E-GOVERNMENT

John C. Reitz

College of Law, University of Iowa

Topic VI Draft: February 10, 2006

E-GOVERNMENT

by John C. Reitz∗

The use of informational and computer technology (ICT) to facilitate interaction between, on the one hand, a public authority and, on the other hand, individual citizens, businesses, or non-governmental organizations is now widely known by the term "e-government." Although it has been characterized as "e-commerce" involving public authorities, only some of the issues raised by e-government are truly similar to the issues raised by e-commerce. Quite a few of the most important issues raised by e-government are different precisely because the government is involved.

The United States has adopted e-government with great enthusiasm in many obvious ways. The federal government, for example, maintains a portal site on the Internet, from which there are links not only to web sites for most, if not all, federal agencies, courts, and officials, but also to state, local, and even tribal government.[1] With just a few mouseclicks, one can find a link to just about any unit of government at any level. Congress has passed the "E-Government Act of 2002"[2] to symbolize the federal government's commitment to e-government. Among other things, the Act provided funds to develop e-government.[3]

Because the term "e-government" covers such a broad field with rather uncertain contours, Section 1 of this report proposes a typology of the different types of e-government as a way of organizing analysis of both potential benefits and problems created by e-government. Since there are so many different legal issues, the report will have to be highly selective in order to be able to say anything meaningful about any of these issues. The focus will be on the federal

---

∗ Edward L. Carmody Professor of Law and Associate Dean for International and Comparative Law Programs at the University of Iowa College of Law. The author would like to acknowledge generous summer research support from the University of Iowa Law Foundation, research assistance from Iowa students Charles Bork, Shigehito Onimura, Ai Tong, and Tyson Wray, and helpful comments and ideas from colleagues Randall Bezanson, Arthur Bonfield, Nicholas Johnson, Larry Ward, and Tung Yin.

[1] http://www.firstgov.gov (last visited on January 17, 2006).

[2] Pub. L. 107-347, Dec. 17, 2002, 116 Stat. 2899 (2002)(codified at various parts of 44 U.S.C. (Supp. II 2002)).

[3] The Act established a fund of $345 million through fiscal year 2006. 44 U.S.C. § 3604 (g) (1)(Supp. II 2002). Although the E-Government Act touches on a number of crucial problems, in general it does not resolve them, but rather seeks to influence action by establishing monetary and political incentives to act, including especially the requirement for agencies to report to the Office of Management and the Budget (OMB) on an annual basis. See, e.g., Section 202(g)(codified at 44 U.S.C. § 3501 note (Supp. II 2002)).

government.[4] Section 2 describes how the interrelated issues of security and privacy protection have been dealt with in the online filing of court documents. Section 3 focuses on one important aspect of e-government that has the potential to enhance democratic governance, the electronic version of the U.S. form of notice and comment rulemaking. Section 4 discusses the problem of setting reasonable limits to the government's awesome power of electronic surveillance. The last section sets forth some brief, general conclusions.

1. Types of E-Government and Overview of Benefits and Problems of Each Type

The chief use of ICT to date by governments at all levels of the United States with respect to their own citizenry has involved the Internet, including e-mail.[5] By far the most important and widespread government use of ICT is for the dissemination or "publication" of information ("e-publication"). Government bodies at every level of government in the United States from the federal government to local municipalities have created web sites to make available to the general public notices, forms, and general information about governmental processes. These web sites generally also list contact information or contain links to the relevant government offices, so that interested citizens with Internet access can easily send messages to agency officials or to his or her elected representatives.

Many government offices at all levels of government also accept online filing of official documents, such as tax returns, corporate and non-profit filings, security interest filings, some kinds of license applications and renewals, and even court pleadings, typically as files attached to e-mail messages ("e-filing").[6] Government use of the Internet for buying and selling goods

---

[4] In general, under the U.S. form of federalism, the federal government may not prescribe the rules for state and local government. Nevertheless, the federal government is often the leader for development of similar rules at the state or local level.

[5] Government uses other forms of ICT, as well, but the only other form this report will consider is the use of computers to extract information about individuals from large bodies of data, including "data mining," which generally refers to the use of computers to identify and analyze patterns in large volumes of data. Other technology that might be considered a form of or related to ICT include, for example, various forms of biometrics (hand scanning, iris scanning) to identify travelers, police tracking of suspects through their cell phones, and electronic voting machines. See generally Robin Feldman, "Considerations on the Emerging Implementation of Biometric Technology," 25 *Hastings Comm. & Ent. L.J.* 653 (2003); Daniel P. Tokaji, "The Paperless Chase: Electronic Voting and Democratic Values," 73 *Fordham L. Rev.* 1711 (2005).

[6] See generally William A. Fenwick & Robert D. Brownstone, "Electronic Filing: What Is It? What Are Its Implications?" 19 *Santa Clara Computer & High Tech. L. J.* 181 (2002)(e-filing in a number of government settings, with special emphasis on electronic filing of court documents).

and services ("e-procurement") constitutes a special subcategory that uses both e-publication and e-filing. E-procurement is the part of e-government that looks the most like e-commerce.[7]

E-publication and e-filing, including e-procurement, involve two simple functions: (1) turning the Internet into a giant bulletin board for government, thereby enhancing the citizen's ability to obtain information from government, including finding out about government purchases and sales of goods and services, and (2) enhancing the citizen's ability to contact government officials and to obtain and file documents and purchase orders or invoices through e-mail and to receive or make payment by electronic funds transfers ("e-payment"). These two functions constitute marvelous enhancements of the relationship between citizen and government. There is no reason to doubt that these functions alone have resulted in enormous savings to both government and citizenry with respect to the cost of getting governmental information and forms to the public and the cost of getting citizen information and documents to governmental officials, including the official filing of various forms with the government.[8] For this very reason, these functions hold the potential to enhance the accessibility of government offices and increase the transparency of government functions. It is arguable that such enhancements contribute to strengthening the overall legitimacy of government.

But the proponents of e-government tend to argue for even greater benefits. They say that the ease of communication provided by computers and the Internet has the potential to revitalize the practices of democracy by bringing government officials into much easier and even more productive communication with the public.[9] I will refer to this use of ICT as "e-democracy." E-democracy thus involves the same basic means of communication over the Internet as e-publication and e-filing, but the focus is on enabling public input into governmental decision making.

These e-democracy issues are perhaps the most interesting of all. Foreign observers who share this enthusiasm for the potential of ICT to enhance democracy should be especially

---

[7] Cf. 41 U.S.C. § 426 (f) (2000) (defining "electronic commerce" for purposes of authorizing its use in federal procurement as "electronic techniques for accomplishing business transactions, including electronic mail or messaging, World Wide Web technology, electronic bulletin boards, purchase cards, electronic funds transfers, and electronic data interchange").

