Journal of Legislation

Volume 26 | Issue 1 Article 3

February 2015

Tyrant's Toolbox: Technology and Privacy in America;Legislative Reform Commentary

Bob Barr

LEGISLATIVE REFORM COMMENTARIES

A Tyrant's Toolbox: Technology and Privacy in America

*The Honorable Bob Barr**

I. Introduction

By its nature, the law is typically a reactive force. It responds to breaches of society's moral code, by outlawing acts that individuals commit that take away those things society values – life, property, the fruits of one's labor. As American society grew and became more complex, federal law reacted with concurrent development. Robber barons acquired monopolies and Congress passed anti-trust laws. Prohibition-era organized crime syndicates began using military weapons on the street and Congress acted to outlaw civilian ownership of such weapons. Drug dealers organized themselves into vertically-integrated distribution networks, and our government enacted laws against money laundering and continuing criminal enterprises. The list is long, and includes the numerous court decisions that have applied statutes to fact situations that were unimaginable earlier in our history or even when the laws were passed.

Generally, courts and legislatures do a good job of molding the law to contend with new factual situations. The most glaring exception to this principle, however, is our legal system's failure to create an effective mechanism for protecting privacy in the Information Age.

The universal currency of political control and economic success in 21st century America will be information. As power was measured by geographic reach of individual landowners and nations in the 19th century and by massed capital in the 20th century, power in the next century will be measured by information – its accumulation, manipulation, and use. Unfortunately, the growth of information technologies, such as e-mail, data warehousing, the Internet, surveillance systems, and personal identifiers, has far outpaced the development of a legal structure to safeguard personal information from government, criminal, or commercial abuses. Unless new protections are put in place, it is unlikely Americans will have any privacy left to protect in a few years.

As information flies across our television and computer screens, we are tempted to examine individual issues in a vacuum. Examining the threat to privacy in America as isolated attacks rather than a concerted campaign to shrink our zones of personal privacy misses the point. Only by collectively examining the many specific threats to privacy can we gain an appreciation for the magnitude of the problem we face. Furthermore, only by looking at the broad implications of information and surveillance technologies can we fashion a legal structure to protect privacy that will not be instantly outdated by next month's technological advancement.

---

* Member, U.S House of Representatives. Congressman Barr represents the 7th District of the State of Georgia in the United States House of Representatives. He received a B.A., *cum laude*, from the University of Southern California, an M.A. in International Relations from George Washington University, and a J.D. from Georgetown University Law Center.

II. Current Threats to Privacy

A. Surveillance Cameras

The number of surveillance cameras of all types in America is staggering and growing every day. Recently, the New York Civil Liberties Union sent a survey team into Manhattan to count surveillance cameras. The team counted more than 2,400 cameras monitoring the movements of pedestrians, drivers, shoppers, and anyone else who wandered into their range.[1] Of course, this figure includes only readily observable cameras. In Great Britain, the world's pioneer of closed circuit television surveillance, over one million cameras are in place. An average person in London is monitored by 300 different cameras on 30 different networks during the course of a single day.[2] Sales of security cameras will near $6 billion by 2002.[3]

Cameras have an obvious attraction to law enforcement. They don't get sick, they never sleep, and you don't have to pay them overtime. They also cost a fraction of the price required for similar coverage of an area by live officers. Currently, monitoring cameras are deployed across America to monitor public buildings, High Occupancy Vehicle lanes, subway stations, hotels, malls, airports, schools, and traffic intersections. In some jurisdictions, cameras have been used to monitor entire neighborhoods that are deemed to be "high crime" areas or heavily used streets.

Closed circuit monitoring is also attractive to employers. If a company is concerned about employees making personal phone calls at work, taking unauthorized breaks, or stealing merchandise, there are few legal impediments to the employer setting up a camera to monitor stockrooms, office cubicles, locker rooms or restrooms. Such cameras, of course, capture the images of every law-biding citizen within their range, not just the occasional scofflaw. In a recent survey of 900 companies by the American Management Association, nearly two-thirds of those surveyed admitted to using some kind of electronic surveillance to monitor their workers.[4]

The same technology also has endless marketing applications. To effectively place products on shelves and design store layouts, marketing experts need detailed information about the habits and reactions of shoppers. Numerous retail establishments have installed cameras to monitor the habits of shoppers.[5] The companies assure their customers that anonymity is protected and the tapes are not distributed. However, the reality is there are virtually no legal restrictions on how a company can monitor its customers and what it can do with the footage. So long as a person's image is not sold commercially, very few, if any, legal protections apply.

The pornography industry also makes use of surveillance cameras. In some cases, these voyeuristic "webcams," which offer live pornographic images to subscribers, prey on individuals who do not know they are being observed and have not consented to the display of sometimes compromising photographs or video on the Internet. In a recent case, a young woman in Miami was startled to learn that surreptitious photographs of her sunbathing found their way onto a half dozen such websites.[6]

---

1. Eric Brazil, *Hidden Cameras Raise Concerns*, S.F. EXAM., Feb. 7, 1999, at A1.
2. Dipesh Gadher, *Smile, You're on 300 Candid Cameras*, SUNDAY TIMES (London), Home News Section, Feb. 14, 1999.
3. Mark Boal, *Spycam City*, THE VILLAGE VOICE, Oct. 6, 1998, at 38.
4. *The Surveillance Society*, THE ECONOMIST (U.S. Edition), May 1, 1999, at 21, 22.
5. *Id.* at 22.
6. Diego Bunuel, *Caught in the Web*, SUN-SENTINEL (Fort Lauderdale, FL), Feb. 25, 1999, at 1B.

Old-fashioned peeping toms have also gone digital. A Maryland couple recently discovered their neighbor was viewing them via a secret camera installed in a bathroom vent. The initial surprise of discovering the camera was exceeded by learning the neighbor's action was not illegal in Maryland.[7]

Hidden cameras also hold attractions for some consumers and families. "Nanny cams" and "granny cams" have found their way into homes across America for monitoring the activities of child care and health care professionals who treat the elderly.[8] While the cameras can help prevent child abuse or mistreatment of elderly patients, they are not being proposed merely in the context of a legal investigation based on probable cause or reasonable suspicion, but as a 24-hour dragnet accumulating vast amounts of material on everyone, law-abiding and law-breaking, victims and non-victims alike. This dragnet use of recording devices surreptitiously records private images of patients being bathed, changed, and treated. As cameras and microphones become smaller and develop longer ranges, it is certain they will be used even more extensively.

