2004

Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations and the Media

Clifford S. Fishman
The Catholic University of America, Columbus School of Law

Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media

Clifford S. Fishman*

* Professor of Law, The Columbus School of Law, The Catholic University of America ("CUA"). B.A., University of Rochester, 1966; J.D., Columbia University Law School, 1969. The views expressed herein are my own and do not necessarily represent those of CUA, The George Washington University, or, for that matter, the National Rifle Association or the American Civil Liberties Union. I am grateful to CUA law librarian Steve Young for cheerfully and quickly fulfilling research requests, which ranged from the unusual, to the weird, to the truly bizarre, and to the editors of The George Washington Law Review for their patience and good will. I want to assure the reader that, despite this Article's occasionally grouchy and curmudgeonly tone, I am actually a reasonably pleasant and generally cheerful fellow.

"An American has no sense of privacy. He does not know what it means. There is no such thing in the country." George Bernard Shaw, Speech at New York (April 11, 1933).[1]

"I might have been a goldfish in a glass bowl for all the privacy I got." SAKI (Hector Hugh Munro), *The Innocence of Reginald, in* Reginald (1904).[2]

"Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men." AYN RAND, THE FOUNTAINHEAD (1943).[3]

Introduction

Somebody may have photographed or videotaped you today without your knowledge or consent. If you used a credit card or grocery store "bonus card," an electronic record now exists of what you bought and where you bought it; someday someone might retrieve that information and use it against you. Someone from a remote location may be reading the financial and other personal data you keep on your home computer's hard drive or may be using your computer to send spam without your knowledge. As you skim this paragraph deciding whether to keep reading, your employer might be doing the same thing to any e-mail you sent from or received at the office. A friend may be posting on the Web, for the perusal of anyone who is curious, what you said or did in what you thought was a private moment. If you insulted, crossed, or disappointed someone, or someone thinks you have done so, he or she probably can humiliate, embarrass, and inconvenience you to an extent that, except for those who have experienced it, none of us can truly imagine. Indeed, someone you never heard of might be preparing to do so; and if that happened and you are even indirectly involved in public matters, there is a pretty good chance the mass media would jump in with both feet.

The papers presented at this Symposium focus primarily on the difficulties in reconciling our demand that the government protect us from terrorists and criminals and our insistence that the government respect our right to privacy. Striking this balance is particularly challenging in light of the technological and social revolution we call the Internet, the outrages perpetrated on September 11, 2001, and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act")[4] enacted the following month. These are important issues. But the likelihood that the government will in fact use USA PA-

---

1 JOHN BARTLETT, BARTLETT'S FAMILIAR QUOTATIONS 571 (Justin Kaplan ed., 16th ed. 1992).

2 *Id.* at 610.

3 *Id.* at 717. That I quote these authors should not be taken to suggest that I align myself with their politics. (Only a schizophrenic could align himself with Rand and Shaw at the same time.)

4 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat.

TRIOT Act provisions or the Internet to intrude on your privacy is, really, quite low. The risk, for the overwhelming majority of Americans, is theoretical, not real.

On the other hand, the intrusions into privacy outlined in the first paragraph of this Article are very real, and, while very few of us will suffer the worst of them, the odds are that each of us submits to some of these intrusions, none of which come from the government, just about every day.

This Article reviews how the Internet and related developments—technological, social, and legal—have magnified the threat to privacy posed by private individuals, commercial enterprises, and the media. It offers a brief overview of the current threats to privacy from sources other than the government, and, in particular, the impact of the Internet in creating or magnifying those threats. Part I discusses the threat to privacy in general, examining how the Internet and developments in surveillance technology, in information storage and retrieval, in dissemination of information, sound, and images, and changes to the informal "social contract" that defines general standards have all endangered privacy as we know it. Part II examines the advantages these developments give to individual betrayers, grudgers,[5] and snoops, who seek to undermine the privacy of particular individuals, and to spammers, who do the same on a much broader scale. Part III reviews the ways in which corporate information gathering intrudes on privacy. Part IV looks at the role the media has played in exploiting and encouraging privacy-threatening developments. The Article ends with a not-particularly-cheerful prognosis.

I. The Threat to Privacy: In General

In considering where we are, it is useful to recall how we got here.

Respect for individual privacy has been a deeply held value throughout the history of Western civilization. We can find an early codification of the principle in *Deuteronomy* 24:10–11: "When you make a loan of any sort to your countryman, you must not enter his house to seize his pledge. You must remain outside, while the man to whom you made the loan brings the pledge out to you."[6] Some 3,000 or more years ago, at a time when "government" as we know it today did not exist, the *Torah*[7] mandated that the rich and powerful must respect the dignity and the privacy of the poor and vulnerable.[8]

272; *see* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145 (2004).

5 I have coined the word "grudgers" to mean "people who have a grudge."

6 *Deuteronomy* 24:10–11. Biblical translations are from JEWISH PUBL'N SOC'Y, TANAKH: A NEW TRANSLATION OF THE HOLY SCRIPTURES ACCORDING TO THE TRADITIONAL HEBREW TEXT (1985). The discussion in this paragraph is taken from Clifford S. Fishman, *Old Testament Justice*, 51 CATH. U. L. REV. 405 (2002), in which I sought to show that many of the fundamental principles underlying contemporary criminal law, criminal procedure, and evidence may be found in the *Torah*.

7 "*Torah*" is a Hebrew word meaning "teaching"; it is also the word used to describe the first five books of the Bible. It is in the latter sense that I use it here.

8 *See, e.g.*, *Exodus* 22:24–26.

> [24] If you lend money to My people, to the poor among you, do not act toward them as a creditor: exact no interest from them. [25] If you take your neighbor's

Although privacy has long been a deeply cherished value, it competes with powerful countervailing pressures and tendencies. First, respect for privacy cannot be so absolute that society is unable to intervene to prevent conduct harmful to others. Second, there is in most of us the desire to know that which is hidden; we like to be in on secrets. Third, many of us have a powerful urge to share such knowledge with others. (The combination of these latter two tendencies explains why gossip has always been among the most popular vices.) Fourth, there is also in some people the urge to share with the public at large information about themselves which most of us would consider private.[9] This "exhibitionist principle" threatens privacy to the extent that it alters public standards of what is acceptable and expected. Fifth, information has always had *value*: someone who knows a great deal about others can use that information to enhance his or her own standing, whether financial, social, or political.

