MIKE GODWIN
Staff Counsel
Electronic Frontier Foundation

It is helpful when reading Denning's comprehensive (if ill-considered) defense of the DOJ/FBI digital telephony initiative, to give thought to the things she omits to mention, and to the questions she does not ask. Throughout her article, Denning accepts uncritically the FBI's appraisal of the problems, in several respects:

1. Denning does not name a single case in which the difficulties supposedly created by digital telephone networks, or by the difficulty in capturing a conversation on, say, CompuServe, has led to a *failed investigation or prosecution.* (She merely refers to some unnamed cases in which wiretaps were not sought or implemented.)

2. Denning equates the costs of implementing digital wiretapping capability by communications providers with the costs of individual investigations. Since we're paying for law enforcement anyway, she argues, why not pay for this? But there is no reason to believe the costs of implementing comprehensive wiretappability on all communications services (from the Regional Bell Operating Companies to the smallest BBSs and PBXs) is at all comparable to the collective costs of the investigations in which wiretapping is authorized each year. I find it far easier to believe a fundamental change in the nation's information-services infrastructure would cost *much more* than it would cost tax-funded law-enforcement agencies to innovate in response to particular challenges posed by particular cases.

3. Her use of statistics is misleading. Denning quotes government statistics about the 7,467 state and federal wiretaps "which have thus far led to 19,259 convictions," but in itself this statistic is useless unless we know how many of these convictions *would not have occurred* had wiretaps been more difficult to implement. On this particular question, Denning is silent.

4. Like the authors of the digital telephony initiative, Denning glosses over the distinction between a) technology's making wiretaps *more difficult* and b) technology's making criminal investigations *impossible.* No one can dispute that technological advances make certain aspects of law enforcement more difficult. The invention of the automobile, for example, made it possible for criminals to commit illegal acts, then leave a jurisdiction before they were caught. And the telephone itself made it possible for criminals to conspire without being seen together—a fact that made crime deterrence and detection harder in the prewiretap era. Denning touts the digital telephony initiative as a way to "ensure" that law enforcement will maintain the ability to wiretap, in spite of the fact that history teaches us that, where technology is concerned, there are no guarantees; the mentality behind this initiative is the mentality of the Maginot line.

5. Denning accepts the misleading rhetoric of the initiative's authors. Specifically, she says the legislation will merely "clarify" service providers' responsibilities under the Wiretap Act. But this is a very odd meaning of the word "clarify," given that this proposed legislation would, among other things, allow the government to impose upon those phone companies and communications-service providers who do not build wiretapping into their systems "a civil penalty of $10,000 per day for each day in violation." By any standards other than those of Denning and other proponents of this initiative, this constitutes new government authority. If this proposal only "clarifies" providers' obligations under the 1968 Act, one shudders to imagine what Denning would classify as a genuine "expansion" of law-enforcement authority.

6. Denning neglects to mention that, for the most part, criminal investigations will be unaffected by whatever difficulties digital communications services pose. For all that wiretaps can be useful in certain kinds of investigations, for example, it is nonetheless the case that the single most useful resource in criminal investigations is the reliance on informants; the use of informants is a tactic that technological advances tend not to affect.

It is clear that Denning, whose decision a couple of years back to question the government's positions in the Craig Neidorf case helped lead to a satisfactory resolution of that case, has had what might be called "a conversation experience." Just as some religious people accept certain scriptures and doctrines on faith, Denning accepts the DOJ's and FBI's arguments uncritically. At the same time, she takes the most critical views possible of the arguments against this initiative.

In particular, Denning misrepresents the positions of many privacy advocates. She claims that privacy advocates articulate "absolutist positions," and insists that those who raise the privacy implications of the digital telephony initiative believe that "citizens have a right to absolute communications secrecy from everyone." She ignores the fact that even those who accept that wiretapping is sometimes justified under the Fourth

Amendment and the Wiretap Act may question a proposal that drastically shifts the balance of power and control to an already pervasive and powerful government.

