

Note: The following paper contains excerpts from the testimony of Michael C. Lamb, Chief Privacy Officer, AT&T Corp. before the House Committee on Energy and Commerce on April 3, 2001. The full testimony can be found at <http://energycommerce.house.gov/107/hearings/04032001Hearing154/Lamb234.htm>

PREPARED STATEMENT OF

MICHAEL C. LAMB

**CHIEF PRIVACY OFFICER
AT&T CORP.**

on

**“AN EXAMINATION OF EXISTING FEDERAL STATUTES
ADDRESSING INFORMATION PRIVACY”**

Before the

COMMITTEE ON ENERGY AND COMMERCE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

April 3, 2001

Thank you, Mr. Chairman. I am Michael Lamb, Chief Privacy Officer of AT&T Corporation. I applaud this Committee's examination of existing federal statutes that govern information privacy in various industry sectors.

II. The Communications Act CPNI Rules

Highlight:* The Federal Communications Commission's Section 222 opt-in rules for telephone customer proprietary network information ("CPNI") were vacated on appeal by the Court of Appeals as for violating the First Amendment.

Section 222 of the Communications Act requires telecommunications carriers to protect the confidentiality of customer proprietary network information ("CPNI"), such as the telephone numbers called by customers and the length of time of the calls. Section 222 is an example of a detailed privacy statute which gave authority to the Federal Communications Commission ("FCC") to enact even more detailed privacy rules.

Section 222 defines "CPNI" as information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. The Act excludes from the definition of CPNI several categories of information, including:

- subscriber list information such as name, address and telephone number;
- aggregate customer information from which individual customer identities have been removed; and

- data from other sources such as data from non-telecom services and data purchased from third parties.

Section 222 provides that, except with customer approval, a carrier receiving or developing CPNI by virtue of providing a telecommunications service shall use individually identifiable CPNI only to provide the type of service from which the CPNI is derived. In applying this rule, the FCC divided telecom services into three categories: local; long distance and wireless services. Under the FCC approach, long distance CPNI can be used to provide and market long distance services, but generally may not be used to market local or wireless service, for example. The FCC also ruled that when a customer purchased service in more than one category from a carrier, the CPNI rules did not prevent the carrier from dealing with the customer on the basis of the overall service relationship, even though that relationship covered multiple service categories.

The FCC decided that customer consent for the purpose of Section 222 should mean express affirmative opt-in consent given after the customer has received notice of what the customer's CPNI rights were. These consent rules, together with the FCC's other implementing rules, were vacated on appeal by the Court of Appeals. See U.S. West, Inc. v FCC, 182 F3d 1224 (10th Cir. 1999). The Court held that the FCC's requirement of an affirmative opt-in consent violated the First Amendment by restricting protected commercial speech. The FCC has not yet acted on remand from the Court, although it believes that its rules, with the exception of the affirmative opt-in consent requirement, are still in effect.

Having restricted how information may be used by a carrier, Section 222 contains no further obligation on carriers to inform customers about how

information is used and contains no restrictions on the collection of CPNI, just on its use and disclosure. There is no private right of action against carriers for violations of Section 222 and no express preemption of state laws.

III. The Cable Act

Highlight:* The Cable Act requires that providers provide various levels of choice to subscribers with respect to the use of their personally identifiable information.

As is true in the telecommunications industry, the historical commitment to consumer privacy in the cable industry is very strong. That historical commitment is bolstered by detailed privacy rules in Section 631 of the Cable Communications Policy Act of 1984, as amended by the Cable Television Consumer Protection and Competition Act of 1992 (47 U.S.C. 551, et seq.). Section 631 applies to cable services and to “other services” provided by the cable operator over cable facilities. Such “other services” arguably include not only traditional cable services but also broadband Internet service, telephony service and interactive television when these services are provided over cable facilities. As new services are provided via cable facilities, there may be some decisions about which privacy regime should apply. For example, Internet/online services offered over cable facilities are arguably subject to detailed strict Cable Act privacy rules that do not apply to other types of online services delivered via other media.