B. Online Tracking

As more and more commercial and social activity becomes "electronic," it becomes possible to track an individual's behavior online with great precision. Such tracking of product purchases, entertainment interests, and the like, is of great attraction to retailers and entertainers who strive to target marketing efforts to the most specific population possible. Commercially, many websites make an effort to identify and track visitors to their sites. Internet service providers also often record the sites accessed by their customers.

Monitoring of online behavior is also a way to prevent electronic crimes. Along with providing numerous commercial, research, and leisure benefits, the Internet has spawned a dark underground world of hackers, child pornographers, hate groups, and con artists. In turn, many law enforcement agencies have set up special task forces to fight electronic crime. Unfortunately, such efforts go largely unmonitored.

Government and private sector entities have proposed or begun online monitoring in order to protect their own systems from hackers. Governmentally, these efforts are coordinated through the National Infrastructure Protection Center (NIPC) created not by law, but by a Presidential directive in 1998.[9] The NIPC aims to protect eight "critical" sectors of the economy – telecommunications, transportation, water, oil and gas, financial services, electricity, emergency services, and government – that have a common dependence on information systems. Proposals for actually accomplishing this task have included improving government and private sector information security, and keeping technical information secret, as well as the more troubling suggestion of monitoring online behavior to identify "anomalous" activities by profiling.[10]

An extension of the idea of protecting critical information systems with online monitoring and developing of profiles on a massive scale, was recently proposed by the Clinton Administration. In a leaked draft version of an internal memorandum, the Administration contemplates, among other things, the establishment of a massive govern-

---

7. Carl Rochelle, *Peeping Tom Goes High Tech* (last modified March 28, 1996) <http://www.cgi.cnn.com/TECH/9603/private_eyes/index.html>.

8. Deborah Sharp, *On the Watch in Nursing Homes, Coalition wants 'Granny Cams' to Protect Elderly from Neglect*, USA.TODAY, Sept. 14, 1999, at 1A.

9. White Paper on The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, available at the Critical Assurance Infrastructure Office's web page (visited Feb. 13, 2000) <http://www.ciao.ncr.gov/CIAO_Document_Library/paper598.html>.

10. James Dempsey and Mark O'Neil, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry* (visited Jul. 6, 1999) <http://www.cdt.org/policy/terrorism/oneildempseymemo.html>.

ment-private sector monitoring network, "FIDNet," that would identify "abnormal" online activity that could threaten information security. Information about those activities would then be shared with all network members.[11]

Of course, any such system has at its heart developing a profile of what constitutes "normal" activity, and identifying – and if necessary terminating – any online activity that deviates from the profile. Responding to widespread public concern stimulated by the leaked proposal, and fueled by the government's recent ham-handed effort to mandate development of customer profiles in the banking industry with proposed "Know Your Customer" regulations, Congress blocked the expenditure of $1.5 billion in the Fiscal Year 2000 budget to start FIDNet.[12] Never one to be thwarted in its work, the Administration has since responded by offering a scaled-back version of the system.[13]

It now appears a recent spate of simplistic hacker attacks on corporate websites have provided more fuel to government efforts to obtain new Internet monitoring and enforcement authority. Just as isolated terrorist incidents became the oft-repeated impetus for new authority that threatened to undermine civil liberties in the 1990s,so has "cyber-terrorism" become an all-encompassing government excuse for more money and power in 2000. Lost in the debate is the simple fact that the denial of service attacks backing these requests can be more accurately and less ominously described as "cyber-vandalism" than "cyber-terrorism." Yet, few are willing to object to requests for more government power, for fear of being labeled "soft" on terrorism." Few will ask why the full weight of federal law enforcement and intelligence powers must be brought to bear on every instance of commercial inconvenience caused by a hacker, any more than the GBI should investigate every stone thrown through the window of commercial buildings every year.

C. Domestic Law Enforcement Surveillance

Better than any other area of the criminal code, wiretapping statutes provide a model of how existing law copes – or fails to cope – with the need to balance government interests with personal privacy. Modern wiretapping statutes, while growing out of the structure allowing the interception of mail by law enforcement only in limited circumstances, afford far less protection. However, they still provide greater protection than that afforded more modern forms of electronic communication.

The law regulating communications outside the home has its roots in an 1877 Supreme Court case establishing the doctrine that "[l]etters and sealed packages ... in the mail are as fully guarded from examination and inspection ... as if they were retained by the parties forwarding them in their own domiciles."[14] This decision extended the full protection of the Fourth Amendment to postal mail.[15]

Telephone conversations, even if they originate from the home, are subject to far less significant restrictions. Wiretapping statutes allow law enforcement to tap phones for up to 30 days based on the (articulable) suspicion that a person will talk about committing a specific crime during that time.[16] Privacy is theoretically protected by the quaint notion of "minimization;" the idea that law enforcement agents can be trusted to

11. NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION (Jun. 7, 1999 Draft Version) available at the Center for Democracy & Technology's web site (visited Feb. 13, 2000) <http://www.cdt.org/policy/terrorism/fidnet/>. The site also includes updated versions of this Plan as well as commentary.

12. John Hanchette, *Looking at Growing Threats to Personal Privacy,* GANNETT NEWS SERVICE, Aug. 31, 1999.

13. Robert O'Harrow, Jr., *Computer Security Proposal is Revised,* WASH. POST, Sept. 22, 1999, at A31.

14. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

15. *Id.*

16. 18 U.S.C. § 2518 (1994).

voluntarily ignore conversations that do not pertain to the specific offense for which the warrant was issued.[17] In practice, it is difficult to say how, or whether, minimization is actually applied. Ever eager for more power and less restrictions, law enforcement in recent years has incessantly sought to expand its power to tap into phone conversations.