As a practical matter, the protection of individual privacy has depended on several factors. The law played its part, but it was far from the most important. Rather, a number of practical limitations combined to protect privacy against those who snooped to satisfy curiosity or for personal gain. Among the most important were the limitations of technology, difficulties in storing and retrieving information, limited means of disseminating information, and the existence of an informal but powerful "social contract" that dictated that certain topics were off-limits to public discourse.

A. Technology

Until a century or so ago, snooping was often difficult. The would-be snoop could not see behind closed doors or hear over more than a short distance. And if the snoop did see or hear something intended to remain private, he could tell others about it, but he could not reproduce it for others to see or hear in turn. This afforded a degree of privacy even with regard to conduct in public places.

Today, of course, surveillance technology is inexpensive and ubiquitous. The ease with which a snoop can use microphones, transmitters, electronic

---

> garment in pledge, you must return it to him before the sun sets; [26] it is his only clothing, the sole covering for his skin. In what else shall he sleep? Therefore, if he cries out to Me, I will pay heed, for I am compassionate.

Id.

The rabbis of the Talmudic era derived further support for the right to privacy from the story of Balaam. Balak, the king of Moab, bribes Balaam, a local prophet, to curse the Israelites; but when Balaam looks out over the Israelite encampment, God has him say, "How fair are your tents, O Jacob, Your dwellings, O Israel!" *Numbers* 24:5.

A rabbinic gloss on this verse explains that Balaam was praising the Israelites' encampment because, out of respect for privacy, they had positioned their tents so that the entrance of no one's tent faced the entrance of another. Talmud Bavli, *Bava Batra* 60a. And while this rabbinic gloss on the verse was not intended to be a statement of historical fact—the rabbis of the *Talmud* could not possibly *know* how their ancient ancestors positioned their tents—it does show how deeply respect for privacy is embedded in Jewish law. The *Torah* and *Talmud* are not unique in this respect; similar passages, instructions, and lessons extolling and protecting personal privacy can be found in the works of most other cultures and societies.

9 *See infra* notes 41–45 and accompanying text.

receivers, key loggers, and the like to eavesdrop on verbal and written communications and hack into private files and data is discussed in a subsequent section of this Article.[10] Permanently mounted video cameras in public places—banks, building lobbies and hallways, elevators, and, recently, street corners and public squares[11]—are so common that we hardly notice them. While many of these have a legitimate and limited purpose, such as cameras at toll booths to assure that tolls are paid, the information recorded by them is susceptible to other uses or misuses.[12]

The individual videocam enthusiast is also ubiquitous, and recent advances in miniaturization and digitization will make it much easier to photograph[13] or videotape[14] others without being noticed. Some of these cameras can "see" even in the dark.[15] Every once in a while one will capture an important event, the beating of Rodney King, for example. Far more often, however, what gets taped is a man hoping not to be noticed as he tugs at his seat or crotch to undo a wedgie, or a woman unaware that her skirt is riding up in back. If they are lucky, neither will learn that the moment has been

---

10 *See infra* Part II.

11 *See, e.g.*, GAO, EXECUTIVE OFFICE OF THE PRESIDENT, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. (2003); Welling Savo, *They're Watching You*, BOSTON MAG., Sept. 2003, at 120, 122 (relating that various traffic and highway authorities in Massachusetts have or soon will have 1232 cameras monitoring state roads, airports, and subway and commuter rail facilities; and noting that there are "at least 128 surveillance cameras in Boston's tightly packed Financial District," and probably many times that, mostly on private property).

12 *See* Savo, *supra* note 11, at 173 (reporting that, in 2002, prosecutors subpoenaed photographs automatically taken at a particular turnpike exit's Fast Lane on the night and in the vicinity that a murder was committed; despite the fact that the turnpike authority promised Fast Lane subscribers that the photographs would be used only for turnpike purposes, a judge upheld the subpoena, concluding, quite reasonably, that it would be absurd to permit a turnpike agency's privacy policies to trump a murder investigation).

13 Digital cameras in cell phones present particularly acute issues. *See, e.g.*, Simon J. Nadel, *In a Flash, Cell Phones with Cameras Can Develop into Major Employer Concern*, 72 U.S.L.W. 2307 (2003) (relating worries that an employee could use a cell phone camera to photograph trade secrets and post them immediately on the Internet, too quickly for the victim to obtain an injunction, or to photograph coworkers and supervisors in unflattering settings or contexts); Kamahria Hopkins, *Cameras Are More Candid at Gyms: Health Clubs Are on Guard for Cell Phone Pictures Snapped in the Locker Room*, OMAHA WORLD HERALD, Nov. 12, 2003, at 1; John Keilman, *Gym Users Back Ban on Cell Phones*, CHI. TRIB., Nov. 15, 2003, § 1, at 18.

14 On November 6, 2003, the *New York Times* reported that Panasonic and Gateway are now marketing completely digitized camcorders that are roughly the size of a bar of soap. One offers excellent visual quality but can be used for only ten minutes before the images have to be offloaded or recorded over; the other lacks a zoom lens and the images it produces are of much poorer quality. But as the article's author points out, "[T]hese first incarnations make it clear that the concept can work. . . . [Y]ou can stuff a camcorder in your pocket along with your keys, and videos can be as convenient to capture as stills." David Pogue, *Camcorders with Tape? How Quaint*, N.Y. TIMES, Nov. 6, 2003, at G1. And on November 21, 2003, the *New York Times* reported on experiments that may someday lead to the development of "molecular-sized circuits, the smallest possible." Kenneth Chang, *Smaller Computer Chips Built Using DNA as Template*, N.Y. TIMES, Nov. 21, 2003, at A22. Israeli scientists are using "strands of DNA, the computer code of life, to create tiny transistors that can literally build themselves." *Id.*

15 *See, e.g.*, Robert Irwin, *What's New in Camcorders*, CAMCORDER & COMPUTER VIDEO, Nov. 2003, at 26, 26 (describing the features of camcorders now on the market, many of which include "the ability to 'see' in total darkness").

recorded. If they are unlucky, they will appear on *Funniest Home Videos* or the like.

Even though the law says that conduct a person knowingly exposes to the public is not *legally* protected,[16] as a practical matter, until recently we still enjoyed substantial privacy even in public because it was unlikely anyone would see or notice what we did; and even if someone did see and notice, the witness had no hard proof. That once-comfortable assumption is no longer one on which we can rely.