Section 631 requires cable operators to give each subscriber an annual notice concerning the personally identifiable information (“PII”) that the operator

collects. The notice must also describe how the subscribers' PII will be used and disclosed. Upon request by a subscriber, a cable operator also must give access to all PII about the subscriber that the cable operator collects and maintains.

The Cable Act generally prohibits the collection or disclosure of subscribers' PII without their prior written or electronic consent. There are, however, broad exceptions to this prior consent obligation. The exceptions include:

- the disclosure of customer names and addresses if customer notice and an opt-out opportunity is first provided and disclosure does not reveal viewing patterns or the nature of transactions performed by the customer; and
- disclosures that are "necessary to render, or conduct a legitimate business activity related to a cable service or other service provided by a cable operator."

Under the Cable Act, PII may only be disclosed to law enforcement officials pursuant to a court order. Moreover, the Act requires that such an order should only issue if the subscriber has been afforded an opportunity to appear and contest the law enforcement request for information.

A cable operator that violates the privacy protections set forth in Section 631 is subject to actual and punitive damages and to awards of attorneys' fees to prevailing plaintiffs. The statute defines "actual" damages to include liquidated damages computed at the higher of \$100 a day for each day of violation or \$1,000, whichever is higher. Thus, no actual harm arguably needs to be demonstrated to collect such "actual damages."

The broad scope of Section 631 creates certain tensions. Telephony service provided over telephone facilities is subject only to the CPNI rules set forth in Section 222 of the Communications Act. Telephony service provided by

a cable operator over cable facilities appears also to be subject to Section 631, an entirely different set of rules. Although the details of CPNI implementation are currently unclear, the now-vacated rules issued by the FCC had different consent mechanisms, different notice procedures and different use restrictions than those in Section 631.

IV. Electronic Communications Privacy Act

Highlights:* ECPA requires government agencies to get the consent of the subscriber (opt-in) before they can get access to subscriber and customer records belonging to electronic service providers.

The Electronic Communication Privacy Act of 1986 (“ECPA”), 18 U.S.C. 2510-2522; 2701; was enacted to address potential privacy issues related to the growing use of computers and other new forms of electronic communications. It added provisions to the federal criminal code that extended the prohibition against the unauthorized interception of communications to specific types of electronic communications, including e-mail, pagers, cellular telephones, voice mail, remote computing services, private communication carriers, and computer transmissions. The Act also identified situations and types of transmissions that would not be protected, most notably an employer's monitoring of employee electronic mail on the employer's system.

ECPA extended Title III privacy protections to the transmission and storage of e-mail and other digitized textual information. ECPA restricted government access to subscriber and customer records belonging to electronic service providers. Unless they have the consent of the subscriber or customer, government agencies must first secure a criminal warrant, court order, or an

authorized administrative or grand jury subpoena to access service provider records.

ECPA requires the government to give a subscriber or user fourteen days' notice before information is disclosed, but it allows delayed notice if there are exigent circumstances such as cases in which notice may: endanger the life or physical safety of an individual; lead to flight from prosecution or destruction or tampering with evidence; or otherwise seriously jeopardize an investigation. 18 U.S.C. sec. 2705(a)(2). ECPA also states that a service provider has a defense to an ECPA violation if it provides information in good faith in response to a request by an investigative or law enforcement officer in emergency situations such as immediate danger of death or serious bodily injury to any person.

Thus, law enforcement agencies have the ability to obtain subscriber information under ECPA with an appropriate court order without notifying a subscriber in advance. In contrast to ECPA, the Cable Act has no provisions that allow information to be provided to law enforcement without notice to a subscriber if such notice would threaten an investigation or that address emergency situations.

This statutory approach creates an issue when law enforcement agencies seek the contents of e-mails from broadband Internet service providers who offer their services over cable facilities – the Cable Act mandates that the subscriber be notified before information is disclosed to an agency and ECPA contemplates only that the agency obtain a court order.

While ECPA was designed to protect the content of electronic communications, it revised the definition of content to specifically exclude the

existence of the communication itself, as well as the identity of the parties involved. This means that government entities such as the Department of Justice and other law enforcement entities have a greater ability to obtain information about a subscriber's identity and about whether or not the subscriber sent or received a particular e-mail than the agencies have to obtain the contents of an e-mail itself.

