

Several recent cases highlight the Constitutional role and protections in relation to electronic privacy issues.

In *Kyllo v United States*,[100] Government investigators had used a thermal imaging device to detect unusually high amounts of heat emanating from a suspect's home, based on which discovery they obtained a search warrant and found marijuana plants being grown in the suspect's home. The question before the court was whether or not the use of the thermal imager to scan the house constituted a "search" within the scope of the Fourth Amendment, and hence would have been presumptively unreasonable if performed without the requisite warrant having first been obtained. The Supreme Court reversed the Ninth Circuit's holding on this issue, following from the test in *Katz*, and ruled that surveillance of this type – where an instrument "not in general public use" was employed "to explore details of the home that would be previously unknowable without physical intrusion" – could be distinguished from purely "visual surveillance" (*ie*, "naked eye" surveillance). The majority of the Court felt that the Fourth Amendment draws both a "firm" and a "bright" line at the entrance to a person's home, and that all details – irrespective of the type, quantity or quality of the information or the value that the homeowner places on such information – occurring within that home were "intimate details" that should be "safe from prying government eyes".

Bartnicki v Vopper,[101] another major case relevant to electronic surveillance and privacy issues, was also decided by the Supreme Court in the same term. The Court ruled in this case that the broadcast of an illegally intercepted telephone call still constituted free speech that was protected by the First Amendment. The facts of *Bartnicki* are fairly unusual, in that a telephone call involving a union official who was engaged in aggressive contract negotiations with a school board was intercepted. The tapping was done by an unknown person, who then sent the recording to an official of another organization in opposition to the union. That official in turn provided the recording to a local radio station which broadcast it. The

---

98 629 F2d 908 (4th Cir 1980), *cert denied*, 454 US 1144 (1982).

99 See discussion on FISA, *infra*.

100 No 99-8508, 190 F 3d. 1041 (argued 20 February 2001; decided 11 June 2001)

101 No 99-1687, 200 F 3d. 109 (argued 5 December 2000; decided 21 May 2001).

Court's decision emphasized the unique fact situation, that the radio station had not participated in the illegal act, and the fact that the topic was a matter of public concern. These factors tipped the scale in favour of allowing dissemination in the greater public interest, even if this had a chilling effect on private speech in this case.

Although it may be unwise to attempt to generalize and make predictions based only on a few cases (particularly in light of the long line of First and Fourth Amendment cases that have come before the Supreme Court), it is noteworthy that over half of the Fourth Amendment decisions by the Supreme Court in its 2000-2001 term fell on the side of individual rights as against law enforcement powers.[102] Some commentators consider this fact "surprising" given the composition and history of the current Supreme Court.[103] However, it must also be noted that *Kyllo* was decided on a 5-4 basis, and *Bartnicki* on a 6-3 basis.[104] Given this fact, and the fact also that a decision in every case must depend on its specific facts, it is difficult, and probably overly bold, to conclude that the Supreme Court has demonstrated a clear and unwavering trend of favouring individual privacy over government surveillance and enforcement powers. Having said that, these cases do show that the Supreme Court is adept at applying Constitutional jurisprudence to the challenge posed to it by new technology (as can be seen in the majority's decision in the *Kyllo* case), and that it will scrutinize the

---

[102] Besides *Kyllo*, other Fourth Amendment cases included *Ferguson v City of Charleston*, No 99-936 (March 2001), *City of Indianopolis v Edmond*, No 99-1030 (November 2000) and *Atwater v City of Lago Vista* (April 2001). For a summary of these and other cases from the Supreme Court's 2000-2001 term, see The Oregon Advocate, "In Review: The October 2000 Term of the Supreme Court" (Vol 3, No 4, Fall 2001), available online at http://www.oregonadvocate.org/pdfs/editions/8.pdf (last accessed: 23 May 2002), and "ACLU Summary of the 2000 Supreme Court Term: Major Civil Liberties Decisions", a report by the ACLU available online at http://www.aclu.org/court/court_summary00.pdf (last accessed: 23 May 2002).

[103] *Ibid.* But see *Courting Disaster: Update 2000-2001*, a report by the People for the American Way Foundation, which expresses the view that a "very conservative" Supreme Court is well on the way to "curtailing or abolishing" some of the fundamental freedoms of Americans, and points out that many of the civil liberties cases were decided by a narrowly divided Court. The report is available online at http://www.pfaw.org/issues/judiciary/reports/courting_disaster_addendum.pdf (last accessed: 23 May 2002). For another view of the Supreme Court 2000-2001 term, see J Bleich, K Klaus and D Pearlstein, "Split Decisions: Looking Back at Term 2000", Oregon State Bar Bulletin (September/October 2001), analysing the many split decisions of the Court in that term and asserting that the "swing" vote representing the "unpredictable and widening center" of the Court holds the balance of power on many important issues. The authors also consider that many members of the current Supreme Court have, over the years, "proven Laurence Tribe's rule that constitutional space warps when confronted by new technology". The article is available online at http://www.osbar.org/2practice/bulletin/01augsept/split.htm (last accessed: 23 May 2002).

[104] *Ferguson* and *Edmond* were also split decisions (6-3 in both cases), while *Atwater* (which ruled in favour of the Government) was decided on a 5-4 basis. Of the 82 cases resolved by the Supreme Court in that term, only 38 were unanimous decisions.

Government's allegations of justified searches (under the Fourth Amendment) very closely in each case.

It will, however, be interesting to chart the development in thinking – and possibly trace the reasoning – of the Supreme Court when it faces fresh arguments about electronic surveillance and privacy, in view of September 11 and the current Government attitude (*viz*, to increase its surveillance and law enforcement powers). Prior to the passage of the PATRIOT Act, Assistant Attorney General Daniel J Bryant had sent a letter to several Senators which stated, in part, that

> … the government's interest has changed from merely conducting foreign intelligence surveillance to counter intelligence operations by other nations, to one of preventing terrorist attacks against American citizens and property within the continental United States itself. The courts have observed that even the use of deadly force is reasonable under the Fourth Amendment if used in self-defense or to protect others … Here, for Fourth Amendment purposes, the right to self-defense is not that of an individual, but that of the nation and its citizens… . If the government's heightened interest in self-defense justifies the use of deadly force, then it certainly would also justify warrantless searches.[105]

A final case that merits discussion is the *Scarfo* case,[106] in which the District Court of New Jersey had to determine if the use of a "key logging" device by the FBI violated the Fourth Amendment rights of a suspect. Mr Scarfo had been suspected of engaging in illegal gambling and loansharking operations. In a previous, authorized search (*ie*, under a warrant), computer files had been discovered, including some encrypted information. In order to decrypt the information, the FBI needed access to Mr Scarfo's passphrases, which they obtained by installing, again under a warrant, a "key logging" device on Mr Scarfo's personal computer, which device captures keystrokes made on that computer. The main pre-trial issue centered around whether the use of the "key logging" device constituted an "interception" of "wire communications" within the scope of the federal wiretap statute; if so, the defense argued, the FBI would have needed a wiretap order and not simply a search warrant. The basis for the defense argument that an "interception" (and wiretap) had been conducted was that Mr Scarfo used the computer to access the Internet via modem; and since

---

[105] See Nancy Chang, "What's So Patriotic About Trampling on the Bill of Rights?", an analysis written for the Center for Constitutional Rights, available online at http://www.ccr-ny.org/whatsnew/usa_patriot_act_1.asp; the article is also an excerpt from her book *Silencing Political Dissent: How Post-September 11 Antiterrorism Measures Threaten Our Civil Liberties* (forthcoming from Seven Stories Press).