Moreover, public electronic visual surveillance may soon be enhanced by biometrics—the ability of machines to read our physical features and identify us from those features. To date, biometric technology has proven useful in controlled situations.[17] Finger scan,[18] hand geometry,[19] retina scan,[20] iris scan,[21] and voice recognition technology[22] have proven useful in confirming the identities of employees, welfare recipients,[23] and persons with access to secured areas and may soon be employed as an immigration control measure.[24] Each of these current or proposed uses of such technology appears to be justified by the benefits that the government agency or private employer derives from use of the technology. These legitimate uses nevertheless make inroads into privacy by affirming identities and making a reliable and easily retrieved record of who-was-where-when. The tendency for employers and others to collect and store data simply because they can may prompt them to require or encourage submission to such technology under

---

16 "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz v. United States, 389 U.S. 347, 351 (1967). Nor is there usually a civil remedy; courts generally require a substantial showing of malice before photographing or videotaping public conduct is actionable. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 272 (2002). Furthermore, only one state has any statutory regulation of such surveillance. *Id.* at 235.

17 Robyn Moo-Young, Note, *"Eyeing" the Future: Surviving the Criticisms of Biometric Authentication*, 5 N.C. BANKING INST. 421, 421–22 (2001).

18 SALIL PRABHAKAR, INT'L BIOMETIC GROUP, FINGERPRINT MATCHING, *at* http://biometrics.cse.msu.edu/fingerprint.html (last visited Aug. 2, 2004).

19 Shaila K. Dewan, *Elementary, Watson: Scan a Palm, Find a Clue*, N.Y. TIMES, Nov. 21, 2003, at A1 (reporting an increased use of palm print databases by law enforcement officials); INT'L BIOMETRIC GROUP, HAND SCAN PROJECTS AND APPLICATIONS (on file with The George Washington Law Review).

20 INT'L BIOMETRIC GROUP, RETINA SCAN TECHNOLOGY (on file with The George Washington Law Review).

21 INT'L BIOMETRIC GROUP, IRIS RECOGNITION: THE TECHNOLOGY (on file with The George Washington Law Review).

22 *See* Moo-Young, *supra* note 17, at 435.

23 James J. Killerlane, III, Note, *Finger Imaging: A 21st Century Solution to Welfare Fraud at Our Fingertips*, 22 FORDHAM URB. L.J. 1327, 1329–30 (1995).

24 *See* Jennifer B. Lee, *The Art and Craft of Security: Passports and Visas to Add High-Tech Identity Features*, N.Y. TIMES, Aug. 24, 2003, at A26; Anitha Reddy, *U.S. Readies Program to Track Visas*, WASH. POST, Sept. 29, 2003, at E1 (reporting a new program, expected to cost between $3 billion and $10 billion, to photograph and finger-scan visa applicants in their home country and check their identities against databases of suspected terrorists); *see also* Philip Shenon, *New Passport Rules to Fight Terrorism Are Put Off for a Year*, N.Y. TIMES, Sept. 9, 2003, at A20.

circumstances where the benefits to society do not compensate for the diminution of individual privacy.[25]

The threat to privacy in public is likely to increase considerably in the near future. Three years ago, articles appeared in the press that Tampa police would use facial recognition technology at Super Bowl XXXV.[26] Cameras would scan the facial geometry of people in the crowd and compare each face to those stored in a database.[27] Despite the publicity, the actual intrusion into privacy appeared to be minor; no record was kept of faces that were scanned, and after more than two years of use, the program was dropped without a single successful identification or arrest attributed to it.[28] If such technology is perfected, however, its impact on personal privacy would be substantial, particularly if it becomes available to private industry and private individuals.

Nor can we assume that we are surveillance-free even in an office, home, or other private place. Sophisticated video cameras can now be hidden in light fixtures, stuffed animals, or even in pinholes in walls. Worse still, the law offers little protection or solace to those whose privacy is violated by such surveillance.[29]

B. Information Storage and Retrieval

Imagine it is 1970. Person X has been targeted for surveillance. Each individual with whom person X interacts learns something about him—the food he buys, the books he reads, how often he is late to work or takes a day of sick leave, whether he is a generous or stingy tipper in restaurants. Recording and storing such information, however, is laborious. It may be difficult and time-consuming for an investigator to develop a reasonably comprehensive list of those with whom person X interacts.[30] Moreover, even

---

25 The otherwise forgettable movie *Minority Report* includes a vivid scene in which Tom Cruise's character is walking through a mall. MINORITY REPORT (Twentieth Century Fox & Dreamworks 2002). Each billboard he passes reads his retinas and addresses him by name as it tries to sell him a product or service. *Id.*

26 *See, e.g.*, Peter Slevin, *Police Video Cameras Taped Football Fans: Super Bowl Surveillance Stirs Debate*, WASH. POST, Feb. 1, 2001, at A1; *see generally* JOHN D. WOODWARD, JR., RAND ARROYO CTR., SUPER BOWL SURVEILLANCE: FACING UP TO BIOMETRICS (2001).

27 INT'L BIOMETRIC GROUP, FACIAL SCAN TECHNOLOGY: HOW IT WORKS, *at* http://www.facial-scan.com/facial-scan_technology.htm (last visited Aug. 2, 2004).

28 Audrey Hudson, *Tampa Cops End Camera Program: High-Tech System Produced No Hits*, WASH. TIMES, Aug. 21, 2003, at A1.

29 It is worth comparing the law governing video surveillance with that governing surveillance of communications. An elaborate federal statutory structure exists regulating government surveillance of communications and protecting them from unauthorized private surveillance. *See generally* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING (2d ed. 1995 & Supp. 2004). For a concise overview, see Patricia Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375 (2004). By contrast, no federal statute generally regulates video surveillance. Thus, to install a camera which does not capture conversations requires only a search warrant, rather than a much more demanding communications interception order. *See* FISHMAN & MCKENNA, *supra*, § 29:20(b). Nor does the use of such a camera by a private party violate federal or most state laws governing electronic surveillance. *Id.* § 2:41(h).

30 The degree of difficulty would vary, of course, depending on whether the target of the surveillance lived in a small town, a suburb, or a large city.

assuming those whom the investigator contacts are willing to share their information about person X, they might not be able to remember it. In sum, the fact that such information about person X is scattered about and haphazardly kept and maintained constitutes a substantial practical defense of person X's privacy.

