Eli M. Noam, Commissioner

New York State Public Service Commission

# Testimony to the Subcommittee on Government Information, Justice, and Agriculture House Committee on Government Operations on H.R. 3669, To Establish a Data Protection Board

U.S. Congress

May 16, 1990

Washington, D.C.

I am not speaking here as a veteran of privacy protection, but as a general telecommunications expert and policy maker. I am normally a Columbia Business School professor, but for the past three years (and the next two weeks) I have served as a public utilities commissioner who has to balance various considerations that may be negatively affected by privacy protection -- economic development, service cost, law enforcement, consumer protection, innovation, freedom of the press, and economic freedom, to mention only a few that are close to my heart. So I am not here as a single-issue advocate.

My comments will support the concept of a Data Privacy Board, as long as its powers are limited much in the way envisioned in HR 3669. Two experiences have shaped my view.

I recently completed writing a two volume book about European telecommunications which also deals with the European approach to data privacy. In a nutshell, I don't like it. They have created a system of data bank registration with fairly rigorous regulations on what data can and can't be stored, and this has spilled over into international data flows and is even used a bit for trade protectionism. This strict model doesn't seem to make sense for the United States.

Often, electronic record-keeping systems must be registered or licensed, and may be subjected to inspection for compliance with the law. Where private record-keeping involves a large number of individuals, it is permissible only if the individuals have a clear relationship with the record-keeping organization.

And the restrictions tend to be aimed more at private parties than at governments.

So my first reaction to the concept of a Data Protection Board in Washington was negative.

But a few months ago I started to look at privacy issues in the telecommunications sector. This was spurred by the caller-ID controversy. Very soon I came to the conclusion that caller ID is merely one element in a much larger set of problems. Without much effort I could identify almost 50 privacy issues in telecommunications -- from the increased use of over-the-air transmission for mobile communication to junk fax and automatic caller identification. Most of the issues were not dramatic, and not likely to get much legislative attention. It became clear that while there was a diversity of problems, there were also commonalities. For example, the question of who should pay if A's new activities jeopardize B's old privacy so that B must spend money to reach her good old status quo in terms of protection.

Or take the question whether "one size fits all" in privacy protection, or whether instead a menu of technological and administrative options could be provided. And if so, whether the market would do it efficiently.

What became clear was that privacy is a complex area where strong feelings coexist with only limited policy analysis, where underlying technology rapidly changing, and where the market structures are in flux.

I therefore reached the conclusion that the ad hoc approach -- let's pass a law, a regulatory rule, or a court ruling when a problem becomes really bad -- had to be supplemented by a more methodical and pro-active look that would bring in a more expertise.

Privacy is an issue with much appeal. Support for it spans the political spectrum. It's also an area of great public and media interest. Yet that does not tell us what the right policies and protections are. To do so requires organized and ongoing attention, criteria for evaluation, and a process that permits identification of problems and options.

For example, at our commission, we recently initiated a proceeding on deregulating the billing and collection of telecommunication services. The early draft dealt with numerous issues but not with privacy. Why not? Not because of opposition or indifference, but simply because no one was in charge of that aspect, so nobody thought of it.

To improve on that situation, our Commission initiated in January of this year a proceeding requesting comments on whether we should adopt a set of proposed policy principles to be applied to privacy jeopardizes. We will decide on that issue a week from now. We've had more than 30 different parties participate with comments.

Having reached these two conclusions -- that the European model of data protection agencies is not desirable, but that a systematic and expert look is necessary -- I was very happy to

read the proposed bill H.R. 3669. I would like to offer my congratulation to the aptly named Chairman Wise, to Congressman McCandless, to their colleagues on the committee, and to their staff. The proposed Data Protection Board strikes just the right balance -- it does not unleash a new bureaucracy, but it sets up a body that can advise, study, educate, anticipate, identity gaps, and serve as a catalyst. It can also translate, so to speak, what other countries rules mean to us, and vice versa. And this is an important point. Regardless of what the US does on Data protection, other countries are setting rules that guide international data flows. And yet the US government is usually not present at the table. This is an aspect of the Board's competence which I would recommend to strengthen beyond the present language.

The concept of privacy is not without its critics. One argument is that privacy is a drag on the economy.

It is true that privacy protections raise the cost of information search, and that transaction costs rise. On the other hand, firms can hold on to their trade secrets and protect themselves from leaks and intrusion. Most information has no protection through property rights, its value must be shielded through confidentiality. To permit its easy breach would lead to a lesser production of such information. It also leads to inefficiency in information flows, because people would use all kinds of hints or codes.

Partly in response to economic and social needs, many transactions have been specifically accorded special informational protection known as "privileges," e.g. between attorney-client, penitent-clergy, patient-doctor, citizen-census taker, etc. The idea in each case is that the protection of information leads to a socially superior result even if it is inconvenient to others who deserve to look at the information for their own purposes.

A second argument against privacy is that it of interest to a small elite only. To the contrary, attention to privacy is widely shared. For example, according to information from the New York Telephone Co., 34% of all residential households in Manhattan and 24% of all its residential households in the State have unpublished telephone numbers at subscribers' request. Most policemen, doctors, or judges, to name but a few occupations, have unlisted numbers. On the West Coast, it appears that the spread of unlisting is still further advanced, reaching 55% in California.

Generally, the remainder of my comments will not be on the nuts and bolts of the bill. For example, I leave to inside-the-beltway experts the question whether the size limitations to 50 staffers is useful, or whether sun-setting is desirable. What I'd like to provide is a broad picture of the advantages of the broad approach inherent in a Data Protection Board.

1. It would help to develop consistent policies that balance various societal interests and steer a course between

anti-technology luddism on the one hand and a technocratic disregard for privacy interests on the other. Technology outpaces regulatory treatment; legislators and regulators have often either let themselves be steamrolled, or else they retarded innovation while learning about an issue. Both choices are unpalatable. In privacy, too, there is a learning curve, and policy wisdom meets the prepared.

A board, in contrast to a court, can initiate its own cases and institutionalize expertise. It need not be purely reactive. This would not void a role for legislation. A board's functions is to flesh out the laws enacted by Congress. Legislative oversight might well be easier over a free-standing small agency than over a section of a huge department.

