
Conning Congress

Privacy and the 1994 Communications Assistance for Law Enforcement Act

— ◆ —

CHARLOTTE TWIGHT

Despite a benign-sounding title, the 1994 federal Communications Assistance for Law Enforcement Act (CALEA)¹ is emblematic of today's ubiquitous government encroachment on the privacy of Americans. Although represented prior to passage as an innocuous measure intended only to maintain existing government authority, CALEA as statutory law immediately became a springboard in the government's quest for increased surveillance power. Indeed, in implementing CALEA through its Third Report and Order of August 31, 1999, the Federal Communications Commission (FCC) gave the Federal Bureau of Investigation (FBI) unprecedented power, first, to track the physical location of cellular phone users and, second, to obtain the content of private communications in a variety of circumstances without a probable-cause warrant. How and why CALEA achieved passage, how overreaching federal officials have used it, and how recent court rulings have affected CALEA's implementation reveal much about the multifaceted threat to privacy emerging in the United States as the new millennium begins.

Today many people resent the invasion of their privacy by commercial firms' use of new Internet software capabilities. As software "cookies" record our paths through the Internet and private firms seek to amass commercially valuable profiles of us,

Charlotte Twight is a professor of economics at Boise State University.

1. *Communications Assistance for Law Enforcement Act*, Public Law 103-414, 103rd Cong., 2d sess., H.R. 4922 (October 25, 1994), 108 Stat. 4279 ff., hereafter cited as CALEA.

The Independent Review, v.VI, n.2, Fall 2001, ISSN 1086-1653, Copyright © 2001, pp. 185-216.

increasingly detailed portraits of our personal lives are being compiled by strangers without our consent.

Yet when government intrudes on personal privacy, the stakes are even higher. Already the central government has mandated the creation of vast databases recording every check we write, every bank deposit we make, every new job we take, every employee we hire, our income, our educational experiences, even medical information given in confidence to physicians (Twight 1999). Federal databases linked to Social Security numbers continue to proliferate. Moreover, although the federal government continues to resist private encryption not transparent to government authorities, projects such as the National Security Agency's (NSA) Echelon and the FBI's Carnivore sweep ever more personal information into the hands of the government.²

The direct threat to individuals arising from the collection of such information is not the only issue. The very existence of widespread surveillance by persons with broad powers and uncertain motivation radically changes the ethos of a free people. Long ago the utilitarian philosopher Jeremy Bentham elucidated the consequences of such intrusions. Seeking a superior method for getting inmates to comply with prison rules, Bentham in 1787 designed an institutional architecture intended to strip inmates of all privacy and to make them continuously vulnerable to observation by a government official. Bentham called it the Panopticon. As Reg Whitaker describes it,

The idea of the Panopticon is simple. Imagine a prison constructed in circular form. On the outer perimeter of each level are the individual cells, each housing a single prisoner and each entirely isolated from the other to make it impossible for a prisoner to see or hear fellow prisoners. Each cell is visible to the gaze of the Inspector, who is housed in a central office from which he can scan all cells on the same level. Through a system of apertures and communication tubes . . . each prisoner is aware of the potential scrutiny of the Inspector at any time of the day or night. (1999, 32–33)

Because the prisoners “fear that they may be constantly watched, and fear punishment for transgressions, they internalize the rules,” so that actual punishment becomes largely unnecessary. Whitaker views this “discipline via surveillance” at the core of Panopticon as a “technique of power internalized, of power exercised without the direct presence of coercion” (33–34).

The broad implications of Bentham's metaphor for the wielding of government power today are apparent. Who can any longer doubt that surveillance has become “a crucial tool . . . the most crucial tool of all” for modern governments? (Whitaker

2. Echelon is a system through which the U.S. National Security Agency (NSA), in cooperation with other countries around the world, conducts surveillance of phone and electronic communications relayed via satellites, with the resulting data shared among participating nations. It has been described as an “enormous network of surveillance stations around the world [used] to scoop up electronic communications and signals of all kinds, often with the cooperation of countries like Britain, Canada, and Germany” (King 2000, A4). Carnivore, an FBI “Internet wiretapping system” described later in this article, has the capability to “give the government, at least theoretically, the ability to eavesdrop on all [Internet] customers’ digital communications, from e-mail to online banking and Web surfing” (King and Bridis 2000, A3).

1999, 41–42). Emphasizing the centrality of information acquisition to the “panoptic state,” Whitaker observes that

the routine gathering of statistics covering every aspect of society, culture, and economy is an activity intrinsic to the modern state, but one that barely existed in anything but the most rudimentary and fragmentary form in earlier eras. . . . The object is always to construct an understanding of the social world in order to change or control it. . . . Statistical surveillance is never knowledge for its own sake. . . . *It is always knowledge for the sake of control, and it has most often been in the service of the state*—although . . . perhaps less so in the present and near future than in the immediate past. (1999, 41–42, my emphasis)

Although Whitaker’s perspective on the future of government surveillance seems overly sanguine, the Panopticon metaphor suggests the dynamics and likely results of the increasing government surveillance now authorized by U.S. statutory law.

Through statutes such as CALEA, the central government is continuing to expand its collection of information about law-abiding American citizens. It is a quest driven in no small part by the government’s continuing success in using political transaction-cost manipulation to achieve its ends.

An Analytical Framework

The passage of CALEA provides some of the most vivid examples of constitutional-level political transaction-cost manipulation that I have seen in the twenty years since I developed a theory of such manipulation and began studying its applicability to U.S. government actions (Twight 1983, 1988, 1994). Because that theory provides a backdrop for the analysis that follows, a brief summary is necessary.

By analogy to economic transaction costs in markets, I define constitutional-level political transaction costs as the costs to individuals of negotiating and enforcing collective political agreements that influence the scope of government authority—in other words, the position of the border between what is handled by government and what is regarded as outside its purview. Constitutional-level political transaction costs thus encompass both costs of perceiving relevant political information (information costs) and costs of acting on those perceptions (which I term *agreement and enforcement costs*). In what follows, I use the shorter phrase *political transaction costs* to denote these costs.

Animating the theory is the idea that government officials as individuals often have both the incentive and the capacity to manipulate the political transaction costs of private citizens (and of each other) so as to achieve more of what officeholders want with less resistance from the public. Officeholders often augment transaction costs, artificially increasing the costs to private citizens or other officeholders of resisting the authority-changing measures the acting officeholders favor. The motive for this

behavior is readily understandable: if government officials can increase the marginal costs to voters or key decision makers of understanding or taking political action to oppose a measure that changes the scope of government authority, they can reduce political resistance to the measure. For example, officeholders may mitigate resistance by misrepresenting the contents of a bill, by using incremental strategies, by tying controversial measures to popular ones, by using tax strategies that obscure a program's cost, and so forth.

Artificially increased political transaction costs in effect drive a wedge between voter preferences and political action responsive to those preferences. The theory identifies various determinants influencing an individual officeholder's decision to favor a measure that increases transaction costs: executive and party support for the measure; impact on officeholder job security and perquisites; third-party payoffs; officeholder ideology; the measure's complexity and perceived importance to constituents; publicity, time, and the existence of an appealing rationale for the measure (Twight 1983, 1988).

Once in place, institutional changes that increase the public's transaction costs of resisting expanded federal authority set in motion a process of accommodative ideological change that further lessens the likelihood of restoring the status quo ante (Higgs 1985, 1987; Twight 1992). Twentieth-century U.S. politics has supplied countless examples of government manipulation of constitutional-level political transaction costs buttressing institutional changes that are later followed by concordant ideological change. The legislative histories of Social Security, income tax withholding, public education, Medicare, and other government-expanding measures have proved consistent with this interpretation (Twight 1993, 1995, 1996, 1997).

The astonishing legislative history of CALEA shows that its passage, like these earlier institutional changes, did not reflect the preferences of the American people at the time. Consistent with transaction-cost manipulation theory, key federal officials lied and used a panoply of related strategies to con Congress and the American people into supporting CALEA. The result has been to empower further the FBI and other law enforcement authorities to reach into domains of personal privacy formerly protected by the Fourth Amendment to the U.S. Constitution.

How did it happen?

Tricks of the Trade: The Passage of CALEA

Beginning in 1991, the FBI began the quest that ultimately resulted in the passage of CALEA. From the outset, the FBI argued that its existing surveillance authority was being thwarted by new technological developments and that only additional legislation could remedy the situation. FBI director Louis Freeh spearheaded the agency's efforts to secure such legislation. For Director Freeh, the 1994 CALEA hearings were the culmination of years of discussions among law enforcement authorities, the telecommunications industry, and privacy groups.

Political transaction-cost manipulation was evident at each stage of the legislative process. Just one set of hearings was held, joint hearings on March 18 and August 11, 1994, before the relevant subcommittees of the House and Senate Judiciary Committees.³ At the March 18 hearing, the CALEA proposal existed only as a closely held draft circulated by the FBI among committee members. With the initial proposal thus shielded from public view, participants developed the modified bill that garnered a favorable report in August from the House Judiciary Committee (U.S. House 1994); the Senate committee issued no report.

On the floor of the House, Representative Jack Brooks (D.-Tex.), chairman of the House Judiciary Committee, secured suspension of the rules in order to pass CALEA. There was no questioning of committee members, no discussion of potential dangers posed by the bill. After brief speeches by Representative Brooks and by the ranking Republican member, Representative Henry Hyde (R.-Ill.), who praised the bill, it was passed on a voice vote without discussion (*Congressional Record*, House, October 4–5, 1994, 10773–83, 10917). The Senate passed the bill by voice vote with no speeches or discussion whatsoever (*Congressional Record*, Senate, October 7, 1994, 14660). Neither the House nor the Senate recorded the names of the members present or how they voted.