In all the material I've seen from Denning and from the government in support of the digital telephony initiative, I have yet to see one critical acknowledgement: that the very Wiretap Act they seek to "clarify" was passed in response to an important Constitutional case, *Katz vs. United States,* 389 U.S. 347 (1967). The U.S. Supreme Court recognized in *Katz* the right to be secure in one's *private conversations* is part of the interest protected by the Fourth Amendment of the U.S. Constitution. In reaching this decision, the Court built upon the philosophy expressed by one of the foremost jurists of this century:

"The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure, and satisfaction of life is to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[1]

The point Brandeis makes—that the authors of the Constitution set out to limit the rights of the government—is particularly relevant here, when the government is seeking to expand its rights drastically. The framers recognized, as we all must recognize, that every guarantee of individual rights has a price: governments have to sacrifice some efficiency to preserve those rights. Denning talks earnestly about a "social contract" that "strikes a balance" between individual rights and government necessity. But the whole point of the Bill of Rights was to *remove* some rights from any balancing act—the framers knew that, absent some kinds of strong rights guarantees, it's invariably easy to justify a small diminution of individual rights when one is concerned about public safety.

Yet, as Benjamin Franklin once observed, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

Thus, even in the face of the best good-faith arguments Denning and the Department of Justice have to offer, I find myself compelled to side with Justice Brandeis, and with Franklin. ■

***Godwin** is a lawyer who has long been involved in computer-related civil-liberties issues.*

[1] *Olmstead vs. United States,* 227 U.S. 438, 478 (1928) (dissenting opinion).

The views and ideas expressed in this commentary do not reflect those of the EFF.

WILLIAM A. BAYSE
Assistant Director
FBI Technical Services Division

Denning is to be complimented for her thoughtful article. Those of us in law enforcement also welcome her positive comments and support for the government's digital telephony legislation and its underlying purpose of maintaining the viability of one of law enforcement's most important investigative techniques—court-ordered electronic surveillance. In her article, Denning recognizes the fundamental importance of law enforcement maintaining its ability to effectively protect the public and enforce the law through electronic surveillance. She correctly observes that court-ordered electronic surveillance is statutorily authorized only when other investigative techniques have been tried and have failed or are too dangerous. Indeed, for many types of serious and life-threatening crime, electronic surveillance is the *only* viable tool for law enforcement to use. As a sensitive investigative technique, it is used selectively and surgically.

We also share Denning's view that the proposed legislation will not impede technological advancement, create network security risks, or harm the telecommunication industry's competitiveness in the global marketplace. In short, the legislation requires industry to consider and accommodate law enforcement's electronic surveillance needs as new technologies are developed so that industry service providers can properly comply with the "assistance" court orders served on them. Denning notes that the ACLU has alleged the legislation requires industry to "dumb down" technology. However, she recognizes that in most instances the appropriate technical response of service providers to the legislation will be to make their networks, equipment, and software *smarter* through designed intercept features.

Although the digital telephony legislation does not pertain to encryption, Denning offers some thoughtful and positive suggestions as to potential means by which communications security can be enhanced while at the same time affording a methodology for law enforcement to intercept such communications in real time when authorized by court order. Like Denning, we support a balanced approach to cryptography which satisfies both the public and law enforcement. ■

MARC ROTENBERG

Director, Washington Office
Computer Professionals for Social Responsibility

In 1968 Congress gave the FBI limited authority to conduct wire surveillance. The law was based on two Supreme Court decisions which said the Fourth Amendment applies to electronic as well as physical searches. The law set out elaborate restrictions on wire surveillance. Agents seeking court permission to conduct a wiretap were required to detail the reasons for the tap, indicate who would be responsible, describe how the tap would be conducted, what efforts would be made to minimize the collection of information, and whether other investigative methods had been tried. Telephone companies were expected to assist on a case-by-case basis, but there was no expectation that systems would be designed to facilitate wire surveillance.

