UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 2

Fall 2000

Regulating the Free Flow of Information: a Privacy Czar as the Ultimate Big Brother, 19 J. Marshall J. Computer & Info. L. 37 (2000)

Jonathan M. Winer

REGULATING THE FREE FLOW OF INFORMATION: A PRIVACY CZAR AS THE ULTIMATE BIG BROTHER

by JONATHAN M. WINER†

I. INTRODUCTION

The free flow of information is critical to any open society. In the United States, a tradition of open information has been central in building American democracy, providing the intellectual oxygen for the development of American freedom, knowledge, technology, and commerce. In contrast to the right to communicate and obtain information on practically anything, privacy has historically not been an established right in the United States, except as a right against physical trespass by the government and in the area of reproductive freedom. A Federal Data Protection Agency, or privacy czar, given the mandate to treat control over individual information as a fundamental human right would necessarily have the responsibility of limiting the unauthorized collection, use, and dissemination of personal information, as have its counterparts in other countries. Such a person or entity, empowered to engage in rulemaking, enforcement, and adjudication to protect individual privacy, could transform the collection, use, or dissemination of any information pertaining to individuals in the United States into regulated acts, making unless exceptions were created by statute, anyone engaged in the activity a member of a regulated industry. In other countries, privacy czars have invariably proven to be privacy advocates. As advocates, they have taken active stances to press for policies that would discourage the free flow of information about persons and limit the dissemination of such information, regardless of the impact on other equities, including long-established rights such as freedom of expression. While the First Amendment would provide some constraint upon a United States privacy czar's ability to limit the dissemination of information, a strong pro-privacy czar would be likely to undertake efforts to bootstrap privacy rights over

† Esq., Alston & Bird, Washington, D.C. Formerly Deputy Assistant U.S. Secretary of State, International Law Enforcement.

other rights indirectly. One obvious technique would be to create a system that coerces adherence to privacy standards developed in other jurisdictions, an approach going through its trial run as a consequence of the recent negotiation of safe harbor provisions on privacy between the United States ("U.S.") and the European Union ("E.U.").

A U.S. privacy czar with more limited powers, who could offer guidance and moral suasion but not regulate, does not remedy this problem. On the one hand, such an entity would not be able to protect individuals against actual abuses. Yet a U.S. privacy czar would, like its foreign counterparts, inevitably align with privacy constituency group pressures to advocate comprehensive privacy policies of the kind adopted in the European Union and Canada.

Under either model for a privacy czar, the U.S. could place at risk essential U.S. values and freedoms, including constitutional protections under the First Amendment, and cause serious practical harm to U.S. technological innovation, economic competitiveness, and governance. These problems are inherent in the privacy czar concept, unavoidable under the U.S. system of government, and already evident in the actions taken by privacy czars elsewhere. No privacy czar is needed to create greater harmonization, as market forces are rapidly forcing harmonized practices concerning personal information without such a position. The current U.S. approach, which adds a counselor in the White House providing guidance to the president to supplement the authority of existing financial regulators and the Federal Trade Commission ("FTC"), industry self-regulation, market factors, and the political process, is functioning adequately. Informed public discussion of trade-offs between the unfettered right to privacy and the unfettered uses of personal data will prove more effective in protecting privacy and other essential freedoms in the long run than all of the work of the world's growing array of data protection czars, commissioners, and agencies.

II. CONCEPTUAL ISSUES—WHY A PRIVACY CZAR AND NOT AN ANIMAL RIGHTS CZAR?

New information technologies have created an unprecedented ability to collect, use, and disseminate information of all kinds, including information on individuals.[1] In 1999 and 2000, serious privacy abuses have

1. *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcment in the Protection of Personal Information* <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm #1A> (accessed Dec. 1, 2000). These technologies began in the post-World War II period with the computer, which dramatically reduced the costs of storing information about persons, and made it, for the first time, readily manipulated. From there developed the networked computer telecommunications systems that could transport information as well as voice, electronic linkages of the world's financial services sectors, photocopying and facsimile devices, the personal computer, electronic mail, the Internet, and over the past dec-

been alleged against a wide range of well-known businesses and institutions: Amazon.com, the presidential campaign site of Vice President Gore, the Web site of the U.S. drug czar, tracking mechanisms on the Intel Pentium III chip, unintentional disclosure of e-mails involving sensitive health matters by Kaiser Permanente, and core new economy businesses such as Geocities, Intuit, Microsoft, Netscape, RealNetworks, and Yahoo.[2] Significantly, with the possible exception of the drug czar case, the alleged abuses have involved entities tracking data for marketing purposes or, as one privacy skeptic has described it, "with the intent of getting people to buy more stuff."[3]

---

ade, http and the other standardizing protocols used to make the World Wide Web interoperable from many platforms. The result is a linking together of separate sources of information into an increasingly accessible, if not yet unified searchable corpus of digitized data. For individuals, the convergence of these technologies means potential online access by any number of persons to their health records, credit history, banking transactions, local and long-distance telephone calls, pay-per-view, VCR rental, cable, and other video records, records of an Internet service provider, and purchases made through direct mail or telephone ordering, as the Clinton Administration's privacy czar, Peter Swire, has observed.

2. *See FTC Investigation of Amazon's Alexa, Compl. of Richard Smith* (Dec. 1999) Bloomberg News, Feb. 8, 2000; Will Rodger, *Computer Cursor Could Be Used to Spy,* USA Today 4A (Nov. 30, 1999); Junkbusters, *Privacy Advocates Call on Congress to Investigate "Cookiegate"* <http://www.junkbusters.com/ht/en/nr38.html> (June 22, 2000); *DoubleClick planned acquisition of Abacus and FTC investigation of DoubleClick,* USA Today (June 7, 2000); Statement of Jodie Bernstein, Director, Bureau of Consumer Protection, *Activists charge DoubleClick double cross FTC* <http://www.ftc.gov/opa/2000/02/dblclickstajb.htm> (Feb. 16, 2000); FTC, *Online Pharmacies Settle FTC Charges* <http://www.ftc.gov/opa/2000/07/iog.htm> (accessed Dec. 6, 2000); FTC, *In the Matter of Geocities* <http://www.ftc.gov/os/1998/9808/index.htm> (accessed Dec. 6, 2000); CBS MarketWatch, *Privacy Groups Plan Intel Boycott* <http://cbs.marketwatch.com/archive/19990124/news/current/intc.htx> (Jan. 24, 1999); Junkbusters News Release, *Privacy Groups Consolidate Intel Case at FTC* <http://www.junkbusters.com/ht/en/nr16.html> (Feb. 26, 1999); Bill Brubaker, *Sensitive Kaiser E-Mails Go Astray*, Wash. Post E1 (Aug. 10, 2000); FTC, *Liberty Financial Companies, Inc.—Analysis* <http://www.ftc.gov/os/1999/9905/libertycom.htm> (accessed Dec. 6, 2000); CNN.com, *Microsoft's GUID Sparks Fears of Privacy Invasion* (Mar. 8, 1999) <http://www.cnn.com/TECH/computing/9903/08/microsoft.privacy.02/index.html> (accessed Dec. 6, 2000); Chris Oakes, *Privacy Suit Targets Netscape*, WiredNews (July 7, 2000) <http://www.wired.com/news/politics/0,1283,37435,00. html>; *Complaint, Wilens v. RealNetworks, Inc.* <http://members.home.net/jeffreywilens-lawoffice/page1.jpg> FTC, *ReverseAuction – Consent & Final Order* <http://www.ftc.gov/os/2000/01/reverseconsent.htm> (accessed Dec. 6, 2000); David Voreacos, *Toys 'R' Us Facing Class-Action Lawsuits* (Aug. 21, 2000) <http://www.bergen.com/news/toysrus200008217.htm> FTC, *FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations* <http://www.ftc.gov/opa/2000/07/toysmart2.htm> (accessed Dec. 6, 2000); *Universal Image Updates Damages Named in Yahoo Suit over Client List*, Bloomberg News (Dec. 23, 1999) (examining the Universal Image suit against Yahoo and Broadcast.com for Yahoo's use of cookies after Yahoo terminated its contract with Universal Image to prevent possible violations by Universal Image of Yahoo privacy policy).

3. Mark Nance, *Corporate and E-Commerce Counsel of VerticalOneCorporation, Internet Privacy: No Race to the Bottom*, 5 Elec. Banking L. and Com. Rpt. 1 (May 2000).

The wide range of cases has suggested to privacy advocates that abuses are rampant.[4] Another view would suggest that new technologies have bred widespread uncertainty about best practices. From this vantage point, the large number of cases are evidence that enforcement mechanisms, both private and public, are already aggressively providing precedent and guidance to shape the handling of personal information by electronic technologies in the immediate future.[5]

The privacy movement predates the Internet and widespread computerization, with its original influences differing in the United States and in Europe. In the latter, the right to privacy has been one consequence of the assertion of individual rights to protect against authoritarian abuses of the kind associated with such regimes as the Nazis and the Soviets. Human rights conventions, beginning with the Universal Declaration on Human Rights of the United Nations in 1948, for the first time provided a basis in many countries for the assertion that individuals had rights that governments could not trump with collective rights.[6] The concept of the individual's rights as creating a protected "personal space" where the government could not legislate was in turn reiterated in a series of human rights and privacy instruments in the United Nations,[7] Council of Europe,[8] and further developed in the area of consumer protection by the Organization of Economic Cooperation and Development (OECD),[9] as well as in a series of instruments in the European Union.[10] Significantly, the concept of privacy was not originally articulated as a right to privacy per se but rather protection against interference by the government with one's mail, telephone, and home life, to

4. *U.S. v. White*, 401 U.S. 745, 767–68 (1971); *Bechhoefer v. U.S. DOJ DEA*, 209 F.3d 57 (2d Cir. 2000); *see generally Anderson v. La Junta State Bank*, 115 F.3d 756, 758 (10th Cir. 1987).

5. *See generally Bigelow v. DOD*, 217 F.3d 875 (D.C. Cir. 2000).