Consider a similar investigation today. Computers gather, store, and offer instant retrieval of huge quantities of information about us. A great deal of information about most people is lawfully available online.[31] Someone who gains access to our credit card bills instantly knows where we shop, where we eat, and a lot about what we do for recreation. Using a supermarket or pharmacy "customer bonus card" permits the store to keep a detailed record of every purchase we make.[32] Every e-mail we send or receive and every click of the mouse while we surf the Web is electronically stored and is, therefore, potentially available to a hacker.

At present, so far as we know, there is no central depository where all of this information is kept. Although a government agency recently proposed assembling such a database, the proposal was quickly rejected by Congress.[33] Still, controllers of these databases are restrained only by promises not to reveal the information and fear of adverse publicity if they do share it. Even if each compiler of information steadfastly refuses to share the information with others, the information may be legally accessible to anyone with a superficially plausible reason to subpoena it.[34]

---

31 *See* John Schwartz & Jonathan Glater, *L.A. Confidential: In Land of Big-Budget Egos, Private Investigators Are a Part of Life*, N.Y. TIMES, Dec. 8, 2003, at C1.

The tool kit for private investigators has expanded with the growth of the Internet and the assembly of online databases of personal information. Data that might once have been inaccessible, or illegal to obtain, can be found "if you intelligently search and mine what is available through the Internet and some of the other online sources," said a retired F.B.I. agent who now runs a private investigation agency in New York City. *Id.* Previously, "you used the gumshoe techniques" before trying any fancy technology. *Id.* Now, he said, the best investigators start their queries at their desks, online. *Id.*

32 *See infra* Part III.C.

33 In 2003, information emerged that the Defense Department's Defense Advanced Research Projects Agency ("DARPA") was working on software that could search the computerized travel, credit, medical, and other records of individuals for information that might reveal preparations for acts of terrorism. Carl Hulse, *Congress Shuts Pentagon Unit over Privacy*, N.Y. TIMES, Sept. 26, 2003, at A20. The project was originally designated the "Total Information Awareness Program," a title that pretty much guaranteed skepticism across the political spectrum. *See id.* Congressional concern about the program was heightened by the fact that the DARPA director responsible for development of the program was retired Admiral John M. Poindexter, who had been significantly involved in the Iran-Contra scandal and who had been accused of lying to Congress. *Id.*; *see* David Corn, *Iran/Contra Rehab*, NATION, Mar. 11, 2002, at 4. A change of name to "Terrorist Information Awareness Program" was insufficient to save the program; Poindexter resigned and the Office of Information Awareness was defunded by Congress. Hulse, *supra*; Michael Sniffen, *High-Tech Spying Program Closed; Lawmakers Rule Office Too Invasive*, CHI. TRIB., Sept. 23, 2003, at 11.

34 *See generally* Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191 (2003).

C. Dissemination

Until recently, it was usually difficult to disseminate information about another. Gossip, as we all know, can spread with distressing speed, but the means to disseminate information beyond a fairly small community were limited. If the mass media (newspapers, magazines, radio, and television) declined to publish or broadcast the information, someone hoping to disseminate it was out of luck.[35]

Today, the Internet has obliterated those restraints. The betrayer or grudger can disseminate even the most private information about individuals at will; and if the information tickles the public fancy, information about private people can become world "news" within days.[36]

D. The "Social Contract"

An informal understanding, or "social contract," has long existed to respect privacy. Its enforcement was far from uniform, but a general understanding existed that certain information was "private," even with regard to public figures. Interestingly, breaches of this understanding played a significant role in the formation of the United States[37] and had an impact on early

---

35 I am not advocating media monopolies. I merely point out that when relatively few individuals or companies control the mass media in a particular community, they can, if they choose, prevent the dissemination of information about the private lives of others.

36 For an example, see *infra* notes 52–61 and accompanying text.

37 In the late 1760s and early 1770s, Benjamin Franklin served as the London agent of Massachusetts and several other American colonies, seeking to negotiate on their behalf with various branches of the British government. THOMAS FLEMING, THE MAN WHO DARED THE LIGHTNING: A NEW LOOK AT BENJAMIN FRANKLIN 259 (1971). At some point Franklin came into possession of letters written by the Royal Governor and Lieutenant Governor of Massachusetts to the government in London during the 1768–69 riots in Boston over the Townshend duties. *Id.* at 225. These letters grossly misrepresented the situation and urged the British government to send troops to cow the colony into submission. *Id.* Franklin forwarded these letters to his associates in Massachusetts. *Id.* The letters were ultimately published in a Boston newspaper, and this became such a scandal in London that a duel was fought when one person falsely accused another of being the source. *Id.* at 237–38. At that point, to foreclose further bloodshed, Franklin, in London, acknowledged that he was the person who had sent the letters to Massachusetts. *Id.* at 239. Franklin's enemies in the British government summoned him to appear before the Privy Counsel on January 29, 1774, where, for almost an hour, the Crown Solicitor General, Alexander Wedderburn, attacked him. *Id.* at 245–49. Wedderburn remarked:

> Private correspondence has hitherto been held sacred in times of the greatest party rage, not only in politics but religion. He [Franklin] has forfeited all the respect of societies and of men. Into what companies will he hereafter go with an unembarrassed face, or the honest intrepidity of virtue? Men will watch him with a jealous eye; they will hide their papers from him, and lock up their escritoires.

Id. at 247. Fleming notes the blatant hypocrisy of Wedderburn's attack; as Wedderburn undoubtedly knew, the British government had been intercepting and reading Franklin's correspondence for years. *Id.* at 247. The British government did not, however, publish the correspondence to the world at large. *See id.* This experience convinced Franklin that reconciliation between Britain and the colonies was impossible. *Id.* at 249–51. Indeed, after the formal meeting broke up, Franklin whispered to Wedderburn, "I will make your master a little king for this." *Id.* at 250. A few months later Franklin returned to Philadelphia, where he became a leading exponent of independence at the Continental Congress. *Id.* at 288–91. (There is a charming coda to this story. Franklin put away the clothing he wore that day and did not wear them again until the day he signed the treaty that ended the Revolutionary War and recognized

twentieth century diplomatic history, as well.[38] This informal understanding explains why the media rarely referred to Franklin Roosevelt's physical infirmities during his presidency and why the media never ran photographs of the president being helped or carried.[39] Similarly, the media never reported on President Kennedy's extramarital dalliances, even though many members of the media were aware of them.[40]