Recently, federal wiretap statutes were vastly expanded with the addition of new "roving" wiretap authority.[18] This significant expansion of federal wiretap authority, sought for years by the FBI and other federal law enforcement agencies, was accomplished not through hearings, legislative mark-up, floor vote, and public input. Rather, it was itself born of a covert operation with nary a hearing. The provision appeared as a surreptitious and non-germane addition to legislation authorizing foreign intelligence activities.[19] Roving wiretaps allow the government to listen in on any phone line a targeted person is likely to use, rather than allowing for a tap only on a particular phone known to be used by the person and which is the specific subject of the court-ordered tap. Prior to this change, under existing law, a roving wiretap required a showing that a person was attempting to evade a tap.[20] Now, because of the 1998 statute, law enforcement need only show the target has the capability of evading a tap by using different phones.[21] It goes without saying that anyone not under house arrest or confined to an oxygen tent is now subject to roving wiretaps.

Not surprisingly, expanding wiretap authority has been accompanied by increasing wiretap use; a sort of Parkinson's law as applied to electronic surveillance.[22] In the most recent federal wiretap report, the total number of state and federal wiretaps rose by 12 percent during a one-year period.[23] The majority of the conversations intercepted do not involve criminal conduct. In 1995, more than four out of five conversations intercepted were non-criminal, resulting in an average of 1,569 innocent conversations intercepted per wiretap.[24] From 1985 to 1995, the American Civil Liberties Union estimates more than 12 million telephone calls were tapped by law enforcement.[25]

Not satisfied with wiretaps alone, federal law enforcement agencies have successfully pushed for laws to force telecommunications companies to install and upgrade monitoring equipment in their systems to make interception by the government easier. Under the 1994 Communications Assistance to Law Enforcement Act (CALEA) – which is presently being implemented by the Federal Communications Commission – telecommunications companies are required to provide and subsidize expanded wiretapping capabilities.[26]

---

17. 18 U.S.C. § 2517 (1994).

18. Intelligence Authorization Act for 1999 § 604, Pub. L. No. 105-272, 1998 U.S.C.C.A.N. (112 Stat. 2397, 2413) (codified at 18 U.S.C. § 2518(11)(b) (Supp. IV 1998)).

19. *See generally*, Intelligence Authorization Act for 1999, Pub. L. No. 105-272, 1998 U.S.C.C.A.N. (112 Stat. 2397).

20. *See*, 18 U.S.C. § 2518(11)(b) (1994).

21. *Compare* 18 U.S.C. § 2518(11)(b) (Supp. IV 1998) *with* 18 U.S.C. § 2518(11)(b) (1994).

22. Parkinson's law states, in essence, the amount of time needed to perform a task expands in direct proportion to the amount of time allocated to perform that task.

23. 1998 WIRETAP REPORT, Administrative Office of the United States Courts, at 5 (1999).

24. Robyn Blumner, *Under Clinton, Government Is All Ears,* THE COMMERCIAL APPEAL (Memphis, TN), Aug. 11, 1996, at 5B.

25. *Big Brother in the Wires: Wiretapping in the Digital Age, ACLU Special Report* (Mar. 1998), (visited Feb. 13, 2000) <http://aclu.org/issues/cyber/wiretap_brother.html>.

26. Pub. L. No. 103-414, 108 Stat. 4279 (1995). However, CALEA provided for partial reimbursement of those costs by the federal government. *See id.* The Omnibus Consolidate Appropriations Act of 1997 arranged for those funds. *See* Pub. L. 104-208, 110 Stat. 3009 (1997) (codified at 47 U.S.C. § 1021(e) (Supp. III 1998)).

In a prescient 1927 dissent to a now-overturned Supreme Court decision allowing virtually unrestricted telephone wiretaps, Justice Louis Brandeis wrote, "[t]he progress of science in furnishing the [g]overnment with means of espionage is not likely to stop with wire-tapping."[27] This principle has been borne out in the shaky development of a wholly inadequate legal structure to protect personal e-mails from government intrusion. Despite the fact that an e-mail message bears more resemblance to postal mail than to an instantaneous telephone conversation, current law affords many fewer protections to e-mails than it does to telephone calls (which in turn have fewer protections than postal mail). For example, there is no statutory exclusionary rule blocking the use of illegally seized e-mails in trials. Moreover, there is no limit on the kind of crimes for which federal agents can obtain a warrant to monitor e-mails, even though specific enumerated crimes are required for telephonic or oral surveillance.[28]

The development of technologies such as the telephone and e-mail has seriously eroded the legal structure providing Fourth Amendment protections to private communications. Nowhere has this erosion been more starkly illustrated than in a recent proposal by the Department of Justice, which would allow federal agents to seek and obtain special secret warrants. This would give operatives the opportunity to surreptitiously enter a private home or business, disable encryption devices and engage in open-ended electronic rummaging to find computer passwords.[29] Although this provision was removed from the final version of the Cyberspace Electronic Security Act the Administration submitted to Congress, if past experience is any guide, efforts to enact it will continue vigorously behind the scenes. We have now come full circle. The development of technology protecting privacy has resulted in a government plan to substantially invade the sanctuary lying at the heart of the Fourth Amendment — our homes.

Of course, domestic law enforcement surveillance does not begin or end with wiretapping. Law enforcement, especially at the federal level, continues to push new authority to monitor and profile data on numerous consumer activities, especially financial transactions. For example, a recent proposal by the Federal Deposit Insurance Commission labeled "Know Your Customer," would have required financial institutions (banks, credit unions, savings and loans, etc.) to develop a profile for the "normal" activity of every one of their customers as well as profiles for all customers in certain groups. If the customer then made a transaction that deviated from his or her personal profile, or from that of others similarly situated, a report to law enforcement would be triggered.

Following a public response of unprecedented size against the proposal, the regulators who proposed it backed down. However, it is a virtual certainty similar proposals will continue to bubble up, so long as the federal government is charged with investigating and prosecuting financial crimes.

D. Foreign Intelligence Surveillance

Foreign intelligence surveillance occupies a legal twilight zone between domestic law enforcement and the laws governing wholly international activities, such as diplomacy and warfare. Insofar as eavesdropping activities relating to foreign intelligence are, theoretically, rarely directed against American citizens, the typical constitutional protections against unauthorized surveillance do not always apply.

---

27. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

28. Megan Connor Berton, Note, *Home Is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail,* 34 AM. CRIM. L. REV. 163, 176-77 (1996).

29. Robert O'Harrow, Jr., *Justice Dept. Pushes for Power to Unlock PC Security Systems,* WASH. POST, Aug. 20, 1999, at A01.