6. United Nations, *Universal Declaration of Human Rights* <http://www.un.org/Overview/rights.html> (accessed Nov. 18, 2000).

7. Europa, *United Nations Guidelines Concerning Computerized Personal Data Files* <http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/un.htm> (accessed Nov. 18, 2000).

8. Europa, *Council of Europe Data Protection Convention* <http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm> (accessed Nov. 18, 2000)

9. Organization of Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (accessed Nov. 18, 2000) [hereinafter, OECD Privacy Guidelines] (constituting nonbinding guidelines on the handling of personal data, including accuracy, security, consent, rights of access, correction, erasure and recourse).

10. *Treaty on European Union* tit. I, art. F <http://europa.eu.int/en/record/mt/title1.html> (Feb. 7, 1992); European T.S. No. 5, *Convention for the Protection of Human Rights and Fundamental Freedoms* <http://www.coe.fr/eng/legaltxt/5e.htm> (Nov. 4, 1950) (guaranteeing European citizens the right to respect for private life, home, mail).

further the core goal of protection of the person.[11]

By contrast, in the United States, rather than a right to privacy, there have always been protections against the government's right to trespass.[12] It was not either the government's or any commercial enterprise's acquisition and use of personal information that concerned the framers of the U.S. Constitution, but the prevention of the abuses associated with King George III—the forced quartering of soldiers in people's homes, trespassing on personal land, the government entering an individual's home without due process of law.[13] At their core, these concepts boil down to the right not to have the government enter one's physical space except under limited, judicially approved circumstances.[14] The principal is a central one to protecting rights in our democracy and has substantial implications for limiting permissible government monitoring of citizens and use of citizen information on the Internet. But the various elements of trespass law enunciated in the Constitution are significantly different from the European privacy law approaches. The U.S. approach focuses on a protected space or location—a person's home—whereas the other approaches focus on protecting the individuals from the government. The distinction arises out of history, as the Bill of Rights under the U.S. Constitution provides for freedom of speech, religion, the press, trial by jury, protection from illegal search and seizure, and so on,[15] in a manner that to this day has never become accepted in most other countries, including those in Europe. In thinking about privacy, the distinction between protecting the invasion of a person's personal space by the government and creating a zone of privacy around a person that no one may enter without right, while subtle, proves significant in consequences.[16]

Although the first major federal privacy law in the U.S. did not address government action until 1974[17] and the first comprehensive fed-

11. *See generally Convention for the Protection of Human Rights and Fundamental Freedoms*, *supra* n. 10; OECD Privacy Guidelines, *supra* n. 9; European T.S. No. 108, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Jan. 28, 1981) <http://www.coe.fr/dataprotection/edocs.htm> (establishing binding rights of access, correction, erasure and recourse for persons in member states of the Council of Europe that ratify the Convention); Council Directive 95/46/EC, 1995 O.J. (L 281) 31 (transforming the OECD Recommendations of 1980 into binding obligations by all E.U. member states).

12. U.S. Const. amend. IV.

13. *See generally* Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U.L. Rev. 925 (1997).

14. *Id.*

15. *See generally* U.S. Const. amend. I–X.

16. U.S. Const. amend. IV. A zone of privacy around the person arises only, and arguably, in the Fifth Amendment's right not to be forced to incriminate oneself in a criminal trial. *Id.* This protection against forced self-incrimination is readily distinguishable from a broader right to control one's personal information for other purposes. *Id.*

17. 5 U.S.C. § 552a (1974).

eral privacy law covering broad sectors of business was not enacted until 1999,[18] many Americans take the idea that privacy is a fundamental right for granted, with some asserting it is based in the Constitution itself. As Harvard law professor and cyberlaw specialist Lawrence Lessig wrote, "the Bill of Rights promised that the federal government will not remove certain protections—of speech, privacy and due process. And it guaranteed that the commitment to these substantive values will remain despite the passing fancy of normal government."[19] In fact, while provisions of the Bill of Rights explicitly protect speech and the Fifth Amendment protects due process,[20] the word "privacy" does not exist anywhere in the Constitution or in any of its amendments. Rather, the Supreme Court has found that the right of privacy exists in the area of reproductive freedom through what Supreme Court Justice William O. Douglas memorably described as "penumbras" in the Bill of Rights.[21] Significantly, the line of Supreme Court cases finding privacy in the penumbras warn that only personal rights that are "fundamental" or "implicit in the concept of ordered liberty" are constitutionally protected.[22]

Under state common law, four privacy-related torts developed in the early 20th century, in a handful of cases, occasionally backed by state statute. These included appropriation, use of a person's name, likeness or identity for trade or advertising purposes without consent; intrusion into someone's private space, an information-gathering, not a publication, tort; public disclosure of embarrassing private facts, an occasionally

18. 15 U.S.C. § 6501 (1999).

19. Lawrence Lessig, *Code and Other Laws of Cyperspace* 7 (Basic Books 1999).

20. U.S. Const. amend. I, V.

21. In *Griswold v. Connecticut*, 381 U.S. 479, (1965) (concerning the constitutionality of a Connecticut law that outlawed giving married persons information, medical advice and services on how to prevent conception, the Supreme Court for the first time found a right to privacy under the Constitution). The majority in Griswold, authored by Justice William O. Douglas, found that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . ." *Id.* Various guarantees create zones of privacy. *Id.* The right of association contained in the penumbra of the First Amendment is one, as we have seen. *See e.g.* U.S. Const. amend III. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. *Id.* U.S. Const. amend IV. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." *Id.* U.S. Const. amend V. The Fifth Amendment in its self-incrimination clause enables the citizen to create a zone of privacy that government may not force him to surrender to his detriment. *Id.* U.S. Const. amend IX. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." *Id.* The penumbras in the Bill of Rights discovered by Justice Douglas in turn became the foundation for the Supreme Court's decision to overturn anti-abortion laws as unconstitutional in *Roe v. Wade,* 410 U.S. 113; *see also Meerwarth v. Meerwarth*, 128 N.J. Super. 285, 319 A.2d 779 (Ch.Div. 1974).

22. *Roe*, 410 U.S. at 152.

alleged tort of questionable constitutionality; and false light, publication of false, highly offensive (but not necessarily defamatory) information about an individual. None of these torts were federalized, and all except the public disclosure tort can be distinguished from a right to privacy, but rather as special cases of trespass, assault, or eavesdropping.[23]

This history is important because it reminds us that although the right to privacy is clearly stated nowhere in the Constitution, the issue of protecting privacy has preoccupied policy makers, lawmakers, and the courts long before the age of the Internet and the era of computerized databases. The extent to which privacy is a personal right has been in contention for a long time, without a clear consensus having developed as to whether privacy is indeed a right and if that right exists, how to reconcile it with other rights.[24] Specifically, the question of whether privacy protection is a right or merely a policy preference remains unanswered, and there is no consensus regarding how best to protect privacy no matter how it is categorized. The question matters because the answer may be relevant to determining what mechanism of governance is best suited for protecting the right or interest. A right, whether constitutional or statutory, may be the kind of equity that requires protections that can only be balanced against other rights of equal and enduring weight.[25] By contrast, a mere policy interest is something that is routinely layered on top of, and balanced against, other competing policy interests. Governmental structures to promote newly emerging policy interests seek to integrate the newly recognized interests in a coherent fashion with existing interests, so as to minimize the disruption to systems and laws people are already relying upon.

Significantly, the only state whose constitution contains explicit language making privacy a right, California, also qualifies that right.[26] In

23. *See Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, (1902) (finding there was no law protecting a girl from having her picture used without permission or compensation to advertise baking flour company). In response, the New York legislature created the first appropriation law (statutory right of privacy) in 1905. *Id.; see also Pavesich v. New England Life Insurance Co.*, 50 S.E. 68 (Ga. 1905). The Georgia Supreme Court became the first court in the U.S. to recognize that a common law right of privacy had been violated when an insurance company used a person's picture to sell insurance without the person's permission. *Id.;* Wilfred Feinberg, *Recent Developments in the Law of Privacy,* 48 Colum. L. Rev. 713 (1948). While the final volume of the First Restatement of Torts, published in 1939, officially recognized a tort for invasion of privacy, as of 1947 only 9 jurisdictions recognized a common law right of privacy. *Id.*

24. *See e.g.*, Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 Santa Clara Computer & High Tech. L.J. 357 (2000).

25. *See e.g.*, Maureen Maginnis, *Maintaining the Privacy of Personal Information: The DPPA and the Right of Privacy*, 51 S.C. L. Rev. 807 (2000); *see generally* Jessica Litman, *Information Privacy*, 52 Stan. L. Rev. 1283 (2000).

26. Cal. Const. art. I, § 1.

1972, California voters passed a ballot initiative on privacy that was then incorporated into the state constitution.[27] In essence, the initiative added to the word "privacy" to a list of existing rights so that the passage read:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life, liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness and privacy.[28]

As a result of the change, California created a private tort for invasion of privacy, which specifies that invasion of "a privacy interest is not a violation of the state constitutional right to privacy if the invasion is justified by a competing interest."[29] In essence, California created a balancing test in which the invasion of privacy is to be measured against "legitimate interests" that "derive from the legally authorized and socially beneficial activities of government and public entities."[30] These legitimate interests can include activities of the private sector if they relate to socially beneficial interests, although the precise nature and extent of how a court may balance these interests is left to future cases.[31]

The California outcome—a balancing test—is a useful reminder that even as a right, privacy is a difficult goal to assess without reference to competing or related values.

California's position differs from that of many proponents of a privacy czar for the U.S. who tend to assume as settled a number of issues that remain in substantial dispute, beginning with the question of whether the protection and control of one's personal data is a fundamental right or merely a policy preference. Privacy advocates refer, variously, to injuries to informational privacy as a "breach," using contract terms; as an "infringement,"[32] treating the information as a property

27. *Id.*

28. *Id.*

29. *Hill v. N.C.A.A.*, 7 Cal. 4th 1, 38 (1994).

30. *Id.*

31. *Id.* at 38–39.