That social contract no longer exists; it certainly has been abolished from the popular culture. Consider: (a) the self-absorption of many in the performing arts, their (unfortunately accurate) assumption that many people want to know about their struggles with alcohol, drugs, unsupportive parents, promiscuity, or the difficulty of living with fame and adulation, and the eagerness of the media to publish or broadcast the performer's self-revelatory ramblings; (b) the belief among many would-be artists and their groupies that virtually any behavior should be permitted, so long as it assists the artist in "saying something";[41] (c) the self-revealing confessions of "guests" on the *Jerry Springer Show* and the like; (d) the eagerness with which contestants on various reality shows share with the camera what would be their most intimate moments and what would be their deepest thoughts; (e) the proliferation of blogs,[42] where people reveal to anyone who logs on intimate thoughts

---

the United States of America as an independent nation. CARL VAN DOREN, BENJAMIN FRANKLIN 478 (1941)).

38 Perhaps the most extreme and misguided example of this general understanding occurred in 1929 when Secretary of State Henry L. Stimson closed the Department of State's code-breaking service, the so-called "Black Chamber," because, as Stimson explained, "Gentlemen do not read each other's mail." DAVID KAHN, THE CODEBREAKERS: THE STORY OF SECRET WRITING 360 (1967); HENRY L. STIMSON & MCGEORGE BUNDY, ON ACTIVE SERVICE IN PEACE AND WAR 188 (1948).

39 ROBERT E. GILBERT, THE MORTAL PRESIDENCY: ILLNESS AND ANGUISH IN THE WHITE HOUSE 48–49 (1998) (reporting the existence of this informal understanding). "If this rule was violated, members of the Secret Service were not averse to seizing the camera of the offending party and exposing the film." *Id.* at 49; *see also* HUGH E. EVANS, THE HIDDEN CAMPAIGN: FDR'S HEALTH AND THE 1944 ELECTION 33 (2002).

40 Timothy Kelly, *Politics Gets Personal*, N.Y. TIMES UPFRONT, Oct. 4, 1999, at 8.

41 *See, e.g.*, Daniel J. Wakin, *Keep the Sex R-Rated, N.Y.U. Tells Film Students*, N.Y. TIMES, Dec. 4, 2003, at B1. A film student at New York University, seeking to "compare the normal behavior of people in their everyday lives versus the animalistic behavior that comes out when they are having sex" (a phenomenon with which most people are already quite familiar), planned to film two volunteers having intercourse in class and, thus, produce a four-minute film which would intersperse "30-second clips of passionate sex with scenes of the couple engaged in more mundane activities, like watching television and reading a newspaper." *Id.* The instructor approved enthusiastically, but then, in a moment of passing good judgment, bounced the idea off University officials. *Id.* The officials politely but firmly said "no" and insisted that student film projects adhere to the Motion Picture Association Guidelines, going no further than an "R" rating would permit. *Id.* (It will, I am sure, surprise no one that the student newspaper and a spokesman for the American Civil Liberties Union expressed dismay and despair that the University would so cruelly stifle student creativity. *Id.*)

42 A "blog," also called a Web log, is "a type of online, hosted chatroom usually devoted to a specific subject the host wants to discuss. . . . [B]loggers are often passionate, if not fanatical, about the subjects they cover." NEWTON'S TELECOM DICTIONARY 115 (19th ed. 2003). Many blogs have specialized professional uses. *See, e.g.*, William O'Shea, *New Economy: The Online Journals Known as Web Logs Are Finding Favor as an Efficient Way to Communicate Within the Workplace*, N.Y. TIMES, July 7, 2003, at C3.

that once were revealed only on the pages of a private diary;[43] (f) the phenomenon of people who, not content merely to *narrate* their thoughts and experiences to the world at large, live their lives in front of Web cams for anyone who logs on to their Web site to see;[44] (g) and the emerging industry of charging customers to log on and watch physically attractive young people who are paid to live in a camera-saturated environment.[45] This list is not

---

43 *See, e.g.*, Warren St. John, *Dating a Blogger, Reading All About It*, N.Y. TIMES, May 18, 2003, § 9, at 1. St. John relates incidents in which bloggers criticized the church to which their parents belonged, insulted close friends, discussed their sex lives with their boyfriends, or offered negative comments about coworkers, and the frequently negative impact that doing so has had on the bloggers' lives, careers, and relationships. *Id.* The article quotes several interviewees (many of whom are also bloggers): "It's like all your friends are reporters now," "the confessional nature of many blogs had 'redrawn the line between what's private and public,'" and that dating a blogger "was an odd feeling that there was a camera on me," particularly because friends and relatives followed the blogger's description of the relationship on line. *Id.* St. John comments: "With so many self-publishing reporters out there, some say they feel a need to watch themselves, for fear that casual comments made to friends might make tomorrow morning's entry." *Id.*

The phenomenon is now international. *See* John Pomfret, *A New Gloss on Freedom: Sexual Revolution Sweeps China's Youth*, WASH. POST, Dec. 6, 2003, at A11; *see also* Michael Snider, *The Intimacy of Blogs*, MACLEAN'S, Sept. 15, 2003, at 40 (estimating in a Canadian news weekly that there are up to two million blogs on the Internet).

44 The first well known instance was the "JenniCam"; twenty-year-old Jennifer Ringley set up a fish-eye camera in her apartment, linked it to the Web, and lived her life in front of it. Jennifer Tanaka, *The Whole World Is Watching*, NEWSWEEK, Sept. 20, 1999, at 74. By 1999, the site received 4.5 million hits a day and hundreds of e-mails, many of which were complaints when she left her apartment. *Id.* at 75. "'People yell at me if I'm not home enough,' she says. 'When I spend the night at my boyfriend's I get e-mail the next morning telling me how dare I be gone.' The solution? She installed a Web cam at his place." *Id.* As of January 2004, however, JenniCam is scheduled to meet the fate that comes eventually to all small-screen entertainment, however popular; it will be disconnected. *Web Watch: Final Days in the Life at Jennicam*, WASH. POST, Dec. 7, 2003, at F7 (quoting one viewer who rued the end of what he called "a sociological experiment and a life-narrative art project"). PayPal, the company through which she collected the annual subscriber fees, announced that it will close her account at the end of the year because from time to time Ringley appeared before the camera naked, and PayPal's policy prohibits "the sale of items for mature audiences." *Id.* A more cynical non-observer might comment hopefully that PayPal's admirable action could have the worthwhile side-effect of prompting Jennie's viewers to get lives of their own.