2. A broader approach would help to define expectations about privacy. This has concrete implications. The Supreme Court has consistently ruled that privacy protection is governed by the standard of reasonable expectations. Thus, privacy principles defined by a board could help establish reasonable expectations, which in turn could establish the sphere of legal protection.

3. There are also practical reasons for being forward-looking on this subject. The European privacy requirements mentioned earlier (and their coordination through a European Convention), may affect the United States. These requirements threaten to restrict data flows to countries whose privacy protection is less assured -- including the United States.

Similarly, it may limit its role in remote-access data processing and in on-line data base publishing. Arguably, the policy consequence should not be to establish strict rules matching the Europeans' often heavy-handed approach, but instead to structure a more flexible system based on choice and "privacy options."

4. Will competition take care of privacy problems in the private sector? Not necessarily. In a competitive environment a user may select a service provider which offers the desired combination of price and privacy protection. But in many other instances, the greater openness of a competitive system and the greater complexities of its multiple networks also mean a greater openness of information. It is easier to control the dissemination of information in a monopoly setting.

5. Another advantage is that such a board could take a national perspective. In telecommunications, for example, the old Bell monopoly has given way to a large number of carriers, leading to an increasingly open network system in which information about use and user is exchanged across companies. Any single state can do only so much to establish protections in this centrifugal and open environment. This is not to suggest that a Washington agency such as the FCC should establish national rules. The state commissions would oppose that. And yet, quite clearly, some nationally principles are necessary. But this should not mean preempting the states, but rather helping them. A Board with its advisory and investigative functions could be perceived by the states as a resource rather

than as a threat, if it forgoes jurisdictional imperialism. Conversely, such a Board could and should be also be a place where the specific policy concerns of state and local governments are considered, and where privacy protection is not seen as something that has to be uniform, once we agree on the floors. Again, one size need not fit all.

I am mindful of the direct and indirect cost of any privacy protection, and of the potential abuse over free information flows. But on balance the benefits to economic efficiency and to free speech values outweigh the costs. And if privacy is to be protected, I'd like to see it done in a well-designed way. Therefore, I support the concept of a data protection board with limited powers.

## APPENDIX A: NEW PRIVACY ISSUES IN TELECOMMUNICATIONS

Almost every new telecommunications service has raised new types of privacy issues and concerns. Not all of them, it should be noted, are within our jurisdiction. But this should not prevent a comprehensive viewing. A list of communications services and related privacy problems follows -- some of them potential and hypothetical, others allegedly concrete.

### A. Wireless Transmission

1. Cellular telephones: monitoring of conversations is possible,[1] with the stationary party often unaware that its call is being "broadcast" to a mobile receiver. It also becomes possible to track a subscriber's travel path by using data on which cells were activated. This also permits employer monitoring of employers movements. The next and "smart" cellular technology that is person-based rather than location-based, and would strengthen the potential for locational tracking.

2. Cordless telephones: a monitoring of conversations by a nearby radio receiver is possible, as is the unauthorized use of a subscriber's telephone number by someone accessing their line with a cordless telephone operating at the same frequency.

3. CT-2: these cordless public phones, now being introduced in the U.K. under the designation of "Telepoint," have been approved by the FCC. They permit an easy surveillance of calls at any such public phone location by a nearby monitor.

---

[1] E.g., many older TV sets can receive cellular UHF frequencies.

4. Pagers and beepers: The monitoring of caller locations and the collection of information about the message volume of a particular called party are possible.

5. Satellites and microwave transmission: permit easier monitoring than landlines.

B. Switch-based Services

6. Voice mail: creates the potential for unauthorized access to messages by third parties. Also permits the unwanted retention of old messages.

7. Remote rerouting of calls: can be done by an unauthorized person, or to a non-consenting person.

8. Bridge or conference calls: allows silent listening-in by unannounced parties.

9. Information safety deposit boxes: unauthorized access to a wide variety of personal information could be obtained.

C. Terminal Equipment

10. Facsimile machines: permit the depositing of unsolicited messages within the premises of the called party (and at the latter's expense of thermal paper).

11. Automatic dialers: have lead to a proliferation of unsolicited and intrusive "junk" calls.[2]

---

[2] For the best analysis of telemarketing privacy, see Nadel (1986).

12. Synthetic voice: facilitates often intrusive automated telemarketing calls that do not permit response or questioning by called party, and may not allow the recipient to hang-up. Facilitates subliminal messages.

13. Answering machines: may present the opportunity for access to messages by unauthorized parties. Routine taping of incoming calls is also possible.

14. Speakerphones: a caller may not be aware, in the absence of a signal, that there is an audience to what is believed to be a private conversation.[3]

15. Picturephones: a receiving party could sell a resulting video recording of the conversation.

16. Remote metering and telemetry: can be intrusive (warrantless entry).

17. Passive monitoring devices: allows sophisticated information gathering (such as voice stress metering over telephone) without notice to tested individual.

D. Networks and Transmission

18. Broadband networks: present plans include a bus-type architecture as a technical solution to local fiber distribution, which create in effect a "party line" with the potential for

---

[3] (This happened recently to President Bush, who began engaging in a confidential political chat while being overheard by an audience of hundreds.)

diverting signals by unauthorized parties in the distribution system.

19. Packet transmission: presents the possibility of diversion of packets, similar to the above. Permits identification of sender and recipient of packets by other parties with access to the overhead part of the packet. This may become an issue in a future broadband SONET fast-packet standard.

20. Interactive or addressable video broadband services: could permit billing records with viewing information like those outlawed in the "Bork bill" for video stores.[4]

21. ISDN: the use of the "D-channel" could provide transaction and signalling information to other parties.

22. Intra-organizational networks: possess the capability to track employee calls, physical presence, and location, and productivity (e.g., number of key-strokes, call handling time, total time on phone, etc.). Permit eavesdropping on conversations without notification to employees as well as non-employee third parties.

23. Call forwarding: re-routing of one's calls to a non-consenting third party can intrude into that party's privacy. Where remote re-routing is possible, an authorized access can divert telephone calls and lead to their interception.