32. This term is used frequently in other countries, such as Canada and New Zealand. *See e.g. Privacy in NZ Broadcasting Law*, 1 PLPR 63 (1994) (citing a television news story involving a coroner's decision not to release woman's body for four months in which the former husband claimed privacy infringement); Hansen, unreported, BSA decision No. 44/93 (Apr. 19, 1993) <http://www.austlii.edu.au/au/other/plpr/vol1/Vol1No04/v01n04b.html.>. The term is also increasingly being used in policy discussions in the U.S. regarding privacy. Brian Krebs, *Advertising Debate Illuminates Privacy Frustrations, Newsbytes* (4/27/00) <http://www.infowar.com/class_1/00/class1_042700a_j.shtml> (accessed Jan. 5, 2001). Recent usages include a statement by Sen. William H. Frist, R-Tenn., describing "the challenge for policy makers is to find the right balance between the benefits of free information flows and the costs of potential privacy infringement." *Id.* State of Hawaii, Office of Information Practices, *The Commercial Use of Personal Information, Individuals At Public Hearings*, <http://www.hawaii.gov/oip/privacy_report_1999.htm> (Dec. 1999). A similar re-

owned by the individual whose use must be licensed, or as a "violation," characterizing use of data as prospectively criminal. Regardless of the frame of reference, almost invariably, the underlying privacy interest is described as a right, and consequently, as inherently incapable of being balanced against any interest other than another right.

Some who are certain that the protection of personal data, such as name, address, photographic image, or telephone number, should be or already is a fundamental right of all Americans, have ably argued for the immediate creation of a U.S. privacy czar.[33] They suggest that a privacy czar is clearly a more effective, systematic, and powerful mechanism to secure that right than alternatives such as privacy through free market self-selection; the setting of industry self-regulatory standards; or even reliance upon existing mechanisms for regulated industries such as financial services.[34]

As this article discusses, a privacy czar may not prove to be a viable solution even for the strongest advocates of privacy protection. For those who remain skeptical of the primacy of privacy as a human right that trumps other policy interests, the call for a privacy czar remains about as resonant as the call for czars to protect other important, but still disputed rights, as well as some that are undisputed.[35] In the former category might be calls for an animal rights czar rather than the Food and Drug Administration ("FDA") to ensure that the fundamental rights of animals are not abused by the meat or cosmetics industry.[36] In the latter category would be calls for a civil rights czar rather than the Department of Justice to insure the enforcement of due process and equal protection laws for minorities; a women's rights czar to enforce equal protection regardless of gender; a children's rights czar rather than state child wel-

---

cent use occurred in 1999 when a professor of law testifying before Hawaii's Office of Information Practices characterized as "privacy infringement" an appropriation case, when, without his knowledge or consent, a local hotel had photographers take pictures of his minor child at the hotel's "Kid's Club" service, and publish it in a Japanese travel guide. *Id.*

33. *See generally* U.S. Const. amend. I–X.

34. *Id.*

35. *Id.*

36. There are millions of Americans who believe that animals have, or should have, protected rights in the United States. The provisions of existing federal privacy laws, such as the Federal Privacy Act of 1980, which apply only to the federal government; the Federal Fair Credit Reporting Act, which applies only to regulated credit reporting agencies; and the Gramm-Leach-Bliley Financial Services Modernization Act of 1999, which applies to regulated financial services entities, neither imply the requirement for a federal privacy czar more nor less than existing Department of Agriculture regulations providing for the humane treatment of animals implies the requirement for a federal animal rights czar. *See* Pub. L. No. 99-198, 1752, 99 Stat. 1354, 1645 (1985) (codified at 7 U.S.C. § 2143(a) (1994)). The 1985 amendments to the Animal Welfare Act ("AWA"), which direct the Secretary of Agriculture to "promulgate standards to govern the humane handling, care, treatment, and transportation of animals by dealers, research facilities, and exhibitors." *Id.*

fare offices to regulate the handling of all possible abuses of children among the states; an elder rights czar to protect against abuses of older Americans, such as forced retirements; and a gun czar, who would protect the rights of American gun owners.[37] The absence in our country of such positions suggests that they are unnecessary and holds implications for those who promote the concept of a privacy czar.

III. POSSIBLE MISSIONS AND MODELS FOR A PRIVACY CZAR

One conceivable approach for responding to privacy issues in the U.S. is to rely upon ordinary mechanisms within government. This approach, which was the one in actual use in the U.S. from 1974 through 1999, relegated privacy issues to management by the Office of Management and Budget ("OMB") within the White House.[38] OMB then provided for both policy guidance and the funding of individual privacy offices, as needed, in particular agencies.[39] This approach has remained largely unchanged, but it has been supplemented over the past 18 months through the creation of a privacy advisor.[40]

The privacy advisor model would perpetuate the existing approach taken by the Clinton Administration, which created a White House advisor to develop policy recommendations on privacy for the Administration.[41]

The first person to hold the position, Peter P. Swire, carries out his White House work on privacy with a staff of four, focusing initially on such issues as requiring all government agencies to post privacy policies.[42] Such advisors can exercise substantial influence on internal decision-making within an administration but may be criticized for having no administrative or legal mechanisms, let alone budgets, to exercise real power.

A slightly more robust privacy maven would be a privacy advocate, created by statute with a separate base of authority within the Executive

37. *See* U.S. Const. amend. IV–XIV. The Constitutional basis for civil rights and in general for women's rights under the equal protection provisions of the 4th and 14th amendments is no longer disputed. *Id.* Children's rights and elder rights issues remain strongly contested. *Id.* There remain strongly held and unreconciled views as to whether the Second Amendment guarantees a right to bear arms that is already being infringed by Congressional and state firearms statutes. *Id.*

38. *See* 5 U.S.C. § 552a; 40 Fed. Reg. 28, 498-79 (1975); 40 Fed. Reg. 56, 741-43 (1975); 48 Fed. Reg. 15, 556-60 (1983); Fed. Reg. 18, 599-601 (1991); Fed. Reg. 6428, 6435-39 (1996).

39. *See* sources cited *supra* n. 38.

40. *Id.*

41. *See generally* Peter Swire, *Peter Swire Home Page* <http://www.osu.edu/units/law/swire1/pshome1.htm> (accessed Nov. 10, 2000).

42. Interview with Peter P. Swire, Chief Counselor for Privacy at the Office of Management and Budget (Aug. 29, 2000).

Branch, along the model of the so-called drug czar, the Director of the White House Office of National Drug Control Policy ("ONDCP"), a position created by Congress in 1988 and reauthorized in 1998.[43] Like the drug czar, the privacy czar's job would be to coordinate administration policy on privacy, including the handling of privacy issues by executive departments.

The third model, an independent regulator, would establish a Data Protection Commission as an independent agency responsible for protecting individual privacy rights, governed by the Administrative Procedures Act ("APA").[44] An existing example of this model is the Canadian Privacy Commissioner.[45] The closest models within the U.S. are the Securities and Exchange Commission ("SEC") and the FTC, both of which have broad regulatory powers to protect consumers based on the activities of those they regulate, and whose chairman, though merely first among equals among commissioners, might have powers correlating to that of a regulatory czar.

A fourth approach, adopted in some civil code counties such as Italy, would create an elected, independent board through a legislative act.[46] The board would exercise czar-like powers directly on behalf of the people, independent of both the legislature and the executive branch. Its mission would be to protect all citizens' rights to privacy, and thus the legislature would need to delegate broad authority over all collectors, users, and disseminators of personal information, commercial and governmental, including law enforcement, intelligence agencies, and the press. In the U.S., such a scheme would run into formidable constitutional barriers wholly apart from questions regarding its substantive merits.[47]

---

43. *See* David Teasley, Congressional Research Service, Library of Congress, no. 98-149 GOV, *Drug Control: Reauthorization of the Office of National Drug Control Policy* (June 29, 1998). The Office of National Drug Control Policy Reauthorization Act of 1998 established, in the Executive Office of the President, an Office of National Drug Control Policy, to: (1) develop national drug control policy; (2) coordinate and oversee the implementation of that national drug control policy; (3) assess and certify the adequacy of national drug control programs and the budget for those programs; and (4) evaluate the effectiveness of the national drug control programs. *Id.* One czar's mandate may collide with another czars. *Id.* In June 2000, privacy advocates severely criticized the U.S. drug czar for using cookies placed by DoubleClick to measure which of the office's anti-drug Internet ads were most effective. *Id.* For more on "Cookiegate," *see* Junkbusters, *Junkbusters press release* <http://www.junkbusters.com/ht/en/nr38.html> (June 22, 2000).

44. 5 U.S.C. §§ 551–808 (1997).

45. *See infra* nn. 55–81.

46. www.privacy.it, *Italian Privacy Law: act no. 675 of 31.12.1996* <http://www.privacy.it/legge675encoord.html> (accessed Nov. 13, 2000).