Congress intended that wire surveillance be difficult. It is far more intrusive than other investigative methods. As Justice Louis Brandeis wrote in an early Supreme Court opinion: "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him."[1]

Also, FBI abuse of wiretap technology was well known by the late 1960s. FBI special agent Jack Levine said in 1964: "It is a matter of common knowledge among the Bureau's agents that much of the wiretapping done by the field offices is not reported to the Bureau. This is the result of pressure for convictions. A still greater number of taps are not reported by the Bureau to the Attorney General or to the Congress."[2]

Since passage of the federal wiretap law, many more abuses have been uncovered. FBI Director J. Edgar Hoover engaged in extensive wire surveillance of civil rights leader Martin Luther King, Jr.[3] In the 1960s and 1970s the FBI used illegal wiretaps to conduct domestic surveillance on dissident groups.[4] The American public remains strongly opposed to wire surveillance.[5]

Now, the FBI has put forward a proposal to require that all communications services in the U.S. be designed to facilitate wire surveillance. The FBI would like to amend the federal wiretap law so that criminal fines will be levied against private individuals who do not design systems in accordance with FBI surveillance standards.

Denning endorses this effort and urges the FBI proposal to "wire the wires" be adopted. She argues that this legislation is necessary to curb crime, that the benefits outweigh the costs, that security problems can be readily solved, that systems designed for surveillance should be developed

LEWIS M. BRANSCOMB*

Director, Program on Science
Technology and Public Policy
Harvard's Kennedy School of Government

ANNE M. BRANSCOMB

Attorney and Author
Harvard Program on Information Resources Policy

Personal privacy, Denning rightly says, must be balanced against our collective interest in law and order through limited delegation of power to the government. Criminals abuse the rights of citizens. Unhappily, so do governments. Criminal intent is not a crime and prior restraint of speech has been judged unconstitutional in many cases. If, in spite of this, we are to reduce the rights of persons suspected of criminal intent, we must also find measures to restrain abuse by government. Denning fails to address this second goal, expressing her faith in courts to guarantee that police will obey the law. Unfortunately, this faith has been abused too many times.

Not only the FBI, but Presidents and their aides have thought themselves beyond the law. Americans remember Nixon's "enemies list." They remember Nixon ordering a cut-off of science funding to MIT because he didn't like MIT's Jerome Wiesner's opposition to the Vietnam War. (The agencies refused.) They remember Watergate, Iran-gate, and Iraq-gate. But Denning piously reassures

by U.S. companies for export, and that there is little reason to believe a law enforcement agency will misuse this capability.

Let's look at these claims more closely.

Denning repeats the claim of the FBI that methods currently used to intercept communications do not work with digital-based technologies. However, she provides no description of current intercept methods and little discussion of technical obstacles. She makes no effort to assess the specific circumstances that create obstacles to wire surveillance. She also does not discuss alternative techniques pursued by the FBI.

The Bureau has been no more forthcoming about the need for the proposal than is Denning. After the FBI failed to describe the technical basis for the proposal, CPSR sent a letter to the FBI, requesting copies of records "regarding the Bureau's decision to seek new legislative authority for wire surveillance in the digital communications networks." We were specifically interested in the reasons for the FBI proposal. Were other investigative methods considered, and if so why were they judged inadequate? We were also interested in whether the FBI had undertaken a risk assessment of the digital telephony proposal, and considered whether the plan might not in fact increase the likelihood of crime and economic damage.

The FBI responded that a search at FBI headquarters "revealed no records responsive to your request." CPSR appealed that determination and learned, not surprisingly, that the FBI does have information in its files on the wiretap plan. We are now in federal court pursuing our right under the Freedom of Information Act to obtain copies of the FBI's records.[6]

This is a dangerous way to make public policy. Other federal agencies, seeking such extensive authority would be expected to detail the circumstances that require such changes. A policy maker might well ask the FBI: "What specific problems have you encountered? What other options have you explored? Have you, or an independent agency, assessed the potential risk of this proposal?" These questions remain unanswered. Most important, the assessment provided by ACM's RISKS subscribers is almost uniformly critical of the proposal.