[8] See, e.g., Cary Coglianese, "E-Rulemaking: Information Technology and the Regulatory Process," 56 *Admin. L. Rev.* 353, 376 (2004)(the Department of Transportation saves over one million dollars per year through storage of documents online); Fenwick & Brownstone, supra n. 6, at 217 (estimating a savings of a "major part of the estimated $11 billion spent for delivering and serving paper court documents").

[9] See generally *Democracy Online: the Prospects for Political Renewal through the Internet* (Peter M. Shane, ed., 2004); John Morison, "e-Democracy: On-Line Civic Space and the Renewal of Democracy?" 17 *Can. J.L. & Juris.* 129 (2004); Beth Simone Noveck, "Designing Deliberative Democracy in Cyberspace: the Role of the Cyberlawyer," 9 *B.U. J. Sci. & Tech. L.* 1 (2003).

interested in these U.S. developments because, while the computer and the Internet can facilitate the sending of communications between citizen and government official, they do nothing to ensure real communication and deliberation, to ensure, for example, that government officials will actually take public comments into account in formulating policy. The United States, however, has over sixty years of experience with rules of administrative procedure[10] that do require agencies, as a general matter, to solicit public comment and to take that comment into consideration before promulgating rules of general applicability (usually referred to in the United States as administrative "rules" or "regulations"). These procedures are known as "informal" or "notice and comment rulemaking," and one of the principal e-democracy issues is thus how those rules have to be modified to take best advantage of the computer and the Internet. Few other countries have such generally applicable rules that seek to ensure a real dialogue between agency policy makers and the public, but if the promise e-government is argued to have with respect to revitalization of democracy is to be realized, it would seem that some similar set of rules would be necessary. It is one thing to convey public comment to a government agency; it is another to ensure that the agency actually considers the comment. Adapting the rules of notice-and-comment rulemaking to electronic form, referred to as "e-rulemaking," is thus one of the most interesting aspects of e-government.[11]

One final function of e-government involves use of the computer to manage agency activities, including the processing and storing of information that the government collects or can access ("e-management"). This function could include the use of computers to collect information about individuals and organizations. To the extent these computerized powers are exercised for the purpose of fulfilling the government's function to protect its people from terrorism and other kinds of crime, we can refer to the activity as "e-surveillance." Once data has been digitized, it can also be stored in electronic form, generally at much lower costs than the storage of paper copies ("e-storage"). Finally, the computer may also be used as a management tool for the agency in ways ranging from docket control ("e-dockets") to efficiency studies on various parts of an agency. As the discussion in Section 2 below about online filing of court documents illustrates, once the public is given access to e-storage or e-dockets, this aspect of e-management merges with e-publication and raises the same issues.

It can thus be seen that e-publication and e-filing are the most basic aspects of e-government. E-procurement, e-rulemaking, and even some aspects of e-management are simply special applications of e-publication and e-filing.

The most basic issue with respect to e-publication and e-filing, and hence with regard to most aspects of e-government, has to do with the "digital divide," the disparity between those who have ready access to computers and know how to use them, and those who do not. This issue of equal access to e-government functions is obviously of fundamental importance to the legitimacy of government and becomes more important as computers become more important to the workings of government. Nevertheless, computer use is so widespread in the United States

---

[10] For the federal government, see 5 U.S.C. § 553 (2000).

[11] Section 3 is devoted to this issue.

that governments cannot afford to sacrifice the efficiencies to be gained from e-government just because some people lack access. The access issue is thus a complex one, for which there is regrettably inadequate space in this report for more than passing coverage.[12]

E-filing of sensitive personal or business information and e-payment raise serious security risks whether the addressee is the government or a private company, and it is here that the issues of e-government dovetail most closely with those of e-commerce. We may use e-filing to send important and sensitive personal information to the government, but hackers and Internet hucksters are waiting to try to access that information, and any personal or business information that is published on the Web is subject to search by people who motives may include blackmail or fraud. Closely related are issues of identity. Where the material we provide the government will be e-published, we may not want our identity disclosed, but reliable forms of individual identification or electronic signatures are vital to any form of online payment or contracting. Just as in non-governmental forms of e-commerce, electronic signatures are crucial to e-procurement, but they have not proven to be highly problematic.[13]

The security and privacy issues that arise in the context of all forms of e-filing and e-

---

[12] The E-Government Act attempts to bridge the digital divide from both ends. It directs agency heads to "(1) ensure that the availability of Government information and services has not been diminished for individuals who lack access to the Internet; and (2) pursue alternate modes of delivery that make Government information and services more accessible to individuals who do not own computers or lack access to the Internet." Section 202 (c) of the E-Government Act, 44 U.S.C. 3501 note (Supp. II 2002). It also provides funds for community technology centers, public libraries, and other institutions to broaden free Internet access to the public. Section 213 (a), (b), (c) of the Act, id. See also Gretchen Ruethling, "Almost All Libraries in U.S. Offer Free Access to Internet," *N.Y. Times*, June 24, 2005, at A11 (reporting on study by the American Library Association); Jaime Klima, "The E-Government Act: Promoting E-Quality or Exaggerating the Digital Divide?" 2003 *Duke L. & Tech. Rev.* 9, *10 (2003)(library access not sufficient for much e-filing).

But the Act protects access only to "information and services." The Securities and Exchange Commission requires all corporate filings to be made electronically through its EDGAR System. See also Arcy Mfg. Co., Inc., 1995 U.S. Comp. Gen. LEXIS 533; 95-2 Comp. Gen. Proc. Dec. P283 (August 14, 1995)(upholding requirement for electronic bids even on contracts exempt from general requirements of formal competitive bidding).

[13] The E-Government Act does not specify which forms of electronic signatures are valid for e-government purposes, but instead requires each executive agency to "ensure that its methods for use and acceptance of electronic signatures are compatible with" the policies issued by the Director of OMB and that each agency's policies permit "efficient interoperability among Executive agencies." Sections 203 (b), (c) (codified at 44 U.S.C. § 3501 note (Supp. II 2002)). The Federal Acquisition Regulations also leave procuring agencies freedom to accept all workable forms of electronic signature. 48 C.F.R. § 4.502(d)(2005).

publication are not conceptually different from those that arise in the absence of computers. To the extent that we citizens give government at any level sensitive personal or business information, we would like assurance that the government will not intentionally or inadvertently permit disclosure of the information to any third party, whether or not we used computers to transmit the information.[14] Clearly, if government is to have a sufficient level of legitimacy within the public to enable it to function, it must prevent major security breaches with respect to all sensitive personal and business data it collects. The question is whether the use of computers magnifies the risks to privacy.