Oddly, under ECPA, private parties have greater rights to obtain the contents of e-mails than law enforcement agencies. The Act requires law enforcement agencies to obtain a criminal warrant or court order whereas a private party in civil litigation can obtain such information simply by having a clerk issue a subpoena. Companies with a commitment to privacy, such as AT&T, address this situation by voluntarily committing to notify customers in advance of releasing personally identifiable information in response to a civil subpoena.

V. Telephone Consumer Protection Act

Highlight:* The TCPA is a consumer choice statute that allows consumers to ask telemarketers not to make telephone solicitations and be added to "do not call lists."

The Telephone Consumer Protection Act of 1991 (47 U.S.C. 227) ("TCPA") was created to govern telephone solicitations and give the Federal Communications Commission rulemaking authority to prescribe regulations necessary to protect residential individuals' privacy by avoiding telephone solicitations to which they object. TCPA in essence is a consumer choice statute. It allows consumers to tell companies: you may have some personal

information about me, but I have the right to restrict how you use it, at least with respect to telemarketing.

The Act, together with the FCC's implementing rules, require companies to maintain do not call lists of all individuals who have requested to be put on such lists. Unless a specific request is made, the individual's do not call request applies to the particular business making the call and not to affiliated entities. Under the FCC's rules, the do-not-call list obligations apply to the specifically-identified telephone numbers of the requesting individuals and thus do not continue to apply to all telephone numbers associated with a person's name. The do not call obligation lasts for ten years after a request is made.

The TCPA also prohibits telemarketing solicitations to consumers before 8 a.m. or after 9 p.m., local time. In addition, it bans unsolicited fax messages.

A person who has received more than one telephone call from a given company within any twelve-month period after making a do not call request may sue for a TCPA violation. The person may recover the greater of actual damages or \$500.

A company must not only establish a do not call list, but also establish a do not call policy and make that policy available on demand. It also must train telephone solicitation personnel in the existence and use of the do not call list. A company has an affirmative defense to a TCPA violation if it can show that it established and implemented, with due care, reasonable practices and procedures to effectively prevent telephone solicitations in violation of the TCPA rules.

The do not call rules have worked fairly well. The ability to rely on the affirmative defense of having reasonable TCPA compliance procedures in effect is very important for a large company such as AT&T. If a complaining individual is on AT&T's do not call list and we believe that we did not call the person, it nevertheless is hard to prove a negative when a consumer claims that we DID place a call.

The ten year prohibition in the Act is an example of a provision that may warrant re-examination in light changed circumstances, such as of the pace with which people move and change telephone numbers in today's world. Do not call lists are based on telephone numbers. If 20% of the individuals on a do not call list move and get new numbers each year, the list will be almost entirely outdated well before the ten-year restriction expires.

VI. Conclusion

AT&T operates under a number of different, and sometimes conflicting, federal statutes governing information privacy. These statutes restrict AT&T's actions in some respects and impose costs on AT&T for customer notices and other requirements. Each one of these statutes was enacted to bolster the privacy protections for individuals, a goal that AT&T whole-heartedly shares. AT&T has a strong corporate commitment to privacy, founded on our view that respecting the concerns and interests of our customers is not only the right thing to do, but it also makes good business sense. In addition, we take seriously our various statutory privacy obligations. We understand that consumers want to know how private information about them will be used and we recognize that in

the competitive marketplace we can only keep our customers happy by using such private information with integrity.

Indeed, AT&T's substantive privacy commitments for the services covered by these statutes, and for AT&T's other services, exceed the obligations set forth in these privacy statutes.

Again, I thank the Committee for the opportunity to participate in this hearing. I believe it is particularly important to understand the scope and overlaps of existing federal statutes before addressing potential changes in privacy rules. This hearing provides a valuable opportunity to discuss the practical consequences of the existing federal privacy statutes as part of a considered and thoughtful evaluation of privacy issues. AT&T looks forward to continuing to work with the Committee in its review of privacy issues.

** These Highlights were prepared by the staff of the Internet Caucus Advisory Committee .*