---

[4] According to New York Attorney General Robert Abrams, "Interactive cable television could generate the single largest repository of personal data and information in the history of the world." (Flaherty, 1985, p.143)

E. Information Services

24. Electronic mail/bulletin boards: the use by fringe user groups has led to Congressional bills requiring the monitoring of bulletin boards by the computer systems operators.

25. Dial-it services: mandatory prior-subscription of certain information services facilitates the creation of lists of their users.

26. Videotex, audiotex: allows records of pages or programs used by a subscriber to be collated to create a profile of business transactions and personal habits.

27. Videotex gateways: could permit carriers to monitor information pages and transactions used by subscribers.

28. Data banks: permit easy recording of numerous personal data, and easy access to them by many parties, including unauthorized ones; permit matching of different records to establish profiles; could be altered surreptitiously by outsiders, including through use of a "virus" program.[5]

29. Personal information services: name-based data systems may be abused by unauthorized entry of names. A recent example is indicated by a petition to the PSC by the State Attorney

---

[5] Florida enacted in 1978 the first state computer crime law, establishing property rights in computer data and barring unauthorized access and alteration. Since then, most states have passed similar statutes. Increasingly, computer data, time and services have been accorded the status of property.

General concerning the inadequate protection in computer-based dating services.

30. Remote accessing to directory information: AT&T plans to offer users nationwide (and later international) access to local phone listings.

F. Signalling and Network Management Information

31. Common Channel Signalling System #7: Provides call transaction information to others, including called party with identification of name, address, and other associated data bases. Types of uses include: ICLID (incoming calling line identification) for 800 and 900 number service; CLASS (customer local area signalling service) for general users; also known as ANI and CNI (automatic or customer number identification), and 911 emergency service.

32. Central-office based information safe deposits: telephone companies are considering offering customers electronic storage space for information such as medical and financial records, which raises the potential for unauthorized access.

33. Automatic Number Identification (ANI):[6] allows identification of calling party's number. This creates a powerful tool for telecommunications-based transactions. It also permits the matching by users of calling party's other data

---

[6] Also known as Caller I.D. A comprehensive legal analysis of ANI issues is provided in Smith (1989).

records. It may reveal a caller's unlisted number to a callee. It permits selective treatment and service grade of incoming calls according to their origin. It may chill certain calls, for example, to counseling services or to journalists.

It is often asserted that ANI identification is analogous to asking for the name of a visitor before opening the door. That is correct but incomplete. An equal analogy would be to require buyers who enter a store or theater to fully identify themselves, and for such information to be kept on file as well as freely sold to others. In any event, the point is not what is most analogous to ANI, but rather what reasonable expectations and patterns of privacy in a calling transaction have evolved over time, and how they are affected. (Marx, 1989.)

On the issue of ANI, the Washington State, New Jersey, and Pennsylvania commissions have recently initiated proceedings. Washington aims to establish cost and benefits of various ANI protection options.

34. 800 and 900 numbers: provide information about incoming call numbers to subscribers.

35. Tone dialing: some toy manufacturers have run TV ads that ask small children to hold their telephone receiver to the TV set. This allows an 800-call dialling be initiated by a broadcasted dial tone-signal, with the aim to record and capture the telephone number for marketing efforts.

G. Locational Monitoring

36. Navigational systems and "tripmaster" systems: permit tracking of vehicles location and operation by driver, including speed, shifting points, idle time, etc.

37. Passive Beeper Bracelets: permits monitoring of an individual's location through phone-based equipment. Presently used for house arrest as an alternative to incarceration, but could be used for employment supervision, for social service cases, etc.

38. Key cards: in connection with communications links, permit remote tracking of movements of individuals within a building.

39. Cam-corders: in connection with a telecommunications link, highly miniaturized electronic cameras and other remote sensors permit hidden video and audio monitoring.

H. Transaction Information

40. Itemized billing: enables unauthorized persons to access the details of toll call information.[7]

---

[7] Here is how the Watergate investigators, ferreting out dirty tricks did it, in their own words: "Bernstein had several sources in the Bell System. He was always reluctant to use them to get information about calls because of the ethical questions involved in breaching the confidentiality of a person's telephone records....Without dwelling on his problem, Bernstein called a telephone company source and asked for a list of Barker's calls." Carl Bernstein and Bob Woodward, All the President's Men, Simon and Schuster, New York 1974, p. 35. See McManus (1989).

41. Hotel telephone bills: user records are largely unprotected from inspection by hotel personnel and often by other guests.

42. General telephone service: nature and details of telephone subscription can be easily ascertained and modified by unauthorized parties, with no identification required at present.

43. Deregulated billing: allows dissemination of telephone records to others, without necessarily users having knowledge.

44. Customer proprietary network information (CPNI): user transaction data provide valuable marketing data for carriers, which could also be sold to third parties.

45. Smart cards: permit storage on the card of the calls made with it. Where smart cards are used for general-purpose charging, a record of a user's consumption and telephone usage and payment and personal history could be established that would be available to a vendor (including a telecommunications carrier) at the next point-of-purchase. Where smart cards are used for government benefits, such as food stamps, they could monitor recipients' usage and movements.

## APPENDIX B: COUNTERVAILING INTERESTS TO TELECOMMUNICATIONS PRIVACY PROTECTION

It is counter-productive to the protection of privacy to engage in single-issue advocacy. There are other legitimate societal interests that must be balanced with privacy. These include:

1. Law enforcement and administrative efficiency: surveillance and electronic data collection and computer matching can be powerful tools to combat criminal or terrorist activities. Access to electronic technologies can counteract the increasing financial and technological sophistication of offenders. Governmental rights may be different from those of private parties.

2. Consumer protection: For example, itemized billing is helpful to users, even though these records may reduce privacy.

3. Economic freedom: any protection that is not based on voluntary exchange transactions may reduce the ability to offer or procure certain services and equipment features.

4. Reducing business risk: vendors or credit companies would assume less risk with greater access to records about customers, employees, and suppliers, and more immediate feedback to their marketing actions. The result could be better service, reduced losses, and lower prices.