Denning's recitation of the FBI's assertions adds little to our understanding of the technical issues surrounding wire surveillance in the digital network or the reasons for the proposal.

It may be many months before the FBI records are disclosed to the public. In the meantime, it is worth considering whether the FBI has lost out because of network developments.

By most investigative standards, recent changes in digital communications provide great benefits to law enforcement. For example, in the old-fashioned analog network there is difficulty identifying the source of a communication. Call set-up information is not easily obtained, and when available, used only for message routing and billing purposes. That is now changing. The digital network provides far more information about callers than was previously available.[7] Phone numbers are also easily linked with reverse directories and provide much quicker access to identifying information about callers. Fax transmissions routinely display the number of the originating machine. Email typically includes the name of the user and the source machine. The digital network has produced mountains of identifying data, unimaginable in the old phone system.

Even the rare data collection is now the routine. In the digital network, call tracing is virtually instantaneous. In fact, in some states it is now

us that the government has no ill-intent.

What she proposes is a new departure from U.S. historical legal tradition. The law serves not to promote government intrusions in the life of its citizens but to limit the power of the state to do so. Our current law tells us what the government can *not* do (open mail, tap phones, and break down doors), except under court order. There is no requirement, express or implied, that telecommunications systems should make police intrusion easy.

Denning and the FBI invite us over the edge of a slippery slope. She admits as much in proposing the freedom of Americans to encrypt domestic traffic should also be limited so that government can listen in. Will Americans next be prevented from using ciphers in their letter mail, or required to use a special envelope glue only the government can open? Or even use door locks that government can open?

The NSA and the FBI have been eager to change the rules ever since Ronald Reagan's election. The NSA first tried to discredit the DES encryption algorithm (adopted as a U.S. standard at NSA's during the 1970s) in order to substitute a secret algorithm of their own design. Americans would have to get their keys from government officials. Congress would have none of it. Now, the government wants to allow DES product exports only if the key is limited to 40-bits, clearly allowing the government to break messages easily. The idea of substituting a government-invented algorithm for DES in domestic use has again been proposed by NIST at NSA urging.

Denning's assurances that tap-prone operating systems of CX switches will be immune to intrusion lacks both argument and conviction. And any crook desiring telephone privacy can avoid intrusion by using public pay phones. American industry is on the verge of offering end-to-end message security, itself a bastion against industrial espionage, embezzlement, and unscrupulous litigants. Her article fails to address this balance, and uncritically asks us to give government the power not just to listen in, but to prevent our industry from protecting the privacy and commercial interests of their customers. ■

*Branscomb served as IBM's liaison with U.S. government intelligence agencies from 1972–1986 during which time the U.S.S.R. tapped the phone transmissions of IBM for industrial espionage. IBM invented, and with NSA's encouragement, helped make the 56-bit key implementation of DES the nation's encryption standard.

available as a regular telephone service, like call waiting or speed dialing.

These changes come with great cost in privacy, and have led many to look for technical and legal measures to restore communications confidentiality.[8] But for the FBI, these developments are an investigative windfall. Messages in the digital environment now routinely provide the identifying details that were missing in the telephone tap days.

Looking at technological developments more broadly, the FBI is clearly in the driver's seat. The Bureau now runs a centralized computer system that contains records on 20 million Americans. The FBI operates a multimillion dollar genetic lab, and is planning to establish a national database with genetic data. (Why a law enforcement agency rather than the FDA is the lead government agency for genetic research should be the subject of another article.) Enhanced monitoring systems, expert systems, and innovations in forensic science have all been incorporated into the Bureau's arsenal.

Denning and the FBI are reluctant to discuss these developments. If the FBI were required to detail all of the current options for conducting investigations in the digital network, its current proposal to "wire the wires" would be viewed more skeptically, perhaps as some commentators have suggested, like the Bureau telling auto manufacturers to limit the speed of cars or (actual story) the Secret Services's current efforts to limit the performance of high-end laser printers.