Still, devotees of the phenomenon need not despair. *See* Julie Szego, *Camgirls*, THE AGE (Melbourne), Feb. 1, 2003, Saturday Extra, at 1 (describing similar individual Web sites and discussing the potential negative effects on both the viewed and the viewer). As an alternative, someone addicted to vicarious living has options such as WebDorm.com, "where you can watch real-life college students eat, sleep and study in their natural habitat 24 hours a day, seven days a week." Tanaka, *supra*, at 75. (Query: does living in front of a camera increase the likelihood that college students will clean their rooms?)

45 Guessing correctly that people would pay to watch such a thing, two enterprising pornographers bought a five-bedroom house in a residential neighborhood in Tampa, Florida, placed cameras everywhere (including the showers), and recruited "young, sexy college girls" to live in it. Francesca Ortiz, *Zoning the Voyeur Dorm: Regulating Home-Based Voyeur Websites Through Land Use Laws*, 34 U.C. DAVIS L. REV. 929, 933 (2001). In "Voyeur Dorm" ("VD"), the women live rent and board free, and their college tuition is paid; in exchange they are encouraged (among other things) to sunbathe nude, shower frequently, have "lingerie parties," strip when asked to do so by subscribers to the special chatline, and entertain their boyfriends. *Id.* at 934. (Although the house has a "no sex on camera" policy, the residents apparently from time to time forget this in the heat of passion. *Id.*) In addition to room, board, and tuition, each

exhaustive. It is tempting to dismiss each of these as unimportant anomalies at the fringes of society, but as such instances multiply, so does the risk that many people will assume they have the "right" to similar information about anyone, including those who wish to keep private matters private.

The social contract no longer exists in advertising either, where, for example, the phrase "erectile dysfunction" may be aired more often than "the quicker picker-upper." Other examples abound.[46]

Even the government plays a part. Information is now available online that was once public in name only and was truly accessible only to those who trooped down to the courthouse or municipal building. Sometimes disclosure of such information has a legitimate public purpose, despite the intrusion into privacy. An example is the posting on the Internet of information about convicted and released sexual predators. Other times, however, posting information online serves no purpose other than to feed the public's appetite for scandal or titillation, sometimes at the expense of the obscure,[47] and

---

resident receives a weekly stipend, the amount depending on the frequency and enthusiasm with which she participates in such activities. *Id.* When the venture proved to be a financial success, the same entrepreneurs, demonstrating that they are equal-opportunity panderers, also started a similar dorm occupied solely by men. *Id.*; *see also* Jennifer Berry, *Dorm Web Cameras Rise in Use*, VISTA (Univ. of San Diego), Mar. 13, 2002, at 1 (reporting that VD grosses $200,000 a month). An Eleventh Circuit decision described in the next paragraph noted that from August 1998 to June 2000, VD generated subscriptions and sales exceeding $3.1 million. Voyeur Dorm v. City of Tampa, 265 F.3d 1232, 1233 (11th Cir. 2001).

Tampa officials attempted to shut down VD as an adult entertainment business unlawfully located in a residential section in violation of the city zoning laws. *Id.* at 1235. The effort was unsuccessful. *Id.* at 1237. The court held that, because no customers actually attended the house in which VD was located and, therefore, did not subject the neighborhood to the negative impact the zoning provision was designed to prevent, VD did not constitute a public offering of adult entertainment as that term is used in Tampa's City Code. *Id.* at 1236–37. With what may have been a sigh of relief, the court concluded that it would "not be necessary for us to analyze the thorny constitutional issues presented in this case." *Id.* at 1235.

46 I have reluctantly accepted the fact that "yeast infection" does not relate to mold on bread; and that is *all* I wish to know on the subject.

47 For example, the sheriff of Maricopa County, Arizona maintains a Web site showing four camera views of life in the county jail, including the holding and search cells and the pre-intake area. Kim Peterson, *Increasing Use of Web Cams Puts Focus on Privacy Issues*, Copley News Serv., Jan. 28, 2002 (on file with The George Washington Law Review). At one point the cameras allegedly showed people dressing and undressing and using the toilet. *Id.* The sheriff explained that he installed the cameras to rebut claims that prison officials physically abuse prisoners: "I decided to let the whole world be my jury," he said. *Id.* Sheriff Joe Arpaio appears to have taken instruction from Gilbert and Sullivan's *The Mikado*:

> My object all sublime
> I shall achieve in time—
> To let the punishment fit the crime—
> The punishment fit the crime;
> And make each prisoner pent
> Unwillingly represent
> A source of innocent merriment!
> Of innocent merriment!

SIR W.S. GILBERT, THE MIKADO 68 (MacMillan & Co. 1928) (1885). As a clever lyric in a witty song, the concept works quite well. As a matter of social policy, however, it is unfortunate. Granted, inmates have little, if any, expectation of privacy from prison officials. *See, e.g.*, Bell v. Wolfish, 441 U.S. 520, 558 (1979). In *Bell*, the Court held that neither sentenced prisoners nor

sometimes at the expense of the famous or notorious.[48]

Needless to say, the informal understanding that certain topics are off-limits has also been rejected by the mainstream media, whose role in undermining privacy is discussed at greater length in Part IV.A.[49]

The limitations on technology; the difficulties involved in acquiring, retrieving and disseminating information; and the informal, but generally recognized understanding that certain information is simply nobody else's business were all extralegal factors that substantially contributed to the protection of privacy. These factors, however, no longer contribute to privacy. Rather, they now undermine the privacy that they previously served to protect.

E. Who Threatens Our Privacy?

Threats to privacy come from a variety of sources, primarily government, private individuals, commercial enterprises (particularly large corporations), and the media.

Inevitably, attention focuses primarily on the government. Other presentations at this Symposium discussed government intrusions on privacy at great length. My focus is on the other individuals and institutions that threaten privacy.