[106] Criminal Action No 00-404, decision on the pre-trial motion discussed in this essay handed down by the District Court of New Jersey on 26 December 2001, available online at http://lawlibrary.rutgers.edu/fed/html/cr00-404-1.html (last accessed: 23 May 2002).

the "key logger" recorded every keystroke made, keystrokes entered during periods when the computer user was accessing the Internet or otherwise communicating through the modem would also have been captured (and a "wire communication" thus "intercepted").[107] The defense also alleged that the search warrants had not been properly issued and executed.

The court dismissed the defense arguments, holding, first, that the search warrant was properly issued in accordance with Fourth Amendment requirements. According to the court, that keystrokes other than the required passphrase were "certainly recorded … is of no consequence". The court analogised this to a common situation where investigators might not know the exact nature of the incriminating evidence that they are searching for until they come across it. Secondly, the court held that the FBI's use of the "key logger" did not amount to an "interception" under the federal wiretap law. On this point, the court found that the device had been configured so as to prohibit the capturing of keystrokes whenever the computer modem was activated; this meant that no interception could take place when keystrokes were entered during such periods.

In coming to its decision, the court appeared mindful of the balance that needed to be struck between individual privacy and effective law enforcement, particularly in view of rapidly advancing technology:

> [W]e must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts … As a result of this surge in so-called "cyber crime," law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.

The fact that the balancing exercise (as mentioned earlier) can only be described at a fairly general, necessarily imprecise, level, yet in coming to its conclusion a court needs to obtain and understand specific details about

---

[107] In August 2001, the court had ordered the Government to produce a full report on how the device and technique worked; in response, the Government filed a request to modify the August order, claiming a need to comply with the Classified Information Procedures Act ("CIPA"). In October 2001, the court ruled that the Government could properly invoke CIPA in this case, and that the Government's proposed unclassified summary of the device and technique would suffice to allow the defense to argue its pre-trial motion to suppress the evidence garnered thereby. For a history of the proceedings in this case and the relevant court orders and documents, see http://www.epic.org/crypto/scarfo.html (last accessed: 23 May 2002).

how a certain type of technology works, presents a striking contrast. Where the "standard" (for the balancing exercise) is necessarily expressed at a "higher", abstract level, the actual performance of the exercise has to be far more particular, detailed and meticulous. In this context, the court's earlier ruling (in October 2001) that the Government need not disclose fully how the "key logging" technique worked,[108] must be noted. The decision to allow the Government to keep much of the technology classified was made after *in camera, ex parte* hearings, and obviously the court in describing these hearings is precluded by their outcome from revealing much about the hows and whys of the process. However, since the court, in weighing the different interests of individual privacy and government power and performing the necessary balancing exercise, must examine all the technical details that are available to it in order to arrive at a fair result, the fact that laws and procedures exist which limit the access of the individual (and the public) to all the available information (albeit for legitimate and even understandable reasons such as national security), means that part of the balancing exercise is hidden from the public eye. In certain cases, as with *Scarfo*, it could also mean that the defendant must comfort herself with the court's assurance that the limited, de-classified information made publicly available is sufficient basis for her to argue her Constitutional case.

The comments of the District Judge in *Scarfo*, as to the delicacy and difficulty of the balancing exercise in cases of electronic surveillance, is reminiscent of similar opinions expressed by other judges in similar cases. In *Berger v New York*,[109] the Supreme Court had stated that "indiscriminate use [of eavesdropping devices] in law enforcement raises grave constitutional questions … Few threats to liberty exist which are greater than those posed by the use of eavesdropping devices". Similar judicial sentiments had already been expressed in *Olmstead* (by Justice Brandeis, in dissent) and in *Katz*. Taken at face value, these statements should provide some assurance that the judiciary will remain fully conscious of its role as a third party arbiter in a conflict between individual privacy and government assertion of overriding national or public interest, and that judicial decisions as to how to resolve these conflicts will not be embarked upon lightly.

D. *The PATRIOT Act and the Foreign Intelligence Surveillance Act*

FISA was enacted in 1978.[110] Among other things, FISA provided for a special court comprising US federal district judges to authorize electronic (and subsequently, physical (in 1994) and pen/trap orders (in 1998))

---

[108] *Ibid.*

[109] 388 US 41 (1967).

[110] Pub L No 95- 511, 92 Stat 1783, codified, as amended, at 50 USC §§ 1801-1811, 1821-1829, 1841-1846, 1861-62.

surveillance[111] within the US, of targets considered to be "foreign powers"[112] or agents thereof, "for the purpose of obtaining "foreign intelligence information" ("FII")[113] for the conduct of US counterintelligence,[114] where such FII cannot reasonably be obtained by normal investigative techniques. FISA authorization is not subject to the Fourth Amendment requirement of "probable cause" that is required for a warrant to be issued in the same way (*viz*, that a crime has been or will be committed), although a FISA authorization must generally be based on the court's belief that there is "probable cause" that the target in question is a foreign power or an agent thereof.[115] Surveillance authorized under FISA,

---

[111] "Electronic surveillance" is defined as "(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes". See § 1801(f).

[112] Defined as including a foreign government (whether or not recognized by the US) or component thereof, an entity controlled and directed by a foreign government, a group engaged in international terrorist activities or "in preparation therefore", or a "foreign-based political organization, not substantially composed of United States persons". The definition is therefore fairly broad; see 50 USC § 1801(a).

[113] Defined as including information that "relates to" (for non-US persons) or, for "United States persons", "necessary to" US ability to protect against potential hostile acts, counterintelligence activities, sabotage or terrorism by a foreign power (or agent thereof); or information as regards a foreign power that "relates to" US national defense, national security or the conduct of its foreign affairs; see 50 USC §1801(e)(1). The distinction between "relates to" and "necessary to" is not specified in the statute. However, it seems clear that this difference in terminology reflects the difference in statutory treatment of the two types of persons.

[114] Defined as information and activities against espionage or other intelligence activity, sabotage, assassinations conducted by or on behalf of foreign governments (or elements thereof), foreign organizations or foreign persons, or international terrorist activities.

[115] According to *US v Cavanagh* (807 F 2d 787 (9th Cir 1987)), such probable cause can be found "when facts and circumstances within the applicant's knowledge and of which he/she has reasonably trustworthy information are sufficient to warrant a person of reasonable caution to believe" the assertion. A further requirement for the "probable cause" finding is that "each of the facilities or places at which the electronic surveillance is directed is being used, or about to be used, by a foreign power or [its] agent" (§ 1805(a)(3)(B)). In determining whether or not probable cause exists, a judge "may consider past activities of the target, as well as facts and circumstances relating to [his] current or future activities": § 1805(b).

therefore, does not have to satisfy the (higher) standard and limitations imposed by the Fourth Amendment.