Similarly, there is the risk that the government itself will abuse its data collection powers in the exercise of e-surveillance. Again, the government's abuse of its powers under this type of e-management is not in principle different from the issues arising with respect to non-computerized surveillance operations by the government. Whether or not computers are involved, the essential question concerns establishing an appropriate balance between individual privacy and government needs to gather information about terrorist attacks and other threats to the country. But the use of computers to collect and manage the surveillance data concerning large numbers of people arguably enhances the potential intrusiveness of the abuse of this power, especially in the post-9/11 world. Concerns about government abuse of its surveillance powers thus complement the concern about unauthorized access to and misuse of computerized databases of sensitive personal information.

2. Security and Privacy Issues in Online Filing of Court Documents

Both federal and state courts have enthusiastically embraced e-filing.[15] By making e-

[14] Cf. William J. Kambas, "Reform and Modernization of the Tax Compliance Process," 108 *Tax Notes* 1447, 1448 (September 19, 2005)(incidents of unauthorized access to Internal Revenue Service electronic databases of sensitive taxpayer information).

[15] See generally Gregory M. Silverman, "Rise of the Machines: Justice Information Systems and the Question of Public Access to Court Records over the Internet," 79 *Wash. L. Rev.* 175 (2004). The impetus to adopt e-filing came from the courts' adoption of e-management systems, especially e-docketing and systems for routing documents internally and tracking court work. Id. at 177-80. According to the Administrative Office of the U.S. Courts, e-management systems and e-filing are now in use "in 89% of the federal courts: 87 district courts, 92 bankruptcy courts, the Court of International Trade, and the Court of Federal Claims." "Case Management/Electronic Case Files (CM/ECF)" (January 2006), at http://www.uscourts.gov/cmecf/cmecf_about.html (last visited January 21, 2006).

For state courts, see http://www.ncsconline.org/WC/Education/ElFileGuide.htm (last visited on Oct. 9, 2005). The web site it links to for individual state courts lists 16 states in which some or all courts accept e-filing of documents. http://www.ncsconline.org/WC/Publications/KIS_ElFileStateLinksPub.pdf (last visited on Oct. 9, 2005).

filing generally available, the federal courts have far exceeded the requirements of the E-Government Act.[16] E-filing prompted the courts to adopt e-storage of documents to secure large savings in storage and retrieval costs,[17] and this development has in turn made online access to court filings feasible.

The issue of online access to court documents, which as a general rule are public documents and must be made available at the courthouse for inspection,[18] has been quite controversial. The federal courts have opted for full online access for all documents available at the courthouse.[19] The Conference of Chief Justices and the Conference of State Court Administrators have not. Rather, the state courts have so far opted for a policy that does not permit remote access to case files, but only to docketing and calendaring information and court judgments or orders.[20]

The argument against giving full online access to all of the case documents which must be provided at the courthouse is based on the "practical obscurity" of court files. The argument essentially asserts that because of the time and effort required, people with bad motives will not generally bother to go to the courthouse to comb through individual paper court records, but if the documents are all accessible online, it will be easy and relatively inexpensive for identity thieves or merchandisers of information to use computer search protocols to generate en masse collections of sensitive personal information concerning many different people for all kinds of bad purposes.[21] A version of this argument was accepted by the Supreme Court in *United States Department of Justice v. Reporters Committee for Freedom of the Press*.[22] The counterargument

---

[16] The E-Government Act requires only that each federal court maintain a web site with information or links to sites containing the following: contact information for the court, all local court rules, docket information for all pending cases, all court opinions issued by the court in text-searchable format, and access to all court records which have been filed in electronic form or converted by the court to electronic form. Section 205 (codified at 44 U.S.C. 3501 note (Supp. II 2002)).

[17] Silverman, supra n. 15, at 196.

[18] Subject, of course, to exception for records in adoption cases and subject to the court's general power to seal a record or any portion of it to protect unnecessary invasions of privacy.

[19] See "Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files," adopted September 2001, at http://www.privacy.uscourts.gov/Policy.htm [hereinafter "Report of Judicial Conference].

[20] Silverman, supra n. 15, at 200-01.

[21] Fenwick & Brownstone, supra n. 6, at 216; Peter A. Winn, "Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information," 79 *Wash. L. Rev.* 307, 316-18 (2004).

[22] 489 U.S. 749, 762, 780 (1989) (disclosure to a third party of an FBI "rap" sheet–a

is that, because court documents are already publicly available at the courthouse, it makes no sense to assume that "practical obscurity" will really suffice to prevent inappropriate use of access to the documents. The solution to the threat of misuse is to prevent the disclosure of sensitive personal information in court documents made available both online and at the courthouse. Advocates of online access also argue that a more restrictive access policy for online case materials simply spurs the development of a "cottage industry" of information merchants who compile data from the court files available at the courthouse and sell them to remote buyers.[23] Finally, the PACER system, which the federal courts use for online court documents, requires users to divulge some personal information to gain access and thus makes a record of those who access the records.[24] This kind of record may provide some deterrent to those who would access the documents solely with mischief in mind though it is hardly a strong defense.

The federal approach to online filing seems at odds with the basic policy judgment implicit in the Supreme Court's adoption of the "practical obscurity" argument in *Reporters Committee*, but the case is certainly distinguishable on technical grounds,[25] and it goes too far to argue, as one commentator has, that there is "a right to privacy in the practical obscurity of judicial records."[26] Moreover, as a result of choosing a policy of equal access to online and courthouse documents, the federal courts have worked out a list of "personal data identifiers" which should be excluded from court documents to be made available to the public, whether in

---

summary of a person's criminal record, each individual part of which would be a matter of public record within the jurisdiction where the arrest, indictment, or conviction took place–would constitute an unwarranted invasion of privacy and is therefore exempted from disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(7)(c)(2000)).

[23] See, e.g., Silverman, supra n. 15, at 198-221 (arguing also that XML provides a flexible system for redacting court documents to mark sensitive data with tags to tell the computer to limit access, whether the document is retrieved online or at the courthouse computer terminal).

[24] To obtain access to PACER, a user has to provide a credit card (to cover the fees for use) and wait a few weeks to obtain a password. Cameron L. Sabin & Kenneth B. Black, "Managing Pandora's Box: Recognizing and Handling the Privacy Risks Associated with Electronic Access to Court Records," 18 *Utah Bar J.* 6, 9 (2005).

[25] *Reporters Committee*, which is based on a statute, not on the Constitution, involved disclosure by the FBI, a federal agency, under the Freedom of Information Act, which does not apply to courts. 5 U.S.C. § 551(1)(B)(2000).