Denning writes the FBI is not seeking a remote monitoring capability. She says the FBI simply wants access to the communications stream. Her interpretation of the proposal may reflect assurances she has received from the Bureau, but it doesn't square with the plain language of the bill. The FBI-drafted proposal speaks of a "government monitoring facility." A facility is a permanent installation. If the FBI did not seek legislative authority for such a facility, it should not have included the language in the proposal.

Denning says that complying with the FBI's requirements is not a problem for U.S. manufacturers, in fact it is a blessing. She says that many "other governments (many which run or oversee their nation's telecommunications networks) might desire similar features in their telecommunications systems."

Let's put this in plain English: "U.S. companies should be encouraged to develop communication products for other governments that favor wire surveillance." Which governments would most likely demand such products? The old Stasi, the secret police of East Germany, might have paid dearly for this capability. The KGB, in their glory days, would no doubt have also pushed Moscow to buy such surveillance tools.

We would have some trouble selling to the Japanese since there is a constitutional prohibition against wire surveillance in Japan. Denning's analysis suggests we view that obstacle as a trade barrier and send our diplomats off to Tokyo urging the restriction be dropped so our companies can sell surveillance software. The reason, simply stated, is they permit too much privacy.

I'd prefer U.S. firms to develop networks that are reliable and secure. I'll bet these products sell better, too.

Denning asks that we allow the chief law enforcement agency in the U.S. to set technical standards for the communications networks. She acknowledges that an appropriate balance must be struck between privacy and law enforcement, and assumes the FBI, with this new legislative authority, will strike that balance.

The computing community has recent experience with law enforcement agencies setting technical standards.[9] The National Institute of Standards and Technology (NIST) recently undertook the development of a public key cryptographic standard, but the National Security Agency "evaluated and provided candidate algorithms including the one ultimately selected by NIST."[10] Here we have a case study of what happens when an agency, with legal authority to conduct wire surveillance, is also given authority to set technical standards for communications networks.[11]

In the July 1992 issue of *Communications,* two leading cryptographers looked at the proposed Digital Signature Standard. MIT's Ron Rivest said: "It is my belief that the NIST proposals represents an attempt to install weak cryptography as a national standard, and that NIST is doing so in order to please the NSA and federal law enforcement agencies" (p. 46).

Stanford Professor Martin Hellman concluded that "NIST's actions give strong indication of favoring protection of NSA's espionage mission at the expense of American business and individual privacy" (p. 49).

The final DSS lacks robust privacy protection and is less useful than currently available commercial products. It is a good example of what the ACLU's Janlori Goldman means when she says the FBI's proposal would "dumb-down" technology.

In conclusion, wiretap law in the U.S. is intended to restrict the government, not to coerce the public. The FBI's proposal would reduce network security, create new vulner-

Wiretap law in the U.S. is intended to restrict the government, not to coerce the public. The FBI's proposal would reduce network security, create new vulnerabilities, invite abuse and diminish communications privacy.

abilities, invite abuse, and diminish communications privacy. It is a backward-looking plan that tries to freeze in place a particular investigative method that is disfavored by law and disliked by Americans.

The new Attorney General is likely to look at the FBI proposal more skeptically than do current supporters of the plan. The enforcement of law is a central goal in every democratic society. But the exercise of law enforcement is a separate matter that requires a careful assessment of methods and objectives. In her support of the wiretap plan, Denning has failed to see this distinction. ■

***Rotenberg** is also chair of the ACM Committee on Scientific Freedom and Human Rights.*

[1]*Olmstead vs. United States*, 277 U.S. 438 (1928).

[2]Fred J. Cook, The FBI Nobody Knows (MacMillan, 1964).