Under FISA, "international terrorism" is defined as activities that (1) involve endangering human life and that would either constitute a violation of the criminal laws of the US or any other state, or if committed within the US or any other state, would constitute such a violation; (2) appear intended to either intimidate or coerce a civilian population, influence government policy through intimidation or coercion, or affect the conduct of a government by assassination or kidnapping; and (3) occur "totally outside" the US, or "transcend national boundaries" through either the means employed, victims affected or locale of origin or asylum of the perpetrators.[116]

One notable feature about FISA is that it treats a "United States person" differently from a non-US person.[117] Where the intended target is a "United States person", more stringent standards have to be satisfied.[118] In addition to the differing language used in defining what constitutes FII for US and non-US persons, the definition of an "agent of a foreign power" requires that a "United States person" "knowingly engages" in (among other things) clandestine intelligence activities, sabotage or terrorism (or "acts in preparation therefore") on behalf of a foreign power, whereas no such showing of knowledge is required (for the most part) in the case of a non-US person.[119] In an Executive Order issued in 1981, the need to respect the rights of "United States persons" was made clear, to the extent that those engaged in intelligence surveillance "shall use the least intrusive collection techniques feasible within the United States or directed against U.S. persons abroad".[120]

(i) *Changes to FISA Made By the PATRIOT Act*

The PATRIOT Act brought about several major changes to FISA. One of these changes was the removal of the need for FII gathering to be the sole or

---

116 See § 1801(c).

117 50 USC §1801(i). The former is defined as "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an associated which is a foreign power, as defined in 50 USC §1801(a)(1), (2), or (3)".

118 *Supra* note 115.

119 See § 1801(b)(1) and (2).

120 EO 12333, which also prohibits the collection, retention, or dissemination of information about US persons except pursuant to procedures established by the head of the relevant agency and approved by the Attorney General. See, generally, *Legal Standards for the Intelligence Community In Conducting Electronic Surveillance*, a report made under the FY2000 Intelligence Authorization Act by the Federation of American Scientists and the National Security Agency, and submitted to Congress in February 2000; available online at http://www.fas.org/irp/nsa/standards.html (last accessed: 13 April 2002).

primary purpose of the electronic surveillance. Instead, Sec 218 of the PATRIOT Act now permits the issuance of court orders where the primary purpose of the surveillance is criminal investigation, and the gathering of FII merely forms a "significant purpose" for the surveillance. The consequence of such a change could be to allow the US Government to bypass the limitations of the Fourth Amendment and other statutory and legal protections in a criminal investigation, so long as it can show that such an investigation will involve the gathering of FII, which gathering forms a "significant purpose" for the investigation. The hitherto differing objective and nature of a foreign intelligence investigation as against a domestic criminal investigation could thus converge and overlap, with potentially privacy-eroding consequences.[121] However, FISA continues to retain the specific "probable cause" threshold, that the court believes the surveillance target is a foreign power or an agent thereof,[122] the definitions of which require some element of involvement in "clandestine intelligence activities" of some sort, or acts of sabotage or international terrorism (or acts in preparation therefor). This FISA requirement can therefore act as a minimum, but substantive, safeguard against abuse of the rather more lax standards as to purpose now in place under FISA.

Whether or not any abuses will occur also depends in part on any limitations imposed by the existing statutory definitions. To this end, it is unfortunate, and potentially difficult, that Sec 218 does not define "significant purpose".[123] It is also unfortunate that FISA continues to distinguish (for purposes of determining what constitutes FII) between information that is "related to" US national security interests, and information that is "necessary to" US national security interests; the former being the definition for FII gathered from a surveillance target who is not a "United States person" and the latter being the definition where the target is a "United States person". Neither FISA nor the PATRIOT Act clarify this difference in definitional language, and since FISA cases are classified, public guidance on actual interpretation of these phrases by the Attorney General or the FISA court is not available.

Another way in which the PATRIOT Act expanded FISA's scope was the authorization of roving wiretaps, which change thus brings FISA in line with the criminal procedures in the ECPA. Sec 206 of the PATRIOT Act permits roving wiretaps by removing the need to specify a communications carrier or similar person, where the surveillance target's actions "may have the effect of thwarting the identification of a specified person". Sec 206 therefore recognizes the reality (already acknowledged in the ECPA) that suspects under investigation can often and easily change and use various

---

[121] The origin of the requirement of a "primary purpose" can probably be traced to decisions such as the *Truong* case: *supra* n 98.

[122] This requirement was not changed by the PATRIOT Act.

[123] Nor does the Field Guidance on New Authorities Enacted in the 2001 Anti-Terrorism Legislation (issued by the US Department of Justice) refer to Sec 218.

service and communications providers and devices in order to evade surveillance. While Sec 206 clearly increases the scope of FISA surveillance, it is possible to argue that this change is appropriate and timely, in light, particularly, of the fact that roving wiretaps are already permitted for non-FISA purposes in other US statutes. However, in light of the risk that a FISA wiretap may now potentially be sought for investigations involving domestic criminal offenses (provided that the application for the wiretap satisfies the "significant purpose" standard), the expansion to include roving wiretaps within the scope of FISA also exposes the privacy restrictions of the PATRIOT Act.

For pen/trap devices used under FISA, Sec 214 of the PATRIOT Act eliminates previous requirements limiting their use to facilities that were used by foreign powers or their agents or individuals engaged in international terrorism or clandestine intelligence activities.[124] As amended, FISA now permits pen/trap orders for any investigation to gather FII that either does not concern a United States person, or to protect against international terrorism or clandestine intelligence activities (provided that where a United States person is being investigated, the investigation is not conducted solely upon the basis of activities protected by the First Amendment).[125] As with the general Pen/Trap statute, there is no "probable cause" requirement that needs to be satisfied. Instead, the court "shall" enter an order approving the installation and use of a pen/trap device if the application satisfies the requirements of § 1842 (which, as described, deals largely with the purpose of the application; it also carries several procedural requirements).

From the above comments, it is clear that the definitions of certain FISA terms (*eg*, a "United States person", "foreign power", "agent of a foreign power", "international terrorism" and "foreign intelligence information") are important in delineating the scope of surveillance orders and their implementation under FISA. These definitions were not modified by the PATRIOT Act. Given the expansive nature of the other PATRIOT Act changes, however, they serve as important safeguards against overreach and abuse of the greater powers now conferred on law enforcement by FISA.

As to the duration of FISA surveillance orders, these were (except for surveillance targeted against a foreign power)[126] previously allowed for a

---

[124] The Department of Justice had previously claimed that, although FISA pen/trap surveillance was intended to mirror the general Pen/Trap statute, this requirement constituted an additional factor that made FISA pen/trap authorizations harder to obtain, to the extent that FISA pen/trap applications were "only slightly less burdensome" than the process for obtaining an electronic surveillance order: see the analysis of the Department of Justice's proposal of mid-September 2001, printed as an appendix to the Administration's *Draft Anti-Terrorism Act of 2001: Hearing Before the House Subcommittee on the Judiciary*, 107th Congress, 1st Session 54 (2001).

[125] Sec 214(a), amending § 1842.

[126] On duration of FISA orders generally, see § 1805(e) and 1824(d). For surveillance of a foreign power (and not its agent), § 1805(e) specifies that the maximum period is one year.

maximum period of ninety days (for electronic surveillance) and forty-five days (for physical search orders), the PATRIOT Act creates a separate duration period for a FISA surveillance order involving the agent of a foreign power. Under the PATRIOT Act, such surveillance could last up to one hundred and twenty days, with extensions for up to one year.