47. *See id.* (providing the structure of the Italian privacy czars' office). Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 Stan. L. Rev. 1049 (2000). Regarding the Constitu-

Advocates for a privacy czar or Data Protection Commission in the U.S., relying in part on functions carried out by privacy czars in other countries, have suggested that the privacy czar's roles might include:

Coordinating the federal government's development of privacy policy and acting as central switching station for the establishment of administration policy on privacy;

Acting as a spokesman for the administration on privacy policy, including the promotion of the administration's policies on privacy to the general public, through ongoing public education, public affairs outreach, and liaison with key constituencies with equities in the handling of privacy;

Undertaking interagency responsibility for harmonizing Executive Branch implementation of applicable federal privacy laws, adopting procedural mechanisms to assist in resolving possible conflicts between privacy issues and other federal equities, such as promotion of e-commerce, technology development, law enforcement, or supervision of financial markets;

Integrating U.S. privacy policy and regulation with international standards and norms to harmonize domestic and foreign standards;

Acting as ombudsman for public complaints about the privacy practices of public or private sector entities, to investigate and resolve such complaints and to recommend changes in practice or law;

Acting as a domestic superregulator, to harmonize privacy practices across regulated sectors throughout the U.S., to create a consistent set of rules governing all U.S. regulated entities and protecting all Americans;

Administering and regulating a federalized right to privacy by regulating all processors of personal information of U.S. citizens, turning every processor of such information into a regulated entity and undertaking adjudications as an independent agency; and

Engaging in random or systematic audits of privacy practices of public or private sector entities, to determine their compliance with privacy

---

tional issues, the most fundamental Constitutional barrier is the First Amendment itself, whose barriers to such a regime. *Id.* But the creation of a privacy czar independent from the President, and the participation of the Congress in selecting such a position, as takes place in Italy, creates additional Constitutional hurdles; *See e.g. Buckley v. Valeo*, 424 U.S. 1 (1976) (noting the Supreme Court holding that the only sort of federal official who can exercise significant executive authority under U.S. law is an "officer of the United States," (as defined in the appointments clause)); *see also INS. v. Chadha,* 462 U.S. 919 (1983) (suggesting strongly that the President is the core locus of executive power, and there are limits on the delegability of that power, and on Congressional participation in the exercise of that power).

statutes.[48]

In the U.S., a nonstatutory position could carry (and is carrying) out the first four of the missions described here, although leadership on international harmonization has been handled by the U.S. Department of Commerce. The same missions could also be carried out by a statutory privacy czar, with a staff and budget similar to that of the drug czar. By contrast, each of the latter four missions clearly require regulatory authority for a true privacy czar or Data Protection Commission to carry out responsibilities under the APA. Although the Commission could have a limited mandate, such as merely covering the Internet, under the European or Canadian model, it would assume responsibility for privacy handled by existing regulators, such as the bank regulators, the SEC, and the FTC. If a U.S. Commission fully followed the E.U. and Canadian model, it would also have jurisdiction to regulate industries that may handle personal information that are not currently regulated. These industries could include Internet service providers ("ISPs"), sellers of goods or services, and every other commercial enterprise that makes use of names, addresses, telephone numbers, e-mails, photographs, or other personal information. In short, in the U.S., a privacy czar would be the super regulator of essentially every commercial entity in the country. With potential extraterritorial reach due to the inherent unboundedness of the Internet, most of the business activities of the entire world would be under the privacy czar's job description. While narrower in scope, the potential jurisdictional reach of the job would vastly exceed that of the U.S. President, who has to limit his efforts to exercise power over other sovereign states.

IV. PRACTICAL EXPERIENCE I: UNITED STATES WITHOUT A CZAR

In the quarter century since the enactment of the Federal Privacy Act of 1974, the U.S. has extensively regulated privacy and government without Congress finding the need to create a privacy czar to centralize and administer the process. Implementation of the Federal Privacy Act, governing all personal information collected by components of the federal government, has been handled through the normal processes of government, and administered through the OMB. Over the years, OMB has ensured that implementing regulations were developed, published in the Federal Register, and subjected to typical public notice and comment. OMB has created positions in various federal agencies to carry out the functions provided for in the Act, and it has acted to update, as neces-

48. Privacy czars now carry out all or most of these functions throughout the E.U., in Canada, and in New Zealand. Privacy czars have recently been given similar authority in Argentina and Australia.

sary, the privacy policies and practices of the federal government as part of its routine business, working closely with the U.S. Department of Justice Office of Information and Privacy ("DOJ-OIP"), which is responsible for enforcing the civil and criminal provisions of the Act.

Since 1974, OMB and DOJ-OIP have provided extensive guidance to federal agencies about what they may and may not do with information.[49] They have worked together to define limitations and procedures for maintaining records on individuals, provide for conditions of disclosure to third parties, establish individual right of access and correction, and specify civil remedies including lawsuits for damages, criminal penalties, and exemptions. Numerous cases have been litigated,[50] and the current DOJ-OIP "Overview" of the Privacy Act runs 147 pages.[51] The Overview begins with a warning that the government has found the substance of the existing Privacy Act to be deeply flawed, due to its imprecise language and limited legislative history, stating flatly: "Even after twenty years of administrative and judicial analysis, numerous Privacy Act issues remain unsolved. . ."[52]

These issues remain unsolved not for lack of effort, resources, or settled policies of the kind that might be resolvable by a privacy czar. Rather, they have been the result of drafting problems in the original legislation, and by the inherent complications of the intersection of federal privacy law with other federal interests. These complications include law enforcement, administrative record keeping, and the difficult problem of aligning the privacy interests of different persons whose personal information may all be contained on one record.

With these flaws inherent in the Privacy Act, administering it has created a broad body of federal privacy law. Solutions have been found on many fundamental issues: what is a record, when dissemination of personal information constitutes unlawful disclosure because it is person-

49. 5 U.S.C. § 552a; 40 Fed. Reg. 28, 498-79 (1975); 40 Fed. Reg. 56, 741-43 (1975); 48 Fed. Reg. 15, 556-60 (1983); Fed. Reg. 18, 599-601 (1991); Fed. Reg. 6428, 6435-39 (1996).

50. *See e.g., Osborne v. United States Postal Service*, No. 94-30353, slip op. at 2-4, 6-11 (N.D. Fla. May 18, 1995) (allowing disclosure of plaintiff's injury-compensation file to a retired employee of the U.S. Postal Service, when the retired employee had prepared the file, to constitute "disclosure" for purposes of the Privacy Act); *Henke v. U.S. Department of Commerce,* No. 94-0189, 1996 WL 692020 at 3 (D.D.C. Aug. 19, 1994) (holding that names of reviewers who evaluated grant applicant's proposal are records pertaining to applicant under Privacy Act); *Williams v. Veterans Administration*, 104 F.3d 370, 673 (4th Cir. 1997) (holding that privacy right to access extends to records that are actually indexed and retrieved by individual's name or personal identifier, but not to records that may have such information but which are not structured to be retrieved to obtain information regarding the individual).

51. DOJ-OIP, *Overview* <http://www.oalj.dol.gov/public/apa/refrnc/privacy.htm> (accessed Oct. 21, 2000) [hereinafter DOJ Overview].

52. *Id.*

ally identifiable, when the right of access and correction does and does not apply, when information can be disclosed to third parties, and when intra-agency disclosure is appropriate.

Over the slow accretion of cases involving the Privacy Act, the ongoing work of hundreds of federal record keepers, designated "Privacy Act officers," administrators, and judges has done much to accomplish the act's four goals:

To restrict disclosure of personally identifiable records maintained by agencies.

To grant individuals increased rights of access to agency records maintained on themselves.

To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.

To establish a code of fair information practices that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Recent public concerns about privacy have not been generated by alleged abuses of privacy by departments or agencies of the federal government. For example, "identity theft" made possible in part by abuses involving the ability of criminals to obtain government records has not involved federal records but only those belonging to states, which cannot be covered under the Privacy Act under the U.S. federal system. The Privacy Act settled that the Federal Government is forbidden from selling or renting such lists, unless Congress specifically so authorizes, and thus federal abuses in this area over the past 25 years have been essentially absent.[53]

This result might imply that whatever the flaws in the substance of the Privacy Act, its administration, without benefit of a czar, has in large measure worked. Indeed, apart from requiring all federal agencies to develop and post privacy policies for their online sites, little to no administrative modification of the existing law has been undertaken as a result of Peter Swire's appointment as the Administration's Privacy Advisor at OMB.[54] Of course, whether policy changes require such a position is a separate question, although the current Administration and Congress seem amply capable of proposing such changes even in the absence of a czar.[55]

---

53. *See* 5 U.S.C. § 552a(n); *see also Disabled Officer's Ass'n v. Rumsfeld*, 428 F. Supp. 454, 459 (D.D.C. 1977), affirmed, 574 F.2d 636 (D.C. Cir. 1978); OMB Guidelines, 40 Fed. Reg. 28,976 (1975).

54. Swire, *supra* n. 41.

55. *See* Library of Congress, *Legislative Information on the Internet* <http://thomas.loc.gov> (accessed Oct. 26, 2000). Thomas, the legislative tracking service of the Congress,

Beyond the Privacy Act, Congress enacted seven other federal privacy laws prior to last year's passage of the Gramm-Leach-Bliley Act of 1999 ("GLB").[56] They include regulation of the credit reporting industry through the Fair Credit Reporting Act,[57] financial services involved in electronic fund transfers through the Electronic Fund Transfer Act of 1978;[58] the cable industry, through the Cable Communications Policy Act of 1984[59] and the Cable Television Consumer Protection and Competition Act of 1992;[60] and regulation of privacy-threatening computer crimes through the Computer Fraud and Abuse Act of 1986,[61] the Electronic Communications Privacy Act of 1986,[62] and the National Infrastructure Protection Act of 1996, which amended the Computer Fraud & Abuse Act of 1996.[63]

For each of these laws, as for GLB, the federal government has protected privacy through the standard process of giving the work to regulators familiar with each of the industries whose privacy practices they will regulate. Under GLB, the banking regulators will be regulating the privacy policies and practices of banks, thrifts, credit unions, and other federal financial institutions;[64] the SEC, will be regulating such policies and practices for investment banks, brokers, and other SEC registered entities;[65] and the FTC will be regulating privacy regimes governing all other entities that are involved in the provision of consumer credit.[66]

Despite the absence of a privacy czar, all of these agencies issued regulations fewer than six months after the passage of the GLB that were similar in substance and identical in purpose, following an unremarkable period of public notice and comment.[67] Although it is premature to conclude with certainty that these regulators will effectively administer their newly issued privacy regulations, each of these regulators has decades of enforcement experience. No evidence suggests that these regulators cannot meet their responsibilities to implement the pri-

---

lists only the first 50 bills introduced on a topic each legislative session; the number was exceeded early in 1999. *Id.* The Administration's most recent privacy initiative was introduced in June 2000. *Id.*

56. 15 U.S.C. §§ 6701–81 (1999).

57. *Id.* at § 1681 (1968).

58. *Id.* at § 1693 (1978).

59. 47 U.S.C. § 551 (1984).

60. *Id.* at §§ 521-73 (1992).

61. 18 U.S.C. § 1030 (1986).

62. § 2510 (1986).

63. *National Information Infrastructure Act of 1996*, Pub. L. No. 104-294, 110 Stat. 3491 (codified as amendments to 18 U.S.C. § 1030).