Generally, the types of activity classified under the rubric of foreign intelligence surveillance include activities such as taking satellite photographs of activities in other countries, listening to foreign radio or electronic traffic, or monitoring cables to and from foreign embassies. However, the rapid development of technology in recent years has largely obliterated what used to be a clear distinction between foreign and domestic surveillance. Years ago, a call from New York to Los Angeles would travel across exclusively domestic wires. Now, the same call may be relayed through one or more satellite or ground facilities, all or some of which may be "international" telecommunications networks, thereby exposing the call to surveillance by American intelligence agencies. Similarly, other communications, such as e-mail, faxes, and data transfers that begin and end in the United States may also be classified as "foreign," simply by crossing international borders at some point or points during their transmission, or by having the misfortune of being relayed over an "international" telecommunications satellite.

Another concern is that increasing cooperation between intelligence agencies of different governments may allow for sharing of information that could not be legally acquired domestically. While such cooperation may be very well intended to fight international crimes such as terrorism and money laundering, it can also be used to violate domestic constitutional guarantees guarding privacy. For example, the National Security Agency (NSA) could acquire information regarding an American citizen from a counterpart in Great Britain; or vice versa. The information could then be passed along by the NSA to other domestic recipients. Such "liaison" is an integral part of the NSA's mission pursuant and essential to its founding directive to share information on "intelligence matters with foreign governmental communications intelligence agencies."[30] It must, however, be conducted within, not outside of, the constitutional boundaries limiting surreptitious eavesdropping on U.S. persons. There are some indications such sharing of information has occurred, and it is reasonable to assume it happens far more frequently than it is reported. For example, according to former Canadian intelligence operative Mike Frost, Canadian intelligence agencies conducted surveillance of American and British citizens at the request of both sister agencies in both countries (which are not allowed to spy on their own citizens). The data collected was then passed along to the agencies that asked for it.[31]

Perhaps the largest single communications interception program in the world is the NSA's Project Echelon, which is operated in collaboration with Australia, Canada, Great Britain, and New Zealand. While the NSA refuses to confirm or deny the existence of the project, it has been documented extensively in numerous media investigations, and in reports commissioned by the European Parliament, which is concerned about both privacy and the threat of economic espionage posed by such a massive system. In fact, the 1998 European report cites a specific case in which NSA intercepts purportedly were used to scuttle an Airbus sale to Saudi Arabia (which benefitted Boeing) by exposing bribery efforts.[32]

The NSA has been reticent to discuss Project Echelon, even to the extent of fighting against providing information to Congress, based on the outlandish claim of "attorney-

30. Memorandum from President Harry S. Truman for the Secretary of State and the Secretary of Defense (Oct. 2, 1950) (on file with the National Security Agency). *See also* President Harry S. Truman, *Truman Memorandum* (visited Feb. 28, 2000) <http:// www.nsa.gov:8080/docs/efoia/released/truman.html>

31. Jason Vest, *Listening In*, THE VILLAGE VOICE, Aug. 18, 1998, at 32.

32. Scott Shane and Tom Bowman, *America's Fortress of Spies*, THE BALTIMORE SUN, Dec. 3, 1995, at 1A.

client privilege."[33] Thus, there is no official figure on the scope of its interception abilities. However, if reports by the European Parliament and others are anywhere near accurate, the system is capable of intercepting "all e-mail, telephone, and fax communications" in Europe and other countries.[34] Figures range to interception and collection of two million intercepts per hour. Currently, the NSA stores this information, sifts through it, and sends interesting items to "customers" in the U.S. and abroad. Present technology allows data transmissions to be searched for keywords; what those keywords are, from day to day or hour to hour, only the interceptors know. Additionally, it is possible to identify and isolate the phone conversations of specific speakers using voice recognition technology.[35] There is no mechanism whatsoever to require even minimal standards of reasonable suspicion.

Intelligence eavesdropping that occurs within the borders of the United States is regulated by the Foreign Intelligence Surveillance Act (FISA).[36] Under FISA, agencies are required to go to a specially constituted federal court to obtain permission to conduct domestic surveillance.[37] Additionally, the Act provides for the same kind of incoherent and largely unenforceable "minimization" requirements that plague criminal wiretap statutes.[38] Charging a panel of federal judges with insufficient background information on specific cases, and little intelligence experience, with approving foreign intelligence surveillance applications has resulted in an essentially rubber stamp process where applications are practically never denied (in the past 20 years, there has been one denial of more than 10,000 applications).[39] In fact, before FISA, CIA requests were approved by an internal panel. Testifying before Congress during the Carter Administration, then CIA Director Stansfield Turner said, "there has been no meeting of the panel at which all of the requests before it were approved."[40] Thus, it appears the creation of FISA courts may actually have resulted in fewer restrictions on the domestic surveillance activities of intelligence agencies. The use of FISA courts is also on the rise, with the number of approvals more than tripling from 1979 - 1995.[41]

When large scale foreign intelligence communications interception programs began decades ago, they took place within the context of the Cold War's essentially clear distinctions between friend and enemy and of domestic versus foreign crime. Today, the same systems are operating in an environment in which preventing money laundering, international organized crime, drug trafficking, terrorism, and industrial espionage, wherever they occur are all priorities of our intelligence agencies. In fact, however, programs like Project Echelon that tap commercial communications are far more useful for

---

33. Hon. Porter J. Goss, *Additional Views of Chairman Porter J. Goss,* INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2000, H.R. REP. No. 106-130 1st Sess. Pt. 1 (1999), *reprinted in* 1999 U.S.C.C.A.N. 304, 319.

34. Steve Wright, *An Appraisal Of The Technologies Of Political Control* 19, European Parliament Directorate General for Research, Directorate B, The STOA Programme (Jan. 6, 1998) available at <http://cryptome.org/stoa-atpc.htm>.

35. DUNCAN CAMPBELL, EUR. PARLIAMENT, DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION: AN APPRAISAL OF TECHNOLOGY FOR POLITICAL CONTROL (2000). *See also* Duncan Campbell, *Interception Capabilities 2000* (visited Feb. 28, 2000) <http:www.iptvreports.mcmail.com/stoa_cover.htm>.

36. Pub. L. No. 95-511, 92 Stat. 1783 (1980) (codified as amended in Titles 18, 47, and 50 of the U.S.C.).

37. 18 U.S.C. § 1801 et. seq. (1994).