Yet another change to FISA that expanded its scope and that was made by the PATRIOT Act is the obtaining of records relating to a person. Under FISA, the Director of the FBI or his/her designee may apply to a court for such records to be released from a list of carriers and providers, for an investigation to gather FII or an FBI investigation of international terrorism. Before the PATRIOT Act, the application for the court order had to specify that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power".[127] Under Sec 215 of the PATRIOT Act, the FBI may now obtain "tangible things (including books, records, papers, documents and other items)" from an expanded list of providers, for which it need only certify that the "tangible things" (which phrase clearly covers more than the previous category of "records") are requested in order to "protect against international terrorism or clandestine intelligence activities", regardless of whether or not the person to whom the records pertain is believed to be a "foreign power" or agent thereof.[128]

After the passage of the PATRIOT Act, the US Department of Justice apparently proposed further amendments to FISA.[129] Among other proposals, the Department recommended removing the need to link a potential target with a "foreign power" or terrorist group on the basis that the existing requirement meant FISA could not be utilized against individuals who did not have a known affiliation with any foreign state or group. The proposed change would expand the scope of FISA and enable it to be used against individuals engaged in terrorist activities. The Department also requested the removal of certain requirements with respect to multipoint roving wiretaps (*eg*, requirements relating to the need to specify the location of the facility to be tapped, if it is not known). Other proposals included extending the period of time for judicial approval of "emergency" FISA applications authorized by the Attorney General to seventy-two hours (instead of the current twenty-four), and correcting certain inconsistencies between the changes made by the PATRIOT Act and the "old" FISA.

The Department's proposals immediately roused the ire of civil liberties groups such as the CDT, which issued a point-by-point critique. With respect to the proposal to expand FISA to cover surveillance of individuals

---

127 See § 1862(a).

128 See Sec 215, PATRIOT Act.

129 See http://www.cdt.org/security/011100fisa.shtml (last accessed: 13 April 2002), reproducing the fax apparently sent by the Department to Capitol Hill, on or before 20 November 2001.

unaffiliated with a foreign state or terrorist group, CDT alleged that this would fundamentally alter the purpose of FISA, particularly in light of the fact that the PATRIOT Act had previously removed the "primary purpose" limitation. Pointing out that FISA's enactment had been based on the perceived distinction between surveillance of foreign powers (and their agents), and surveillance of other persons, where the latter was largely for the purpose of criminal investigations and where FII obtained under FISA, and FISA surveillance targets, was generally not intended for use in domestic criminal prosecutions. Based on this distinction, it was therefore not necessary for FISA surveillance orders to be subject to Constitutional and due process limitations.

The CDT's concern on this point is thus largely that an expanded FISA would permit the US Government to circumvent the restrictions on electronic surveillance currently imposed by (among other laws) Title III and the Fourth Amendment. Essentially, instead of having to satisfy the stringent standards of those laws, it would be possible to subject an individual within the US to electronic surveillance via a FISA order; and the surveillance would not necessarily even (nor would it need to) result in useful counterintelligence information.[130] In addition, it is feared that such a change would further erode the distinction between intelligence and law enforcement, at least in the context of surveillance.[131]

As the changes to FISA made by the PATRIOT Act are scheduled to expire on 31 December 2005 (being subject to the "sunset" provisions of Sec 224), whether or not this post-PATRIOT Act request for further amendments to FISA will pass muster with Congress is an important issue. It may be that any further amendment (if at all) will represent an attempt to compromise between the Department's wish to simplify its investigative tasks and the public concern that any further modification of FISA will lead to greater erosion of privacy. In any case, Congress' action or inaction on this point will be a useful indicator of post-PATRIOT Act legislative thinking.

IV. "CARNIVORE" AND THE PATRIOT ACT

Carnivore (which is now referred to as "DCS 1000" by the FBI) grew out of an earlier FBI project known as "Omnivore", work on which commenced in

---

[130] Interestingly, in late April 2002, statistics released by the US Government showed that the number of court-ordered warrants under FISA actually decreased in 2001 (where 934 were approved, compared to 1,003 in 2000). It may be, however, that the decrease could be due to factors such as a single warrant covering several surveillance requests, and investigatory reliance on other information-gathering tools such as subpoenas.

[131] See, *eg*, Jim McGee, *Bush Team Seeks Broader Surveillance Powers*, a report for the Washington Post, 2 December 2001, available online at http://www. washingtonpost. com/ac2/wp-dyn?pagename=article&node=&contentId=A44003-2001Dec1 (last accessed: 30 May 2002).

February 1997. Omnivore was, however, soon shut down due to "deficiencies that rendered the design solution unacceptable". However, in September 1998, it was switched to run on a Windows NT platform, the result of this being Carnivore, which emerged from beta testing in September 1999. Carnivore first came to public attention in July 2000, when several news articles carried reports about this new investigative tool of the FBI. Carnivore[132] works based on how the Internet operates, *viz*, information over the Internet is transmitted in separate "packets" of data, which are routed, interpreted and prioritised by computers and routers, sent via the shortest and most efficient route determined to be then available, and ultimately reassembled at the final "destination". Carnivore utilizes "packet sniffer" technology, which means it is largely similar to other network diagnostic tools employed by ISPs to manage their network traffic and troubleshoot. Unlike these other diagnostic tools, however, which cannot distinguish particular communications to the exclusion of other messages, Carnivore is apparently advanced enough to "filter" the data traffic flowing through the network in order to deliver to the FBI investigators only those data "packets" which they have been authorized to obtain under the requisite court order. In other words, Carnivore can be configured such as to intercept precisely only those communications emanating from or being delivered to the subject of the surveillance. Carnivore is installed at the facilities of an ISP to monitor data traffic moving through that ISP's networks, and as such requires the assistance and cooperation of that particular ISP.

In testimony before the US Senate in September 2000, the FBI maintained that, due to the "stringent requirements" of existing US legislation (such as Title III and ECPA) mandating intense judicial scrutiny of any wiretap application, the FBI could not and would not engage in a "broad brush acquisition" of the contents of all user communications on an ISP's network, as to do so would amount to an unauthorized wiretap under Title III.[133] In addition, Carnivore's installation on an ISP's network is in isolated fashion, meaning that it would focus only on that small segment of the network through which the target's communications was channelled; hence, Carnivore does not operate in a "Big Brother mode", accessing all subscriber traffic throughout the entire network. Further, in cases where the

---

[132] For the sake of accuracy, it must be noted that Carnivore is part of a software suite referred to by the FBI as "Dragon Ware". Where the Carnivore "packet sniffer" tool captures relevant data traffic, a program called "Packeteer" performs the processing of those packets, and another program known as "Cool Miner" then organizes and displays the processed data. However, for the sake of clarity and convenience, this essay does not distinguish between these various software programs in its use of the term "Carnivore". For a description of the Carnivore technology, its attendant legal risks and the implications for government surveillance, see E Judson Jennings, "Carnivore: US Government of Internet Surveillance Transactions" 6 Va JL & Tech 10 (Summer 2001).

[133] See Congressional Statement by Mr Donald Kerr, *supra* n 9.

relevant ISP was able to comply with the court order authorizing the surveillance, the FBI would not use Carnivore for the same purpose.