---

pretrial detainees have Fourth Amendment protection from Bureau of Prison regulations requiring all prisoners to submit to strip and body-cavity searches after every "contact visit" with a person from outside the institution. *Id.* at 560. The Court upheld the regulations because this denial of privacy was a reasonable measure to assure that contraband is not smuggled into the institution. *Id.* at 559–60. To offer Web cam views of prison life to titillate the public, however, is reminiscent of the days when the well-to-do would visit insane asylums to be entertained by the antics of the inmates; hopefully we have progressed beyond that point, at least. *See, e.g.*, Huskey v. NBC, 632 F. Supp. 1282, 1292 (N.D. Ill. 1986) (holding that an inmate in a state prison had a reasonable expectation that he would not be monitored by nonprison officials while working out in a prison gym). The use of Web cams in the Maricopa prison not only intrudes upon the limited privacy expectation of the prisoners, but teaches disrespect for privacy generally, even when it does so in the context of prisons and prisoners.

48 Consider mug shots. Their official purposes are: (a) to make a record of a defendant's appearance when arrested; and (b) to provide investigators with a tool for use in future investigations. Thanks to the Internet, mug shots of the famous or notorious are now also popular entertainment. Ginia Bellafante, *Headshots That Don't Guarantee the Agent Will Call Back*, N.Y. TIMES, Nov. 30, 2003, § 9, at 2 (showing, in addition to Michael Jackson ("Mr. Jackson appears with the maquillage of a geisha, his eyebrows shaped like boomerangs and an expression that seems to say, 'Please, when you're finished, may I have my gummy bears back?'"), mug shots of Nick Nolte, Hugh Grant, Glen Campbell ("looking like a deranged member of a Depression-era chain gang"), Paul Reubens ("Pee-wee Herman"), and Wynonna Judd). Just about everyone has seen the mug shot of Michael Jackson looking like a zombie of uncertain gender, but his is not the only celebrity mugshot making the rounds. *Id.* At least three Web sites are devoted to them. *Id.*

49 *See infra* Part IV.A.

II. Betrayers, Grudgers, Spammers, and Snoops

A. Betrayers and Grudgers

When we voluntarily disclose private information to another, we do so knowing that he or she might reveal it to others.[50] Although society might morally condemn the betrayal, it offers no formal form of relief to the betrayed.[51] This has been true, probably, for as long as human society has existed. What is different today, of course, is the ease with which the betrayal can be broadcast to the world. As an object lesson, consider *The Sad Affair of Brad the Cad and Claire the Fair.*

Once upon a time in Jolly Olde England, a lass named Claire and a lad named Brad had an intimate encounter.[52] Brad apparently demonstrated such considerable skill that Claire wrote him a note of thanks in which she described in some detail the aspects of the encounter she found particularly satisfying.[53] However adept Brad may have been at certain "manly arts," he was no gentleman. He decided to share Claire's note with a few friends at work.[54]

If this had all happened, say, twenty years ago, Claire would have handwritten her note, perhaps on scented stationery. Brad and his friends would have shared a snigger at her expense. Word of the letter might have spread to a few others, but that is as far as it would have gone.

But Brad and Claire's encounter took place in December 2000, and Claire sent her note by e-mail (with her full name and address attached).[55] With a few clicks of his mouse, Brad forwarded the e-mail (thus adding his own full name and address) to a few friends.[56] They forwarded it to their friends, who forwarded it to other friends, and within a very few days hundreds of thousands of people had read Claire's note and Brad's smug reaction to it, had added their own comments, and had passed it on to still others.[57] A Web site was established featuring the original e-mail and much of the subsequent commentary.[58] The British press, acting with the discretion and good taste for which it is properly famous, printed the story, including names, addresses, and photographs of the unhappy uncouple, and hounded them mercilessly.[59] Dozens of men named Brad received abusive e-mails and

---

50 *Cf.* Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

51 Exceptions exist; unauthorized disclosure of privileged information may in some circumstances be actionable. For example, a client may sue an attorney who wrongfully discloses information the client communicated in confidence. Similarly, medical personnel may be liable for damages for unauthorized disclosure of a patient's medical records.

52 T.R. Reid, *Thanks for Last Night! (cc: The Entire World)*, WASH. POST, Dec. 18, 2000, at C1.

53 *Id.*

54 *Id.*

55 *Id.*

56 *Id.*

57 *Id.*

58 *Id.*

59 *Id*; *see also* T.R. Reid, *Brad the Cad Disciplined but Not Fired*, WASH. POST, Dec. 22, 2000, at C3 (relating that Brad and the co-employees who, after receiving Brad's e-mail and

phone calls.[60] At least one woman with the same first and last name as Claire's also received a deluge of unwanted attention—even though she resides on this side of the Atlantic.[61]

The Sad Affair of Brad the Cad and Claire the Fair illustrates that betrayals of confidence now pose an enormous threat to privacy. Anyone with access to the Internet can post information,[62] embarrassing photographs,[63] and videotapes,[64] and, for that matter, unverified allegations and outright lies about anyone and anything. If the matter arouses sufficient public interest (prurient or otherwise), the content may reach an audience of millions. Once the information or image is uploaded to the Internet, the target's privacy in the matter is gone, and the law can often offer no remedy.[65]

---

passing it on to others, were disciplined but not fired by the law firm where they worked). In the latter article, reporter Reid wrote: "On grounds of privacy and taste, *The Washington Post* is not publishing the full names of the principals or the Web site. Consequently, the hundreds of readers demanding this information should get a life and leave this reporter alone." *Id.*

60 Reid, *supra* note 52.

61 After I described the *Affair of Brad and Claire* at the Symposium, another participant in the Symposium related that his wife has the same name and that even now, nearly two years later, she still receives e-mails from yahoos who assume that she is her more notorious English namesake.

62 In accord with common journalistic standards and a court order, the media has to date (December 2003) refrained from mentioning the name of the woman who accused L.A. Laker basketball star Kobe Bryant of sexual assault. Nevertheless, her name, and virtually every detail of her life, has been available on the Internet almost since the accusation became public, and a Los Angeles radio talk show has used her name on the air on a regular basis. *See, e.g.*, Chris Frates, *L.A. Radio Show Names Bryant's Accuser*, DENVER POST, July 24, 2003, at B1. When the editor of the *Aspen Daily News* announced that his paper would no longer print stories about the Bryant trial until there was a verdict or some other aspect of the case emerged which had a direct impact on the community the newspaper served, the decision received both praise and criticism. *See* Michael Tracey, *Courageous Stand of Aspen Editor: Decision to Avoid Saturation Coverage of Kobe Bryant Case Impractical for Others*, ROCKY MTN. NEWS, Oct. 18, 2003, at 14C.