38. *Id.*

39. PATRICK POOLE AND WAYNE MADSEN, THE PRIVACY PAPERS 11, 5 (1999).

40. JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY Ch. 10 (1983).

41. *Foreign Intelligence Surveillance Act Orders 1979-95* (visited Jul. 6, 1999) <http://www.epic.org/privacy/wiretap/stats/fisa_stats.html>.

monitoring personal and business conversations than they are for gathering intelligence-from secure military networks.

There are troubling cases long after the legendary intelligence abuses of the Nixon presidency, that indicate quite conclusively intelligence surveillance programs remain subject to abuse. During the Reagan Administration, the NSA used Echelon to intercept phone conversations between Nicaraguan officials and Democrat Congressman Michael Barnes. Those conversations were subsequently leaked to the press.[42] In 1998, a NSA contractor revealed the Echelon system was used to spy on Senator Strom Thurmond's private phone conversations, which confirmed previous reports to the Senator's office that the NSA was monitoring him.[43] Following the reports, an investigation discovered there were no significant restrictions on who could target individuals for surveillance.[44] Members of Congress actually have some small chance of exposing government surveillance directed at us. If we can be targeted, it is certain similar activities are being quietly conducted against others beneath the exposed tip of the iceberg.

E. Databases

If wiretapping, signals intelligence, surveillance cameras, and online tracking act as a massive surveillance vacuum cleaner, databases are the bag attached to it. Domestic policy goals such as preventing the employment of illegal aliens, tracking the spread of diseases, and enforcing the payment of child support, have led to a government push for larger, more closely linked databases. Fortunately, a combination of grassroots opposition, existing statutory limits, and bureaucratic incompetence, has slowed – but by no means stopped–the expansion and cross-referencing of government databases.

For example, a recent attempt by the Secret Service to build a comprehensive national anti-fraud database linking drivers license photos to names was abruptly canceled following public outcry. Before its cancellation, however, the program had already purchased the names and photographs of more than 22 million Americans from several states.[45] Even DNA has become fodder for government databases, with 43 states now operating databases storing DNA samples from convicted felons.[46] Some law enforcement officials have called for mandatory collection of DNA samples on every person arrested.[47] While these databases are powerful tools for catching repeat offenders, their use would raise significant privacy concerns if they were expanded to cover not only convicted felons, but all persons arrested or the general population.

The private sector, however, is not impeded by even those restrictions limiting government collection. Commercial compilation of personal information, chiefly for marketing purposes, has already reached record levels, and the size of private databases continues to expand exponentially. We all see the effects of such databases when, for example, we purchase a home and are instantly deluged with phone calls offering vinyl siding, security systems, lower interest loans or mortgage insurance. The same databases are used by list vending companies to target individuals for solicitation based on past products purchased, to which magazines they subscribe, or traits such as race, income, and marital status. The massive size of these databases is illustrated by the fact that one

42. Otis Port and Inka Resch, *They're Listening to Your Calls*, BUSINESS WEEK, May 31, 1999, at 110.
43. Pete Carey, *NSA Accused of Forbidden Phone Taps*, SAN JOSE MERCURY NEWS, Jul. 2, 1998, at 1A.
44. Duncan Campbell, *Somebody's Listening*, THE NEW STATESMAN & SOCIETY, Aug. 12, 1998, at 11.
45. *See supra* note 4, at 22
46. Adam Cohen, *DNA: Putting Bad Guys Away Too*, TIME, Sept. 13, 1999, at 28.
47. Joseph Perkins, *The Thought Police want to Know What You've Been Doing*, THE VENTURA COUNTY STAR (Ventura County, CA), Sept. 14, 1999, at B6.

company has a public and consumer information database covering 95% of American households.[48]

The data compiled by financial services companies, such as banks, credit card companies, and credit-reporting firms is even more extensive than that held by list vendors. Furthermore, as making and storing backup tapes of information on computer networks becomes routine, hapless computer users are frequently confronted with electronic data, such as e-mails, that they assumed were deleted. Such recovered data has become a fixture in many types of civil litigation. Similarly, images and sounds from video surveillance can now be efficiently and cheaply stored on a variety of electronic media. Gone are the days when videotapes of closed-circuit monitoring systems were recycled. Thanks to digital technology, in most cases now, the data they capture is permanently stored. Recent growth among data storage companies has been tremendous. For example, the EMC corporation, considered the market leader in data storage, has grown by 30% for nine consecutive quarters, and plans to be a $10 billion company by 2001.[49]

III. Privacy in the Future

A. Personal Identifiers

As corporate America confronts the brave new world of electronic commerce, an increasing emphasis is being placed on the establishment of mechanisms for authenticating the identity of an individual who wishes to engage in a transaction. In order for electronic commerce to move beyond simple online credit card purchases, and into more complex transactions involving contracts, financing, and the like, some form of "digital signature" mechanism is a certain development. While such a signature would make new commercial transactions possible, it also raises significant privacy concerns, because if safeguards are not built into such a system, it would create permanent electronic tracks.

Even more troubling are so-called "smart card" proposals. Assuming consumers will remain willing to sacrifice privacy for convenience, the creation of a single card or number, that bundles commercial and government transactions requiring authentication, is a likely possibility. This would be the commercial counterpart to the recently derailed federal plan to implement a national identification card system, which would have required states to develop standardized drivers licenses in order for the holder of each license to be eligible for any federal benefit, program or requirement.

Currently, most of us use many different activity-specific identifiers. We have separate identifiers for checking accounts, credit cards, drivers licenses, health insurance, video rentals, "frequent flier" programs, passports, Social Security, and practically every other program in which we participate. The result of all this fragmentation in identifiers is that firewalls are automatically built into databases because we have different identifiers for different purposes. The downside is that we are inconvenienced by carrying wallets full of cards, rather than carrying one universal card that does everything. However, this seems a small price to pay for retaining a minimal level of privacy. Ari Schwartz, of the Center for Democracy and Technology, compares the alternative to a system where everyone exchanges their key rings for one universal key that unlocks home, office, and

48. *Id.*

49. Frances Hong, *What's In Store for EMC?*, (visited Oct. 5, 1999) <http:/www.cnbc.com/ commentary>.

car.[50] Sure, you'd carry fewer keys, but do you really want to give a valet your house key?