The statements of Representative Brooks and Representative Hyde on the House floor significantly raised the transaction costs to other members of the House of Representatives, and hence to the public, of discovering whether the CALEA bill contained anything troublesome. Representative Brooks stated, “It is essential that we support the very real law enforcement objectives at the heart of the legislation without minimizing industry’s legitimate concerns regarding both privacy protections and costs resulting from installing new technology,” adding that “the bill laudably protects public safety by requiring telecommunications carriers to be able to fulfill court authorized requests for interceptions without overreaching into protected privacy areas. . . . [T]his bill does not expand law enforcement authority to conduct these interceptions. In fact, the bill includes several provisions to improve the privacy and security in the telecommunications network” (*Congressional Record*, House, October 4, 1994, 10779). Of the six representatives who commented on H.R. 4922, including Representative Brooks, Representative Hyde, and Representative Don Edwards (D.-Calif.), who was the chairman of the Judiciary Subcommittee on Civil and Constitutional Rights, not one raised any question or concern about the bill. Instead, they simply repeated misleading FBI statements made in the 1994 joint hearings. They had accepted the FBI’s story hook, line, and sinker.

3. U.S. House and Senate 1995. These hearings, held in 1994 but published in 1995, are hereafter referred to as the 1994 joint hearings in the text, but are parenthetically cited as U.S. House and Senate 1995 for reference purposes.

The FBI's Story

The FBI contended that, because of developments in telecommunications technology, law enforcement officials were gradually losing their ability to execute lawfully authorized wiretaps. The FBI claimed that law enforcement officials frequently encountered situations in which they had court authorization to wiretap, but owing to the inability of old-fashioned wiretaps to obtain information in an era of wireless phones, electronic communications, call forwarding, and the like—combined with the failure of telecommunications companies to design wiretap-facilitating capabilities into their new systems—they could no longer acquire information previously accessible to law enforcement. That incapacity, they alleged, threatened their ability to identify and prosecute drug kingpins, terrorists, and other malefactors.

The FBI presented CALEA as a remedy. The central idea of the bill was to require telecommunications carriers (“common carriers” including traditional telephone/wire carriers as well as electronic communications carriers) to install and maintain equipment that would enable authorized law enforcement officials to receive, in real time or with only brief delay, information about a targeted individual’s communications. The bill allowed the federal government to specify assistance capability and capacity requirements with which the companies must comply and authorized government compensation to private firms for compliance costs of as much as \$500 million annually during the first four years after its passage.

The Statutory Backdrop

When CALEA was proposed, there were two main categories of court-authorized wiretaps: *intercepts* and *pen registers* (or *trap-and-trace devices*), plus a third set of rules pertaining to stored electronic mail and “transactional records.”

The law was clear with respect to intercepts versus pen registers and trap-trace devices. Intercepts by definition sought the *content* of a targeted individual’s communications; the Fourth Amendment therefore allowed intercepts only when authorized by a court-issued warrant based on probable cause. Pen registers and trap-trace devices, on the other hand, sought only the *telephone numbers* of calls made from and to the targeted individual’s phone.⁴ Because law enforcement officials with pen register or trap-trace authority would not obtain the content of the target’s communications, a much lower standard for court authorization existed. In fact, the relevant statute specified that a court was *required* to issue an ex parte order authorizing use of a pen register or trap-trace device “if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation” (Public Law 99-508, §301).

4. See Center for Democracy and Technology 2000c, discussion of “Statutory Background—Electronic Surveillance” within the brief’s “Joint Statement of Facts.”

This basic distinction between intercepts and pen registers/trap-trace devices was made statutory law by the 1986 Electronic Communications Privacy Act (ECPA),⁵ which modified Title III of the 1968 Omnibus Crime Control and Safe Streets Act.⁶ Title III established the probable-cause standard for intercepts (18 U.S.C. §2518); eighteen years later, the ECPA codified the lower standard for court authorization of pen registers and trap-trace devices (18 U.S.C. §3123). In addition, the ECPA created a third set of rules for “stored wire and electronic communications and transactional records access” that entailed relatively low standards for government access to a wide range of electronic mail stored in electronic communications systems as well as to so-called transactional records regarding subscribers’ accounts (18 U.S.C. §2703).

In this statutory context, the 1994 CALEA provisions modified the 1986 ECPA and the 1968 Omnibus Crime Control Act specifically to require carriers to provide CALEA-mandated surveillance assistance to law enforcement authorities.

Before CALEA’s Passage: Misleading Congress

In the 1994 joint hearings, FBI director Louis Freeh repeatedly misled Congress about the FBI’s interpretation of CALEA and intentions regarding its use. The truth became apparent as soon as the FCC began to formulate regulations implementing CALEA. Once CALEA’s provisions had been established as statutory law, the FBI quickly reversed itself, claiming power and authority under CALEA that Freeh had explicitly disclaimed and repudiated in the joint hearings. The key misrepresentations fell into three categories:

No New Authority

In his congressional testimony, Director Freeh strongly asserted that the CALEA measure conferred no new authority on law enforcement officials, insisting that it merely maintained the status quo. He stated:

- We are not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago. . . . I believe that we are asking for the balance to be maintained instead of being changed. (U.S. House and Senate 1995, 6)
- The purpose of this legislation, quite simply, is to maintain technological capabilities commensurate with existing statutory authority—that is, to prevent advanced telecommunications technology from repealing, de facto, statutory authority now

5. *Electronic Communications Privacy Act of 1986*, Public Law 99-508, 99th Cong., 2nd sess. (October 21, 1986), 100 Stat. 1848 ff., hereafter cited as ECPA.

6. *Omnibus Crime Control and Safe Streets Act of 1968*, Public Law 90-351, 99th Cong., 2nd sess. (June 19, 1968), 82 Stat. 197 ff.

existing and conferred to us by the Congress. The proposed legislation explicitly states that it does not alter the Government's authority to conduct court-authorized electronic surveillance and use pen registers or trap and trace devices. (U.S. House and Senate 1995, 7)

- [W]e want this committee to set and mandate requirements in future equipment which is currently being engineered and deployed to give us the continued access, the access which the Congress gave us in 1968. (U.S. House and Senate 1995, 13)
- There appears to be general agreement within the government and industry that this would not extend law enforcement's electronic surveillance authority. (U.S. House and Senate 1995, 23)
- The proposed legislation explicitly states that the legislation does not enlarge or reduce the government's authority to lawfully intercept the content of communications or install or use pen register or trap and trace devices pursuant to court authorization. (U.S. House and Senate 1995, 27)
- [T]he proposed legislation does not seek to expand the current laws authorizing the interception of wire or electronic communications. To the contrary, this proposal simply seeks to maintain law enforcement's ability to conduct the types of surveillances currently authorized. (U.S. House and Senate 1995, 29, under the subheading "No Change in Legal Authority")
- [T]he government's legislative proposal simply seeks to maintain the legal/technical status quo. (U.S. House and Senate 1995, 40)

Committee members included the same message in the House report, stating that the "FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past" (U.S. House 1994, 22).

Although committee members bought the FBI's line and later repeated it on the floor of the House of Representatives, Roy Neel (president of the U.S. Telephone Association) was not convinced. In his written testimony, he questioned the FBI's claim, stating that "this proposal does, in fact, dramatically broaden the ability of law enforcement to gain access to a much wider range of information about customers." Neel added: "In describing its proposal, the FBI strongly asserts that it is not seeking expanded authority. We must, with all due respect, disagree. We believe that this is a level of surveillance capability unprecedented in terms of immediacy, breadth of application or capability for routine surveillance of individual citizens" (U.S. House and Senate 1995, 53, 59).

Consistent with this assessment, the FBI's actions after CALEA's passage revealed that Freeh's statements to Congress beforehand were not only wrong but seemingly disingenuous.

No Location Information

Another key issue during the hearings was fear that the FBI would use CALEA to obtain information about the physical location of cellular phone users. Evidence indicated that some telecommunications carriers had been providing cell phone location information to the FBI on mere pen register authority, and Congress wanted to block such disclosure. Concern was heightened by legislators' knowledge that pen register procedure, though it involved a "court order," allowed judges no legal discretion to deny requests made in the proper format and claiming relevance to an ongoing criminal investigation.

Underlying that congressional fear was the language used in CALEA to refer to the incoming and outgoing telephone numbers traditionally sought by pen registers and trap-trace devices. Like prior statutes, CALEA was structured to distinguish interception of call contents from pen register/trap-trace access to dialing information. Echoing the familiar dichotomy, it required telecommunications carriers to have the capability of:

1. expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, *to intercept*, to the exclusion of any other communications, all wire and electronic communications carried by the carrier . . . [and]
2. expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, *to access call-identifying information* that is reasonably available to the carrier. (CALEA, Public Law 103-414, §103[a], *my emphasis*)

Dialing information thus was covered in CALEA by the phrase *call-identifying information*," originally termed *call-setup information* in the draft bill. CALEA defined call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier" (CALEA, Public Law 103-414, §102[2]).