64. 15 U.S.C. § 6753 (1999).

65. 12 U.S.C. § 1844 (1999).

66. *Id.* at § 1607(c) (1996).

67. 65 Fed. Reg. 106, June 1, 2000, 35162-236.

vacy laws Congress has passed. Thus, the shifting of their roles to a new and untested office of a privacy czar could perversely prove in practice to reduce the effectiveness of existing privacy protections, especially during a transition.

The massive regulatory, administrative, enforcement, and judicial activity over the past 25 years of implementation of the Privacy Act as well as the more than six decades of regulatory history of our other new privacy regulators under GLB provide some precedent to suggest that a privacy czar or Data Protection Commission may not be needed to enforce national privacy laws, regardless of whether broadened privacy laws are or are not good public policy. The implications and risks of creating such a czar for policy purposes are evident in the Canadian model.

V. PRACTICAL EXPERIENCE II: CANADA WITH A CZAR

Although Canada has recently begun to legislate broad privacy protections governing the use of personally identifiable information by commercial entities through the bill known as C-6,[68] for the past 17 years the principal distinguishing difference between the U.S. and Canada on privacy has been the latter country's creation of a privacy czar. That position, termed Privacy Commissioner, was created in 1983 to centralize the administration of Canada's federal privacy laws and to provide policy guidance to Canada on privacy-related issues arising at the federal level.[69]

Each year, the Commissioner prepares an annual report to the Canadian Parliament describing the Commission's work over the previous year and providing policy prescriptions.[70] The sole holder of the position, Bruce Philips, a respected career journalist and privacy advocate, prefaced his March 2000 report with approving quotations among others from the Greek philosopher Neocles, "Conceal your life," dated to the third century B.C.[71] In the report itself, Commissioner Philips repeated his longstanding call for greater protections for individuals "in the ongo-

68. House of Commons, Bill C-6, 48-49 Elizabeth II, c. 5 <www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/c-6/c-6_3/C-6TOCE.html> (accessed Nov. 10, 2000).

69. R.S.C. 1985, c. P-21, s. 53. Canada's provincial privacy commissioners operate at different levels of intensity to implement privacy standards set by provincial legislatures. *Id. See e.g.* Commission d'accès à l'information du Québec, *Publications* <http://www.cai.gouv.qc.ca/publicat.htm> (accessed Nov. 14, 2000). It is difficult to compare the standards and effectiveness of these provincial commissioners, because of the widely varying degree to which they produce published materials describing their activities and their alternating use of French and English. *Id.*

70. The Privacy Commissioner of Canada, *Privacy Commissioner of Canada Annual Reports* <http://www.privcom.gc.ca/english/02_04_e.htm> (accessed Nov. 14, 2000).

71. The Privacy Commissioner of Canada, *Annual Report* (1999-2000) 5 <http://www.privcom.gc.ca/english/02_04_08_e.htm> (accessed Oct. 24, 2000).

ing battle to protect the right to a life free of surveillance and intrusion," calling for an expansion of legal regimes to cover video surveillance, physical privacy, biomedical privacy, drug and DNA testing, and other new technologies.[72] He closed his reflections with the statement that the position of the Privacy Commissioner is "a bully pulpit" that must be dedicated solely to the advancement of human freedom.[73]

Despite the Commissioner's strong personal views in favor of greater regulation of privacy, his mandate for the enforcement of Canada's law until the passage of C-6 has differed little from the mandate of OMB-DOJ-OIP under U.S. law.[74] Both laws have covered government records only.[75] In a typical year, such as 1998-1999, the Privacy Commissioner's office receives about 4,000 complaints.[76] Over the first ten years of the office's existence, about half of all complaints alleged that an agency had exceeded the time limit for responding to a privacy-related inquiry.[77] One third of the complaints alleged failures to receive adequate access to personal information maintained by an agency.[78] Just three percent alleged improper collection of data.[79] The largest percentage of complaints involved, respectively, the Canadian prison system (about 20%), the Canadian defense forces and Canadian tax collectors (about 8% each), and Canadian benefits providers and Canadian immigration service (about 6% each).[80] Over the ten years, about 30% of all complaints were found to be "well-founded."[81]

An analysis of the kind of complaints filed mirrors the kind of litigation seen in the U.S., except that it reflects greater involvement by the Commission on issues that might not be addressed in the U.S. Among the principal cases reported by the privacy czar in recent years are:

A case in which Canadian immigration denied a Canadian access to her personal information and had not returned her original birth certificate. A subsequent investigation revealed that Canadian immigration routinely destroyed staff investigators' handwritten notes and observations, and the Commissioner recommended that notes used to make any administrative decision, including access, must be retained to protect the individual's rights.[82]

---

72. *Id.* at 8.

73. *Id.*

74. *See supra* pt. 2.

75. *See DOJ Overview*, *supra* n. 51; *see also* House of Commons, *supra* n. 68.

76. The Privacy Commissioner of Canada, *Annual Report* (1998-1999) 38 <http://www.privcom.gc.ca/english/02_04_07_e.htm> (accessed Oct. 24, 2000).

77. *Annual Report*, *supra* n. 76, at 53.

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.*

82. *Id.* at 43–44.

A sexual harassment case involving Environment Canada, in which handwritten records pertaining to the investigation were missing, although unsigned typewritten records were retained. The Commissioner found the employee's claims that her right to access had been violated were well-founded, given the obvious loss of some of the records.[83]

Disclosure by Canada's postal service of a vacation schedule of one of its employees to the Worker's Compensation Board investigating his wife's continuing disability claim. The Commissioner ruled that the postal service could not disclose the information to the Board, because it had been collected solely for the purpose of administering vacation credits and work schedules, and its dissemination to another government agency for any other purpose was not authorized.[84]

In several of these areas, particularly those dealing with law enforcement, the substantive decisions of the Canadian Commissioner differ from those of the U.S. judges who have reviewed similar provisions of the U.S. Privacy Act.[85] Indeed, in each of the three cases specified above,

83. *Id.* at 46–47.

84. *Id.* at 50.

85. For the first two of the Canadian cases cited here, the differing result in the U.S. is a consequence of OMB Guidelines which state that under the U.S. statute, access to documents must be provided only if they are part of a system of records. Such a system only exists if: (1) there is an "indexing or retrieval capability using identifying particulars [that is] built into the system"; and (2) the agency "does, in fact, retrieve records about individuals by reference to some personal identifier." *Id.* OMB Guidelines, 40 Fed. Reg. 28,948, 28,952 (1975). The Guidelines state that the "is retrieved by" criterion "implies that the grouping of records under the control of an agency is accessed by the agency by use of a personal identifier; not merely that a capability or potential for retrieval exists." *Id.* (emphasis added). The U.S. Court of Appeals for the District of Columbia Circuit addressed the "system of records" definition in the context of computerized information in *Henke v. United States Dep't of Commerce*, 83 F.3d 1453 (D.C. Cir. 1996), and noted that "the OMB guidelines make it clear that it is not sufficient that an agency has the capability to retrieve information indexed under a person's name, but the agency must in fact retrieve records in this way in order for a system of records to exist." *Id.* at 1460 n. 12. *See Smith v. Henderson*, No. C-99-4665, 1999 WL 1029862, at *5 (N.D. Cal. Oct. 29, 1999) (applying *Henke* and finding that "locked drawer containing a file folder in which [were] kept . . . notes or various other pieces of paper relating to special circumstances hires" did not constitute a system of records because the agency "did not utilize the drawer to systematically file and retrieve information about individuals indexed by their names.") (appeal pending). Regarding the final Canadian case, under U.S. law, agencies may routinely disclose any records indicating a possible violation of law (regardless of the purpose for collection) to law enforcement agencies for purposes of investigation/prosecution. *See* OMB Guidelines, 40 Fed. Reg. at 28, 953; 120 Cong. Rec. 36,967, 40,884 (1974), reprinted in Source Book at 957-58, 995 (remarks of Congressman Moorhead); *see also* 28 U.S.C. § 535(b) (1994) (requiring agencies of the Executive Branch to expeditiously report "[a]ny information, allegation, or complaint" relating to crimes involving government officers and employees to U.S. Attorney General.); *see also* 28 U.S.C. § 534 (1994 & Supp. III 1997) (authorizing Attorney General to exchange criminal records with authorized officials of the Federal Government, the states, cities, and penal and other institutions).

U.S. courts took the opposite point of view from that of the Commissioner. What is striking is that the despite the differences, the practical protection given to the privacy of government records concerning individuals within the federal governments of the U.S. and Canada remain at rough equivalence. Most of the cases litigated in the U.S. or subject to the Commissioner's purview in Canada could have just as easily arisen in the system of the other.

One signal difference between the two systems is that the U.S. judges administering the Privacy Act profess to be neutral. The Canadian Privacy Commissioner, by contrast, wears his pro-privacy label on his chest, both within his mandate and, according to the Commissioner, in some cases beyond it.[86] Within the mandate, the Commissioner acts not only as administrator of Canada's Privacy Act, but as a privacy advocate, privacy lobbyist, and privacy educator. Under the mandate, the Commissioner has continuously gone to the public to assert that privacy is imperiled and to ask for additional powers. Most recently, he requested that the Commissioner be given the job of representing all persons in Canada who believe their privacy rights have been injured and the power to limit any activities by government and business he views to be incompatible with privacy protection for Canadians.[87]

U.S. judges, with the occasional exception of those sitting in the Supreme Court, do not profess to make policy. When it comes to policy, Canada's Privacy Commissioner takes a back seat to no one. In his most recent report to Parliament, the Commissioner criticized the use of DNA analysis for forensic identification to the extent it could permit the compiling of genetic dossiers on large numbers of citizens;[88] opposed drug testing that "has given the state and employers unprecedented power to peer into our bodies at random, searching for evidence of socially unacceptable behavior;"[89] and warned that biometrics, such as digitized fingerprints, retinal scans, and facial recognition technology create the risk of pressing "our very bodies into service as personal identifiers," with "intimate, indelible information . . . then scattered and shared beyond our control."[90]

In his report, the Commissioner criticized the U.S. for its lack of attention to privacy in these areas, expressing particular ire that all Canadian trucking firms that use U.S. roads must conduct mandatory drug testing, which he views as providing no protection to public safety but

86. *Annual report*, supra n. 76.