In addition to private sector speculation, there are specific government proposals to create personal identifiers. Several years ago, a provision designed to deter the employment of illegal immigrants by linking every state drivers license to a federal Social Security number found its way, quite stealthily, into an appropriation bill.[51] In effect, this proposal would have nationalized the fragmented state drivers identification system, creating a national identification card.

While opponents of this system have succeeded in blocking its implementation so far, there is no guarantee we will always be successful in doing so. As with many privacy-reducing pieces of legislation, it was not characterized by its author as such. Rather, as is usually the case, it was presented as a necessary and limited tool to accomplish a result with which no one could easily disagree: guarding against illegal immigration by making drivers licenses harder to forge. Almost always, legislative proposals to restrict privacy are marketed by Democrats and Republicans alike, as bills to counter the drug, terrorist, or illegal immigrant threat. Moreover, such legislation is almost never proposed as a stand-alone bill, subject to hearings and open debate. More often than not, these proposals succeed because they are slipped into a larger bill, regardless of relevance, often toward the end of the congressional session.

Another federal plan calls for the establishment of a national health identifier. Proponents promise that assigning every American a permanent identifier to track personal health history will help fight disease, improve hospital care, and lower the cost of health insurance. However, even assuming this dubious argument to be true, in the process the most intimate details of our health history would be subject to the prying eyes of anyone with the legal or illegal ability to tap into the database. It is not hard to imagine that such a system would result in far fewer patients seeking treatment for potentially embarrassing problems such as mental illness, sexually transmitted diseases, or substance abuse. Furthermore, it could provide a powerful tool allowing unscrupulous insurance companies to silently deny coverage to anyone with a hint of major health problems or who possesses certain "problematic" characteristics. Although Americans assume health information enjoys legal protection, under current law, there are in fact few significant restrictions on medical data sharing.

The spectre of unique identifiers includes identifying the machines we use to engage in transactions. For example, it has been reported that Intel built an identifier into each of its new Pentium III chips. This identifier allows website operators to identify and track particular computers online. Although Intel claims to have created a mechanism for turning the identifier off, privacy advocates are justifiably dubious about software fixes for the problem.[52]

B. A Seamlessly Networked World

Today's pervasive presence of cellular telephones, laptop computers, network terminals, and palm pilots pales in comparison to the seamlessly networked world envisioned by the vanguard of technological development. Currently, these systems still exist independently. For example, your cellular telephone does not share information

50. Ari Schwartz, *Smart Cards at the Crossroads: Authenticator or Privacy Invader?*, 19 AT HOME WITH CONSUMERS December 1998, Number 3 (published by the Direct Selling Education Foundation), also available at <http://www.cdt.org/digsig/idansmartcards.shtml>.

51. Illegal Immigration Reform & Responsibility Act of 19996, H.R. 2202, 104th Cong. § 656.

52. *Privacy Advocates Letter to Intel on Pentium III*, (visited Jul. 6, 1999) <http://www.cdt.org/privacy/intel.letter.shtml>.

with your network terminal at work. The result is that failsafe universal real-time tracking of a person's activities is still only the stuff of science fiction ... but not for long.

Programs such as the Oxygen Project being developed by MIT's Laboratory for Computer Science are hard at work to turn fiction into fact. Oxygen has received tens of millions of dollars from sources as diverse as Bill Gates and the Defense Department's Advanced Research Projects Agency.[53] Oxygen hinges on two pieces of hardware: the portable Handy21 computer (which combines the functions of cellular telephone, computer, television, beeper, and radio), and the Enviro21 unit, which would be embedded in buildings and cars. The two devices would work together to create a wired world that never becomes unplugged.[54] Clearly, it would be nice to make airline reservations on a subway using a handheld computer that communicates with another computer built into the subway car, which is in turn up-linked to an airline company. The Oxygen concept would also allow for instant tele- or videoconferences between system users. However, without major safeguards, such a seamless system would eliminate any pretense of personal privacy or anonymity. The brave new world of the futuristic novel would become everyday; forever.

C. Data Searching Advances

Right now, the best protection of personal privacy in America is not any type of limit on compiling and storing data. Rather, technological limits on isolating useful information in massive databases makes possible the small degree of anonymity we have left. However, it is a certainty this will not long be the case. A top data storage executive describes the current system as an "information archipelago" where data exists in unlinked islands.[55] Now, in most cases, a user looking for data needs to have a fairly firm grasp on precisely what it is he or she is looking for and a degree of technical expertise not possessed by the average computer user or government bureaucrat. Eager to provide wider capabilities, however, data companies have made bridging these islands of data a top priority. The result will be more comprehensive search capabilities, far more understandable and useable than today, but which will further erode privacy.

Specific technologies also promise to make more information about each of us available and searchable and therefore able to be stored and manipulated. Currently, state of the art speech recognition systems are capable of pinpointing the words of a specific speaker. However, the technology has not developed to the extent that it is capable of isolating specific spoken key words. When such a capability does appear – and it will – companies and government agencies will be handed a powerful new tool for monitoring very specific activities of concern reflected in the words and phrases we utter, rather than simply tracking particular speakers. Similarly, photographic and video recognition technologies promise the ability to massively expand the utility of existing surveillance systems. Imagine the law enforcement and marketing possibilities if a database of stored footage from a camera network could be tasked to trace the movements of a particular person as they moved from camera to camera over the course of a particular day, or even the past year.

---

53. Norm Alster, *MIT Lab's Michael Dertouzos' Vision of the Future*, UPSIDE, Aug. 1999 at 116.

54. *Id.*

55. Mike Ruettgers, Remarks at the Mission Critical Computing Conference (Oct. 2, 1998) (transcript available in office of Congressman Bob Barr).

IV. Updating the Legal Structure

A. Removing Legal Impediments to Self-Protection

The best way to protect privacy is to give individuals the tools to do it themselves. With the advent of technologies that can theoretically provide unbreachable data protection, such self-protection is a real possibility. However, making their use commonplace will require a loosening of existing government mandates on such technologies.