This language overlaid long-standing (and unchanged) statutory definitions of pen registers and trap-trace devices as instruments identifying "numbers dialed" from and to a suspect's phone.⁷ The new reference to "signaling information" was widely understood as intended to encompass call-forwarding features available with current technology. Nonetheless, committee members and others worried that the FBI was using slippery language to enable law enforcement authorities to gain access, under

7. The 1986 ECPA defined a pen register as "a device which records or decodes electronic or other impulses which identify the *numbers dialed or otherwise transmitted* on the telephone line to which such device is attached" and a trap-and-trace device as "a device which captures the incoming electronic or other impulses which identify the *originating number* of an instrument or device from which a wire or electronic communication was transmitted" (ECPA, Public Law 99-508, §301[a]; 18 U.S.C. §3127).

the rubric of call-identifying information or call-setup information, to location information pertaining to users of mobile/cellular phones.

Freeh repeatedly denied that the CALEA language would permit law enforcement access to such location information. He stated:

The term “*call setup information*” is essentially the dialing information associated with any communication which identifies the origin and destination of a wire or electronic communication obtained through the use of a pen register or trap and trace device pursuant to court order. *It does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service.* There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called “tracking” information. (U.S. House and Senate 1995, 29, my emphasis)

Freeh repeatedly equated call-setup information with dialing information, stating that common carriers “are required to ensure that the content of communications and call setup information (dialing information) can be intercepted, acquired, and provided to the law enforcement agency” (U.S. House and Senate 1995, 27, parenthetical words in original). He reassured the committees that “[u]nder the proposed legislation, law enforcement would acquire this dialing information *as it does today—no more no less*” (U.S. House and Senate 1995, 40, emphasis in original).

To counter congressional concern about cell phone location information, Freeh emphasized that call-setup information “relates to dialing type information—information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address” (U.S. House and Senate 1995, 33). He explicitly denied the validity of the privacy issues that had been raised regarding the gathering of location data: “Several privacy-based spokespersons have criticized the wording of the definition regarding this long-standing requirement, alleging that the government is seeking a new, pervasive, automated ‘tracking’ capability. Such allegations are completely wrong” (U.S. House and Senate 1995, 33). Although Freeh acknowledged that “[s]ome cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes,” he said that “this information is not the specific type of information obtained from ‘true’ tracking devices” and that “[e]ven when such generalized location information, or any other type of ‘transactional’ information, is obtained from communications service providers, court orders or subpoenas are required and are obtained” (U.S. House and Senate 1995, 33). Finally, Freeh made what appeared to be a bold conciliatory gesture, stating:

In order to make clear that the acquisition of such [location] information is not being sought through the use of a pen register or trap and trace device, *and is not included within the term “call setup information,”* we are

prepared to add a concluding phrase to this definition to explicitly clarify the point: “ * * * , except that *such [call-setup] information shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number’s area code or exchange* . (U.S. House and Senate 1995, 33, my emphasis)

As actually written into CALEA, this reassurance appears immediately after the capability requirements in section 103, paragraphs (1) and (2), quoted earlier, which mandate carrier equipment and services facilitating government interceptions and access to call-identifying information. It reads as follows: “except that, with regard to information acquired solely pursuant to the authority of pen registers and trap and trace devices . . . , such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)” (CALEA, Public Law 103-414, §103[a][2][B]).⁸ As we will see, the slight change in wording between Freeh’s promised provision and the actual statutory phraseology became the opening wedge allowing the FBI to claim, contrary to Freeh’s prior representations, that call-identifying information was meant to *include* location information in all cases except when it was sought via pen register/trap-trace authority, thus creating a pretext for forcing carriers to design their equipment and facilities to make location information available to law enforcement officials.

As the hearings drew to a close, many of the participants reiterated the theme that location information had been explicitly excluded from call-identifying information, making it inaccessible to law enforcement officials under CALEA. However, although others did not notice or call attention to it at the time, Freeh became more circumspect, seeming to support the common understanding while omitting any reference to call-identifying information. In support of the revised CALEA draft, he stated: “Location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders is now excluded, another important improvement” (U.S. House and Senate 1995, 114). And again: “the assistance requirements in these bills exempt the provision of any location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders” (U.S. House and Senate 1995, 116).

Others expressed in broader terms what they thought the revised CALEA draft had accomplished. Privacy advocate Jerry Berman, director of policy for the Electronic Frontier Foundation (EFF), stated that “one of the requirements that the committee has imposed is a *requirement not to design ongoing location features into the electronic technology for communications*,” adding that “[w]e do not want to turn our cellular and radio-based communications systems into nationwide tracking systems

8. In addition, CALEA requires government agencies using pen register authority to employ technology to limit the electronic and other impulses collected “to the dialing and signaling information utilized in call processing,” thereby excluding location information (CALEA, Public Law 103-414, §207[b], amending 18 U.S.C. §3121).

for persons who may be of interest to law enforcement and who are not subject to a warrant” (U.S. House and Senate 1995, 158, my emphasis).

The House report on the bill reiterated this understanding, stating that “the bill requires telecommunications carriers to ensure their systems have the capability to . . . [i]solate expeditiously information identifying the originating and destination numbers of targeted communications, *but not the physical location of targets*” (U.S. House 1994, 16, my emphasis). Under the subheading “The Legislation Addresses Privacy Concerns,” the House report explained that CALEA “[e]xpressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information,” remedying a situation in which “[c]urrently, in some cellular systems, transactional data that could be obtained by a pen register may include location information” (U.S. House 1994, 17). The report emphasized that call-identifying information was to include only “numbers dialed” (U.S. House 1994, 21).

That understanding was turned on its head soon after CALEA was passed.

Improving Privacy Protection

Throughout the joint hearings, Freeh portrayed CALEA as an unmitigated improvement in privacy protection: at no time did he mention the unraveling of privacy under the auspices of CALEA for which the FBI would argue soon thereafter.

Without doubt, a few provisions in CALEA did enhance personal privacy. These included a provision to add the radio portion of cordless telephone communication (between a handset and the base unit) to the definition of wire communications whose interception is governed by the Title III rules (CALEA, Public Law 103-414, §202); and a provision strengthening the protections accorded stored wire and electronic communications and transactional records, such as telephone billing information and certain stored e-mail (CALEA, Public Law 103-414, §207). Unfortunately, these beneficial changes served to cover up more profound threats to privacy embedded in CALEA.

In the hearings, Freeh never wavered from representing CALEA as a pro-privacy measure, repeating his refrain that CALEA would “improve communications privacy.” He stated:

- Also included in the legislation are amendments to the Federal criminal electronic surveillance laws (“Title III”) which improve communications privacy protection: privacy protection for handheld “cordless” telephones on a par with wireline and cellular telephones, clarification of privacy protection for electronic communications transmitted by radio, and privacy protection for communications transmitted using security-enhancing modulation techniques. (U.S. House and Senate 1995, 15)
- An additional purpose of the act is to improve communications privacy protection for users of cordless telephones, certain radio-based data communications and net-

works, communications transmitted using certain privacy-enhancing modulation techniques, and to clarify the lawfulness of quality control and service provision monitoring of electronic communications on a par with wire communications. (U.S. House and Senate 1995, 27)

- The legislation includes several provisions that are intended to improve communications privacy. These include the conferral of full privacy protection for cordless telephones, including those transmissions occurring in the radio link between the telephone handset and base station. (U.S. House and Senate 1995, 29)
- With respect to the security systems involved in these provisions . . . they do, in fact, enhance privacy and security by requiring, for instance, that switch-based intercept efforts be activated only with the affirmative intervention of a carrier employee. . . . Enhanced privacy protection regarding governmental access to stored transactional records is included, which again, by my own admission, is a vast improvement from the initial draft which the Government proposed. There is the requirement to utilize pen register technology when reasonably available that restricts the recording of electronic impulses to the dialing or signaling information used in call processing. Location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders is now excluded, another important improvement. (U.S. House and Senate 1995, 113–14)

He called the act a “remarkable compromise and achievement” in “balancing all the technology and privacy concerns which are so precious to all of us” while “preserving” electronic surveillance “as it has existed since 1968” (U.S. House and Senate 1995, 113).

Even the EFF’s Jerry Berman gave his approval, offering commendations to the committee chairmen “for having really done an incredible job in transforming a bill which we saw as a potential privacy nightmare into a bill which is carefully crafted to protect privacy” (U.S. House and Senate 1995, 157). The House report expressed the same assessment, stating without qualification that “[t]he legislation also expands privacy and security protection for telephone and computer communications” based on provisions involving cordless phones, transactional data, and restrictions on the use of pen register devices for tracking purposes (U.S. House 1994, 10).

Privacy threats that remained in CALEA were not mentioned in any statement to Congress before the bill was passed.

After CALEA’s Passage: Removing the Veil

The big question was how the new law would be implemented. In what was called a “safe harbor” provision, CALEA deemed telecommunications carriers to be in compliance if they complied with “publicly available technical requirements or standards adopted by an industry association or standard-setting organization” (CALEA, Public

Law 103-414, §107). If those entities did not establish such standards, or if anyone were dissatisfied with the standards put forth, then any of the interested parties could ask the FCC to issue standards. After more than two years of negotiation between the interested parties, the Telecommunications Industry Association (TIA) did develop an interim standard for compliance, but dissatisfied parties on both sides requested that the FCC review the interim standard (also known as J-STD-025 or the J-Standard) and independently determine standards for CALEA compliance. The FCC's deliberations over final rules for CALEA compliance thus provided a regulatory forum in which fundamental questions regarding proper interpretation of the statute were aired.