[26] Winn, supra n. 21, at 325. In fact, all one can really say is that the Court found the practical obscurity argument persuasive in striking the balance between publicity and privacy in the context of criminal rap sheets and the FOIA, and it is not at all clear how that balance might be struck in other contexts.

hard copy or online. These identifiers are Social Security numbers, dates of birth, financial account numbers, and names of minor children, and street addresses. If these types of data are necessary to resolution of issues in the case, then the data may be modified in the publicly available records, for example, by including only the last four digits of a person's Social Security number, the year of birth, the last four digits of financial account numbers, the initials of a minor child. As a general rule, only the city and state are to be indicated for a person's address.[27] Federal cases reviewing decisions by the Social Security Administration are also excluded from this policy.[28]

Perhaps the federal rules make more work for courts and attorneys because now all court filings have to be redacted for e-publication, and there may be some increase in the number of protective motions filed to seal all or part of some court records as parties and their attorneys become more aware of the risks posed by online filing.[29] The debate on this topic is, however, not yet over. Even if the state practice generally comes around to the federal practice—a development that seems most likely if the federal policies do not result in major problems--there are still important issues that the federal policies do not deal with adequately. The most important problem concerns figuring out how to protect parties not represented by counsel and non-parties like "jurors, witnesses, victims of crimes, and their family members."[30]

---

[27] Report of Judicial Conference, supra n. 19. Street addresses were first addressed in the special rule on criminal actions, "Guidance for Implementation of the Judicial Conference Policy on Privacy and Public Access to Electronic Criminal Case Files," adopted March 2004, at http://www.privacy.uscourts.gov/crimimpl.htm (accessed on Oct. 10, 2005)[hereinafter "Guidance for Criminal Files"], and should be included in the general policy.

[28] Social Security cases are excluded from online access because they tend to involve detailed medical records and other personal information. Report of Judicial Conference, supra n. 19. Neither bankruptcy nor criminal cases are excluded from the general policy, however. Criminal cases were initially excluded, but after satisfactory experimentation in a few districts, even criminal cases were added to the policy. Guidance for Criminal Files, supra n. 27.

[29] As one critic has groused, "it appears that a technological revolution that was supposed to be labor saving will require greater exertion than before from courts and attorneys." Winn, supra n. 21, at 327. But arguably too much private information was being left in court filings that lawyers should have been trying to protect. It may be true that online filing and access will make it more challenging to practice law. Sabin & Black, supra n. 24. At least since the invention of photocopiers, lawyers have had to deal with the phenomenon that as technology makes it possible for an attorney to do more, more is expected of the attorney.

[30] Winn, supra n. 21, at 324. It does not seem reasonable to expect the counsel in the case to do the job adequately. The federal courts have said that they will not do it, but it seems likely that a court clerk or other publicly funded position is going to have to be made available to look out for the privacy interests of all of the participants who cannot be expected to be represented by a lawyer.

3. Issues of E-Democracy: Computers' Potential to Reinvigorate Democracy through E-Rulemaking?

As indicated in the introduction, "informal or notice and comment rulemaking" is the procedure in American administrative law which is designed to promote a dialogue between government officials and the public and to ensure that the government really listens to the public before exercising authority delegated by Congress to promulgate rules of general applicability. The federal Administrative Procedure Act (APA) sets forth a deceptively simple procedure, consisting of a requirement that the agency (1) give notice in the Federal Register of the kind of regulation it intends to promulgate and (2) give the public a reasonable period of time (usually no less than 30 days) to submit comments, after which (3) when the agency promulgates the final version of its rule in the Federal Register, it must include a statement of reasons.[31]

A variety of pressures--including judicial review and standardized rulemaking formats developed by the Office of Management and Budget (OMB) and by the Federal Register, as well as special statutory requirements for specific subject matters and the practicalities of the notice and comment procedure--have molded the actual rulemaking process so that it is a bit more complicated.[32] In giving notice, agencies uniformly publish a text of the proposed rule, together with lengthy preambles discussing the information, data, and analyses upon which the agency relied in developing the rule. The courts have in effect expanded the requirement to give notice. The courts have also expanded the requirement to give reasons so that, when the agency publishes the final version of the rule, the preambles have become veritable legal briefs explaining and justifying the agency's choices in great detail. In effect, the courts have required the agencies to respond to all reasonable issues raised in the comments,[33] and it is this requirement that, in a rough way, forces the agencies actually to listen to the public. The courts enforce this requirement by invalidating rules if they do not find the agency's statement of reasons "reasonable." The standard of "reasoned rationality" will not be met where there are important issues or alternatives the agency has not examined in its statement of reasons. A good

---

[31] 5 U.S.C. § 553 (2000). The notice and comment procedure does not apply to certain types of rulemakings on the basis of subject matter (e.g., military, foreign affairs, agency organization or procedure), if good cause (such as emergency) is shown, or if the rules are only interpretative or general statements of policy not meant to have the force of law with respect to the public. State administrative procedure acts also adopt very similar versions of notice and comment rulemaking. See Arthur E. Bonfield, *State Administrative Rule Making* (1986).

[32] Cornelius M. Kerwin, *Rulemaking* 39-86 (3d ed. 2003).

[33] See, e.g., United States v. Nova Scotia Food Products Corp., 568 F.2d 240 (2d Cir. 1977) (requiring notice of studies, full statement of reasons, and agency response to all reasonable objections to course of action agency chose).

way to demonstrate lack of rationality is to show that the reasons given by the agency fail to respond to significant ideas or information provided by public comment.[34]

In the days before computers and the Internet, finding notice of a specific proposed rulemaking required combing through the voluminous tomes of the Federal Register, which was generally available only in certain public or law libraries.[35] Submitting a comment was a fairly informal process, but it required sending a letter. And if you wanted to review studies that the agency cited in the notice of its proposed rule or comments submitted in the course of the comment period and which the agency made available in a "rulemaking docket," in general you or your representative had to be in Washington because the rulemaking dockets were generally made available to the public only there at the agency's main office.[36] As a result, few individuals filed comments; notice and comment rulemaking was largely the province of organizations that had staff or representatives in Washington, D.C.

The computer and the Internet have changed the Washington-centered nature of notice and comment rulemaking by making it much more accessible to people outside the nation's capital. One important improvement has been e-publishing of the Federal Register since 1994.[37] Already in the middle to late 1990s--well before the E-Government Act of 2002--several federal agencies experimented with using the Internet to obtain public comment.[38] Thus the requirement in the E-Government Act of 2002 that "to the extent practicable," federal agencies accept comments by electronic means and put the contents of each rulemaking docket, including all comments, whether submitted in e-form or not, on its agency web site[39] simply codified a practice developing among federal agencies. The E-Government Act does, in any event, fill a gap in the APA, which does not by express terms require the agency to make the comments its receives during the comment process available to the public.

The Clinton and Bush Administrations have been solidly behind e-rulemaking initiatives. As a result, there is now a web portal which provides a consolidated, searchable entry point for

---

[34] See, e.g., Motor Vehicle Manufacturers Ass'n of the U.S., Inc. v. State Farm Mutual Automobile Ins. Co., 463 U.S. 29 (1983).

[35] Coglianese, supra n. 8, at 362.

[36] The rulemaking dockets, composed of large cabinets full of documents, were often quite bulky and awkward to review, and they were often archived on microfiche, also filed in cabinets. Id.