Specifically, the development and wide availability of powerful encryption technologies promises to return anonymity to many aspects of the electronic world by allowing individuals to protect their own data from companies, criminals, or the government. Of course, the utility of encryption technology depends on its being impossible for someone else – including the government – to crack. If law enforcement and intelligence agencies continue efforts to keep encryption at "crackable" levels or lobby for back-door entrances such as key recovery or intentional flaws, the viability of encryption to protect privacy would be gutted. While the Clinton Administration has shown recent signs of belated acquiescence to demands for effective, widely-available, and affordable encryption, there are some who see this new policy as a sign that law enforcement has simply decided to work with manufacturers behind the scenes to preserve its access to encrypted information.[56] The Administration's recent submission of the Cyberspace Electronic Security Act (CESA) to Congress provides some support for this view. Alarmingly, an early draft of the document contained expansive break-in and search procedures that were much more troubling than the Administration's initial efforts to restrict encryption exports are. While this provision was dropped from the final piece of legislation the White House submitted to Congress, it is safe to presume it is far from dead in the minds of federal law enforcement.[57]

Even the U.S. Postal Service is getting into the act. Recent law enforcement efforts to force holders of anonymous mailboxes to reveal their identities to mailbox providers also strike a blow against self-protection of privacy. Undoubtedly, similar efforts will be directed at companies that provide applications allowing anonymous Internet surfing and e-mail. When those efforts come, and they will, Congress and private industry should, but probably won't, vehemently resist them for a combination of commercial and bureaucratic reasons.

B. Notification of Surveillance

Federal and state laws should be passed to require government agencies to notify the public about the existence and use of audio and visual monitoring systems. The requirement for government entities should be an absolute one. It should also be viewed as a minimal first step and not as a step giving the government a green light to invade our privacy at will so long as it notifies us first. If a government agency uses surveillance – from HOV lane cameras to sidewalk microphones – it should be required to post signs in plain view within the monitored area notifying the public about the surveillance. There is no legitimate downside to establishing such policies at the state and federal levels. The cost would be insignificant, and it would likely enhance law enforcement effort by deterring crime.

The situation in the private sector is problematic as well. In the case of public accommodations, such as restaurants, malls, and hotels, it seems quite reasonable to apply

---

56. Declan McCullagh, Decoding the Crypto Policy Change, (visited Oct. 5, 1999) <http://www.wired.com/news/politics/story/21810.html>.

57. President's Message to Congress Transmitting the Proposed "Cyberspace Electronic Security Act of 1999" 35 WEEKLY COMP. PRES. DOC. 1760-1761 (Sept. 16, 1999).

notification requirements such as those envisioned for government agencies. Private companies that routinely monitor their workers in the absence of any indication of a crime might appropriately be forced to notify workers of the surveillance. It is difficult to argue a large company should be able, for example, to surreptitiously tape activities in its bathrooms or break rooms.

Finally, we should examine laws protecting individuals from illegal use of their video or photographic image to see if there is a constitutionally and practically sound way to strengthen them. Few Americans would appreciate the surreptitious posting of their image on a commercial website, and existing laws need to be updated to prevent such deplorable conduct.

C. Consent for Data Compilation and Transfers

At the very least, the law should require government agencies to notify individuals when personal data on them is compiled. Individuals do not have the same options in dealing with government agencies that they have with the private sector. If we are unhappy with the privacy policy of the Internal Revenue Service, we do not have the option of paying our taxes elsewhere, i.e., to another agency that provides greater privacy and responsibility. Therefore, if the government wants to force us to deal with the IRS, the IRS has a responsibility to tell us what information it is compiling on us, how long that information will be recorded, and for what purposes it will be used. Although some laws, such as the Privacy Act of 1974[58] and Freedom of Information Act (FOIA)[59] aim to do this, they are either inadequate to the task, too complex for consumers to use, or apply only to federal agencies. Both these laws were drafted, debated, and passed over a generation ago, when the ability to electronically identify, collect and manipulate vast quantities of personal information was in its infancy. Neither law has been significantly considered or modified since then.

Government agencies should also be absolutely prevented from marketing or transferring information in their databases to private companies. Information given to the government is not backed by any type of consent, such as might apply to private sector transactions. For example, when we engage in an essentially mandatory transfer of personal data to the government in exchange for a drivers license, it is reasonable to demand the government to which it is surrendered not share that information without our consent to any other entity.

Conversely, media-driven proposals for government regulation of private information, such as direct mail lists, are constitutionally and practically problematic. In fact, it is likely such efforts would backfire by requiring government to track the very information proponents of "regulated privacy" are attempting to keep anonymous.

There are already some welcome signs the private sector is regulating itself, as solid, privacy protective corporate policies become a commercial asset that consumers demand, and for which many will even pay a premium. In cases where anonymity is very important, it can be specifically contracted for, giving it legal protection.

The only exception to this principle occurs in the case of particularly sensitive information, where a compelling public interest demands an explicit consent requirement before information can be shared between, and in some cases within, commercial entities. However, very few types of information fall into this category. In fact, a persuasive case can be made that such an exception should be made only for health information and particularly sensitive financial facts. Additionally, it is both necessary and appropriate to

58. Pub. L. No. 93-579, 88 Stat. 1896 (1976) (codified as amended at 5 U.S.C. § 552a (1994)).
59. Pub. L. No. 89-554, 80 Stat. 383 (1967) (codified as amended at 5 U.S.C. § 552 (1994)).

safeguard information about minors from falling into the hands of those who would use it malevolently.

The real danger lies not in private companies sharing information, but in government coercing or forcing companies into giving it such information or making it so beneficial that they do so that the companies "can't refuse." For this reason, there should be stricter limits on what the government can acquire from the private sector as well as what it can transfer to private entities. In an era in which government heavily regulates virtually every sector of our economy, businesses and companies do not have much choice when the same government that regulates them asks for information on their customers. Therefore, the law should establish firm limits on government's ability to acquire and use information on individuals "voluntarily" obtained from the private sector without a warrant.

Government mandates, such as some anti-money laundering statutes, which require companies to track the activities of their customers based on "suspicious activity," also should be examined anew.[60] In many cases, these statutes not only give the government too much information, they also allow companies to compile, use, and share more information than is necessary for legitimate business purposes. Unfortunately this appears to be something many companies willingly do, even while complaining their hands are tied because the government "made them do it." Without such mandates, consumers could demand greater privacy protections by voting with their wallets and going to other businesses. However, with the mandates, all institutions compile the same information, consumers are left with no choice, and the market cannot effectively create greater privacy protections on its own.