[3]For a history on the FBI and the investigation of Martin Luther King Jr., see David Garrow, *The FBI and Martin Luther King Jr.* (W.W. Norton 1981). See also Richard Powers's biography of Hoover, *Secrecy and Power* (The Free Press, 1987)

[4]Report of the Church Committee, Select Committee to Study Government Operations with Respect to Intelligence Activities, U.S. Senate (Report 94-755) (1975)

[5]U.S. Department of Justice Bureau of Justice Statistics, Sourcebook of Criminal Justice Statistics—1991, 208–209 ("Question: 'Everything considered, would you say that you approve or disapprove of wiretapping?'").

[6]*CPSR vs. FBI*, District Court for the District of Columbia, C.A. No. 92-2117-HHG.

[7]"Caller ID" is one example of a new, albeit controversial, phone service that arose from the development of the digital communications network. The FBI has welcomed this service, and opposed efforts to restrict its use by law enforcement.

[8]Many states have opposed Caller ID, and efforts are underway to preserve anonymity in the communications infrastructure. See, for example, David Chaum, "Achieving Electronic Privacy," *Scientific American* (Aug. 1992).

[9]The DSS proposal is described at length in the July 1992 issue of *Communications of the ACM*.

[10]Letter from Michael B. Conn, Chief, Information Policy, National Security Agency to Mitt Ratcliffe, *MacWeek*, Oct. 31, 1991.

[11]In 1989 I testified before the House Subcommittee on National Security and Legislation that the proposed agreement between NIST and the NSA to implement the Computer Security Act of 1987 was a mistake and would lead to technical standards that favored intelligence agencies over civilian needs. The development of the DSS proved my point.

RONALD L. RIVEST

Webster Professor of Computer Science

MIT Department of Electrical Engineering and Computer Science

Denning does an excellent job of reviewing the issues surrounding the question of whether we should work to preserve the ability of law enforcement agencies to tap into private communications. I would like to support Denning's attempt to introduce some clarity and rational debate. The set of issues addressed are important, and deserve our careful consideration. ☎ I would also like to encourage the search for alternative technical approaches. It seems likely there may be new approaches that achieve different balance-points between individual privacy and government abilities. Micali's "split-key cryptography," mentioned by Denning, is an excellent example of such a new approach. We desperately need to flesh out our menu of policies that are technically supportable. Otherwise, we may well settle on a policy that is far from optimal, out of ignorance of what is our true range of alternatives. ☎ My personal opinion is the current round of proposals from the law enforcement agencies are doomed to failure because they are *technically unworkable* and *politically unacceptable.* Let me elaborate.

From a technical point of view, the proposed approaches suffer from a narrow vision of our communications future, which is destined to be rich, diverse, and rapidly evolving. The whole notion of "tapping" presupposes a notion of communication that is rapidly becoming dated; a circuit-oriented real-time interactive dialogue between two people. In the future, communications are likely to be packet-based as much as circuit-oriented; are likely to be one-way as much as interactive; and are as likely to be between computers or electronic agents as between people. For example, Denning's key set-up protocol is limited because it requires that both participants be simultaneously "on-line." In the future, merely specifying the communications to be tapped may become extraordinarily complex, when messages may be routinely sent between electronic agents that migrate between various laptop (or wearable) computers in the service of a user's requests. The complexity of our communications infrastructure will continue to outpace any systematic attempt to provide a tapping capability for law enforcement. In addition, the ease with which effective cryptography can be implemented means anyone with a minimum of resources can achieve truly private communications.

My second major point is that I believe laws requiring that intercept capabilities be systematically built into our communications infrastructure will be found to be politically unacceptable to the majority of Americans. I'm sure many feel it is

better to let a few criminals get away than to put a comprehensive surveillance technology in the hands of the government. Our recent history is riddled with examples of governmental abuse of power; giving the government extensive power to monitor all private conversations would not be tolerated without the most extreme justification. The checks and balances envisioned (such as the required use of court orders) are not viewed as credible or sufficient to limit the potential abuse.