87. *Id.* at 48. "[T]he Commissioner has no legislative mandate to educate the public about their information privacy rights. . . this silence has not prevented the Privacy Commissioner from pushing the limits when the public's privacy rights were at risk." *Id.*

88. *Id.* at 18.

89. *Id.*

90. *Id.*

merely creating a "humiliating intrusion into workers' private lives."[91]

Some might take issue with the Commissioner's vision. It is not unreasonable to argue that photographs on driver's licenses have been used as personal identifiers throughout much of the world for decades to cash checks, demonstrate that one is of age for the purposes of buying alcohol, and assist in similar legitimate public identifying functions. Nor is it inherently incredible to believe that drug (or alcohol) testing of truckers reduces the number of deaths of innocent persons on the roads or that new technologies such as biometrics could be socially beneficial.[92]

What is certain is that the Canadian Privacy Commissioner has in fact combined the roles of neutral fact-finder, unprejudiced judge, and aggressive advocate within a single office.[93] While administering existing privacy law, the Commissioner has strongly endorsed extremely far-reaching new privacy regimes.[94] The only proper policy result, he has argued in his official reports, is for a privacy czar to be devoted to ensuring that the individual controls all the information that others have about the individual and how that information is used, in the individual's purest "rational self interest," without reference to any other value society may have.[95] When a privacy issue arises, the Commissioner "will assert the privacy claim [and] only this claim."[96] Acknowledging that there are "other values and interests," the Commissioner goes on to state, "they will be for others to assert."[97]

The Commissioner's combination of rule-maker, prosecutor, judge, and advocate roles has disturbed some Canadians, who have questioned whether a person in an appointed position with such enforcement responsibilities should also have the right to make policy. Some disagree with the proposition that privacy as a right trumps every other public goal, right, equity, or interest, such as protecting the public from public transportation workers on drugs, helping the government discourage fraud, or protecting a public space for public discourse as is required in the U.S. under the First Amendment.[98] For those, there is no recourse, as the Commissioner's independence of the Canadian federal government has been designed precisely to counter any potential political pres-

91. *Id.* at 23.

92. *Id.* at 19.

93. *See generally* Brian Foran, Anne Rooke, & Gerald Neary, Presentation, *The Role of the Federal Privacy Commissioner,* <http://www.privcom.gc.ca/english/02_05_a_000221_2_e.htm>; (Feb. 21, 2000) *Annual Report, supra* n. 76.

94. *See generally* Foran, *supra* n. 93; *Annual Report, supra* n. 76.

95. *Id.*

96. *Annual Report, supra* n. 76, at 2.

97. *See generally* sources cited *supra* n. 94.

98. U.S. Const. amend. I.

sures upon the position.[99] In the U.S. system, at least, such an arrangement would present significant constitutional issues.[100]

Significantly, in the U.S. system, advocacy for the view that privacy trumps other rights and policies is often ably articulated by non-profit organizations, such as the American Civil Liberties Union, and by certain privacy advocates, such as Marc Rotenberg of the Electronic Privacy Information Center ("EPIC"), who undertake the kind of public policy, legislative, lobbying, and litigation efforts initiated in Canada by the Commissioner with great effectiveness.[101] Any review of the most important privacy cases in North America undertaken over the past year would suggest that they have been made not by any public official, including the Commissioner, but by private litigants turning to the courts under existing law, including EPIC.[102]

Meanwhile in Canada, the privacy czar's role has expanded from responsibility for privacy issues limited to the government to that of the entire Canadian economy. C-6, the new Canadian privacy law, to be administered by the Privacy Commissioner, has its initial effective date January 1, 2001, for most regulated businesses, with complete implementation due by January 1, 2004, when the law will extend to every organization that collects, uses, or discloses personal information in Canada.[103] The substance of the law follows the standard models of the OECD and the E.U., setting forth ten principles that together constitute a detailed code of privacy protection for individuals to which all businesses must comply.[104] The Commissioner has hailed the bill, which his office helped draft.[105] However, others in Canada have criticized the specifics of the Act as ambiguous and poorly drafted.[106] Among the most

---

99. *Annual Report, supra* n. 76, at 13.

100. *See Buckley v. Valeo,* 424 U.S. 1 (1976); *INS. v. Chadha,* 462 U.S. 919 (1983).

101. *See generally* American Civil Liberties Union <www.aclu.org>; EPIC <www.epic.org>.

102. *See* sources cited *supra* n. 2, and accompanying text. During 1999 and 2000, EPIC and persons associated with it played a catalytic role in initiating and publicizing many major privacy cases. *Id.*

103. House of Commons, *supra* n. 68.

104. *Id.* The ten principles are accountability, identifying purpose of use at collection, consent, limiting collection to what is necessary, limiting use, disclosure and retention, accuracy, safeguards, openness, access, and opportunity to challenge compliance. *Id.*

105. *Id.*

106. *See e.g.* Mr. Robert Keyes, Senior Vice-president, International, the Canadian Chamber of Commerce, *Testimony before Canadian House Committee on Industry* <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (Mar. 2, 1999); Mr. Phil Saunders, Vice-president, Commercial Relations, Northern Telecom Limited, *Testimony before Canadian House Committee on Industry* <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (Mar. 2, 1999); (noting that Mr. Saunders is also from the Canadian Chamber of Commerce); Jayson Myers, Senior Vice-President and Chief Economist, Alliance of Manufacturers and Exporters Canada, *Testimony before Canadian House Committee on Industry*

concrete criticisms is the focus on C-6's recurrent shifting between statements of "shalls," or mandatory obligations, and statements of "shoulds," or mere recommendations for compliance, creating substantial uncertainties about what is expected.[107]

On jurisdiction, the bill clearly provided everything the Commissioner had been seeking to assert his authority over the broadest possible number of Canadians with the greatest possible amount of power.[108] Under C-6, the Commissioner has the power to initiate complaints, rather than merely to respond to them; to conduct investigations; to audit an organization's information management practices; to compel persons to give evidence under oath and to produce records; and to enter any premises occupied by an organization, converse with its employees, and examine its records.[109] Any willful violation of cooperation with the Commissioner may constitute an indictable offense, potentially subjecting the violator to a fine of up to 100,000 Canadian dollars per offense.[110]

Commissioner Phillips was succeeded by a new Privacy Commissioner late in 2000 and so will not be personally responsible for administering the new Act. Nevertheless, assuming Canada's new Commissioner will feel bound by the parameters established by the first Commissioner, it may be instructive for the U.S. to see whether in practice the office finds itself able to regulate all Canadian gatherers of personal information effectively and fairly. Alternatively, U.S. policy makers may well find themselves justified in what the Commissioner has already described as their "uneasiness about the act and the Privacy Commissioner's role."[111]

<http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (March 2, 1999); Don Brazier, director of labour relations from CP Rail, *Testimony before Canadian House Committee on Industry* <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (March 3, 1999); Mr. David Olsen, Assistant General Counsel for Canada Post, *Testimony before Canadian House Committee on Industry* <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (March 3, 1999); and Ms. Leslie-Anne Lewis, Manager, Employment Legislation, from CN Rail, *Testimony before Canadian House Committee on Industry* <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (Mar. 3, 1999); Ms. Cynthia A. Rathwell, Vice-President, Legal Affairs, Canadian Association of Broadcasters, *Testimony before Canadian House Committee on Industry* (Mar. 11, 1999) <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (accessed Oct. 21, 2000); *see also* editorial, *C-6 is a Bad Prescription*, Canadian Medical Association 106 (Nov. 16, 1999) <http://www.cma.ca/cmanews/vol-9/issue-12/004.htm#2> (accessed Oct. 21, 2000).

107. House of Commons, *supra* n. 68.

108. *Id.*

109. *Id.* at Part 1.

110. *Id.* at § 28(b).

111. *Annual Report*, *supra* n. 76, at 33.

VI. PRACTICAL EXPERIENCE III: OTHER CZARS

The countries of the E.U. have both a settled regional privacy standard, in the form of the 1995 E.U. Directive on the Protection of Personal Data ("Privacy Directive,"),[112] and a settled administrative approach for administering the national laws required to be enacted to meet the requirements of the standard. Each of the 15 member states now has a privacy czar, typically termed a Data Protection Authority or a Data Protection Commission, hereafter both referred to as "DPA," the acronym used within the E.U.[113]

Like Canada's czar, the DPAs in Europe have multiple functions, from drafting regulations and carrying out enforcement activities to making policy recommendations and even drafting model agreements for businesses to use in sharing personal information to perform services for their customers.[114]

Each DPA is created under the domestic laws of an individual country and is theoretically subject to the laws and governments of that country.[115] However, the DPAs have also come to see themselves as a having a common interest that transcends their national one: the interest of protecting privacy.[116] Accordingly, they have formed working groups to standardize their practices, developed a pattern of conducting regular meetings in Brussels in which only DPAs may participate, and from time to time, undertake DPA-only conferences to issue DPA-only statements on important privacy topics.[117] Thus, the DPAs are rapidly becoming semiautonomous, chartered by their domestic governments and funded by them but operating by their own, self-directed, global standards without regard to domestic government policy.[118]

The DPAs advocate new standards that often would oppose forms of data collection that might be useful to businesses or to governments but that might undermine privacy. They include active badges for workers to be used as a mechanism to control security at high-risk sites; video cameras placed for safety reasons at entrances or in places requiring a high level of security; telephone call accounting systems that record the time

112. European Parliament and the Council, *Directive 95/46/EC* <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html> (Nov. 23, 1995) (discussing protection of individuals with regard to the processing of personal data and on the free movement of such data).

113. *See id.*

114. *See generally* Europa, *Data Protection: Background Information* <http://www.europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm> (accessed Jan. 6, 2001).