5. Increasing the cost of information: privacy protection may raise the cost of information search, storage, and

transmission. This makes information-based transactions more expensive.

6. Efficiency and innovation: Privacy protection is not free. The cost of providing privacy protection may discourage or delay entry and new services or make them more expensive. Technology retardation may result from protection of privacy.

7. Operational ease: network operations may be affected by privacy protections. The concept of a network is based on the sharing of resources, including of information: Greater difficulty in coordinating the interaction of multiple networks may result from imposing privacy protections that limit such sharing, e.g., of computer database connections. The basic philosophy of a network arrangement is that everyone gives up a bit in order for the total system to work.

8. Freedom of the press; freedom of information; access to government records: an individual's privacy sphere may conflict with the press' desire to publish details about individual, and with the public's "right to know."[8]

9. Personal mobility: communications technologies present opportunities for much greater personal mobility (for example, through cellular telephones, or by calls automatically tracking individuals as they travel from one location to another), which

---

[8] See the 1989 U.S. Supreme Court decision in B.J.F. v. The Florida Star U.S. 109 S. Ct. 2603 (1989), in which the court declined to hold the press unreachable by actions against its truthful reporting of the public record when it violated state protections of privacy.

could be limited if the database intelligence needed for these systems would be constrained.

10. Conflicting privacy interests: privacies of several parties to a communications may clash. For example, a called party's desire to being "left alone" and be protected from harassment may conflict with a calling party's desire for anonymity.

11. Affordable basic telephone rates: revenue from new services may help keep basic rates low. If restrained or delayed by privacy protection measures, revenues that could contribute towards basic rates may not be generated.

12. National uniformity: if state-specific privacy provisions are adopted, the ability to provide nationwide services may be impaired.

13. Open networks: ONA (Open network architecture)-type unbundling provides for equal treatment of enhanced service providers competing with local exchange companies. To achieve full competitive equality, local exchange telephone companies (LECs) may have to disclose transaction and customer information to those ESPs. If such disclosure would be curtailed under privacy protection provisions, the LEC may also have to forfeit using the information at its disposal, which would be inefficient considering its economic value and ready availability.

## APPENDIX C: EXISTING STATUTORY AND PSC FRAMEWORK

### 1. Constitutional

The U.S. Constitution protects communications by an individual or business only against governmental action. Such protection does not normally exist with respect to actions by private parties such as carriers or others (though some constitutional protection theoretically may apply if "state action" is involved).

Even with respect to government, the evolution of constitutional protection has been an uneven process, especially considering that the word "privacy" does not appear in the Constitution. Until 1967, telephone wiretapping did not require a warrant. Today, for example, beeper tracking devices on public streets are permissible without warrant, though such a warrant is required if the car enters a private garage. Helicopter overflights by police of private property to take pictures are lawful. The Court test has been users' expectation of privacy. But this permits a process of erosion: the more one gets used to monitoring of calls or transactions, the less legally protected they become.

The constitutional provisions are the

- First Amendment, freedom of speech and association, individual autonomy
- Fourth Amendment, protection of persons and property against unreasonable search

- Fifth Amendment, freedom from self-incrimination
- "Penumbral or implied rights," referring to the foregoing Amendments as well as the 3rd (protection of the home), 9th (reserving right to the people), and 14th (deprivation of liberty).[9]

This has led the court to protect the following:
- not to have information regarding prescription drugs or medical procedures maintained in individually identifiable fashion.
- a right not to have membership in (controversial) organizations disclosed.
- an interest in protecting reputational dignity against libel and breach of privacy.
- Lately, in cases relating to the privacy aspects of abortions and sexual conduct, the U.S. Supreme Court has cut back on federal constitutional privacy, referring privacy to actions by legislatures (and thus also to independent regulatory agencies to which they have delegated powers).[10]

Thus, federal constitutional provisions afford only limited privacy protection with respect to government actions, and hardly

---

[9] Justice William Douglas wrote of constitutional privacy rights as found "in penumbras formed by emanations."

[10] Webster v. Reproductive Health Services, U.S. 109 S.Ct. 3040 (1989); Bowers v. Hardwick, (1987).

any with respect to private actions. Some state constitutions, though not New York's, have explicit protections of privacy that provide more protection than the U.S. Constitution, (examples: Alaska, California, Florida). This leaves most of the issues to statutory or regulatory treatment.[11] Some of these statutes are provided in the following.

2. Statutory

A. Federal

(i) Electronic Surveillance

1) Communications Act (1934) Section 605

- "No person not being authorized by the sender shall intercept any communication and divulge...the contents..."

2) Katz v. US, 389 U.S. 347 (1967), overruling Olmstead v. United States, 277 U.S. 438, (1927) established necessity of warrant and criteria of probable cause for wiretap, discussing "reasonable expectation of privacy." (Similarly, Berger v. New York (1967), overturned the New York wiretap statute as not particular enough in describing time, place or subject.)

---

[11] For example, in 1976 the U.S. Supreme court rejected a constitutional right to bank records privacy; whereupon Congress enacted the Right to Financial Privacy Act in 1978.

3) Omnibus Crime Control Act (1968), Title III

- Prohibits law enforcement agencies from using electronic surveillance of conversations except under court order. Title III permits wiretaps when: a) a warrant has been issued; b) when there is the consent of at least one party to the conversation; or c) in an emergency; d) when the President ordered it in order to protect the national security; and e) only when there are no less intrusive means.
- State laws on wiretapping are specifically allowed. A majority of the states in 1986 have such laws.[12]

4) Foreign Intelligence Surveillance Act (1978)

- Regulates electronic surveillance of US citizens, in the US, for foreign intelligence and counter-intelligence purposes.
- Note, US v. US District Court, 407 U.S. 297 (1972) -- held that warrant and probable cause requirements had to be satisfied even for national security wiretaps.

5) Privacy Protection Act (1980)

- Prohibits the search of press offices and files if there is no one in a press room who is suspected of a crime.

---

[12] In 1988, there were more court-sanctioned wiretaps in New York than in any other state. Privacy Journal, Oct. 1989, Vol. XV, No. 12, p. 3.