To the astonishment of industry and privacy interests who thought they had worked out legislative compromises with the FBI, the FBI's arguments before the FCC were utterly inconsistent with its prior commitments to Congress. It quickly cast aside its "no new authority," "no location information," and "improving privacy protection" themes. Whereas the FBI had previously assured Congress that call-identifying information did not include information about the location of cell phone users, it now argued before the FCC that call-identifying information did include such location information. Whereas the FBI had assured Congress that CALEA was a privacy-enhancing measure, it now argued before the FCC that telecommunications carriers should be forced to turn over to the FBI "packet-mode communications" that included the *content* of an individual's communications along with call-identifying information, even if law enforcement officials were authorized to receive only call-identifying information. Finally, whereas the FBI had assured Congress that CALEA created no new government surveillance authority, it now requested a number of new authorities as part of what it called a "punch list" of additional requirements that it asked the FCC to force on telecommunications carriers as part of the CALEA mandate.

In its Third Report and Order,⁹ adopted August 26 and released August 31, 1999, the FCC established final CALEA rules, setting forth the arguments made by the interested parties as well as the FCC's discussion of each issue. The FCC's decisions embraced the FBI's position on most of the contested issues. Consider the FBI's views presented to the FCC.

Demanding Location Information

Reversing their earlier testimony to Congress, FBI officials argued before the FCC that location information pertaining to cellular phone use *is* call-identifying information. As the FCC stated,

DoJ [Department of Justice]/FBI argue that location information is call-identifying. . . . DoJ/FBI state that they agree that the interim standard requires only that cell site location at the beginning and end of a call be pro-

9. Federal Communications Commission 1999. A summary of the FCC's Third Report and Order was published in the *Federal Register*, vol. 64, no. 185, 51710 ff., September 24, 1999.

vided, and maintain that CALEA embodies a compromise regarding location information: When a LEA [law enforcement agency] is proceeding “solely pursuant to the authority for pen registers and trap and trace devices,” carriers are not to treat location information as call-identifying information, but when a LEA has been duly authorized to acquire location information under other electronic surveillance statutes, location information remains part of call-identifying information. (FCC 1999, ¶42)

The FCC sided with the FBI, finding that “a subject’s cell site location at the beginning and end of a call is call-identifying information under CALEA.” A remarkable statement followed:

With respect to CALEA’s express statement that “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number),” we agree with DoJ/FBI that *this provision does not exclude location information from the category of “call-identifying information,”* but simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices. (FCC 1999, ¶44, my emphasis)

Of course, as Freeh himself had testified, call-identifying information by definition means information acquired through pen registers and trap-trace devices. Nonetheless, the FCC’s ruling was unequivocal: “We mandate a location capability that will identify cell site location at the beginning and termination of a call” (FCC 1999, ¶46).

In its judicial appeal of the FCC’s ruling, the Center for Democracy and Technology (CDT) set forth many reasons why this interpretation was incorrect in light of CALEA’s legislative history. The CDT pointed out, for example, that CALEA was structured to maintain the existing scope of surveillance authority, which established rules for government access to only two types of information about private communications: content and dialing information. Noting that the physical location of cell phone users did not fall into either category, the CDT argued that CALEA did not authorize a government mandate for the availability of this new category of information (CDT 2000a, §§IA–IC; 2000b, §V, 2000c, §II).

From a political transaction-cost manipulation perspective, however, the most arresting aspect of this outcome is that the FBI tricked Congress, enormously increasing the cost to legislators and the public of maintaining the pre-CALEA scope of surveillance authority as Congress intended to do and thought it was doing through CALEA. One need only juxtapose the FBI’s earlier statements to Congress with those made to the FCC. Even if one parses Freeh’s statements in a manner most favorable to the FBI’s subsequent claims, the best that can be said is that he deliber-

ately used language in ways he knew would be understood by Congress to exclude the very authority he and his agency later claimed. Moreover, as we have seen, Freeh repeatedly gave legislators broad, unqualified assurance that “[t]he term ‘call setup information’ . . . does not include any information which might disclose the general location of a mobile facility or service” (U.S. House and Senate 1995, 29). Unfortunately, committee members believed what the FBI told them, and then on the basis of that false understanding they persuaded Congress to adopt CALEA.

Degrading Privacy Protection

Contravening their earlier claim that CALEA improved privacy protection, FBI officials subsequently supported interpretations of CALEA that would seriously degrade privacy. One important example involved *packet-mode communication*. In contrast to traditional circuit-mode technology, packet-mode technology includes both call-content information and call-identifying information in a single stream or “packet.” The interim standard (J-STD-025) allowed packet-mode communication to be turned over to law enforcement agencies authorized to obtain either the content of a communication or its call-identifying information. This requirement threatened privacy because law enforcement officials authorized to obtain only call-identifying information, using pen register/trap-trace authority, could also obtain within the packet the content of the communication, for which they possessed no probable-cause warrant.

Privacy groups—including the CDT, the EFF, the Electronic Privacy Information Center (EPIC), and the American Civil Liberties Union (ACLU)—argued against this interpretation of CALEA. As the FCC explained, “CDT states that carriers using packet technologies have an obligation under CALEA to protect privacy by distinguishing between call content and call-identifying information, so that a LEA does not intercept the former when it has only the narrower authority for the latter” (FCC 1999, ¶50). The EFF, EPIC, and the ACLU stated that “the interim standard’s requirement to deliver the entire packet data stream associated with a given communication violates the privacy provisions” of CALEA (FCC 1999, ¶49).

The FBI, however, embraced the interim standard’s treatment of packet-mode communications. As the FCC reported, “DoJ/FBI argue that the interim standard’s treatment of packet-mode communications in pen register cases does not conflict with anything in CALEA” (FCC 1999, ¶54). The FCC acknowledged, however, that the interim standard’s treatment of packet-mode communications “raises significant technical and privacy concerns”: “Under this standard, LEAs would be provided with both call-identifying information and call content even in cases where a LEA is authorized only to receive call-identifying information (i.e., under a pen register)” (FCC 1999, ¶55). With the stunning statement that “[w]e believe that further efforts can be made to find ways to better protect privacy by providing law enforcement only with the information to which it is lawfully entitled,” the FCC concluded that, in the meantime, “packet-mode communications, including call identifying information

and call content, may be delivered to law enforcement under the interim standard.” Conceding that this “solution . . . is not perfect because a LEA may receive both call identifying information and call content under a pen register,” it nonetheless mandated that such packet-mode communications “be delivered to LEAs under that standard no later than September 30, 2001” (FCC 1999, ¶155). The FCC said this stipulation would be only a “temporary remedy” and promised to seek a more satisfactory outcome in the future.

Expanding Government Surveillance Authority

In addition to the expansion of surveillance authority evident in the foregoing interpretations of CALEA, the FBI sought other new powers enumerated in what it called a punch list. This list utterly belied the FBI’s earlier statements to Congress that CALEA established no new surveillance authority—that it merely maintained the status quo. The nine powers on the FBI’s punch list were: (1) content of subject-initiated conference calls; (2) party hold, join, drop on conference calls; (3) subject-initiated dialing and signaling information; (4) in-band and out-of-band signaling; (5) timing information; (6) surveillance status; (7) continuity check tone; (8) feature status; and (9) dialed digit extraction. In its Third Report and Order, the FCC allowed the FBI to obtain most of the powers it sought: six of the nine punch-list items were at least partially approved. The key issue here, however, is not the number of new powers the FCC granted, but the FBI’s assertion so soon after CALEA’s passage that these new powers were authorized by the very provisions that the FBI had earlier testified did not create new surveillance authority.

The punch list unmasked this FBI misrepresentation to Congress. Despite the FCC’s willingness to grant most of what the FBI wanted, even the FCC conceded that three of the information categories demanded of carriers—surveillance status, continuity check tone, and feature status—though they “could assist LEAs in determining the status of a wiretap” or “could be useful to a LEA,” nonetheless were not surveillance assistance capabilities authorized by CALEA’s provisions. The FBI and Department of Justice, however, strongly insisted that these new capabilities fell within CALEA’s mandates (FCC 1999, ¶101, 106, 111).

The FBI’s aggressiveness in using CALEA to justify new powers was particularly evident in its quest for feature status information, a capability that “would require a carrier to notify the LEA when specific subscription-based calling services [such as call waiting, call hold, and the like] are added to or deleted from the facilities under surveillance” (FCC 1999, ¶107). U.S. West saw in the FBI’s demand an unexplained desire for unprecedented access to telecommunications carriers’ databases. As the FCC reported, “US West stated that it has provided LEAs with expeditious access to feature status information in the past and will do so in the future. US West also contends that *LEAs never before had the access that DoJ/FBI now is demanding to carriers’ databases*, and that DoJ/FBI’s reasons for seeking this access are unconvincing”

(FCC 1999, ¶109, my emphasis). Such was the FBI's concept of maintaining the status quo.

The pattern was the same for most items on the punch list. Under the heading “content of subject-initiated conference calls,” the FBI sought CALEA surveillance capabilities that would “permit the LEA to monitor the content of conversations connected via a conference call set up by the facilities under surveillance,” insisting that the “ability to monitor would continue even after the subject drops off the conference call” (FCC 1999, ¶58). Carriers such as Bell Atlantic noted that this provision represented an “expanded capability” for LEAs because in the past “LEAs have not had the ability to monitor all parties to a multiparty conference call after the subject of the surveillance has left the call or has put the call on hold” (FCC 1999, ¶61). This new capability was exactly what the FBI wanted as it claimed that “the proposed conference calling capability is consistent with CALEA” (FCC 1999, ¶63).