[37] At http://www.gpoaccess.gov/fr/index.html (last accessed on January 22, 2006). See generally Coglianese, supra n. 8, at 363.

[38] For short histories, see C. Kerwin, supra n. 32, at 193; Coglianese, supra n. 8, at 364-65; Beth Simone Noveck, "The Electronic Revolution in Rulemaking," 53 *Emory L.J.* 433, 472-73 (2004).

[39] Section 206 (c), (d) (codified at 44 U.S.C. § 3501 note (Supp. II 2002).

filing comments in any federal rulemaking proceeding,[40] and it is linked to the general "Firstgov" portal. Most federal agencies have initiated some aspects of e-rulemaking.[41] But, at least as of 2003, quite a few of these agencies were still not realizing the handling and storage savings that e-filing can achieve because they were still printing out all e-filed comments and storing them in hard copy.[42] The E-Government Act will require them eventually to make all comments available online, and when they do so, they will undoubtedly switch to electronic storage, as well, because of the large potential savings in storage costs.[43]

Despite these achievements, there are issues warranting further attention. Because e-rulemaking is a form of e-publication, it may raise the same kinds of privacy issues as were discussed in the previous section of the report on online access to court documents. In general, however, since rulemaking usually concerns rules of general applicability, rulemaking dockets should not be expected to be as full of personal information as court files. Nevertheless, a similar solution seems warranted: The "personal identifiers" excluded or partially omitted in court documents ought also to be excluded or partially omitted from comments filed in rulemaking, and instructions for e-filing of comments should caution against including unredacted sensitive personal or business information.[44]

Another issue concerns anonymous comments. Should commentors be permitted to file comments without identifying themselves? It seems quite reasonable to allow anonymous browsing of the e-dockets, including all comments already filed. Because the comments are not expected to be full of sensitive personal data, there is no need for controlled access such as the PACER system provides for federal court files. But anonymity is a more questionable policy with regard to filing comments. The sender's identity may be important for evaluating the comment, and anonymity could promote untruthful comment. In reaction to these concerns, it has been suggested that commentors be permitted or required to use an e-signature or some form of e-mail confirmation to verify their comment.[45] As a requirement, electronic verification may

---

[40] http://www.regulations.gov. See generally Coglianese, supra n. 8, at 355, 365.

[41] Kerwin concluded in 2003 that "[m]ost federal agencies have an electronic-rulemaking program in use or are in the process of implementing one." C. Kerwin, supra n. 32, at 196; but see Coglianese, supra n. 8, at 367 (taking less rosy view in 2004, but relying entirely on data published in 2002).

[42] Coglianese, supra n. 8, at 367.

[43] Noveck, supra n. 38, at 474.

[44] For protection of confidential business data in informal rulemaking, see Coglianese, supra n. 8, at 384; Heather E. Kilgore, Note, "Signed, Sealed, Protected: Solutions to Agency Handling of Confidential Business Information in Informal Rulemaking," 56 *Admin. L. Rev.* 519 (2004).

[45] Noveck, supra n. 38, at 481-82.

be overkill. A simple admonition on the site where comments are solicited to the effect that signed comments are preferred and that the agency will not be able to attribute much weight to anonymous comments whose validity assertedly comes from personal experience or involvement with the activities subject to the proposed regulations should suffice. At a minimum, however, it seems that commentors ought to be allowed to mask their e-mail addresses, if they wish.[46]

Other issues have to do with enhancements to the notice and comment process which ICT could make possible but which are not currently being achieved. The first is notice. Notice is the lynchpin of the whole process because without adequate notice, there can be no comments, and therefore none of the benefits of dialogue with the public that are expected to accrue to government from use of notice and comment rulemaking. The APA requires notice only in the Federal Register, but some commentators have advocated more proactive use of e-mail lists and listservs for delivering notice directly to recipients who have indicated an interest in specific subjects.[47] There is, of course, nothing to prevent agencies from voluntarily supplementing Federal Register notice with these means, and agencies that hope to enhance public acceptance of their rules through notice and comment rulemaking have an incentive to conduct the process in a way that actually succeeds in attracting public comment from a large number of parties. Without some additional requirement for more active efforts to reach the relevant public, notice and comment proceedings are likely to remain dominated by the business and other special interests that can afford Washington lawyers and lobbyists, but the computer has at least made it easier for members of the public to find proposed regulations on which they might wish to comment if they are willing and able to look.[48]

The trend is clearly toward putting the entire rulemaking docket online, as the commentators uniformly recommend. The trend is the product of the ways in which both notice and comment procedures have been expanded. The government is required to include in the notice of a proposed rule all the studies and other sources of data on which it intends to rely to justify the rule that it intends to promulgate. In addition, the E-Government Act requires agencies to put all comments online. In many rulemakings, by the time the agency has complied with these two rules, it might as well have put the whole docket online, and doing so obviates any issues about whether it has fully disclosed all important studies upon which it will base its final rule.

---

[46] Coglianese, supra n. 8, at 1440 n.74; Noveck, supra n. 38, at 488-89.

[47] Barbara H. Brandon & Robert D. Carlitz, "Online Rulemaking and Other Tools for Strengthening Our Civil Infrastructure," 54 *Admin. L. Rev.* 1421, 1455-59 (2002); Coglianese, supra n. 8, at 370; Noveck, supra n. 38, at 492.

[48] The federal consolidated web portal site for rulemaking brings together on one site links to all open comment proceedings, and the portal offers a search engine for searching those links by subject matter. The main page for the online version of the Federal Register, in which all comment proceedings are published, also contains a search engine. Finally, there are many other search engines available on the Web.

There is one issue that explicitly ties notice and comment phases together. The notice requirement has been construed to require an agency to begin again with a new notice of proposed rulemaking and comment period if, as a result of comments received in a first comment period, the agency decides to modify its proposed regulation in such a way that is substantially different from the proposal set forth in its original notice.[49] The line between changes that may be made and those that may not without initiating a new comment period is not clear and breeds much litigation. In an effort to preserve agency flexibility and yet encourage agencies to be open to learning from public comment, some courts have held that comments submitted during the comment process and made available to the public can provide notice that the rulemaking procedure has changed its focus and that the agency is now considering a somewhat different rule from the one it originally proposed.[50] Making all comments available online provides a much better basis for such a rule than did the old system of making comments available at an agency office, especially if the online comments can be searched by word or phrase or subject matter key words. But this line of cases is problematic because it in effect imposes on all interested parties a duty of continuous monitoring of all rulemakings in which they are interested. A better solution may be for the agency to provide a reasonable rebuttal period after the initial comment period. During the rebuttal period, comment would be allowed only in rebuttal to comment submitted during the initial period. If the agency is thinking about adopting an approach suggested by some of the comments that diverges in a significant way from the original proposal, it can so indicate at the start of the rebuttal period, in effect giving adequate notice of the important change. Indeed, there already appears to be a trend toward this solution.[51] However, the danger is that rebuttal periods may morph into successive extensions of the comment period with the result that concepts of agency "record" and "final agency action," both of which are important for effective judicial review, are unduly blurred.[52]

E-rulemaking procedures subject agencies to the challenge of "spam"–that is, the kind of messages, sometimes in standardized format, that interest groups try to mobilize their members to send in huge numbers in response to the call for comment. The worry is that this kind of spam may overwhelm the agency with masses of comments, overtaxing the agency's ability to analyze and respond coherently to the concerns. Agencies have responded by contracting out the job of

---

[49] The standard test is that a new notice and comment procedure must be used unless the final rule is a "logical outgrowth" of the draft rule set out in the original notice. Natural Resources Defense Council v. U.S. Environmental Protection Agency, 279 F.3d 1180 (9th Cir. 2002).