In other words, I think most Americans feel they have a basic right to a private conversation. This right was not built into the Constitution because it was a "self-evident truth" at the time. Although the ease with which telephones can be tapped has led to a period where the right to a private conversation has eroded, the availability of effective cryptography now makes the right to a private conversation once again natural and easily achievable. The "status quo" that is to be maintained is not the current one in which government access to private conversations is easily arranged, but rather the prior one in which the government's powers to intrude on the affairs of private individuals is greatly restricted. The use of cryptography can be viewed not as a threat to the status quo, but rather as a technological correction that restores the balance between individuals and their government.

Thus, I believe that mandating comprehensive "solutions" that attempt to ensure the government can access all private communications is technically unworkable and politically unacceptable. Our legitimate law-enforcement needs will have to be met by measures that are less ambitious and all-encompassing. ■

***Rivest**, along with Adi Shamir and Leonard Adleman, invented the RSA algorithm in 1978.*

ANDREW GROSSO

Assistant U.S Attorney, Boston

U.S. Dept. of Justice

The year was 1928, long before the dawn of digital networks, infrared night vision, or reconnaissance satellites. In a now famous dissenting opinion, Justice Louis D. Brandeis of the U.S. Supreme Court gave identity to the most precious right held by any citizen, that of the right to protection from governmental intrusion, or in his words, "the right to be alone—the most comprehensive of rights and the right most valued by civilized man."[1]

Our system of jurisprudence has long recognized that this right is not absolute, and must sometimes bend to other concerns, one of which is law enforcement. Thus, arrest warrants, search warrants, and wiretaps have their place in our Constitution and in our laws. However, the burden of carrying out such intrusions has always rested with the agency or person seeking the warrant or tap. The digital telephony legislation seeks to change that.

Because of advances in technology, the value of a significant investigatory tool—the wiretap—is now compromised. The legislation seeks to rescue that tool by poking holes in the security of the "common man's" privacy. Think of opaque walls built around a person's life, protecting the details accessible only to those with the means and determination, as well as the right, to make a key which will open a door through those walls. This is as it should be, if the protection of privacy is to have any meaning to the common citizen.

Instead, the legislation would shift the burden. It would require all to live within transparent walls. The value to law enforcement is obvious; it need not expend resources in order to design and make a key to open the door. The harm to the individual is enormous. In one's own mind, one can never be sure who is outside, peering from a distant hideaway, watching every move. In place of opaque walls, the legislation proposes that law enforcement and industry shall make a promise: no one shall look through those walls unless a court approves. However, the history of politics and civilizations makes it clear that promises are broken, by individuals as well as by governments. People know this.

Advances in technology are not all harmful to the goals of law enforcement. The rapist who escaped last year will be caught today because of DNA matching; the drug smuggler will be captured because of satellite surveillance; the terrorist will be identified and tracked down using an international network of computers processing megafiles of data. Law enforcement often gains from technology. It is not unreasonable to acknowledge that, sometimes, it will lose.

Our jurisprudence recognizes that in order to protect certain critical social values, some criminals will remain uncaught and unpunished. This is the price we pay for living in a nontotalitarian state. If Congress, law enforcement, and society-at-large conclude the wiretap an indispensable part of our national safety and must be preserved, then a remedy is to provide the financing which will enable law enforcement to effectively tap digital telephony. If this costs hundreds of millions of dollars, then so be it. Our nation has spent untold more in the defense of our rights in the past, and will continue to do so in the future.

It is worth the price so we, as free individuals, can be sure of being left alone. ■

[1] *Olmstead vs. United States*, 227 U.S. 438, 478 (1928) (dissenting opinion).

The views and ideas expressed in this commentary do not reflect those of the U.S. Department of Justice.

GARY T. MARX
Director, Center for the Social Study of Information Technology
University of Colorado, Boulder

Denning's fair presentation of the major issues involved in this question is useful and helps to focus the debate. She also has a clear point of view. Yet in issues as murky as this, I am reminded of Whitehead's observation: "there are no whole truths; all truths are half-truths. It is trying to treat them as whole truths that plays the devil."