The FBI also claimed that Carnivore worked in such a way that it possesses "key legal, evidentiary and privacy-enhancing features", and hence Carnivore would actually improve privacy protection in many instances, *eg*, where it is employed in "pen register" or "trap and trace" mode. This is because many conventional devices such as commercial "sniffers", when operated in the context of differing network protocols, dynamic IP addressing and non-uniform uses of the transactional information attached to a transmitted communication (*eg*, the header and subject line), either collect too much information (*ie*, going beyond what was authorized by the court order) or do not collect the information sought at all. In comparison, Carnivore's "surgical" precision and filtering ability, combined with the fact that the processing of the data "packets" largely takes place unseen by humans (who ultimately receive and view only the processed, filtered data), means it can be tailored to collect only specific, targeted information.[134]

It is interesting that the FBI seems to have admitted in its testimony that certain electronic surveillance tools did not operate with as much precision as the detailed specificity of the authorizing court order would seem to envisage.[135] Without going so far as to admit that its use of pre-Carnivore surveillance technology resulted in its agents actually viewing and possessing a great deal more information than was authorized to be collected by the court order, the FBI's testimony on this point does at least raise the question whether simply requiring that certain information be provided to the court in an application for a wiretap order, and that the court be satisfied that probable cause exists, is sufficient to safeguard a person's privacy in his/her electronic communications. This in turn raises the question whether the mere fact of specificity (being those details required to apply for and obtain a court order) achieves any purpose other than the admittedly important possibility of acting as a deterrent to frivolous or excessive applications for wiretaps. If the answer to either or both questions is no, how much assurance can one get from the knowledge that such particularity is stipulated by law?

In the FBI's Senate testimony, the FBI also pointed out that Congress has itself played an active role in ensuring that electronic surveillance legislation and its impact on privacy are first carefully considered before any new law is enacted or existing law amended. Taken together, this

---

[134] But see Geoffrey A North, "Carnivore in Cyberspace: Extending the Electronic Communication Privacy Act's Framework to Carnivore Surveillance" (2002) 28 Rutgers Computer & Tech L J 155, pointing out that the technology behind Carnivore has the ability to first gather all electronic communications before filtering out those not warranting investigation.

[135] See, *eg*, the discussion of Title III, *supra* n 77-81 (and accompanying main text) and the list of facts required to be stated and determined before the court can authorize a wiretap.

means that electronic surveillance powers come under the scrutiny of all three branches of government: the executive (through the senior federal officers who must first approve the application to court for a wiretap order), the judiciary (through its scrutiny of the application) and the legislative (through Congressional examination and review).

The FBI had also requested an independent "technical" review of Carnivore, which was conducted by the Illinois Institute of Technology Research Institute ("IITRI"). In its Report,[136] IITRI expressly stated that "questions of constitutionality and of illegal activity by the FBI" were excluded from the scope of its review. However, it expressed concern that the use of Carnivore without safeguards (such as those recommended in the Report) would "fuel the concerns of responsible privacy advocates and [reduce] the privacy expectations by citizens at large", as well as "[increase] public concern about the potential unauthorized activity of law enforcement agents".

The IITRI Report was greeted with relief by the FBI and criticism by privacy advocates.[137] Essentially, the IITRI concluded that Carnivore "reduces, but does not eliminate" the risk of unauthorized collection of electronic communications (including intentional unauthorized acquisition of such information), and despite apparent sound operating procedures and practices, does not provide "protections commensurate with the level of the risks". In a public statement, the Electronic Privacy Information Center ("EPIC") highlighted several findings of the IITRI that it considered revealing of Carnivore's weaknesses in terms of privacy protection; these included the fact that Carnivore can, if "incorrectly configured", conduct "broad sweeps" and "record any traffic it monitors". When added to the fact that the system also lacked individual accountability (*eg*, it is very difficult to track down who set and who changed particular filter settings), this feature opens the door to potential, possibly intentional abuse. EPIC thought that such weaknesses constituted an "inherent flaw" in the system that was not removable by means of a technical "fix". EPIC also took the opportunity to point out certain discrepancies between the FBI's public claims about the filtering ability of Carnivore[138] and the statements and

---

[136] *Independent Review of the Carnivore System: Final Report*, prepared by the IITRI and released on 8 December 2000. The Report is available online at http://www.cdt.org/security/carnivore/001214carniv_final.pdf (last accessed: 3 May 2002).

[137] See, *eg*, the 1 December 2000 comments by the ACLU on the IITRI's draft report (available online at http://www.aclu.org/news/2000/carnivore_comments.html, last accessed: 20 May 2002), reiterating earlier objections to the composition and scope of work of the IITRI team. See also the Comments on the Carnivore System Technical Review by leading computer scientists (Stephen Bellovin and Matt Blaze of AT & T Laboratories, David Farber of the University of Pennsylvania, Peter Neumann of SRI International and Eugene Spafford of Purdue University CERIAS) released on 3 December 2000 and available at http://www.cdt.org/security/carnivore/001203comments.html (last accessed: 21 May 2002).

[138] See, *eg*, Mr Donald Kerr's testimony, *supra* n 9.

facts found in some of the documents publicly released by the FBI in relation to Carnivore.

The FBI's use of Carnivore is a prime example of law enforcement using cutting-edge technology to combat crimes utilizing similarly advanced technology. In relation to terrorism, where there seems no doubt that the Internet, email, encryption and other technology is regularly used by terrorist groups including Osama bin Laden and Al-Qaeda,[139] it has been pointed out that "[e]very day that passes with outdated statutes and the old rules of engagement is a day that terrorists have a competitive advantage".[140]

It is probably true to say, however, that the primary concern over Carnivore is the very secrecy with which the FBI has elected to veil it. In July 2000, shortly after the existence of Carnivore was made public, EPIC filed a request under the US Freedom of Information Act (the "FOIA"), seeking further details about Carnivore (including its source code) and raising concerns regarding the implications for electronic privacy. Between October 2000 and May 2002, documents were released by the FBI at various times in response to the FOIA request (although the FBI had to be ordered by the court to conduct a further search for documents in March 2002). The most recently released documents included an FBI memo that detailed how the use of Carnivore in at least one instance may have disrupted an anti-terrorism investigation relating to Osama bin Laden, as Carnivore did not "work correctly" and hence picked up emails from persons other than the target (which mistake could constitute a violation of the federal wiretap laws). These documents therefore reveal that the technology behind Carnivore does not necessarily work as intended in practice, and this fact must certainly colour any conviction as to the effectiveness of Carnivore in protecting privacy.

Another, related, concern raised by the use of Carnivore is the relatively indiscriminate "first stage" (*ie*, pre-filtering phase) of information gathering.[141] Although it is said that Carnivore does not "read and record all incoming and outgoing email messages" (including header information) but rather "stores packets for later analysis only after they are positively linked by the filter settings to a target", that it cannot monitor the Internet usage habits of all an ISP's users (recording only some files retrieved by a target) or monitor all the traffic routed through that ISP,[142] the reluctance of the

---

[139] See, *eg*, J Lewis, "Carnivore – The FBI's Surveillance System: Is It A Rampaging Emailasaurus Rex Devouring Your Constitutional Rights?" 23 Whittier L Rev 317 (Winter 2001).

[140] Attorney General John Ashcroft, testifying before the House Judiciary Committee on 24 September 2001, regarding the draft Anti-Terrorism Act. Testimony available online at http://commdocs.house.gov/committees/judiciary/hju75288.000/hju75288_0f.htm (last accessed: 16 May 2002).

[141] See North, *supra* n 134, Jennings, *supra* n 132 and Lewis, *supra* n 139.

[142] See the IITRI Report, *supra* n 136.

FBI to discuss the technology publicly only contributes to the uncertainty over what, exactly, Carnivore can and cannot do.

This lack of public disclosure, coupled with the insistence of the FBI that sufficient legal safeguards exist in current legislation to ensure that the technology is not abused (which insistence the FBI may feel justifies keeping the exact scope and operational capabilities of Carnivore secret), means that the official attitude toward demands for more public discussion and transparency is to simply ask the public to "trust us, we're the Government". While public trust in the legitimate intentions of a democratically-elected and stable government is certainly necessary, when the corresponding rationale given for changes to those very laws that are meant to check abuses is simply "national security" (in all its imprecision[143]), it is natural and reasonable to ask that same Government to be forthcoming as to how it intends to safeguard privacy protections and civil liberties.