6) - US v. Knotts, 103 Supreme Court 1081 (1983), allows without warrant, the tracking of movements of electronic beeper location devices over public streets. However, US v. Karo, 104 Supreme Court 3296 (1984), holds that using a trailing a container into a private house by use of an electronic location beeper does violate the fourth amendment. In general, the Court has been reluctant to extend the 4th Amendment to new technological devices.

7) Electronic Communications Privacy Act (1986) [ECPA]
- Probable cause needed to obtain order to intercept non-aural communications. Overturns Smith v. Maryland, 442 U.S. 735 (1979) and determines that transactional data such as telephone toll records are private and subject to federal wiretap law restrictions.[13] Primary application is to electronic mail, cellular telephones, pagers, and data transmission.
- Generally prohibits a person or entity providing public wire or electronic communications services to divulge the contents of the communication only to the intended recipient, and to no other person. (Pen registers and "trap-and-trace" devices are included in

---

[13] See Berman & Goldman, p.22, as well as a useful general treatment of the issues and compilation of relevant statutory and case law.

the prohibition, reversing a 1978 Supreme Court decision holding that pen registers are not covered by 4th Amendment.)

- The ECPA also diminished privacy protection however, because it narrowed the Title III "content" definition to exclude information about "the existence of a communication" and the "identity of parties." Governmental access to this usage data requires a warrant but provides for no advance notice. Moreover, providers of communications services are permitted, without restriction, to reveal such usage data to any non-government entity.[14]
- The Act also broadened the grounds for government interception, and so in some ways liberalized government access.
- The Act also protects a variety of radio signals from warrantless interception by governments or by private individuals. Radio signals include those which are encrypted, transmitted through a common carrier or constitute a portion of a cellular phone call. But do not include cordless telephone conversations. Stiff penalties are specified if private interceptions are

---

[14] See Katz, pp. 357-360 for particular detail and analysis of ECPA and also the more generally the valuable analysis of electronic privacy issues.

made for illegal commercial gain (e.g. insider trading). Lighter penalties for idle eavesdroppers.

(ii) Information Privacy

1) Freedom of Information Act (1966)

- Requires public access to federal records and documents, unless specifically exempt. Two such exceptions are for "personnel and medical files and similar files" and law-enforcement files "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."
- Other exemptions for: national security information; internal agency rules; exemptions from other statutes; business information; inter & intra-agency memoranda; records of financial institutions; and oil well data.

2) Fair Credit Reporting Act (1970)

- Credit agencies must allow consumers to review credit records.
- Credit agencies can only share credit info with authorized customers.
- But "authorized" means anyone with a "legitimate business need." A recent Business Week report shows that there is little effort to screen "authorized customers."

3) Bank Secrecy Act (1970)

- Allows federal government to require financial institutions to maintain records on customers. However, access is governed by existing legal process.

4) Rowan v. Post Office Dept. (1970), upheld a federal statute which gave recipients of US mail the right to insist that their names be removed from a mailing list if they receive unsolicited mail which they find sexually offensive. The court rejected the argument that a vendor's right's include the delivery, into the home, of unsolicited material. As the court stated, "the asserted right of a mailer... stops at the outer boundary of every person's domain."

5) Crime Control Act (1973)

- State criminal justice information systems must protect privacy and security of information.

6) Equal Credit Opportunity Act (1974)

- Limits types of information that creditor can collect, including race, color, religion, sex and marital status.

7) Privacy Act (1974)

- Prohibits Federal agencies from allowing information they have gathered be used for another purpose.
- Loopholes allow sharing.
- Set up the U.S. Privacy Protection Commission.

8) Family Educational Rights and Privacy Act (1974) (Buckley Amendment)

- Requires educational records be made available to students and limits disclosure to third-parties.

9) US v. Miller (1974), Supreme Court rules 5-4 that bank customer can have no legitimate "expectation of privacy" in bank records.

10) Right To Financial Privacy Act (1978)

- Limits Federal access to customer records in banks.
- Law does not apply to state or local governments and allow exceptions for FBI and U.S. attorneys.

11) Tax Reform Act of 1976

- Tax returns and personal information collected by the IRS may not be released without individual's permission.
- Limits IRS access to some sources by requiring notice and an opportunity to challenge.

12) Electronic Funds Transfer Act (1980)

- Institutions must notify customers of third-party access to customer information on electronic funds transfers.

13) Paperwork Reduction Act (1980)

- The Office of Management and Budget (OMB) must approve federal agency efforts to collect information.

- Federal requests for information must disclose why it is requested, how it will be used and whether providing the information is voluntary or mandatory.

14) Debt Collection Act (1982)

- Requires that due process protections must be met before information on an individual's federal debt may be revealed to a private credit bureau.

15) Cable Communications Policy Act (1984)

- Restricts cable operators' collection and disclosure of personally identifiable information regarding cable service, and restricts government surveillance.

16) Computer Fraud and Abuse Act (1986) makes criminal illegal entry into computers to obtain classified information.

17) Budget Deficit Reduction Act (1984) requires states to correlate tax, medical and social security records in order to receive federal funds for welfare programs.

18) Video Privacy Protection Act (1988)

- Forbids video retailers from selling or disclosing rental records without customer consent or court order.
- Known as the "Bork bill," because Robert Bork was subject of video store revelations in 1987 by the City Paper, while a nominee for the Supreme Court.

19) Computer Matching and Privacy Protection Act (1988)

- Restricts federal agencies from using computer matching of data to verify eligibility for benefits programs or for collecting delinquent debts.

20) Employee Polygraph Protection Act (1988) prohibits lie detectors in random testing of private employees and in pre-employment screening.

21) In addition to statutory protections, there is a whole array of judicially imposed orders regarding trial and pre-trial proceedings -- including limitations on public and press access to discovery materials and hearings, or sealing of certain records -- for purposes of protecting trade secrets as well as more personal privacy interests.

B. New York State

Relevant privacy protections in New York State include the following:

1. Bill of Rights Article 1, §12 Security Against Unreasonable Searches, Seizures and Interceptions.

"The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated ..."