Under the heading of “party hold, join, drop on conference calls,” the FBI sought a CALEA mandate that telecommunications carriers deliver “messages identifying the parties to a conversation at all times” (FCC 1999, ¶68). Carriers reported that this provision would not maintain the status quo but instead would represent a “significant enhancement to existing or previous wiretapping capabilities,” one “beyond the scope” of CALEA (FCC 1999, ¶71).

With its request for “subject-initiated dialing and signaling information,” the FBI sought capabilities enabling the LEA “to be informed when a subject . . . uses services such as call forwarding, call waiting, call hold, and three-way calling” (FCC 1999, ¶76). Despite industry statements that such information was not call-identifying information and would require manufacturers “to make fairly substantial modifications to their equipment” to obtain and report such information, the FCC mandated most of the capabilities the FBI sought as part of this punch-list item.

In seeking “in-band and out-of-band signaling,” the FBI sought other capabilities not previously available to law enforcement—including reports of ringing, busy signals, call-waiting signals, message lights, and the like associated with targeted equipment. The Department of Justice and the FBI convinced the FCC to categorize most of these signals as call-identifying information, thus contradicting the FBI's repeated statements to Congress that call-identifying information was merely dialing information (FCC 1999, ¶83, 88, 89). Similarly, the FBI's request for “timing information” succeeded in imposing another new requirement on telecommunications carriers: the creation of a “time stamp” on each call-identifying message, with specific requirements for how quickly (in seconds) the time-stamped messages must reach the LEAs and the milliseconds of accuracy required (FCC 1999, ¶90–96).

Perhaps most revealing is the punch-list item labeled “dialed digit extraction.” As the FCC stated, this capability would require the telecommunications carriers “to provide to the LEA . . . the identity of any digits dialed by the subject after connecting to another carrier's service (also known as ‘post-cut-through digits’)” (FCC

1999, ¶112). Such post-cut-through digits might include numbers dialed after reaching an 800 number for a long-distance service—or they might include personal information such as a bank account or credit card number. Either way, once the initial connection was established, that information would be considered content from the perspective of the original carrier. Nonetheless, the FBI sought to gain access to such call content information on the weak authority of a pen register. Privacy groups as well as telecommunications industry groups told the FCC that this information was call content information, not call-identifying information, and should not be obtainable on mere pen register authority (FCC 1999, ¶114–116).

The FBI insisted that those groups were wrong. It claimed that, in the absence of carrier capability to distinguish which post-cut-through digits would be used for call completion and which were personal information such as bank account numbers, “the carrier must [under CALEA] deliver all post-cut-through digits to the LEA” acting on only pen register authority (FCC 1999, ¶118). The FCC bluntly agreed: “Accordingly, while we are concerned about the costs of a dialed digit extraction capability to originating carriers, as well as the privacy implications of permitting LEAs to access non-call-identifying digits (such as bank account numbers) with only a pen register warrant, we find that requiring this capability is appropriate” (FCC 1999, ¶123). All these expanded surveillance capabilities came at the behest of the same FBI that had persuaded Congress to pass CALEA on the rationale that the FBI was “not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago” (U.S. House and Senate 1995, 6) and that the purpose of CALEA was merely “to maintain technological capabilities commensurate with existing statutory authority” (U.S. House and Senate 1995, 7).

The stark conclusion is that FBI officials conned Congress into passing CALEA. The FBI’s three main themes before Congress—that CALEA contained no new surveillance authority, that CALEA could not be used to mandate accessibility of cell phone location information, and that CALEA would improve privacy protection—all were false. This key element of the political transaction-cost manipulation surrounding CALEA’s passage dramatically increased the cost to legislators of maintaining government surveillance authority at the level they desired.

Court of Appeals Decision

Challenges to the FCC’s Third Report and Order by privacy organizations and telecommunications industry associations led to a decision on CALEA by the U.S. Court of

10. In November 1999, the U.S. Telecom Association (USTA), the Cellular Telecommunications Industry Association (CTIA), the CDT, the EPIC, the ACLU, and the EFF challenged the FCC’s Third Order in court, seeking review of the FCC’s action by the U.S. Court of Appeals for the District of Columbia Circuit. *U.S. Telecom Association et al. v. Federal Communications Commission and U.S.A.*, U.S. Court of Appeals, District of Columbia Circuit, nos. 99-1442, 99-1466, 99-1475, and 99-1523 (August 15, 2000), 227 *Fed. Rep. 3d* 450; hereafter cited as *USTA v. FCC* 2000.

Appeals (D.C.) on August 15, 2000.¹⁰ At issue were the FCC orders regarding location information, packet-mode communications, and four approved punch-list items (post-cut-through dialed digit extraction, party hold/join/drop information, subject-initiated dialing and signaling information, and in-band/out-of-band signaling).¹¹

Location Information

As the FBI sought, the U.S. Court of Appeals held that the FCC was correct in deeming cell phone location to be call-identifying information and in upholding the J-Standard requirement that carriers record the physical location of the nearest antenna tower at the beginning and end of every mobile phone call. However, the court also recognized that in order to gain access to such location information, law enforcement authorities would have to have authorization stronger than mere pen register/trap-trace authority. Without specifying the exact nature of the required authorization, the court praised both the FCC for “its understanding that antenna location information could only be obtained with something more than a pen register order” and the Justice Department for its concession that a “pen register order does not by itself provide law enforcement with authority to obtain location information” (*USTA v. FCC* 2000, 464).

The result was that, contrary to Freeh’s denials during the CALEA hearings, the government now in effect requires telecommunications carriers to design and maintain equipment and facilities capable of tracking cell phone location—information that in large metropolitan areas often pinpoints the caller’s location to within one city block. In addition, law enforcement officials apparently will enjoy access to that information on authority weaker than a probable-cause warrant.

Packet-Mode Data

The Court of Appeals also let stand the FCC’s decision regarding packet-mode data, with one important qualification. Recognizing that packet-mode data transmission may commingle pen register (dialing) information with call content, the court found a probable-cause warrant to be required in these circumstances. The court was outspoken:

[N]othing in the Commission’s treatment of packet-mode data requires carriers to turn over call content to law enforcement agencies absent lawful authorization. Although the Commission appears to have interpreted the J-Standard as expanding the authority of law enforcement agencies to obtain the contents of communications, . . . the Commission was simply mistaken. All of CALEA’s required capabilities are expressly premised on the

11. The other two punch-list items approved in part by the FCC—the content of subject-initiated conference calls and timing information—were not challenged in this lawsuit.

condition that any information will be obtained “pursuant to a court order or other lawful authorization.” . . . CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is “not authorized to be intercepted.” (*USTA v. FCC* 2000, 465)

In other words, despite the FCC’s attempted circumvention of those evidentiary standards, the Court of Appeals upheld in this context the long-standing requirement for a warrant based on probable cause when information to be obtained includes call content.

Punch-List Items

The court struck down the four challenged punch-list items but remanded the issue to the FCC. The FCC is now trying to find ways to meet the court’s objections and to reinstate revised versions of these punch-list capabilities.

The court agreed with the petitioners’ claim that “the Commission’s decision to modify the J-Standard to include the punch list reflects a lack of reasoned decision-making” (*USTA v. FCC* 2000, 460). Chiding the FCC for its failure to give justification for deeming the punch-list items to be call-identifying information, the court stated that the FCC “never explained—not in the Order and not in its brief—the basis for this conclusion. Nowhere in the record did the Commission explain how the key statutory terms—origin, direction, destination, and termination—can cover the wide variety of information required by the punch list. . . . Instead, it simply concluded, with neither analysis nor explanation, that each capability is required by CALEA” (*USTA v. FCC* 2000, 460).

The court also criticized the FCC for arbitrary decisions regarding the CALEA requirement for implementation of the statute by “cost-effective methods.” As the CDT and other privacy groups had pointed out, the FCC’s Third Report and Order claimed time and again to satisfy that CALEA provision by simply asserting, without explanation, that the costs involved were “not so exorbitant” as to violate CALEA’s mandate. The Court of Appeals asked: “But why? The Commission failed to explain how it decided that implementing the punch list capabilities, which increase J-Standard costs by more than 45 percent (even by the Commission’s conservative estimates) is ‘not so exorbitant’” (*USTA v. FCC* 2000, 461). This approach the court deemed “a classic case of arbitrary and capricious agency action” (*USTA v. FCC* 2000, 461).

Also criticized in the opinion was the FCC’s inadequate attention to the CALEA requirement that the rules “protect the privacy and security of communications not authorized to be intercepted” (CALEA, Public Law 103-414, §107[b][2]; 47 U.S.C §1006[b][2]). In particular, the court singled out the FCC’s authorization for all post-cut-through digits—including call “content” such as bank account numbers,

passwords, and prescription numbers—to be delivered to law enforcement officials on mere pen register authority. Without so ruling, the court stated that “it may be that a Title III warrant is required to receive all post-cut-through digits” (*USTA v. FCC* 2000, 462). Moreover, the court found the FCC’s rejection of privacy-protecting alternatives based only on costs to law enforcement agencies to be “an entirely unsatisfactory response to CALEA’s privacy provisions” (*USTA v. FCC* 2000, 462).