Under the PATRIOT Act, changes to the Pen/Trap statute described earlier could affect the extent to which, and how, law enforcement officials deploy Carnivore. For example, Carnivore allegedly has the capability and functionality to act as pen/trap devices; given that these have now been clarified to be usable in obtaining non-content information in the form of electronic communications, Carnivore can thus be deployed under the far less rigorous standards of the Pen/Trap statute (where a judge "shall" make the order to install and use the device upon the Government's certification that the information obtained thereby "is likely to be relevant to an ongoing criminal investigation") rather than the "probable cause" requirement for a search warrant or interception order. Further, the expansion of FISA to include roving wiretaps, and its applicability to cases where "a significant purpose" of the surveillance is to obtain foreign intelligence information (rather than the pre-PATRIOT Act standard of that being "the purpose"), means that Carnivore could also be used under FISA instead of non-FISA laws.

In December 2001, the 21st Century Department of Justice Appropriations Authorization Act[144] was passed by the Senate. Among other things, the Act requires the Attorney General to report periodically on the use of Carnivore for interceptions using wiretaps, pen register and trap and trace devices. As such, it can be argued that this further adds to the safeguards against possible abuse of Carnivore by the FBI.

---

[143] The phrase "national security" necessarily varies in meaning and scope according to context, perception/perspective, and in light of different types and effects of the events affecting a country's survival. See Banks and Bowman, *supra* n 4.

[144] HR 2215 (107th Congress, 1st Session).

V. Some Further Developments

Several post-PATRIOT Act developments are noteworthy in that they emphasize the US Government's determination to bolster and continue its anti-terrorism efforts.

A. *The Attorney General Guidelines*

On 30 May 2002, the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (the "Guidelines") were released. The Guidelines have been in existence since 1976, although they have been amended over the years; they provide general guidance for the FBI's investigations of crime and criminal intelligence by classifying various types of crimes and their investigations, and delineating the methods and scope of such investigations. According to Attorney General Ashcroft, the reissued Guidelines are intended to encapsulate four "overriding principles": first, that "the war against terrorism is the highest priority and central mission" of the FBI; secondly, that the prevention of terrorism is the key objective; thirdly, that the effective detection, investigation and prevention of terrorism should not be hindered by unnecessary red tape and bureaucracy; and fourthly, that in identifying potential terrorist threats, the FBI must "draw proactively on all lawful sources of information".[145]

The Guidelines make clear that, particularly with respect to the investigation of terrorist crimes and terrorism enterprise, the FBI "shall not hesitate to use any lawful techniques consistent with [the] Guidelines, even if intrusive, where the intrusiveness is warranted in light of the seriousness of a crime or the strength of the information indicating its commission". Factors relevant to intrusiveness include the effect on an individual's privacy and potential damage to reputation. The Guidelines make clear, however, that the conduct of electronic surveillance must comply with the relevant laws, *eg*, the wiretap law.

Perhaps the most significant Guidelines directly relevant to electronic privacy are found in Part VI, which deals with preventing terrorism. Part VI clarifies that authorized law enforcement activities of the FBI include "surfing the Internet as any member of the public might do … to detect terrorist and other criminal activities" (including identifying bulletin boards, chat rooms and websites through which information such as bomb making instructions are disseminated). The activities authorized in Part VI can be undertaken even in the absence of the checking of leads or the type of

---

[145] See Prepared Remarks of Attorney General John Ashcroft: Attorney General Guidelines, 30 May 2002, available online at http://www.usdoj.gov/ag/speeches/2002/53002agpreparedremarks.htm (last accessed: 18 June 2002). The text of the Guidelines are available from the website of the US Department of Justice's Office of Legal Policy, at http://www.usdoj.gov/olp/generalcrimes2.pdf (last accessed: 18 June 2002).

investigations authorized in earlier Parts of the Guidelines. Specifically, the FBI may "operate and participate in identification, tracking and information systems" in order to detect and prosecute terrorist activities, including identifying and locating terrorists. Information systems include databases and information obtained from previous investigations, other governmental entities (including foreign intelligence information) and any "publicly available information" (including that obtained from commercial sources). The FBI may also attend public events and visit public places, like any other member of the public, provided that no information collected therefrom is retained unless it relates to "potential criminal or terrorist activity".

The lack of judicial or other oversight, and the generality and breadth of the authorized activities in Part VI, have raised the ire of privacy advocates, who believe that the wide scope of Part VI allows the FBI to go on "fishing expeditions" where there is no evidence a crime has been or will be committed.[146] The Guidelines also underscore the fact that, besides electronic surveillance and monitoring of the sort covered by the wiretap and similar laws, law enforcement and intelligence gathering can utilize new technological tools in ways not covered by these laws, *ie*, being thereby considered "lawful" investigatory techniques.

B. *Organizing Homeland Security*

In September 2001, President Bush had announced through executive order the creation of a new Office of Homeland Security at the White House, headed by Governor Tom Ridge. Dissatisfaction with the scope of authority and effectiveness of this Office, largely centering around budgetary limitations and the apparent lack of an immediate strategy led certain members of Congress to propose various bills in April and May 2002 that would either clearly empower Mr Ridge or, more boldly, create an entirely new Department of Homeland Security, to which umbrella authority would be transferred existing agencies involved in homeland security activities (such as the Customs Service, the border management and law enforcement arms of the Immigration and Naturalization Service, the Coast Guard and parts of the FBI). In June 2002, President Bush responded by sending a bill to Congress proposing the creation of a similar federal Department of Homeland Security, which would have as its functions the prevention of terrorist attacks in the US, the reduction of the vulnerability of the US to terrorism, and the minimization of damage in the event of any terrorist attacks in the US. The Department is intended to unify the homeland

---

[146] See the ACLU's open letter, *Analysis of Legal Changes to the Attorney General Guidelines*, 5 June 2002, available online at http://www.aclu.org/congress/l060602c.html; and EPIC's position on the Guidelines, available online at http://www.epic.org/privacy/fbi/ (last accessed: 19 June 2002).

security structure of the US by combining the existing "patchwork" of government agencies and activities in this area into a single department with a clear primary mission.[147]

The coordination and integration of a large number of diverse, potentially overlapping, existing agencies, as well as the funding of a unifying structure for such agencies, are immense and difficult tasks. In addition, it will be necessary to define and implement clear lines of authority, specific agency missions, a meaningful organizational structure and a unifying corporate culture. Given the urgency and priority accorded to the prevention and combating of terrorism by the US Government, it is difficult to see how these tasks can be accomplished quickly and effectively. While it is encouraging to see that the US Government seems not only willing to acknowledge but also to overcome the confusion and bureaucracy within and among various federal agencies whose anti-terrorism efforts may overlap with one another's, it would be impractical to think that a new Department of Homeland Security could in the very short term make significant changes to the direction, emphasis or even implementation of current US Government policy. However, it is also unlikely that the Government will in the short to medium term waver from or alter its stance as regards giving the highest priority to the fight against terrorism. To that extent, it is likely that further programs, guidelines and implementation proposals will continue to be refined and issued by the various federal agencies charged with anti-terrorism efforts, either separately or from within a single organizational structure.