2. Criminal Procedure Law §700.05 Eavesdropping Warrants.

New York's prior system of eavesdropping regulation was struck down as unconstitutional in Berger v. New York, 388 U.S. 41 (1967). CPL Article 700 authorizes wiretapping and bugging

only in conformance with the Omnibus Federal Act. In determining designated offenses, there is a general two-prong test of dangerousness to life, limb or property and of punishment by more than one year of imprisonment. New York enacted a very specific designated offense list which has become subject to some recent expansions.

3. Executive Law §830 Liability for Obscenity, Defamation and Invasion of Privacy.

A cable television operator is not liable for "invasion of privacy during any program when the cable company does not originate or produce such program."

4. Civil Rights §50 Right of Privacy

The name, or picture of any living person cannot be used without consent.

5. Public Officers Law Article 6 Freedom of Information Law.

Requires public access to government records; exceptions include portions that if disclosed would constitute unwarranted invasion of personal privacy.

6. PSL§91 [Telephone and Telegraph] Adequate service; just and reasonable charges; unjust discrimination; unreasonable preference; protection of privacy.

"No telegraph corporation or telephone corporation shall sell or offer for sale any names and/or addresses of any of its customers whose listings have been omitted from the telephone company's published directory at the request of the customer."

7. Protection of Personal Privacy in Public Records Act (1984)

Assigns to the State Committee on Open Government responsibility to assure implementation, in effect establishing it as a quasi-data protection board.

8. Penal Law - Article 156 - Computer Crime.

Several provisions of the penal law address various types of computer-related crime, for example theft of service, unauthorized use falsifying business records or computer tampering (by use of destructive computer virus or other means).

9. One New York court decision has imposed limits on the Commission's powers. In the matter of the City of New York v. Public Service Commission of the State of New York, 84 Misc. 2d 1058, aff'd 53 A.D. 2d 164, aff'd 42 N.Y. 2d 916 (1976), reversed a Commission order which had required all telephone companies to notify their subscribers in advance of releasing subscriber toll records to law enforcement entities under a lawfully issued subpoena. The court held that the PSC had, in effect, attempted to create a right superior to the powers of courts and law enforcement entities without the statutory power to do so.

But the court did not address warrantless searches where, in other states, a privacy right has been found to exist.[15] And because the court was dealing with the privacy rights of individuals versus governmental authorities, it did not specifically address the respective privacy rights between private parties.[16] Subsequent legislation, (1984 amendments to PSL section 91, discussed above), addressed a subset of these issues and directed the PSC to ensure that telephone companies do not sell unpublished names and addresses of its customers. To the extent that the PSC is precluded from some efforts to protect privacy among private parties as part of assuring proper and adequate telephone service, it may want to consider if it wishes to recommend legislative action.

---

[15] See, for example, People v. Chapman, 36 Cal.3d 98 (1984), People v. Blair, 25 Cal.3d 640 (1979), People v. McKunes, 51 Cal. App.3d 487 (1975), and Commonwealth of Pennsylvania v. Thompson, 16 Phila. 525 (1987).

[16] At the time of the court decision, few of the entities were in existence which now may have access to significant transactional information about a communications user. As discussed earlier, such entities could include ESPs, resellers, videotex and database providers, packet switched networks, etc.

## APPENDIX D: GENERAL PRINCIPLES OF PRIVACY PROTECTION IN TELECOMMUNICATIONS

### A. Establishing a System of Privacy Choices

1. No privacy luddism. There should be no enforced reduction of network intelligence or capabilities to protect privacy. Instead, it should be public policy to actively establish a system of multiple software and hardware options that would assure privacy protection.

2. A multi-level approach to privacy protection:

(a) First, an adequate level of "standard privacy protection as a floor for protection. It would be part of basic network service, and no separate charge would exist to receive it. Implicit in the common carrier obligation is a notion of an acceptable quality of service; and this quality includes a privacy protection component.

(b) Second, added options of "premium privacy" protection should be available to those users and enhanced service providers who have a special demand for them, and at additional charges.

The key questions then are, for each new service:

(a) What must be the level of standard privacy protection?

(b) What added elements of premium protection should be available for user choice?

(c) What should be the charges for such premium privacy protection?

If standard protection is minimal and premium protection expensive, most users will end up unprotected. On the other hand, if standard protection is high, and the price for premium protection is kept artificially low, there may be an over-investment in privacy protection relative to its direct resource cost, and relative to the burden on some of the countervailing interests.

Conceivably, a user could also opt to have a lower level of protection than offered the standard level. Such "sub-basic privacy protection," should also be available as long as it does not compromise the privacy of third parties, and as long as its selection would result in an extra charge if resource costs are involved in the non-standard choice.

Thus, several levels of privacy protection would be available to users. Those with high demand for protection need not accept the standard one; nor must most users operate with protection needlessly strict for their purpose.

To receive the standard protection, no user action would be necessary; while for deviation (either higher or lower protection) an affirmative act of selection would be required.

3. Encouragement of privacy and security technology. Regulatory commissions, to the extent of their jurisdiction, should encourage the development and offering of privacy-enhancing service elements in hardware and software, both for standard and premium protection levels. (Examples: ONA basic

service elements (BSEs) providing high access protection; ANI service that can be switched on and off by the calling party ("ANI call-blocking") or set permanently ("electronic unlisting"); central-office blocking option for incoming calls by a party which does not identify itself; blocking option against unsolicited telemarketing; a "no-solicitation" signal available in the switch or CPE to warn-off unsolicited telemarketing phone calls; end-to-end encryption service; buffers and dummy-numbers that establish an information distance between the parties to a communication, etc.[17] Electronic unlisting must be assured. In some instances, trials of privacy-protecting technology, software, and applications should be supported by the Commission.

4. Premium privacy should pay its own way. Privacy protection enhancements beyond basic protection should be priced at a level that covers its cost. Basic protection should be priced as part of basic service with no extra charge.

---

[17] For ANI such protective options would include blocking of the caller's number, both on a per-call basis or for all calls of a subscriber who chooses such an option. The called party would receive a "P" signal indicating that the caller did not desire to identify itself, and the call would or would not be accepted according to the called party's preferences. Such preferences could also be programmed into a customer terminal or PBX, or offered as a blocking option in the switch. Another option could be a signal tone that would alert callers to the presence of a caller-identification mechanism, and permit them to terminate the call before its commencement.