Although privacy organizations were gratified by the court’s comments, the FCC has continued its efforts on behalf of the punch-list items. On October 17, 2000, it issued a public notice “solicit[ing] comment on the issues raised in the court’s remand decision.”¹² Privacy groups have again filed statements with the FCC to oppose the reemergence of the temporarily thwarted punch-list items.

After expending significant resources to alter CALEA’s privacy-threatening provisions prior to passage and to participate in implementation discussions for the nearly five years between CALEA’s 1994 passage and the FCC’s 1999 Final Order, privacy groups and telecommunications industry associations also have borne the additional legal costs of a court challenge.¹³ Ten years later, having spent countless thousands of dollars, these groups have experienced firsthand the CALEA-related increases in the transaction costs of protecting people’s privacy against further government intrusions.

CALEA-Related Tactics: A Broader View

Even if privacy and civil liberties groups ultimately prevail on some aspects of this case, the actions by government officials that artificially increased the political transaction costs of resisting expanded federal surveillance authority have dampened overt resistance to these measures. The result is public acquiescence to a larger scope of surveillance authority than would have been tolerated if political transaction costs had not been artificially increased.

The most dramatic of the maneuvers that increased political transaction costs in this case was the FCC’s implementation of CALEA through its Third Report and Order. We have seen the broad construction of CALEA embodied in the FCC’s mandates. When, as seems apparent here, an agency such as the FCC construes a statute to create more government power than Congress intended, the transaction-cost burden of maintaining the status quo ante is shifted to those who oppose such unauthorized expansion of government authority. Had the FCC (or the FBI) forthrightly sought to establish legislatively the power it asserted bureaucratically, it would have borne substantial political transaction costs in convincing Congress to

12. Federal Communications Commission, Public Notice, DA 00-2342, “Commission Seeks Comments to Update the Record in the CALEA Technical Capabilities Proceeding,” CC Docket No. 97-213, October 17, 2000. In a separate proceeding, the FBI in 2001 again pressed the FCC to mandate carrier use of automated surveillance-status messages, a punch-list item previously rejected by the FCC in its Third Report and Order (FCC 1999). The FBI once more lost on this issue (FCC 2001, 2, 6–7).

13. See Center for Democracy and Technology 2000a, 2000b, 2000c.

create, for example, federal authority to mandate availability of location information for mobile cell phone use. Instead, the FCC simply “interpreted” a statute that Congress had passed on the understanding that it was *not* establishing certain powers as if it *had* created them, thus forcing those who sought to uphold the existing scope of government surveillance authority to bear the additional transaction costs of a court challenge to the FCC’s action.¹⁴

The passage of CALEA was rife with other forms of political transaction-cost manipulation as well. Most important were incrementalism, concealment of CALEA’s cost (Higgs 1985; Higgs 1987, 62–67), and the unabashed FBI misrepresentations documented earlier in this article.

Government authorities’ incrementalism manifested itself in the progression from the Bush administration’s suggestions in 1991 to the 1994 Clinton administration proposal. Having started with all-encompassing proposals that quickly met defeat, advocates deliberately narrowed the bill in order to craft a proposal that could gain passage and serve as a statutory foot in the door. Freeh himself explained the 1994 proposal’s focus on common carriers and exclusion of other types of companies as a “concerted effort” undertaken “to narrow the impact and focus of the legislation,” to “narrow the package” (U.S. House and Senate 1995, 49).

Roy Neel, president of the U.S. Telephone Association, described it in practical political terms, stating that the FBI bill “was narrowed and those kinds of services were exempted to avoid the kinds of problems that you might have in enacting this proposal—in other words, to take out of the picture the opposition from a number of technologies and companies and so on who might oppose this” (U.S. House and Senate 1995, 55). That strategic decision, however, did not reflect a change in the FBI’s long-run surveillance objectives. When Senator Pressler, inquiring about the exclusions, asked Freeh, “but in the future, will you be seeking the ability to tap into those other forms of communications?” Freeh replied, “It is certainly a possibility” (U.S. House and Senate 1995, 202).

Nonetheless, the House report assured Congress that the CALEA proposal had a “[n]arrow scope” (U.S. House 1994, 18). To anyone who read the fine print, however, the report’s explanation of CALEA’s coverage of telecommunications carriers might have given a different impression. The report stated:

A “telecommunications carrier” is defined as any person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire . . . and includes a commercial mobile service. . . . This definition encompasses such service providers as local exchange carriers, interexchange carriers, competitive access providers (CAPs), cellular carriers,

14. The broader public had little opportunity to understand the implications of the FCC decision, which was reported under such news headlines as “FCC Approval of Wiretap Standards Brings Law Enforcement to Digital Age” (Wigfield 1999).

providers of personal communications services (PCS), satellite-based service providers, cable operators and electric or other utilities that provide telecommunications services for hire to the public, and any other common carrier that offers wireline or wireless service for hire to the public. (U.S. House 1994, 20)

Moreover, CALEA gave the FCC broad discretion to extend CALEA's applicability, authorizing the FCC "to deem other persons and entities to be telecommunications carriers subject to the assistance capability and capacity requirements to the extent that such person or entity serves as a replacement for local telephone service to a substantial portion of the public within a state" (U.S. House 1994, 20). Although this provision undercut attestations of the narrow scope of the measure, it was not discussed in either the joint hearings on or the House floor consideration of CALEA.

In the end, however, packaging CALEA as a "narrow" measure—compared to the more overt overreaching in earlier bills—worked, both as rhetoric and as actual strategy. Even the EFF's Jerry Berman reflected the strategy's success, voicing support for CALEA in part because "we believe that this legislation is substantially less intrusive than the original FBI proposals" (U.S. House and Senate 1995, 160).

The FBI's incremental approach represented a familiar political transaction-cost manipulation strategy, one that reduced the perceived marginal cost to legislators and their constituents of passing CALEA and thus supported the FBI's effort to increase government authority. Another such tactic was apparent in CALEA advocates' efforts to conceal the apparent cost of the measure. Although CALEA's language authorized the appropriation of \$500 million dollars annually for fiscal years 1995 through 1998, telecommunications industry spokesmen emphasized that actual costs would greatly exceed that amount and that the industry would have to bear much of that cost because of CALEA's requirements after fiscal year 1998. As Berman stated, "after four years, reimbursement will be limited to costs incurred for adding capacity only, not including surveillance capability in new services," which "defeats the purpose of providing public scrutiny of the government's surveillance expenditures" (U.S. House and Senate 1995, 163). Neel testified that "failure to compensate for government surveillance activities effectively hides the government's expenditures from public scrutiny" (U.S. Senate and House 1995, 140). Forcing these costs onto the private sector made them disappear from the perception of most legislators and taxpayers, further lowering the apparent cost of adopting the measure and increasing the political transaction costs of resisting it.

Finally, there was the FBI's unabashed misrepresentation of CALEA to Congress and the public, documented earlier in this article. When respected public officials repeatedly misrepresent their interpretation of proposed statutory language and then reverse their position the moment the ink is dry on newly enacted legislation, they increase enormously the transaction costs to the public and to Congress of understanding and resisting legislation that expands government authority.

Why CALEA-Related Political Transaction-Cost Manipulation?

The deception and other government manipulation of political transaction costs that accompanied the emergence and implementation of CALEA were consistent with my theoretical expectations. Key variables emphasized by political transaction-cost manipulation theory had the predicted impacts in this case. The legislative history of CALEA suggests that the most important variables were an appealing rationale, the complexity of the measure, executive support, party support, and ideology.

Advocates of the bill repeated the appealing rationale at every turn. In the 1994 joint hearings, Freeh testified:

Unless Congress creates a new law, law enforcement's ability to protect the public against crime will, in my view, be gravely eroded and the national security placed at risk. Wiretapping is used in the most important life-and-death cases: terrorism, espionage, drug trafficking, organized crime, kidnapping, and a variety of other crimes. Without a new statute, law enforcement at the Federal, State, and local levels will be crippled . . . [;] an already over-burdened law enforcement system will be fighting with one hand behind its back. (U.S. House and Senate 1995, 6)

He cited terrorist incidents and child abductions to bolster his case (U.S. House and Senate 1995, 13). The power of the law enforcement theme was evident as each legislator prefaced his remarks about the CALEA bill with a statement of support for law enforcement. For example, Senator Patrick J. Leahy (D.-Vt.), chairman of the Subcommittee on Technology and the Law, stated: "I do not want law enforcement to lose its capability to use this powerful tool in its crime-fighting arsenal. . . . I know that wiretaps can produce powerful evidence against our most dangerous criminals at the lowest risk to the agents involved" (U.S. House and Senate 1995, 108). Representative Howard Coble (R.-N.C.) likewise averred that "I in no way want to emasculate or weaken law enforcement in its capability" (U.S. House and Senate 1995, 111). Representative Henry J. Hyde (R.-Ill.), ranking member of the House Subcommittee on Civil and Constitutional Rights, stated on the House floor that "[f]ailure to pass this legislation will have dire consequences for law enforcement, public safety and our national security" (*Congressional Record*, House, October 4, 1994, 10780). The refrain was ubiquitous.