D. Law Enforcement Surveillance

Electronic mail should be granted explicit statutory protections above the level of a telephone call, similar to the status enjoyed by first class postal mail. In fact, e-mails are very similar to first class mail. They are sent from a specific person to another specific person or persons, and they are intended only for opening and viewing by their recipient(s). At the very least, e-mail should be protected by a statutory exclusionary rule, so that material obtained unconstitutionally can never be used in court. Furthermore, procedures should be instituted to ensure the Fourth Amendment's particularity requirement is met in searches of e-mail messages, so that law enforcement cannot engage in open-ended rummaging through private mail simply because it occurs digitally rather than on paper.

Expanded roving wiretap authority should also be curtailed so that federal agents cannot tap an entire city because there is a possibility a lawfully targeted individual might use a phone "somewhere" in that city. Current laws place far too much confidence in the good faith of federal law enforcement officials to use unnecessarily vast power in a circumspect fashion. Rather than blithely counting on good faith, our legal structure should have specific statutory provisions embodying articulated – and enforceable – limits based on reasonableness. The previous roving wiretap prerequisite of showing that a target was attempting to evade a wiretap should be reinstated.

Efforts to create online monitoring programs, such as FIDNet, that link all major private and public systems should be intensely and critically examined before they are allowed to be implemented. It is very questionable that a network of such scope and pervasiveness is truly necessary to protect an information structure that is just as vulnerable to physical destruction as it is to sexy, high-tech cyber-assaults of bureaucratic

60. *See e.g.*, 31 U.S.C. § 5318(g) (1994) (authorizing the Secretary of the Treasury to require a financial institution to report "any suspicious transaction relevant to a possible violation of a law or regulation").

fantasy. If such a system were ever necessary, it should only be implemented with foolproof privacy protection mechanisms, such as are clearly neither contemplated nor desired by current proponents in the Clinton Administration. Otherwise, the price for information security would be far too high.

In the future, efforts by federal law enforcement to unreasonably expand surveillance powers should be met with critical analysis, open hearings and debate, rather than a quick (and often secret) rubber stamp. We should oppose even more vehemently efforts to improve law enforcement and the administration of government services that would establish an all-purpose national identification card.

In the final analysis, law enforcement needs to come to the realization that surveillance is not the panacea for preventing crime and Congress must be reminded that making law enforcement's job "easier" is not the only criterion validating the enactment of provisions that rob our citizens of privacy. In fact, a persuasive argument can be made that an obsession with surveillance in both law enforcement and foreign intelligence has contributed to lower overall effectiveness by diverting resources from time-tested traditional investigative methods.

E. Foreign Intelligence Surveillance

Our foreign intelligence laws should be updated to reflect the realization that, for purposes of electronic and telephone communications, international boundaries are an insignificant and no longer relevant distinction. Current law still provides constitutional protections against unlawful surveillance based on where a call takes place. Unfortunately, international communications networks have obliterated this distinction, opening a Pandora's Box of unchecked foreign intelligence surveillance.[61]

Instead, the law should be changed to provide protections based on who participates in a communication, rather than where it takes place. Our foreign intelligence agencies should not be allowed to engage in unauthorized and unsupervised monitoring of calls clearly involving only U.S. citizens, regardless of where such calls begin, end, and travel absent compliance with constitutional guarantees found in law and court decisions. In cases in which U.S. citizens and foreign nationals are joint parties in a conversation, the law should be beefed up to require real minimization procedures to reduce the likelihood of snooping on Americans. Furthermore, tough and enforceable criminal penalties should be provided for any government employee who disseminates illegally-acquired information on American citizens. Additionally, explicit statutory firewalls are needed to prevent American intelligence agencies from improperly obtaining information from, or disseminating obtained information to, their foreign counterparts. The FISA court has proven itself so willing to grant domestic surveillance authority, that current safeguards represent no more than a minor inconvenience to intelligence agencies.

Most importantly, intelligence agencies must be forced to cooperate with oversight by Congress. There are disturbing indications efforts to fight oversight are alive and well. For example, the National Security Agency recently refused to give information to the House Permanent Select Committee on Intelligence by citing an attorney-client privilege based on the discredited and far-reaching argument that government agencies are the clients of their internal attorneys. If intelligence oversight is to mean anything, this is a fight from which Congress cannot walk away.

---

61. As a practical matter, a domestic telephonic, e-mail, or Internet transmission, is just as likely to be transmitted in whole or in part over an "international" telecommunications satellite as over a "domestic" one.

V. Conclusion

The answer to protecting privacy in an age where technological advances are faster than the development of applicable law is to legislate based on enduring principles applied to changing technologies. Currently, we are not even doing a good job of reacting to specific developments in specific technologies, a reactive approach akin to a game of Spy versus Spy in which privacy advocates will always remain a giant step behind snoops.

These principles are fairly simple. First, individuals should have access to products that allow them to communicate privately. Second, government agencies and private companies that engage in surveillance should be required to notify their targets unless they have a compelling reason not to do so and comply with constitutional safeguards. Third, government agencies and a very limited number of private companies should be barred from inappropriately obtaining or sharing private information. Finally, information about law enforcement and intelligence surveillance should be publicly available to the greatest extent possible, and all surveillance activities should be kept strictly within the boundaries of the Constitution. Of course, no new legislative steps to enact these safeguards can be taken unless the public demands them. Furthermore, Congress must strengthen its resolve and develop enough of an understanding to actually be a leader on this issue. Such, however, is a course of conduct not often observed, largely because of the prevalence of less complex issues and the necessity of taking on large, well-entrenched bureaucracies.

If we follow these principles, we will be placing the decision about privacy directly in the hands of the American people. Agencies that compile information on us without our consent or knowledge would be allowed to do so only within strict constitutional and statutory limits. Consumers would be aware of what information is being collected about them, and would have the choice of deciding for themselves how much importance to place on privacy.

If we fail to follow these principles, we will either respond piecemeal to privacy threats or ignore them entirely, guaranteeing that personal privacy will be the first and greatest casualty of the new millennium. Existing and potential massive surveillance capabilities are already radically altering our political landscape. We would be foolhardy to create more of them, institute no safeguards, and blindly trust future government officials to use them responsibly, rather than tyrannically. History and practice tells us they would not.