I have three major concerns with the article: the implication that a cost-free solution is possible to a moral dilemma; conclusions are based on the claims of interested parties rather than on independent research; and failure to acknowledge this proposed change creates a precedent which may take us places we do not wish to go.

Folk singer Tom Rush sings about "making the best of a bad situation." That is certainly where we are in confronting this issue. Individual liberty can not be absolute, but neither can the power of government. The choice between anarchy and repression is not a happy one, wherever the balance is struck. Whatever solution is adopted there are costs. I would like to see Denning give greater attention to the clear costs and risks of legally requiring that technologies be designed to facilitate government surveillance.

Interest groups must advocate, however academicians ought to be more neutral, at least until they have adequate data. Once they have the data, their advocacy must be restrained, particularly when the case involves moral dilemmas. They must acknowledge that even with an acceptable utilitarian calculus, the choice involves competing wrongs. The dangers of automatically applied technical solutions lies in their potential for generating the self-deluding and morally numbing conclusion that a cost-free solution is possible. In my own research on undercover police practices I eventually came to adopt a supportive position, but I did so with profound moral ambivalence and extensive consideration of the dangers and protections that were needed.

I know too little about this specific issue to take a strong position. Given the absence of systematic research with clear indicators and a prioritizing of values, it is not now possible to suggest the government's ability to wiretap is all that stands between us and chaos, as some of Denning's rhetoric implies. Nor can we conclude it is the best approach, or even a necessary approach. There is much more wiretapping in the U.S. than in other industrial democracies, yet societies with strong limitations on wiretapping such as France, Germany and Japan on wiretapping do not seem greatly disadvantaged.

Certainly there are wrenching tales of horrors prevented or punished as a result of wiretapping. As numerous government commissions and researchers have shown, there are also horrible tales of the violation of liberty. An opponent could write an equally compelling article citing victims of government surveillance and abuses by telephone company employees as grounds for welcoming new restrictions on wiretapping.

Rather than argument by example or justifications from interested parties, we need careful independent research on the effectiveness, costs and risks of wiretapping. This has never been done. Such research should weigh the likely consequences of using other means, as well as of lessor and greater restrictions on wiretapping.

For example, what if the money spent on wiretapping were spent on rewards for criminal information or on drug education? What if the Fifth Amendment against self-incrimination were weakened in order to strengthen the Fourth Amendment against searches? Most European countries do not have the equivalent of our Fifth Amendment, nor do they make much use of wiretapping or undercover police practices. What would happen to the *need* for wiretapping if drugs were treated as a health rather than a criminal problem? Denning's article takes the status quo as a given and defers to government claims. Independent academics ought to be subjecting everyone's claims to critical analysis (including their own, of course).

Finally, Denning treats this as a circumscribed little technical issue with ample legal precedent. I disagree. This issue is important precisely because it introduces something qualitatively different. Once the precedent is legally and culturally established that designers and manufacturers of technology must build-in standards that facilitate surveillance, something important has changed. A change of this magnitude ought not to be treated as just another legislative proposal.

Samuel Goldwyn once said, "I never make forecasts, especially about the future." But such wisdom aside and apart from the specifics, this issue should receive extensive public scrutiny because of what it might imply for our future. If one accepts Denning's arguments, it is easy to imagine justifications for a variety of new laws to facilitate emerging forms of techno-surveillance. This might involve the outlawing of sophisticated forms of encryption and related means of protecting the security and privacy of communications, including bans on anti-bugging devices. It might require buildings be constructed with materials that do not inhibit heat-imaging, laser and satellite surveillance technologies, or that clothes be made with materials that do not inhibit night vision technology. Indeed, it might require all persons have a permanent automatic location device with a unique identifier implanted at birth. ■

***Marx** is the author of* Undercover, *(Berkeley Press, 1988) and the forthcoming* Crime and Inequality *(University of Chicago Press).*