Of comparable importance was the complexity of the legislation and the technology to which it applied. Not even Freeh seemed sure of what it covered—or at least the measure's complexity made it credible for him to assume that posture. At one point Senator Larry Pressler (R.-S.D.) asked Freeh whether the bill covered "strictly telephone, what is said over a telephone," and Freeh replied, "That is the

way I understand it, yes, sir.” Jerry Berman of the EFF corrected Freeh, pointing out that “the Internet traverses the public switch telephone network” and therefore “uses the transmission and switching facilities of the networks that are covered under this legislation.” As Berman explained, because “that communications stream has to be delivered into the future by common carriers,” it would mean that “a communication that is travelling across the Internet which is the subject of a court-ordered wiretap would be intercepted” (U.S. House and Senate 1995, 202–3). CALEA’s complexity also was evident in Representative Coble’s (R-N.C.) remark that he was “about to steam into computerized waters that are always invested with rocks, shoals, and reefs for me because of lack of information computerwise” (U.S. House and Senate 1995, 199). Consistent with the theory’s predictions, complexity facilitated support for the transaction-cost-increasing measures that became part and parcel of CALEA’s passage and subsequent FCC-engineered expansion.

Other variables identified by the theory as determinants of political transaction-cost manipulation also contributed to that support. For instance, executive support for the bill was strong, as was support from both political parties. Ideology also reinforced support for CALEA because the measure was cast as an uncontroversial law enforcement issue acceptable across much of the ideological spectrum. The perceived importance of CALEA to constituents as a law enforcement measure played a similar role. Finally, publicity given to a measure’s transaction-cost-increasing features is predicted to reduce support for the measure. With CALEA, a lack of media attention to those features was consistent with the measure’s passage.

Thus, government manipulation of political transaction costs flourished in an environment of complexity and appealing rationale, buttressed by executive support, party support, and concordant ideologies.

“A Legible People”

As James Scott (1998) has noted, governments for centuries have taken steps to render society “legible” to government officials and hence susceptible to government’s understanding and manipulation. For Scott, “legibility” denotes the state’s “gradually get[ting] a handle on its subjects and their environment,” a multifaceted process by which, over time, “officials [took] exceptionally complex, illegible, and local social practices . . . and [created] a standard grid whereby it [could] be centrally recorded and monitored” (1998, 2).

It is no surprise that the quest continues in the computer age. The federal government’s surveillance can be seen as an effort to create a “legible people” (Scott 1998, 65). By seeking expansive government ability to track the physical location of cellular phone users and to obtain the content of private communications in a variety of circumstances without a probable-cause warrant, the Justice Department is using CALEA to further this age-old quest.

Of course, those on both sides of the CALEA debate support law enforcement's ability to protect law-abiding people from terrorists and killers. The real issue is the opportunity cost of ever-expanding government surveillance—an opportunity cost that includes encroachment on long-standing privacy values, potential misuse of surveillance authority, and a chilling effect on intellectual independence and overt expression of dissent.

Those who dismiss privacy concerns about CALEA and related measures argue that people who have not broken the law and have “nothing to hide” need not fear government surveillance. Although this view resonates deeply with many people, it does not withstand careful scrutiny. It assumes: (1) that the law is knowable, so people can be confident that they have not broken the law; (2) that people who have done nothing “wrong” have no valid reason to object to federal officials examining the most intimate details of their lives; and (3) that government officials will not exceed established limits on their surveillance authority. Each of these assumptions is false. Given today's millions of pages of abstruse U.S. statutes, regulations, and judicial interpretations, ordinary Americans—and often even legal experts—cannot know if they have violated the law, and therefore rationally they must perceive government surveillance as a threat. Moreover, law-abiding people cherish privacy, a value fundamental to our individuality, autonomy, and freedom. As a Privacy and Technology Task Force appointed by Senator Leahy reported in 1991: “People care deeply about their privacy, and cherish the ability to control personal information. Even if they have done nothing wrong, or have nothing to hide, most people are offended if they are denied the ability to keep certain personal information confidential. Crucial to one's sense of self is the right to maintain some decision-making power over what information to divulge, to whom, and for what purpose” (U.S. House and Senate 1995, 180).¹⁵ Governments that disregard people's privacy establish regimes utterly inconsistent with the values and the Constitution on which this nation was founded. Moreover, U.S. scandals from Filegate to Chinagate have demonstrated beyond any doubt that “trusting” government officials not to exceed their authority is foolhardy.

Recent history in particular does not inspire confidence in the FBI's institutional commitment to seek and use information lawfully. When, during President Clinton's first term, FBI operatives transferred some nine hundred files to the White House for political use, it was not the first instance of improper FBI use of personal information. In the late 1980s, for example, evidence surfaced of the FBI's Library Awareness Program, a program active from the 1970s forward in which “the bureau asked librarians around the country to monitor patrons with foreign-sounding names or accents who checked out books on technical and scientific subjects” (Rosen 2000, 167). Ulrika

15. Quoted from the “Final Report of the Privacy and Technology Task Force Submitted to Senator Patrick J. Leahy, May 29, 1991,” prepared by a fifteen-member task force and included in the 1994 joint hearings.

Ekman Ault demonstrated that there was “little evidence” to support the FBI’s contention that the Library Awareness Program was an educational program, concluding that it “instead must be understood as an investigative effort by the FBI to obtain information about library patrons, including their names, reading habits, and nationalities or national origins, by means of unsupervised surveillance” (1990, 1536–37).

The quest for unsupervised surveillance continues today. The FBI has sought congressional funding of its Digital Storm technology, even while attempting to dispel public outrage over its recently disclosed Carnivore Internet surveillance program. With Digital Storm, the FBI plans to acquire new technology that will allow greater synthesis of data about people through more extensive and intensive “data mining.” According to *Washington Post* staff writer Robert O’Harrow Jr., an FBI spokesman “acknowledged that the bureau’s ability to manage that data will soar with the new technology,” and FBI budget documents estimated that the new technology “would so improve the ability to conduct wiretaps that the number of approved taps would grow by 300 percent over the next decade.” Equally important, O’Harrow reported that “[t]he agency would also continue expanding its use of commercial databases containing credit information, real estate records, vehicle registrations and a plethora of other personal details.” Because Digital Storm presages a “huge increase in data collection and analysis,” critics have become “alarmed that the bureau’s proposals could erode constitutional protections that limit government searches, with almost no discussion to date about the implications on Capitol Hill” (2000, A1).

In contrast, the FBI’s newly revealed Carnivore program has already sparked serious discussion in Congress and in the popular press (King and Bridis 2000; Labaton 2000; Wingfield and Clark 2000). Carnivore is designed to collect electronic data such as e-mail and other personal transmissions that pass through an Internet service provider (ISP) as people use the World Wide Web. With a court order, the FBI can attach a device—essentially an FBI laptop computer with a Carnivore filter and hard drive—to the facilities of an ISP. Once installed, the Carnivore system is locked, making it accessible only to the FBI and preventing the ISP from monitoring the FBI’s activities. According to the FBI, the filter would be programmed to select and record only those communications that pertain to the suspect.

From a privacy perspective, the problem is that *all* the ISP’s e-mail and other digital traffic would run through the FBI filter, including the communications of innocent people not suspected of wrongdoing. Although the FBI is keen to convince the public that Carnivore would be used only with a court order, nothing guarantees that, with this cornucopia of data running through the Carnivore filter, the FBI would limit itself to the data it has been authorized to collect (Wingfield and Clark 2000). Once the Carnivore system has been attached, the FBI could surreptitiously reprogram the device to obtain other materials or to shift targeted parties. Moreover, the Carnivore system enables the FBI to gain access to the content of communications when it has only pen register and trap-trace authority. As Alan B. Davidson, staff counsel for the CDT, testified regarding Carnivore on July 24, 2000, “Such a

system—with easy access to unauthorized data and no current potential for oversight—creates tremendous potential for misuse. . . . [I]t is easy to believe Carnivore could be exceeding the legal authority of a particular order—quite possibly by mistake or error” (2000, §2A). Davidson characterized Internet technology as “a boon to government surveillance and law enforcement,” and cautioned that the attempt to apply preexisting telephone wiretapping concepts in an Internet environment “should not become an excuse for creating a massive technical architecture for surveillance that, given the nature of the Internet, could be far more invasive than anything we have seen to date” (2000, §4).

Service providers now have little choice regarding Carnivore. When EarthLink challenged an FBI Carnivore installation, arguing that Carnivore’s operation impaired EarthLink’s service to its customers and threatened their privacy, a federal magistrate ruled against the company and “forc[ed] it to give the FBI access to its system” (Wingfield, Bridis, and King 2000). The *New York Times* reported that some ISPs and privacy groups had suggested, to no avail, a “less intrusive alternative” to Carnivore: “The providers, like AOL or the Microsoft Network, could be ordered by a court to turn over specific material, rather than give the F.B.I. unlimited access to the network” (Labaton 2000, WK3). What a novel idea: relinquishing *specific* material to the government rather than letting government agents rifle through material for which they have no warrant. How cavalierly do some federal officials now contravene the Fourth Amendment proclamation that “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Can anyone honestly reconcile a Carnivore-wielding FBI’s “unlimited access to the network” with that pesky Fourth Amendment?

At the conclusion of the 1994 joint hearings on CALEA, legislators reassured each other that all would be well because “reasonableness” was built into the bill. Senator Leahy remarked that “I think, though, in the testimony and the discussions I have had with the FBI and others, that there is a sense of reasonableness that we are trying to build into the legislation” (U.S. House and Senate 1995, 194). As the FBI’s about-face after CALEA’s enactment made clear, today as always it is a dangerous game to stake fundamental rights on the “reasonableness” and self-restraint of law enforcement authorities. The FBI’s prior misuse of its power undermines any credible foundation for such trust: memories linger of the Library Assistance Program, Filegate, and the rest.