VI. Summary and Conclusion

It has been said that policymakers should "look not at what technology makes possible, but at the core values the [US] Constitution enshrines."[148] To that one may add, in the context of a post-September 11 world, that while effective and appropriate responses must be developed to counter the threat of terrorism, such responses also must not unduly restrict personal privacy. If, in the interests of national security, the counter-terrorism policies and measures adopted by a government sacrifice a disproportionate amount of individual privacy and liberty, the "very center of liberal societies … that is the real target of international terrorism"[149] will have

---

147 On the existing Office and proposed Department for Homeland Security, see the White House documents at http://www.whitehouse.gov/homeland/. On the history, issues and developments surrounding homeland security since 11 September 2001, see http://www.whitehouse.gov/homeland/ (last accessed: 19 June 2002).

148 Laurence Tribe, "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier", the keynote address at the First Conference on Computers, Freedom and Privacy (Boston, March 1991), cited in Robert A Reilly, "Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward" 6 Richmond JL & Tech 6 (Fall 1999).

149 Merl, *supra* n 7, at 259.

been destroyed, from within that society. The fact that the "balancing exercise" that has to be performed, to weigh the interests of national security against that of individual freedom and privacy, is not a precise test adds to the difficulty of this enterprise.

What then, is the final analysis of the PATRIOT Act in this respect? From the foregoing discussion, it must be clear that those provisions of the PATRIOT Act concerning electronic surveillance cannot be looked at in isolation from judicial observations regarding Constitutional safeguards against the over-zealous use of such surveillance technology by government agencies. In this regard, Attorney General Ashcroft's remarks to the House Judiciary Committee on 24 September 2001 are worth noting:

> [T]here is absolutely no guarantee that [the PATRIOT Act] safeguards would have avoided the September 11 occurrence. We do know that without them, the occurrence took place, and we do know that each of them would strengthen our ability to curtail, disrupt and prevent terrorism. But we have absolutely no assurance. Nor can I assure this Committee that we won't have terrorist attacks in the future. The mere fact that we can't do everything should not keep us from doing what we can do …"[150]

At the same hearing, Mr Ashcroft also stated that, despite the "clear and present danger" which terrorism poses to America and Americans, the rights guaranteed to Americans under the Constitution would not be changed by the new legislation. However, he went on to say that the fight against terrorism is no longer "merely or primarily a criminal justice endeavor" but rather involves the defense of America and its citizens. By that statement, Mr Ashcroft has clearly indicated that national security concerns figure extremely highly in – and form the predominant interest behind – the US' post-September 11 anti-terrorism proposals. In characterizing any proposed, potentially restrictive, measures as being in the interests of defense and national security, the resulting public perception – and hence acceptance – could be that there is a greater, more pressing and heightened need for such measures. In other words, where the pursuit of "domestic criminal justice" might seem a necessary and constant fact of everyday life, the argument that terrorism constitutes a "clear and present danger" to individual safety and national security strikes a more urgent note, in that such dangers need to be met with all means and tools available to governments to combat them.

From the public statements of US Government officials and agencies, it seems clear that the US Government does not believe the PATRIOT Act (and its predecessor bills) affect Constitutional rights of privacy to any significant extent. However, as has been pointed out by EPIC, the ACLU,

---

[150] *Supra* n 140.

the CDT and other privacy groups and advocates, it is also clear that the "pro-surveillance" provisions of the PATRIOT Act discussed in this essay constitute a very real threat to privacy, in the sense that the expanded powers conferred on law enforcement officers by the PATRIOT Act may be more easily abused because of the following factors:

- the decrease in judicial scrutiny over the conduct of Government surveillance (*eg*, through the nationwide applicability of search warrants and pen/trap orders);
- the secrecy of FISA court proceedings;
- the uncertainty surrounding the capabilities and operations of Carnivore;
- the legislative history of Title III and ECPA (*eg*, as regards the increasing list of crimes for which wiretaps can be ordered and the fact that few applications for court authorizations seem to be refused);
- the merging of the intelligence and law enforcement functions of Government agencies (*eg*, through the information sharing provisions of the PATRIOT Act and the relaxing of the "foreign intelligence" purposes of FISA); and
- the fear that some of the PATRIOT Act's provisions might allow the Government to circumvent the requirements and safeguards of the wiretap law and the Fourth Amendment in a criminal investigation (*eg*, by utilizing a FISA application instead).

As against these risks and problems, the safeguards and procedures enacted by the PATRIOT Act have to be weighed. These include the requirement that records of pen/trap devices be kept and delivered to the court, the implementation of procedures governing disclosure of information sharing amongst agencies, the provision of Congressional oversight with respect to information regarding production of tangible things and the imposition of civil liability for unauthorized disclosures by investigative or law enforcement officers or their agencies or departments.[151] Most importantly, the "sunset" provisions of Sec 224 may act as a kind of "reporting benchmark" for the effectiveness of many of the changes made to US surveillance and privacy laws by the PATRIOT Act.

In a speech at New York University Law School in October 2001, Supreme Court Justice Stephen Breyer spoke of the complex privacy problems – and the difficulty with crafting appropriate legal solutions – posed by technology.[152] He recognized that changes to privacy law must

---

[151] Sec 216(3), 203, 215 and 223 respectively.

[152] Justice Stephen Breyer, The Fall 2001 James Madison Lecture at New York University Law School, on "Our Democratic Constitution", held on 22 October 2001, available online

balance societal values with a prediction as to the further development of technology, and considered that the complexity of the problems called for a form of "participatory democracy", where ordinary citizens, the media, scientists, lawyers, lawmakers and administrators would all engage in the process of evolving the appropriate legal responses. He thought that "participatory democracy" of this type called for "judicial caution" and modesty, pointing to *Bartnicki* and *Kyllo* as recent instances where the Supreme Court has exercised restraint in interfering with the process of "participatory democracy" (by issuing a very narrow holding in the former case, and merely "pouring old wine into new technological bottles" in the latter case). Finally, Justice Breyer stated that

> It is important that the public, trying to cope with the problems of Nation, State, and local community, understand that the Constitution does not resolve, and was not intended to resolve, society's problems. Rather, the Constitution provides a framework for the creation of democratically determined solutions, which protect each individual's basic liberties and assures that individual equal respect by government, while securing a democratic form of government. We judges cannot insist that Americans participate in that government, but we can make clear that our Constitution depends upon it.

On March 8, 2002, almost six months after the terrorist attacks of September 11, the ACLU issued a statement alleging that the PATRIOT Act and other laws and measures introduced by the Government in that six-month period have contributed toward an "ongoing pattern of erosion" of civil liberties in America.[153] The ACLU urged the adoption of a two-pronged "necessary and defensible" test for each Government anti-terrorism proposal that would restrict privacy. The test would necessitate asking the following questions: (1) Does the Government already possess the resources to combat the problem that the new proposal is meant to address? (2) Is the proposal "narrowly tailored [so as] to limit the adverse impact on civil liberties"? And (3) Does the proposal genuinely combat terrorism, or does it represent a wider legislative change unrelated to September 11?

Without taking at face value the ACLU's assertions and suspicions about executive eagerness to restrict privacy by expanding its powers, the proposal of a "necessary and defensible" test echoes, for the executive branch, the call for restraint (by the judiciary) from Justice Breyer. Similarly, the ACLU's role (and that of other advocacy and awareness groups) in raising public consciousness and compelling wider discussion of

---

at http://www.supremecourtus.gov/publicinfo/speeches/sp_10-22-01.html (last accessed: 22 May 2002).