5. The cost of restoring the status-quo in privacy protection should be borne by those who alter it. New services should cover the cost of significant privacy reduction from the previous status quo to other participants in a network. Suppose, for example, that a new service (such as Caller-ID) leads many subscribers who value privacy to require blocking in order to maintain their "privacy status-quo." It would seem that included in the cost of the new service should be the cost of such adjustment by existing subscribers, and that subscribers or providers to a new service would have to cover the cost of other subscribers maintaining their status-quo. On the other hand, this could make it prohibitively expensive to offer a new service or be among its first users. Furthermore, the potential usefulness of the new service to be available as an option to many must also be considered a benefit. Hence, some balance needs to be struck between the cost burden on present and future users and beneficiaries.

B. Principles of Disclosure

6. Need for privacy disclosure of jeopardies. Where tariffed services are filed with the commission, they should be accompanied by a description of the impact, if any, on privacy, and the options available to small as well as large users to protect themselves. For both tariffed and untariffed services subject to its regulation, the commission should require the

disclosure of privacy jeopardies to customers, especially to residential ones.

7. Informational symmetry. Where technically possible, non-obvious privacy jeopardies should be disclosed to a partner in communications by a network or terminal equipment signal.[18]

8. Information trusteeship. Organizations which select the carrier or other communications service for others should inform them of privacy jeopardies. The extent of the responsibility depends on the nature of the relation. There should be no monitoring, without notice, of calls that involve non-employee third parties using public networks. While this is outside the scope of our jurisdiction, it would seem reasonable for employees to expect that they should be fully informed of warrantless monitoring practices by employers that involve the telephone.

C. Principles of Non-Disclosure

9. Need-to-know; need-to-store. Offerors of regulated communications services under PSC jurisdiction should establish internal protection structures and procedures to protect

---

[18] E.g., the stationary party in a call may not be aware that it is communicating to a cellular phone and that their call is therefore subject to easy monitoring. A simple periodic beep signal programmed into cellular or bridge communications would resolve this problem.

information about users from unauthorized outsiders and insiders.

Procedures should assure that data collected in bottleneck situations should be erased as soon as not required operationally, subject to criteria of reasonableness. This includes transaction data such as billing or content information, such as voice-mail messages.

10. Information segmentation. Carriers providing gateway services should be segmented from information about what specific data or text pages are accessed by the caller. Itemized billing charges for information services should not reveal the content accessed, except by user request.

11. Privacy within interconnection. Collocation, ONA-elements, and other interconnection arrangements must be structured mindful of the privacy protections of endusers.

12. Core v. periphery The transfer of signalling information between communications providers is acceptable for the establishment of basic transmission. The more the signalling information reaches the public or unregulated service providers, the greater the expectations of disclosure and protection options (absent contractual provisions to the contrary).

D. Transaction Information

13. Joint ownership in transaction-generated information

Both parties to a telecommunications transaction subject to our jurisdiction hold property rights to information generated by the transaction. Unless the parties to the transaction have a different understanding, they are joint owners of the information generated by the transaction if they are identified in such information. Such information therefore cannot be resold to third parties without their approval.

E. Protection from Intrusion

14. The right to be left alone. To protect against unsolicited calls and facsimile transmission, network-based options must be provided. (These could include: A "no-solicitation" signal available in the switch or CPE to warn-off unsolicited phone calls; user-initiated blocking of certain prefixes assigned to telemarketers;[19] and the establishment of a market system in which telemarketers could pay telephone subscribers for access to their home and time, e.g., through a credit on their telephone bill.)

---

[19] Classification as telemarketers would be by self-selection, but telemarketers not listing themselves as such could be subject to civil legal actions for nuisance. A bill for restricting unsolicited facsimile transmission is before the New York legislature.

15. The purposeful monitoring by private parties of communications not meant for them is illegal. This merely restates the law.

16. Privacy violation is no sport. Willful computer break-ins are a serious breach of others' privacy. There should be "virus" programs and unauthorized break-ins into computers; (b) termination of telephone service to anyone convicted of such offenses during the period of conviction, and disconnection, for that period, of a telephone number where the violation originated, if the offense was or should have been known to the subscriber of that number.

## VIII. QUESTIONS TO COMMENTORS

### SECTION I. NEED FOR TELECOMMUNICATIONS PRIVACY POLICY

1. Should the commission undertake a systematic review of privacy issues?

2. What is the overall impact of a more competitive and more technologically advanced environment on telecommunications privacy protection?

### SECTION III. TELECOMMUNICATIONS SERVICES AND PRIVACY JEOPARDIES

3. What technologies can provide users options in the level of privacy protection they can choose?

4. Comment on the factual correctness of the points mentioned in Section III. Beyond those listed, what other telecommunications services or technologies may raise privacy concerns?

### SECTION IV. COUNTERVAILING INTERESTS TO TELECOMMUNICATIONS PRIVACY PROTECTION

5. Comment on the countervailing interests to privacy discussed in Section IV, and the extent to which pricing protection affects competition and new services. Beyond those listed, what other

societal interests should be balanced against the telecommunications users' interests in privacy?

**SECTION V. EXISTING STATUTORY AND PSC REGULATORY FRAMEWORK**

6. Comment on the adequacy of the existing regulatory and statutory framework discussed in Section V. Beyond those listed, what other regulations or statutes have bearing on telecommunications privacy?

**SECTION VI. PROPOSED GENERAL PRINCIPLES OF PRIVACY PROTECTION FOR THE COMMISSION**

7. Most importantly for this proceeding: Comment on the principles proposed in this section. Which of the principles set out in Section VI. are desireable? Which should be modified, and how? What additional principles should the Commission adopt? Which should be differentiated according to the category of customer (small; large)? Which should receive priority?

## APPENDIX E: SELECTED BIBLIOGRAPHY


Aumente, Jerome, New Electronic Pathways: Videotex, Teletext, and Online Databases, Newbury Park, California: Sage Publications, Inc., 1987.