What can one conclude from the CALEA case? With the ongoing push for new legislation “to make it easier for authorities to eavesdrop on internet communications such as electronic mail” (Bridis 2000, A3), government manipulation of political transaction costs surrounding this issue no doubt will continue. The familiar themes again will echo through the halls of Congress, asserting that government surveillance must be increased to protect America from terrorists and criminals in the computer age, that law-abiding people have nothing to fear, and that we can trust law enforcement

authorities not to misuse the new powers. Symbolic expressions of government concern about privacy are likely to continue, even increase. Privacy-threatening measures will continue to be put forth as privacy-protecting measures. The FBI, for example, recently reassured people that Digital Storm would pose no problem because the FBI had established a privacy council within the bureau (O’Harrow 2000). Nothing was said about foxes and hen houses.

Increasingly attuned to public relations, the FBI will be more careful in the future not to give intrusive surveillance proposals names such as Carnivore, Omnivore, Digital Storm, and Root Canal. Already FBI officials “have been expressing regrets about the system’s name”: Attorney General Janet Reno “called for a name change,” and Director Freeh asked “how the bureau could have had such a tin ear” (Bridis and King 2000, A28).¹⁶ A soft-pedaling FBI is now describing Carnivore as a “diagnostic tool,” conveying the message that it “is a surgical law-enforcement device used rarely and only under strict court orders” (Bridis and King 2000, A28).

Underlying these maneuvers, however, political transaction costs are being altered at a deeper level. The confluence of CALEA, federally mandated electronic databases of personal information, Carnivore, Digital Storm, Echelon, and the like have established a web of federal surveillance never before known in the United States. This systematic federal surveillance of ordinary Americans *is itself* a form of government manipulation of political transaction costs that works, as do other forms, to increase the costs of resisting expanded federal power. Bentham’s Panopticon, we have seen, displayed the profound role of government surveillance in creating uncertainties that stimulate compliance without overt coercion. Commenting on U.S. government data collection, Paul Schwartz noted the same linkage: “Americans no longer know how their personal information will be applied, who will gain access to it, and what decisions will be made with it. The resulting uncertainty increases pressure for conformity. Individuals whose personal data are shared, processed and stored by a mysterious, incalculable bureaucracy will be more likely to act as the government wishes them to behave” (1992, 1374). CALEA is a harbinger. One way or another, we will soon learn that the resistance-inhibiting power of broad-based government surveillance is potentially the most liberty-endangering form of political transaction-cost manipulation confronting Americans—and freedom-loving people everywhere—in the new millennium.

References

- Ault, Ulrika Ekman. 1990. The FBI’s Library Awareness Program: Is Big Brother Reading Over Your Shoulder? *New York University Law Review* 65 (December): 1532–65.
- Berkowitz, Bruce. 2000. “Carnivore” Won’t Devour Cyber-Privacy. *Wall Street Journal*, July 19, A22.

16. Bruce Berkowitz, Hoover Institution research fellow, suggested that the FBI “[h]ire a better public relations firm, and name your next project ‘Vegetarian.’” Downplaying concerns about the privacy implications of Carnivore, Berkowitz argued that it is “getting harder, not easier, for our law enforcement and intelligence organizations to listen in on communications” (2000, A22).

- Bridis, Ted. 2000. Updating Wiretap Law for E-Mail Urged. *Wall Street Journal*, July 12, A3.
- Bridis, Ted, and Neil King Jr. 2000. Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI. *Wall Street Journal*, July 20, A28.
- Center for Democracy and Technology. 2000a. *Reply Brief of Petitioners United States Telecom Association, Cellular Telecommunications Industry Association, and Center for Democracy and Technology*. In the United States Court of Appeals for the District of Columbia Circuit, Nos. 99-1442, 99-1466, 99-1475, 99-1523, April 4. Available at: <http://www.cdt.org>.
- . 2000b. *Reply Comments of the Center for Democracy and Technology: In the Matter of Communications Assistance for Law Enforcement Act*. Before the Federal Communications Commission, CC Docket No. 97-213, FCC 98-282. January 27. Available at: <http://www.cdt.org>.
- . 2000c. *USTA/CTIA/CDT vs. FCC on Petition for Review of an Order of the Federal Communications Commission, Brief of Petitioners United States Telecom Association, Cellular Telecommunications Industry Association, and Center for Democracy and Technology: In the Matter of Communications Assistance for Law Enforcement Act*. In the United States Court of Appeals for the District of Columbia Circuit, Nos. 99-1442, 99-1466, 99-1475, 99-1523, January 20. Available at: <http://www.cdt.org>.
- Congressional Record*. 1994. 103rd Cong., 2d sess., vol. 140.
- Davidson, Alan B. 2000. Carnivore's Challenge to Privacy and Security Online. Testimony before the House Committee on the Judiciary, Subcommittee on the Constitution. Center for Democracy and Technology: <http://www.cdt.org>. July 24.
- Federal Communications Commission. 1999. *Third Report and Order, Communications Assistance for Law Enforcement Act*. CC Docket No. 97-213, FCC 98-282, 14 FCC Rcd. 16794. August 26.
- . 2001. *Second Order on Reconsideration, Communications Assistance for Law Enforcement Act*. CC Docket No. 97-213, FCC 01-126. April 9.
- Higgs, Robert. 1985. Crisis, Bigger Government, and Ideological Change: Two Hypotheses on the Ratchet Phenomenon. *Explorations in Economic History* 22:1-28.
- . 1987. *Crisis and Leviathan: Critical Episodes in the Growth of American Government*. New York: Oxford University Press.
- King, Neil, Jr. 2000. NSA Faulted on Privacy Invasion, Tech Weakness. *Wall Street Journal*, February 25, A4.
- King, Neil, Jr., and Ted Bridis. 2000. FBI's Wiretaps to Scan E-Mail Spark Concern. *Wall Street Journal*, July 11, A3.
- Labaton, Stephen. 2000. Learning to Live with Big Brother. *New York Times*, July 23, WK3.
- O'Harrow Jr., Robert. 2000. "Digital Storm" Brews at FBI. *Washington Post*, April 6, A1.
- Rosen, Jeffrey. 2000. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.
- Schwartz, Paul. 1992. Data Processing and Government Administration: The Failure of the American Legal Response to the Computer. *Hastings Law Journal* 43 (part 2): 1321-89.
- Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven and London: Yale University Press.

- Twight, Charlotte. 1983. Government Manipulation of Constitutional-Level Transaction Costs: An Economic Theory and Its Application to Off-Budget Expenditure through the Federal Financing Bank. Ph.D. diss., University of Washington, Seattle.
- . 1988. Government Manipulation of Constitutional-Level Transaction Costs: A General Theory of Transaction-Cost Augmentation and the Growth of Government. *Public Choice* 56: 131–52.
- . 1992. Constitutional Renegotiation: Impediments to Consensual Revision. *Constitutional Political Economy* 3: 89–112.
- . 1993. Channeling Ideological Change: The Political Economy of Dependence on Government. *Kyklos* 46, no. 4: 497–527.
- . 1994. Political Transaction-Cost Manipulation: An Integrating Theory. *Journal of Theoretical Politics* 6, no. 2: 189–216.
- . 1995. Evolution of Federal Income Tax Withholding: The Machinery of Institutional Change. *Cato Journal* 14, no. 3: 359–95.
- . 1996. Federal Control over Education: Crisis, Deception, and Institutional Change. *Journal of Economic Behavior and Organization* 877: 1–35.
- . 1997. Medicare's Origin: The Economics and Politics of Dependency. *Cato Journal* 16, no. 3: 309–38.
- . 1999. Watching You: Systematic Federal Surveillance of Ordinary Americans. *The Independent Review* 4, no. 2: 165–200.
- U.S. House of Representatives. 1994. *Communications Assistance for Law Enforcement Act: Report of the Judiciary Committee* [To Accompany H.R. 4922], House Report No. 103-827, 103rd Cong., 2d sess., October 4. Reprinted in *U.S. Congressional Code and Administrative News* (USCCAN), Public Law 103-414, 3489 ff.
- U.S. House of Representatives and Senate. 1995. Subcommittee on Technology and the Law of the Senate Committee on the Judiciary, and Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary. *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375*. 103rd Cong., 2d sess., March 18 and August 22, 1994.
- U.S. Telecom Association et al. v. Federal Communications Commission and U.S.A.*, 2000. U.S. Court of Appeals, District of Columbia Circuit, nos. 99-1442, 99-1466, 99-1475, and 99-1523 (August 15), 227 *Fed. Rep. 3d* 450.
- Whitaker, Reg. 1999. *The End of Privacy: How Total Surveillance Is Becoming a Reality*. New York: New Press.
- Wigfield, Mark. 1999. FCC Approval of Wiretap Standards Brings Law Enforcement to Digital Age. *Wall Street Journal*, August 30, A15.
- Wingfield, Nick, and Don Clark. 2000. Internet Companies Criticize Potential for Excess Monitoring by FBI Wiretaps. *Wall Street Journal*, July 12, A4.
- Wingfield, Nick, Ted Bridis, and Neil King Jr. 2000. EarthLink Says It Won't Install Device for FBI. *Wall Street Journal*, July 14, A16.