[153] See the ACLU press release, "On Eve of Six Month Anniversary of September 11, ACLU Says Terrorist Attacks Have Changed American Law, Society", 8 March 2002, available online at http://www.aclu.org/news/2002/n030802c.html (last accessed: 22 May 2002).

issues, puts into action Justice Breyer's plea for "participatory democracy". The CDT has also called for "active vigilance" of "empowered individuals" on privacy issues, particularly given the global reach and impact of the Internet.[154] Against these appeals for public awareness and open discussion, matters such as the FBI's closeness regarding Carnivore, the secrecy of FISA proceedings and the lack of information about detainees and immigration arrests[155] stand in fairly sharp contrast.

Studies have identified four types[156] of persons to show different public attitudes toward balancing the rights of individuals with the needs of society: (1) "privacy libertarianism" (who value individual autonomy); (2) "lifestyle conservatives" (for whom the benefits of privacy do not extend to issues of morality); (3) "harm principle liberals" (who generally are in agreement with the privacy libertarians but who possess a more acute concern for public safety);[157] and (4) "classical conservatives" (who would consider the need for the prevention of harm to be paramount, and hence would not value lifestyle privacy). The four groups thus show a range of positions and fairly substantial differences regarding the right of governments (and society at large) to regulate individual behavior in relation to matters that impinge on an individual's privacy; *eg*, where group (1) would tend to believe that privacy rights are essential for individual freedom (and hence that any government intervention would need to be minimal), group (4) would tend to believe that government (as representing society collectively) has a right to regulate individual behavior, particularly in areas they would consider damaging to society (such as morality).

---

[154] J Berman and P Bruening, *Is Privacy Still Possible in the Twenty-First Century?*, a publication of the CDT, available online at http://www.cdt.org/publications/privacystill.shtml (last accessed: 24 May 2002). The authors point to incidents such as Doubleclick Inc's drawback from its plan to incorporate its online databases with the offline ones of one of its acquired companies (Abacus Direct) after public outcry and the commencement of class action litigation, and to Intel's disabling of a tracking function on its Pentium III chip, as successful examples of such individual empowerment.

[155] See, *eg*, "Amnesty International's Concerns Regarding Post-September 11 Detentions in the USA", a memorandum released on 14 March 2002, which alleges not only lack of information about the numbers, names and locations of detainees, but also refers to the length of their detentions, the conditions thereof and the possibility of "closed door" hearings for "special cases", as prescribed in a memorandum issued by the US Chief Immigration Judge on 21 September 2001. The Amnesty International memorandum is available online at http://www.amnesty-usa.org/usacrisis/9.11.detentions2.pdf (last accessed: 23 May 2002).

[156] See John F Kozlowicz and Charles E Cottle, "Conceptions of Privacy: A Q-Method Study of Lay and Professional Viewpoints", a paper prepared for delivery at the 9th Annual Conference on the Scientific Study of Subjectivity, 7-9 October 1993, at the School of Journalism, University of Missouri-Columbia; study available online at http://facstaff.uww.edu/cottlec/QArchive/privacy.htm (last accessed: 15 April 2002).

[157] Group (3) therefore embodies John Stuart Mill's "harm principle", *viz*, "the only purpose for which power can be rightfully exercised over any member of a civilized community, against his or her will, is to prevent harm to others".

If Justice Breyer's call for "participatory democracy" is to be respected, the fact that a community is made up of individuals who may fall variously into each of the four groups must be taken into account. The ACLU, EPIC and other privacy advocates do not represent all these groups; however, they provide an important foil to government officials who support greater government regulation (and increased powers for the enforcement thereof). In the US, the legal changes introduced through the PATRIOT Act show that Congress, after careful scrutiny of the needs, issues and problems arising from the events of September 11, elected to give the executive Government expanded powers in recognition of the "greater" claims of anti-terrorism and national security, while attempting to minimize unnecessary restrictions to individual privacy (*eg*, through the insistence on "sunset" provisions). Such close and continuing Congressional scrutiny of the Government's exercise of its increased powers and of its anti-terrorism efforts[158] is to be applauded. At the same time, privacy groups have kept pressure on the Government by analyzing its proposals closely and providing the public with information, documents and news.[159]

Moving beyond domestic US law and concerns, the Task Force on Information Exchange and Financial Privacy released a report on "Financial Privacy, Law Enforcement and Terrorism"[160] in March 2002. The Report analyses current and proposed US and international laws and programs governing international information exchange policies (including the PATRIOT Act and the EU Savings Tax Directive), in the context of money laundering and tax administration programs. In the Report, the Task Force concluded that it may be possible to "achieve the dual objectives, usually portrayed as competing, of improving law enforcement and national security, and respecting the rights, enhancing the privacy and maintaining the standard of living for law-abiding Americans". The Task Force noted that attempts to systemize international information exchange programs began only after September 11 (*eg*, through the setting up of an

---

[158] Between 3 October 2001 and 17 April 2002, the various Subcommittees of as well as the full Judiciary Committee held 14 hearings on terrorism, including matters such as oversight of the Department of Justice in its anti-terrorism efforts, the threat of new technology (such as biometrics) and the need to protect constitutional freedom in the face of terrorism. The full list of Senate Judiciary Committee hearings is available online at http://judiciary.senate.gov; information about other Senate Committees and hearings are available from the official Senate website at http://www.senate.gov.

[159] See, *eg*, the websites of the ACLU, EPIC, and the CDT, among many others.

[160] The Task Force was set up by the Prosperity Institute, a US-based educational and research organization; the Report was released on 25 March 2002 and is available online at http://www.prosperity-institute.org/projects/PI-TF-Report.pdf (last accessed: 30 May 2002). The Task Force criticized the PATRIOT Act for expanding the pre-existing reporting system for money laundering activities, preferring instead an information exchange system involving closer cooperation between financial institutions and governments, combining computer technology (for quick and sophisticated matching of government watch list information with data in financial databases) and high legal standards and practices (to ensure the proper use and safeguarding of such information).

international terrorism database overseen by Interpol), and calls for the US to spearhead a Privacy and International Exchange Convention that would export (*ie*, internationalize) traditional US legal principles such as those espoused by the Fourth Amendment.

To the extent that the PATRIOT Act exemplifies the current US executive and Congressional approach toward combating terrorism, one can only hope that similar intensive policy, legislative and public scrutiny (as witnessed by the number and scope of Congressional hearings on this issue both prior to and after the passage of the PATRIOT Act, and the continuing commentary and follow-up actions by privacy advocates and the media in the US) will take place in any serious attempt to adopt or follow the US approach. In this context, the continuing media and public attention toward new surveillance technology in the US – from proposals for a "national ID card" to the use of biometrics and facial recognition software – is helpful. At the same time, the limitations and privacy risks identified in the PATRIOT Act must be noted, and a similar "balancing exercise" between national security/foreign affairs interests and individual privacy rights and considerations conducted. Given the US' long history of Constitutional and judicial checks on executive power, it may be that, come December 2005, when many of the more extreme surveillance provisions of the PATRIOT Act "sunset", it will be possible to conclude that the US Government's actions continue to "uphold the principles of a democratic society, accountable government and international law, and that all decisions are taken in a manner consistent with the Constitution."[161]

---

[161] Quote taken from the "ten point" Statement in Defense of Freedom, issued on 20 September 2001 and supported by over 300 law professors, 40 computer scientists and 150 organizations (including the In Defense of Freedom Coalition), available online at http://www.indefenseoffreedom.org (last accessed: 28 May 2002).