[50] United Steelworkers v. Schuylkill Metals Corp., 828 F.2d 314 (5th Cir. 1987); District of Columbia v. Train, 521 F.2d 971, 997 (D.C. Cir. 1975). But see Horsehead Resource Devel. Co. v. Browner, 16 F.3d 1246 (D.C. Cir. 1994) (notice of change must come from agency); National Black Media Coalition v. FCC, 791 F.2d 1016 (2d Cir. 1986)(same).

[51] Brandon & Carlitz, supra n. 47, at 1430-31.

[52] Id. at 1443.

organizing and analyzing the comments or by employing expensive computer programs to subject the comments to a type of data mining to discern the patterns into which the comments fall.[53] A number of creative ways have been proposed to use software to avoid spam and similar problems by forcing commentors to respond to each other in submitting comments[54] or to appoint a moderator to monitor the comments in a "chat room" setting to avoid incivilities and encourage commentors to speak to the concerns already expressed by other commentors.[55] Regulation, however, of the comment process may discourage bona fide comment, and to the extent that the regulation even appears to suppress expression, it may violate the First Amendment.[56] I therefore favor the "low tech" solutions of (1) encouraging agencies to articulate in the notice of rulemaking the specific issues on which they want comment and (2) educating the commenting public, through boilerplate inserted into the notice of rulemaking or included on a tutorial web site linked to the portal site for rulemakings, on the most effective ways of drafting comments.[57]

4. Government Abuse of E-Surveillance

Perhaps the most important of all e-government issues concerns government abuse of e-surveillance, in which ICT magnifies the surveillance powers of the government and its concomitant power to invade the privacy of citizens. Of course, the power of e-surveillance may be of great use in detecting, prosecuting, or even preventing crime or acts of terrorism. E-surveillance clearly has its legitimate uses. But these uses carry with them the potential for abuse because of the secrecy with which surveillance has to be carried out to be effective. Consequently, the challenge in this area is to find the proper balance between the interests of national security and crime control, on the one hand, and individual privacy, on the other. This is a hugely important issue, the outlines of which can only be sketched in this report.[58]

---

[53] Fred Emery & Andrew Emery, "A Modest Proposal: Improve E-Rulemaking by Improving Comments," 31 *Admin. & Reg. L. News* 8 (Fall 2005); Noveck, supra n. 38, at 441-43, 479-80.

[54] Id. at 480-92.

[55] Brandon & Carlitz, supra n. 47, at 1474.

[56] Id. at 1474-76.

[57] Accord Emery & Emery, supra n. 53.

[58] See, e.g., "The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA Patriot Act," 72 *Geo. Wash. L. Rev.* 1139 (2004)(introduction to symposium). See especially Peter P. Swire, "The System of Foreign Intelligence Surveillance Law," 72 *Geo. Wash. L. Rev.* 1306 (2004). The Electronic Privacy Information Center maintains an informative Internet site dedicated to this issue at http://www.epic.org (last visited on

The most fundamental legal framework for protecting the public from abusive surveillance of any form is, of course, the Fourth Amendment's protections against unreasonable searches and seizures. The Fourth Amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Absent exigent circumstances, the police may invade this sphere of individual privacy in general only by securing a judicial warrant, which the court will issue only upon a showing of "probable cause." For searches, this means that the police have to have reasonable and trustworthy information indicating that particular evidence of a specific crime will be found in a particular place.

The modern application of this law to e-surveillance starts with two cases in 1967, in which the Supreme Court held that the full Fourth Amendment protections apply to wiretaps on private telephone conversations.[59] Congress responded to these decisions by enacting Title III of the 1968 crime bill, and the "Title III" rules of that bill, which set forth concrete, rather strict standards for the use of wiretaps, still apply today.[60] Another major general source of rules concerning e-surveillance within the United States is the Electronic Communications Privacy Act of 1986 ("ECPA"),[61] which extended the protections of Title III to e-mail and other forms of electronic communications. Chief among the protections codified by Title III and the ECPA are the requirements for (a) judicial supervision (the warrant requirement, based on probable cause), (b) notice to the subject of the e-surveillance after the wiretap has expired, and (c) minimization of privacy intrusions that take the investigation beyond the purposes of the law enforcement investigation. However, electronic communications under the ECPA do not enjoy three important protections that do apply to wire and oral communications under Title III: (1) the requirement of approval from the highest levels of the Department of Justice before conducting surveillance, (2) a restriction to a list of serious offenses, and (3) an exclusionary rule to suppress evidence obtained in violation of the rules.[62]

September 20, 2005).

[59] Katz v. United States, 389 U.S. 347 (1967) (federal government); Berger v. New York, 388 U.S. 41 (1967) (state government).

[60] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified at 18 U.S.C. §§ 2510-2521 (2000)).

[61] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). See especially 18 U.S.C. § 2510 (12) (2000) (adding definition of "electronic communication" to bring e-mail within the coverage of Title III rules).

[62] Swire, supra n. 58, at 1312 text & n.30.

Other acts may affect government management, use, and retention of records of information gained from surveillance of any kind. The Privacy Act, 5 U.S.C. § 552a (2000), sets limits on the collection, disclosure, and use of personal information by agencies. The Federal Information Security Management Act of 2002, Title III of the E-Government Act (codified principally at 44 U.S.C. §§ 3541-49 (Supp. II 2002)), requires agencies to develop information

This legal regulation of e-surveillance, which is rooted in the recognition that there need to be some limits on executive branch surveillance in order to protect individual privacy, has long existed in tension with the perceived need to employ e-surveillance against the international enemies of the state, including foreign nations, their agents and spies, and international terrorist groups. Since Franklin Roosevelt, U.S. presidents have claimed the power to employ e-surveillance against international enemies without regard to Fourth Amendment considerations. Presidents assert their authority on the basis of their status as head of the executive branch and commander in chief of the military. That power would appear to extend unproblematically to spying against foreign nationals and states abroad, but the claim is more controversial with respect to snooping that takes place on U.S. soil. In 1972, the U.S. Supreme Court unanimously ruled that the presidential power to "preserve, protect, and defend the Constitution" could not substitute for a warrant issued by a neutral magistrate in the case of a domestic wiretap justified on national security grounds against a U.S. citizen who was being investigated in connection with the bombing of a CIA office in Michigan.[63] The Court explicitly reserved, however, the issues of foreign intelligence surveillance conducted on domestic soil and invited Congress to provide rules for this area. Congress was impelled to take up this invitation in the wake of the Watergate scandal, which brought to light the shocking degree to which the FBI, the CIA, the Army, the IRS, and other units of the federal government had abused the national security rationale to conduct an extensive program of spying on domestic groups, including civil rights groups and the political opposition to those then in power.[64] In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA).[65]