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

and duration of incoming, outgoing, internal or external calls; the installation of network-based or satellite communications devices in homes or vehicles; and all forms of the technologies used in telework that could enable an employer to know whether an employee is actually working.

The use of each of the technologies described above would be limited in the E.U. if the DPAs implement their current recommendations. The limitations would include restricting use to situations in which the subject of the information had consented and providing data subjects the right to inspect all the data collected pertaining to them (including all video footage) and the ability to revoke their consent to the use of the items. The DPAs have also recommended that labor unions have the right to veto any fundamental change to "the structure of information technology in use at the workplace."[119] The DPAs did not dwell on the practical means of implementing their suggestions. For example, they did not specify how a commercial establishment using a video camera for safety at the entrance of a building was to secure such consent in practice.[120] The DPAs often treat government interests and commercial interests similarly. For example, another DPA consensus report strongly criticized law enforcement wiretaps lawfully initiated against criminal organizations or in connection with official corruption cases, alleging that "these categories of offences have not yet been and cannot be precisely defined," although in fact, both categories are well-established in the domestic laws of most of the countries of the world.[121] These standards, once established by DPAs acting in concert, are implemented domestically.[122]

Apart from such group actions, the core responsibilities of the DPAs are to administer and enforce their national laws. In this area, it is useful not only to look at what DPAs statutory duties but also to focus on what they have been able to do in exercising their authority. In most cases, the gap between their statutory obligations and their actual implementation of their work is huge.

For example, the United Kingdom ("U.K.") DPA is a commissioner who is appointed by the Queen but who reports directly to Parliament.

---

119. European Union Data Protection Commissioner, *Report and Recommendations on Telecommunications and Privacy in Labor Relations* (Feb. 13, 1997) <http://www.datenschutz-berlin.de/sonstige/konferen/iwgdpt/12_51.htm>.

120. *Id.*

121. Working Group, *Report on Telecommunication and Media on Problems Relating to the Secrecy of Telecommunications and Satellite Communications and Common Statement of the International Conference of Data Protection and Privacy Commissioners* (Oct. 29, 1992) <http://www.datenschutz-berlin.de/informa/heft14/b3.htm>. A working group of DPAs at the International Conference of Data Protection and Privacy Commissioners issued this report in Sydney, Australia, in 1992. *Id.*

122. *See infra* nn. 123-29 and accompanying text.

The commissioner assesses whether anyone who is processing personal data involving a U.K. citizen is in compliance with the 1998 British Data Protection Act, which updates and replaces its 1984 predecessor.[123]

The commissioner has broad powers to engage in enforcement actions against any entity that may be contravening any "Data Protection Principles," including initiating prosecution as a criminal offense against anyone who refuses to comply with a commission order, with a fine that can be unlimited, depending on the court where the offense is brought. When a commissioner suspects an offense has been committed against privacy, he or she can apply to a judge for a warrant to enter and search the premises of the alleged offender, inspect and operate any equipment on the promises that could be used for the processing of personal data, and inspect and seize any evidence of an offense.

In the U.K., every business that processes personal information of any kind must register with the commissioner, describing what kind of personal data they process, the purposes for which the data is collected, and any names of any countries outside the E.U. where the data might be transferred. After a transition period that ends October 23, 2001, all entities processing such information electronically must complete this registration or be subject to an unlimited fine, again depending on the court where the offense is brought. It is no defense to this crime, or to most of the other offenses in the British statute, to state that one was unaware of its applicability. As the DPA guidance states, although the exercise of all due diligence to comply with a duty may be a defense in general, "[t]his is a strict liability offense."[124] Ironically, although every data processor must register, the information is not treated as public record by the commissioner, who instead forbids that any part of the register be copied without the commissioner's express permission.[125]

Criminal offenses subject to enforcement by the commissioner include "processing without notification," "failure to notify the Commission of changes to the notification register entry," "processing before expiry of assessable processing time limits," "failure to comply with written request for particulars," "failure to comply with an enforcement notice," "knowingly or recklessly making a false statement in compliance with an information notice," "intentional obstruction of or failure to give reasonable assistance in, execution of a warrant," all punishable by fines of 5,000

123. *See generally Introduction to the 1998 Act* <http://wood.ccta.gov.uk/dpr/dpdoc> (accessed Oct. 24, 2000). This and the following paragraphs are based on a document produced in October 1998 that the U.K. DPA recently described as the most up-to-date guidance on the 1998 Act. *Id.*

124. *Id.* at ch. 8, § 6.1.

125. The Data Protection Public Register, *Notification Under the Data Protection Act of 1998 and the Data Protection Register* <http://www.dpr.gov.uk> (accessed Oct. 25, 2000).

pounds per offense or an unlimited amount in crown courts.[126]

Although the commissioner has not issued regulations in many areas under the 1998 Act, the office has begun to issue guidance on difficult questions, setting forth standards to guide uses of closed-circuit television monitoring consistent with the E.U. DPA standards on new technologies. The commissioner's new standards include specifying where equipment may be located, what areas of public space may be covered, limitations on the adjustability of cameras to insure that operators cannot manipulate them to view spaces that are not supposed to be covered, the placement of signs warning the public that television monitoring is being undertaken, the size of signs depending on their use, and the material that the signs must specify, such as who is undertaking the monitoring, the reason for the monitoring, and a contact number. The commissioner also has established standards for video equipment and components, specifying that tapes be of good quality, that the medium on which the images are captured must be cleaned so that images are not recorded on top of images recorded previously, that the medium on which the images have been recorded should not be used when the quality of images has deteriorated, and so on. Recommendations are given for the length of time of keeping recorded images (no longer than seven days), where recorded images may be viewed (only in a manager's or designate member of staff's office), and how images removed for viewing should be documented (date and time of removal, who removed the image, reason for viewing, outcome of viewing, data and time images were returned to the system, etc.)[127] The guidance reads more like a manual than a set of principles and is at a level of detail that invites compliance problems, which may be perceived as inflexible, unworkable, and costly.

By contrast, rather than provide comprehensive schemes for regulation of data processing, the Italian privacy czar prohibits all such processing, unless the Italian DPA explicitly permits it. Accordingly, the Italian DPA has issued a series of decrees, termed "authorizations," which specify that the processing of personal data is prohibited and then has granted an "authority" for certain kinds of processing. For example, one authorization permits banks, credit unions, insurance companies, fund managers, tourist agencies, and transportation companies to process personal data for the fulfillment of their obligations within their relevant sectors of activity. Another authorization deals with processing by private detectives. A third deals with processing of judicial data by private entities and public bodies. In each case, after a broad prohibition

126. Data Protection Commissioner, *Introduction to the 1998 Act,* Offenses Under the Act, Ch. 7, Ch. 8 <http://wood.ccta.gov.uk/dpr/dpdoc.nsf> (accessed Oct. 21, 2000) (setting forth the offenses).

127. British Data Privacy Commissioner, *CCTV Code of Practice* <http://wood.ccta.gov.uk/dpr/dpdoc> (accessed Oct. 25, 2000).

against processing personal data, the authority states that the data may be processed to the extent the processing is necessary for the task, without a definition of what is and is not necessary. While purporting to regulate all commercial activity pertaining to individuals and their data, the Italian authorizations are so vague and general, they in practice regulate none.[128]

Many DPAs fall between the British and the Italian approach. All the DPAs have their own approach to privacy enforcement, and none have in practice secured substantial compliance. In June 2000, representatives of U.S. companies met with the U.S. Department of Commerce in Washington to be briefed on the final iteration of the U.S.-E.U. safe harbor arrangement. At the meeting, senior Commerce officials were asked whether the U.S. had sought to determine the extent to which E.U. firms were themselves in compliance with the Privacy Directive. The U.S. officials advised that they had asked this question of their counterparts in the European Commission on several occasions, who in turn had asked this question of representatives of the DPAs. No answers to this question were ever provided. The U.S. officials concluded that no one in the E.U. had undertaken any serious efforts to find out.[129]

In short, in Europe, the DPAs have asserted broad authority and in some cases issued detailed prescriptions of what behavior is permissible, but they have enforced implementation of national privacy laws and the E.U. Privacy Directive in an inconsistent and incomplete manner.

In New Zealand, the tone differs substantially from that used by DPAs in Canada and the E.U., even though their privacy czar, with a staff of 20, theoretically exercises similar powers, covering every person in the country's use of personal data. The New Zealand privacy czar, who is independent of the executive branch, issues opinions on proposed legislation, makes policy recommendations, issues guidelines and regulations, and investigates complaints from individuals, always acting as a strong privacy advocate. For example, in the policy area, the commissioner has entered into such controversial areas as suggesting that New Zealand "rethink" exemptions from privacy law given to Parliament and the news media.[130] Interestingly, few of the cases the commissioner has actually handled have related to weighty issues involving violations of privacy of many people. Instead, they are often the kind of matters that

128. *See e.g.*, Authorization No. 5/1999, *Processing of Sensitive Data by Various Categories of Data Controllers* <http://www.dataprotection.org/garante/prewiew/1,1724,460,00.html?sezione=123&LANG=2> (Sept. 29, 1999).

129. Interview with U.S. Department of Commerce and representatives of U.S. business (May 2000). The author has also asked this question directly to various members of the European Commission and various DPAs, with the same response.

130. Bruce Slane, *Report of the Privacy Commissioner for the Year Ended 30 June 1999* (July 20, 1998) 7 <http://www.dataprotection.gov.uk/report98/app12.pdf>.

in the U.S. would be handled by a state trial court. For example, in 1999 the commissioner handled:

The disclosure by a church official about an individual to the congregation before asking the congregation to pray for the person and his wife. The case was settled when the church apologized.

Provision by a psychiatrist of health information about a person to four government agencies, including his children's school. The case resulted in a monetary settlement of $8,000 New Zealand dollars.

Improper disclosure by an employer investigating concerns that an employee was stealing from the employer, who expressed his fears about the theft to the employee's wife.