Berman, J. & Goldman, J., A Federal Right of Information Privacy: The Need for Reform, Benton Foundation, 1989.

Bloustein, Edward J., "Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory," 12 Ga. L. Rev. 429 (1978).

Bok, Sissela, Secrets: On the Ethics of Concealment and Revelation, New York: Pantheon Books, 1982.

Brown, James Jr., and Gordon, Kenneth, "Economics and Telecommunications Privacy: Framework for Analysis," FCC, OPP, Working Paper, 1980.

Burnham, David, The Rise of the Computer State, New York: Random House, 1983.

Burns, Peter T., "Privacy and the Common Law: A tangled Skein Unravelling?" in Dale Givson, ed., Aspects of Privacy Law (Toronto: Butterworths, 1980), pp. 21-40.

Collingwood-Nash, Deanna and Smith, John B., Interactive Home Media and Privacy. Prepared for the Office of Policy Planning, U.S. Federal Trade Commission (Washington, DC: Collingwood Associates, Inc., January 1981).

Federal Government Information Technology: Electronic Surveillance and Civil Liberties, Washington, D.C.: U.S. Congress, Office of Technology Assessment, OTA-CIT-293, October 1985.

Flaherty, David H., ed., Privacy and Data Protection: An International Bibliography (London, U.K.: Mansell, 1984; Knowledge Industry Publications, Inc., 1984).

Flaherty, David H., Protecting Privacy in Two-Way Electronic Services, White Plains, New York: Knowledge Industry Publications, Inc., 1985.

Flaherty, David H., "The Need for an American Privacy Protection Commission," Government Information Quarterly, I, 1984, pp. 235-258.

Freedman, Warren, The Right of Privacy in the Computer Age, New York: Quorum Books, 1987.

Gardner, Sidney L. and White, Robin, "New Technology and the Right to Privacy: State Responses to Federal Inaction." A Report to the New York State Consumer Protection Board. (Unpublished draft, August 1982.)

Greenawalt, Kent and Noam, Eli, "Confidentiality Claims of Business Organizations," in Harvey J. Goldschmid, ed., Business Disclosure: Government's Need to Know 378, 1979.

Hirshleifer, Jack, "Privacy: Its Origin, Function, and Future," 9J. Legal Stud. (1980).

Hirshleifer, Jack, "The Private and Social Value of Information and the Reward to Inventive Activity," 61 Am. Econ. Rev. 561 (1971).

Hixson, R., Privacy in a Public Society, New York Oxford University Press 1987.

Katz, James, E., "U.S. telecommunications privacy policy," Telecommunications Policy, Dec. 1988.

Linowes, David E., Privacy in America: Is Your Private Life in the Public Eye, Chicago: University of Illinois Press, 1989.

Marx, Gary T., "The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures," The Social Fabric: Dimensions and Issues, James E. Short, Jr., ed., Sage Publications, Beverly Hills, CA, 1986.

Marx, Gary T., Testimony before the Pennsylvania Utility Commission, Docket No. R-891200, PPUC v. Bell of Pennsylvania, May 1989.

Marx, Gary T. and Sherizen, Sanford, "Monitoring on the Job," Technology Review, Nov./Dec. 1986, pp. 63-72.

McManus, Thomas E., "Telephone Transaction-Generated Information: Rights and Restrictions," Program of Information Resources Policy, Harvard University, August 1989. Permission to cite gratefully acknowledged.

Nadel, Mark S., "Rings of Privacy: Unsolicited telephone Calls and the Right of Privacy," 4 Yale J. on Regulation, No. 1 (Dec. 1986), pp. 99-128.

Newpert Jr., John Paul, American Express: Service That Sells, Fortune, Vol. 120, No. 12, Nov. 20, 1989, p. 82.

Noam, Eli, and Greenawalt, Kent, "Confidentiality claims of Business Organizations," in Harvey J. Goldschmid, ed., Business Disclosure: Government's Need to Know, McGraw-Hill, 1979, pp. 378-412.

Posner, Richard, The Economics of Justice, Cambridge, MA: Harvard Univ. Press, 1981, p. 272.

Presidential Privacy Protection Study Commission, Personal Privacy in an Information Society, July 1977, Gov. Printing Office, #052-003-00395-3.

Prosser, William L., "Privacy," 48 Calif. L. Rev. 383 (1960).
Roszak, T., The Cult of Information, New York Pantheon 1986.

Rule, James; McAdam, Douglas; Stearns, Linda; Uglow, David, The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies, New York: Elsevier North Holland, Inc., 1980.

Seipp, David John, The Right to Privacy in American History, Cambridge, MA: Harvard Program on Information Resources Policy, p. 78-3, 1978.

Simmel, G., "The Sociology of Secrecy and of Secret Societies," 11 Am. J. Soc. 441, 446, 450 (1906).

Smith, Glenn Chatmas, Constitutional to Give it Out?): Caller Identification Technology and the Right to Informational Privacy, 37 UCLA L.R. 145 (1989).

Smith, Robert Ellis, Compilation of State & Federal Privacy Laws, Privacy Journal, Washington, D.C. (1988)

Spence, A. Michael, Market Signaling (1974).

Toth, Victor J., "Update on Telecom Privacy and Free Speech," Washington Perspective, Sept. 1989, pp. 80-87.

Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy," 4 Harv. L. Rev. 193, 196 (1890).

Weingarten, Fred W. "Information Technology and Privacy Trends in Products and Services," in Invited Papers on Privacy: Law, Ethics, and Technology. Presented at the National Symposium on Personal Privacy and Information Technology, (Washington, DC: American Bar Association, 1982), pp. 15-26.

Westin, Alan F., "Privacy in Western Society: From the Age of Pericles to the American Republic" 44 (Report to Assn. of Bar of City of N.Y. Spec. Comm. on Sci. and Law, Feb. 15, 1965).

Westin, Alan F., Privacy and Freedom (New York: Atheneum, 1967), p. 7.

Westin, Alan F., "Home Information Systems: The Privacy Debate," Datamation, XXVIII, No. 7 (July 1982), p. 104.

Wicklein, John, Electronic Nightmare: The New Communications and Freedom (New York: The Viking Press, 1979), p. 145.