FISA leaves the Title III rules in place generally for domestic snooping, but instead of accepting presidential oversight as a substitute for a judicial warrant in the case of domestic e-surveillance against "foreign powers" or "agents of a foreign power,"[66] FISA requires that e-surveillance be authorized by a special court, the Foreign Intelligence Surveillance Court (FISC), which is now composed of eleven district court judges chosen by the Chief Justice of the United States.[67] Denials may be appealed to the Foreign Intelligence Surveillance Court of Review

---

security programs to protect all personal data from unauthorized access or disclosure. Section 208 of the E-Government Act (codified at 44 U.S.C. 3501 note (Supp. II 2002)) requires agencies to conduct privacy impact assessments which examine conformity of agency data handling with applicable laws regarding privacy, the risks and effects of data collection in electronic form, and the possible protections and alternative information handling processes to mitigate privacy risks.

[63] United States v. U.S. Dist. Court (Keith), 407 U.S. 297 (1972).

[64] See generally Swire, supra n. 58, at 1315-20.

[65] 50 U.S.C. §§ 1801-1811 (2000).

[66] 50 U.S. C. § 1801(a)-(b)(2000).

[67] 50 U.S.C. § 1803 (Supp. II 2002)(as amended).

(FISCR), and ultimately to the Supreme Court.[68] Judges of the FISC in effect are supposed to exercise the same kind of separation of powers restraint on the executive that the regular warrant requirement provides, but the standards for judicial approval of e-surveillance against foreign powers and their agents are quite different. The court "shall enter" an ex parte order authorizing the e-surveillance if, on application authorized by the Attorney General, there is "probable cause to believe that . . . the target . . . is a foreign power or agent of a foreign power."[69]

Unlike Title III, FISA does not require after-the-fact notification of targets. However, like Title III, FISA incorporates the exclusionary rule.[70] It also requires similar "minimization procedures," which in the case of the FISA, mean procedures to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information" concerning U.S. citizens and permanent residents, including a prohibition on retaining records of such information longer than 72 hours unless a court order is obtained from FISC or the Attorney General "determines that the information indicates a threat of death or serious bodily harm."[71] Like Title III, FISA makes provision for emergency procedures to allow surveillance to begin right away, subject to quick, subsequent approval by a judge.[72]

The statutory distinction between domestic surveillance conducted for normal criminal matters under the rules of Title III and foreign intelligence surveillance conducted under FISA was matched by the creation of a bureaucratic "wall" to keep the FBI out of foreign intelligence surveillance. The FBI remains responsible for Title III surveillance, but the National Security Agency (NSA), the biggest American intelligence agency with a network of satellites and listening devices around the world to gather overseas intelligence, takes the lead in conducting foreign intelligence surveillance both at home and abroad. Inevitably, some foreign intelligence surveillance uncovers evidence of crime, and while NSA was not supposed to be looking for that kind of evidence, there was a "gatekeeper" in the wall, the Justice Department's Office of Intelligence Policy and Review (OIPR), that generally supervised all contacts by the FBI and the Criminal Division of Justice with foreign intelligence and could permit the sharing, in a limited number of cases, of such information. The basic charge of OIPR, however, was to prevent the kind of massive abuse of the national security rationale for surveillance that had so badly tarnished the reputation of the FBI during the Watergate era.[73]

The statutory and bureaucratic structures set in place after Watergate to prevent a

---

[68] 50 U.S.C. § 1803 (b) (2000) (Chief Justice appoints three judges to the FISCR).

[69] 50 U.S.C. § 1805 (2000).

[70] 18 U.S.C. § 2515 (2000); 50 U.S.C. § 1806 (g) (2000).

[71] 50 U.S.C. § 1801 (h)(1), (4) (Supp. II 2002)(as amended).

[72] FISA: 50 U.S.C. § 1805(f) (Supp. II 2002)(currently 72 hours); Title III: 18 U.S.C. § 2518(7)(2002)(48 hours).

[73] Swire, supra n. 58, at 1327-28.

recurrence of massive governmental spying on U.S. citizens has been shaken by developments under the current President Bush. The Patriot Act[74] is part of the story. Based on the rationale that the 9/11 attack in 2001 showed that the executive branch needed to have much stronger intelligence tools, the Act loosened the restrictions in FISA and broadened it applications. Its major effect on e-surveillance was to water down the original requirement in FISA that the surveillance allowed under the Act have foreign intelligence as its "primary purpose." The Patriot Act specifies that "a significant purpose" is sufficient.[75] At the same time, the Bush Administration has deliberately set about dismantling the bureaucratic "wall." New guidelines issued by Attorney General Ashcroft in March, 2002, called for "the complete exchange of information and advice between intelligence and law enforcement officials."[76]

These changes led the FISC to issue its first published decision, in May of 2002, in which all seven of the judges on the FISC at that time issued detailed orders to maintain the "wall" between foreign intelligence and criminal investigations.[77] The court did so because of government admissions that in a series of over seventy-five FISA applications since 2000, it had made material misstatements and omissions "involving information sharing and unauthorized disseminations to criminal investigators and prosecutors."[78] On appeal, the FISCR disagreed that the law required a "wall" in light of the changes wrought by the Patriot Act. The court therefore reversed the FISC and upheld the greatly expanded sharing of information between foreign intelligence and law enforcement investigations.[79] Nevertheless, it is now a matter of public record that the government had been misleading the special court when the "wall" was more firmly in place.

More evidence of the Administration's disregard for congressional restrictions on its power concerned data mining. In the guidelines Attorney General Ashcroft issued in 2002 dismantling the "wall," he also authorized data mining of personal information about citizens and organizations from commercial databases without any limits on the sharing or retention of that data, thus raising the issue of compliance with the minimization requirements of Title III and

---

[74] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[75] 50 U.S.C. § 1804 (a)(7)(B) (Supp. II 2002)(as amended). For a discussion of the change, see Swire, supra n. 58, at 1330.

[76] Id. at 1335 (quoting "Ashcroft Guidelines").

[77] In re All Matters to Foreign Intelligence Surveillance (FISC Decision), 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002). See generally Swire, supra n. 58, at 1336-37.

[78] 218 F. Supp. 2d at 621.