Covert videotaping of women in a store changing room by a man with a fetish for viewing women in their underwear.[131]

In addition, New Zealand's commissioner granted four applications to companies seeking to disclose personal information to the government. In one such case, the permission was required to permit a health care company to provide the name of patients to enable the patients to be listed on a waiting list of a health care facility administered by the government. In a second case, New Zealand's Meat Board requested the right to have meat processors disclose their "levy payer list" so the Board could contact the livestock farmers on policy issues. In a third case, a company asked for permission to advertise the list of former clients who were entitled to a share of money owed to them as a result of a settlement of wrongdoing by a former employee of the company. A similar fourth case required the commissioner's permission before a company could reach out to former employees to advise them of money owed them under a company retirement plan.[132]

New Zealand, with a population of less than 3.5 million people, may find it appropriate for a regulatory body within the national government to have the responsibility to issue these kinds of permissions, although the commissioner has expressed frustration with his inability to handle all of the cases that are brought to him in a timely fashion.[133] A comparable body in the U.S., staffed at the level of 1,600 people by a ratio to reflect the difference in the respective size of the county's populations, would be hard pressed to handle the volume of cases that would be generated by this kind of cradle-to-grave supervision of all aspects of the extensive use of personal information by the 250 million people of the U.S. The likely delays in responding to inquiries, or to initiating investigations by such a body, inevitably strapped for resources, might be found

131. *Id.* at 37–41.

132. *Id.* at 56–58.

133. *Id.*

less efficient than the U.S. system of civil litigation.[134]

VII. CZARS VERSUS THE PUBLIC SPACE

Although a number of privacy czars now regulate throughout the world, no single official in any country is responsible for maintaining public space. Indeed, the U.S. tradition of insuring that people have the right to free and fair association, the right to gather in public places, the right to speak their mind about any topic, including the right to gossip about their neighbors, is so embedded in the foundation of the Constitution's Bill of Rights that Americans often take it for granted.

Ironically, new assertions of the right to privacy directly threaten the public space in country after country, and privacy czars in many countries have come to consistently take actions to reduce the area of information available to the public, if that information could relate to any individual. This trend is already evident in emerging privacy law in the E.U. For example, under the E.U. Privacy Directive, all information that can be related to an identifiable person—including name, address, telephone number, and picture or photograph—is subject to regulation. Although exceptions to the requirement for notice and consent exist in such areas as national security and law enforcement, in general, personal data can only be processed with the permission of that individual. Under Article 18(3) of the Directive, even public information cannot be processed except with the data subject's consent, unless the public information is required to be collected under domestic law for public purposes. An individual in the E.U. may have the right to go to public records to gather information on other citizens, from public registries, but the individual may not use such information for a commercial purpose without the consent of all the data subjects.

For example, as Article 18(3) has been initially interpreted by E.U. privacy mavens, voting lists, census and population registries, court records, and case-law databases may be available to someone wanting to exercise their rights as a citizen but cannot be lawfully placed on the Internet without the consent of every individual in the list, registry, or record.

The E.U. privacy czars have made a direct and substantial contribution to this shrinking of public space. In March 1999, the Article 29 Data Protection Working Party established under the Directive (made up of representatives of the E.U.'s privacy czars and the European Commis-

134. *See generally* The Australian Privacy Commissioner's Website <http://www.privacy.gov.au> (accessed Dec. 2, 2000); *Office of the Privacy Commissioner for Personal Data, Hong Kong* <http://www.pco.org.hk> (accessed Dec. 2, 2000). Other privacy czars in the Asia Pacific region, operating in Australia and Hong Kong, hold offices established very recently, and remain too new to provide much in the way of guidance. *Id.*

sion) took the position in a published opinion that special precautions should be undertaken to prevent case-law databases from being used as information files on individuals, rather than merely being consulted to ascertain case law and legal precedent.[135] The opinion favorably cites a proposal from a Belgian privacy commission that court decisions not be indexed by names, to prevent searches from being made on the basis of the names of the parties. The opinion also supports a French approach to voting data that prohibits commercial usage of electoral lists. According to the opinion, France has also successfully taken administrative measures to ensure that querying computerized versions of the telephone directory using the first few letters of the surname—a staple of U.S.-based Internet searches using wildcards—is technically impossible in France. The opinion further suggests that the E.U. provide that publishers of all telephone and address directories in any medium provide a no-cost opt-out for individuals who do not want their personal data accessible for commercial purposes.[136]

In the U.S., even in the absence of the activity of any privacy czar, a number of recent legislative efforts have attempted to further limit the uses of public record materials. For example, a Minnesota bill would prohibit the release of real estate property records for all nongovernmental purposes, except with the consent of the property holder, effectively making property ownership secret.[137] A South Carolina bill introduced earlier this year would make the access, release, or disclosure of personal information without prior written consent from that person a felony subject to ten years imprisonment, defining the term "personal information" as any information relating to personal purchasing habits or preferences, as well as financial records, regardless of the source.[138] President Clinton, in his privacy initiative, proposed a formal study of whether federal bankruptcy files should be made confidential to protect bankrupt persons from predatory activity.[139] Even without a privacy czar, the U.S. commitment to maintain a large space for public information appears to be shrinking.

The tension between privacy and the public space has perhaps best been articulated by Canada's recently departed Privacy Commissioner, Bruce Philips, taking as always the side of privacy:

---

135. Working Party, *Opinion No. 3/99 on Public Sector Information and the Protection of Personal Data* (May 3, 1999) <http://europe.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp20en.htm> (accessed Oct. 24, 2000).

136. *Id.*

137. Minn. H. File 3615, 81st Reg. Sess. (Mar. 15, 2000).

138. S.C. H. 4469 § 2(B) (2000) (amendment to § 16-13-550).

139. Office of the White House Press Secretary, *Fact Sheet on Plan to Enhance Consumers' Financial Privacy* <http://www.ofcn.org/cyber.serv/teledem/pb/2000/apr/msg00241.html> (Apr. 30, 2000).

Defenders of a private life are often accused of interfering with an "open" society, as if freedom of information and a free press obliges everyone to live in metaphorical glass houses. Certainly, government must be open and accountable to its citizens, allowing us to draw conclusions about the quality of government policy and administration. And the media has the right and responsibility to report on matters of public interest, guided (one fervently hopes) by a concern for accuracy and fairness. But there is no obligation in a free society for individuals' lives to become an open book for government, the media, or their neighbors.[140]

The distinction that Commissioner Philips seeks to draw, between the rights of the press to report "on matters of public interest" as lawful and other inquiries or disclosures as unlawful, is provocative. It suggests, for example, that the press may not lawfully report on topics that are deemed to be not of public interest. Who decides which category information may be in? Whatever the answer, material is removed from legitimate public discourse, small or large, depending on where the barriers to "what is public" are placed. In China, all information about the business activities of state-sponsored enterprises may be ordinarily considered private and dissemination of information about this sector may be unlawful, making it extremely dangerous and difficult to penetrate cases involving corruption or other issues that could be of considerable interest to the public. Similarly, Commissioner Philips draws the dichotomy between the rights of the press, which he acknowledges, and the lesser rights of those not in the media to investigate issues they may consider to be in the public interest. How can one decide what is "the media," and what is merely a "private person" who is interested in personal information for some purpose now deemed improper? The test, especially in the age of the Internet, is not an obvious one, but it suggests the possibility that someone would need to segregate the sheep (the media) from the goats (the rest of us) through a form of licensing or permission. Again, wherever the line is drawn, an attenuation of the public space results. Commissioner Philips may be comfortable deciding what is lawful communication by whom and what is not. The rest of us may wish to pause, and shiver.

VIII. PRIVACY CZAR AS BIG BROTHER: TAKING THE ORWELL TEST

The title of this article states clearly the concern that a privacy czar, designed to protect personal liberty, turns out to be a position that inherently limits personal liberty by regulating the flow of information. A review of the actual activities of privacy czars in other countries shows them asserting authority over a remarkably broad swath of human activ-

140. *Annual Report*, *supra* n. 76, at 7.

ity, including issues affecting the delivery of health services, crime prevention, what kind of information can lawfully be made public, and what kind of statements people may lawfully make about other people. Apart from the world's privacy czars, and the national security and police services of countries that are not democratic, few government agencies have these kinds of authorities or powers broadly to regulate and control what information people may gather and say. These kind of controls have been found historically in dictatorships. They are inconsistent with democracy. Vesting such powers in a privacy czar in the U.S. would surely be unconstitutional. But even assuming some limits on the power of a czar to accommodate the Constitution, the concept is inherently risky, as the following comparison of the powers of Orwell's Big Brother, and the inherent powers of many of the world's privacy czars, helps to demonstrate:

ORWELL'S BIG BROTHER: Able to determine what information is lawful, and what information is unlawful, to acquire, process, and disseminate

PRIVACY CZARS: Ditto.

ORWELL'S BIG BROTHER: Able to enter your place of business, go through your records, and search and seize any information that Big Brother deems improper.

PRIVACY CZARS: Ditto.

ORWELL'S BIG BROTHER: Able to punish you if you say the wrong thing or send information you shouldn't to someone you shouldn't.

PRIVACY CZARS: Ditto.

ORWELL'S BIG BROTHER: Able to order that your business be shut down, without due process of law, if he determines that you have violated Big Brother's information policies.

PRIVACY CZARS: Ditto.

ORWELL'S BIG BROTHER: Able to order photographs or documents to be airbrushed or changed, if Big Brother decides the original is not politically correct.

PRIVACY CZARS: Ditto.

ORWELL'S BIG BROTHER: Able to force you to disclose under threat of imprisonment with whom you have shared information, so that they can get the information back and punish others who have disseminated it.

PRIVACY CZARS: Ditto.

CONCLUSION

The intellectual and spiritual father of the world's privacy czars is not Thomas Jefferson. It is not even Louis Brandeis.

It is Big Brother.[141]

141. *See* George Orwell, *1984* (Harcourt 1949). The hero of the novel, one Winston Smith, finds himself subjected to all of the powers of the novel's privacy czar equivalent, whose principal mission appears to be controlling individuals through controlling the information they are permitted to acquire, process, use, and disseminate, doing so through use of the kinds of powers set off in the text above. *Id.*