[79] In re Sealed Case (FISCR Decision), 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev. 2002). For criticism of this decision, see Swire, supra n. 58, at 1337-39.

FISA.[80] In 2005, the General Accountability Office (GAO) issued a report on data mining by federal agencies.[81] The report concluded that "none of the agencies followed all the key privacy and security provisions . . . ."[82]

Finally, this whole issue was thrown in high relief when it was revealed for the first time on December 16, 2005, that President Bush had secretly sidestepped the Title III and FISA framework by issuing a classified executive order in 2002 authorizing the NSA, on grounds of national security, to monitor international telephone calls and e-mail messages of both Americans and foreigners inside the United States without seeking authorization from the FISC.[83] Though public details about this program are still sketchy, it appears that at President Bush's order, the NSA had obtained access to major electronic "switches" that function as gateways between U.S. communications networks and international networks. The NSA was using that access to conduct major programs of data mining on huge volumes of telephone and e-mail communications that certainly included large numbers of messages sent by or to U.S. persons on U.S. soil.[84]

The disclosure by the *New York Times* immediately raised a public outcry and played an important role in the subsequent defeat in the Senate of the attempt to reauthorize those parts of the Patriot Act that were due to expire at the end of 2005.[85] The Bush administration has asserted the usual argument about the president's powers as head of the executive branch and commander-in-chief, but it has also argued that the congressional authorization to use military force in response to the 9/11 attacks, which consists of one sentence authorizing the president "to

---

[80] Swire, supra n. 58, at 1335.

[81] General Accountability Office, Report to the Ranking Minority Member, Subcomm. on Oversight of Government Management, Comm. on Homeland Security and Gov't Affairs, U.S. Senate, "Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain," GAO-05-866 (August 2005).

[82] Id. at 28.

[83] James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, Dec. 16, 2005, at A1.

[84] Eric Lichtblau & James Risen, "Spy Agency Mined Vast Data Trove, Officials Report," *N.Y. Times*, Dec. 24, 2005, at A1. The data mining employed pattern analysis to determine, for telephone calls, who was calling whom, for how long, and at what time of day. Plans for similar data mining programs–"Total Information Awareness," which was promoted by the Pentagon for tracking terrorist suspects, and the "Capps" program of the Department of Homeland Security for screening airline passengers–had previously been cancelled after public outcries. Id.

[85] David E. Sanger, "In Speech, Bush Says He Ordered Domestic Spying," *N.Y. Times*, Dec. 18, 2005, at A1.

use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001," constituted a delegation of power to deviate from the requirements of FISA in investigating terrorists.[86] At this writing in January 2006, the full extent of the political fallout of the revelations is not yet clear, but the incident underscores the tendency of the national security rationale to lead the executive branch to undertake expansive surveillance which catches up citizens in activities in their own country. The most troublesome aspect of this story is not that the Bush administration asserts constitutional and statutory arguments not to follow the rules laid down by Congress for e-surveillance, but the suggestion that the Bush administration is not willing to give Congress clear notice of its refusal to abide by those rules.[87]

---

[86] David Johnston & Linda Greenhouse, "'01 Resolution Is Central to '05 Controversy," *N.Y. Times*, Dec. 20, 2005, at A20; Richard W. Stevenson & Adam Liptak, "Cheney Defends Eavesdropping Without Warrants," *N.Y. Times*, Dec. 21, 2005, at A22. The Democratic Senator who was majority leader of the Senate at the time the resolution was passed has publicly disputed this claim. Richard W. Stevenson, "Congress Never Authorized Spying Effort, Daschle Says," *N.Y. Times*, Dec. 24, 2005, at A12. The congressional resolution is the Authorization for Use of Military Force (AUMF), 115 Stat. 224 (2001). The government's argument draws strength from Hamdi v. Rumsfeld, 542 U.S. 507, 517-19 (2004) (O'Connor, J., for plurality, holding that AUMF is the express authorization required by statute for detention of U.S. citizens captured as enemy combatants). See also id. at 591 (Thomas, J., dissenting on grounds of broader, plenary powers on part of executive to detain enemy combatants). Nevertheless, four justices in Hamdi thought the AUMF did not constitute authorization for Hamdi's detention, and Hamdi's detention on a battlefield is arguably more obviously within the scope of the AUMF than warrantless interception of citizens' e-mail and telephone conversations in the U.S. in violation of an express statute.

The Bush administration also argues that the FISA procedures were too cumbersome to permit the NSA to investigate terrorists effectively although the FISC could provide review "within hours," Risen & Lichtblau, supra n. 83, the FISC had overwhelmingly approved requests for surveillance (denying only four requests through the end of 2003 despite a case load that had reached over 1700 requests in 2003 alone, Swire, supra n. 58, at 1324 text & n.118, 1329), and FISA itself makes express provision for surveillance to start immediately with judicial approval coming after the fact in case of emergency. See supra n. 72.

[87] The Bush administration has argued that it notified key congressional leaders of this program, but it seems clear at a minimum that the notifications were not in writing and that the formal congressional notification requirements of FISA were circumvented. See 50 U.S.C. §§ 1807-08 (2000). In addition, some of the congressmen who were allegedly briefed have disputed that they were told enough to understand what the government was doing or have said that they objected at the time. Douglas Jehl, "Spy Briefings Failed to Meet Legal Test, Lawmakers Say," *N.Y. Times*, Dec. 21, 2005, at A22.

5. Conclusions

The U.S. experience illustrates two important features of e-government. First, there is nothing especially new about the relevant legal issues. In fact, the importance and interest in the field lies precisely in thinking through how tried-and-true legal principles, like equal access to government, reasonable protection for privacy, notice and comment rulemaking, and prevention of the misuse of the government's surveillance power should apply to the new technology.

Second, despite the awesome power of ICT, it is unreasonable to expect technology to cure the ills of democracy, for example, by facilitating communication between government and the people. Nor is it reasonable to wring our hands and expect that ICT's effect on government will inevitably be insidious because of the huge increase in the potential for oppressive government surveillance that ICT makes possible. Technology is neither good nor bad. It is just a tool and it will do the good and bad things we make it do. It is a recurring theme of human history that technological advances are looked at as solutions to basic problems of human society, but they are not. They just change somewhat the nature of the challenges. Privacy can be protected in online documents, but it may take extra work. The deliberative form of democracy, whether done with or without computers, still requires actual exchange of ideas and a time-consuming and resource-consuming process of persuasion, if it is to work in a way that makes the participants feel as if they are truly part of the democratic process. E-surveillance does not have to threaten the privacy of all citizens if it is subject to reasonable controls, but especially with respect to processes like e-surveillance, which necessarily entails a large measure of secrecy, good laws are not enough. The legal controls have to include institutional checks and balances, and in the end, we cannot escape the necessity of having executive and legislative leaders whom we can trust to subject the secret processes to fair and vigilant oversight.