63 In the fall of 1998, someone posted on the Internet nude photographs of a conservative radio talk show host taken twenty-three years earlier. James Bone, *Radio Agony Aunt Apologises as Nude Pictures of Her Appear on Internet*, TIMES (London), Nov. 6, 1998, at 20. She had posed for the man she was seeing at the time, long before she adopted the views for which she is beloved by some and hated by others. *Id.* Newspaper articles reported that the ex-lover, by then eighty years old, sold them for thousands of dollars to a company that specializes in marketing salacious materials. *Id.*; *see also* David Rosenzweig, *Celebrities Lose Nude Photo Cases*, L.A. TIMES, Nov. 3, 1998, at B1. (I decline to include the name of the woman victimized by this betrayal nor the people referred to in the next note, because to do so would, if only in a small way, make me an accomplice in the invasion of their privacy or, in one case, in her subsequent exploitation of the resultant notoriety. Readers who do not know already who they are and have a burning need to know can look it up themselves.)

64 In the fall of 1998, the Internet sleaze merchant referred to in the previous note posted on the Internet, for its members, a sexually intimate videotape taken by a famous actor and actress on their honeymoon. Rosenzweig, *supra* note 63. (How the company got its hands on the video was never made clear.) The couple sued. *Id.* The company agreed to take the video off its members-only Web site; having done so, it proceeded to sell hundreds of thousands of copies of it to the public at large. *Id.* Similarly, in the fall of 2003, a video of an actress–heiress cavorting with her (soon to be ex-) boyfriend became the primary attraction on a pornography Web log. *See* Andrew Ross Sorkin, *Building a Web Media Empire on a Daily Dose of Fresh Links*, N.Y. TIMES, Nov. 17, 2003, at C1.

65 *See* Rosenzweig, *supra* note 63. The judge lifted the temporary injunction which had been granted on behalf of the radio talk show host because "the photos had been replicated

The Internet threatens privacy because it gives someone who wishes to betray a confidence or exercise a grudge heretofore unimaginable power to disseminate information. This publication of private information is not only embarrassing; it also may distort or even dictate how the victim is viewed by others.[66]

B. Snoops

The power to embarrass or betray confidences is also available to someone who acquires information or images surreptitiously, rather than by betrayal. The private snoop (whether acting for fun or profit) has always been with us. Media articles and court opinions continue to relate examples of surreptitious videotaping[67] and wiretapping.[68] Miniaturization and other technological enhancements to surveillance equipment magnify the possibilities for privacy intrusion.[69]

Technologies which make it more convenient for us to "keep in touch" also make it easier for others to snoop. Cordless and cellular phones are increasingly popular despite the fact that they are much more vulnerable to illicit monitoring than hardwired phones. Scanners, of which an estimated half a million are sold each year,[70] are capable of monitoring cordless and

---

anonymously on countless news group [Web] sites, making them accessible to millions of Internet users worldwide. 'Simply stated,' [lawyers for the sleaze merchant said smugly], 'the photographs are no longer "private facts."'" *Id.*

66 Consider the words of Professor Jeffrey Rosen:

> Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. . . . [W]hen our reading habits or private e-mails are exposed to strangers, we may be reduced, in the public eye, to nothing more than the most salacious book we once read or the most vulgar joke we once told.

JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8–9 (2000).

67 *See, e.g.*, Deibler v. State, 776 A.2d 657, 666 (Md. 2001). Diebler was prosecuted for hiding a video camera in a bathroom in a friend's home and taping his friend's aunt taking a shower. *Id.* at 659. Interestingly, the court held that, although the videotaping itself violated no law, the defendant could be prosecuted for unlawfully intercepting the oral communications that were incidental to the activities that were videotaped. *Id.* at 666. For a similar holding, see *State v. O'Brien*, 774 A.2d 89 (R.I. 2001), a prosecution of a college student who persuaded a fraternity brother to hide in the closet of his dorm room and secretly videotape the defendant and his girlfriend having sex. *Id.* at 92. For a list of several similar acts of betrayal involving videotaping of sexual or bathroom activity, see Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1023 n.194 (1995).

68 *See, e.g.*, Bernard Weinraub, *Talk of Wiretaps Rattles Hollywood*, N.Y. TIMES, Nov. 11, 2003, at C1. FBI agents searched the computer of a private investigator who has worked for, among others, Michael Jackson, Kevin Costner, Sylvester Stallone, and Roseanne Barr, finding what appeared to be numerous wiretap transcripts. *Id.* Six days later the *New York Times* reported that the private investigator began serving a jail sentence for a weapons violation; the investigation into his alleged wiretapping continued. Laura M. Holson & Bernard Weinraub, *Hollywood's Investigator to the Stars Heads to Jail*, N.Y. TIMES, Nov. 17, 2003, at A16.

69 *See supra* notes 13–14 (discussing cell phone cameras and miniature camcorders).

70 *See, e.g.*, Mary Spicuzza, *Scanners' Drone Is Music to Ears of These "Freeks,"* SEATTLE TIMES, Sept. 4, 2003, at B1.

cellular phone transmissions.[71] Wireless "nanny-cams," which permit busy parents to monitor how in-home childcare providers treat their children, also permit anyone with a computer equipped with a receiver to view the images.[72] It would pose no great challenge for the snoop to release "newsworthy" information thus obtained to the media, as has happened more than once,[73] or, for that matter, to post such illicitly obtained conversations, images, or information on the Internet.

---

71 The signals from the earliest cordless phones could sometimes be picked up on ordinary AM or FM radios, baby monitors, and the like, and, therefore, were not legally protected from monitoring. *See* S. REP. NO. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 (explaining the lack of legal protection for cordless phones in the Electronic Communications Privacy Act of 1986). Improvements ironed out these problems, but cordless phone transmissions were still highly susceptible to interception by scanners. (Most scanner enthusiasts use the devices to monitor police, fire, and airline radio communications, but many of the scanners are also equipped to scan the frequencies on which cordless and cellular phone calls are transmitted.) Nevertheless, political pressure from the telecommunications industry ultimately persuaded Congress to afford some protection to cordless phone users in 1994. *See* FISHMAN & MCKENNA, *supra* note 29, § 3:19. As of the Communications Assistance for Law Enforcement Act ("CALEA") of 1994, cordless phone transmissions now receive the same legal protection as cellular and hard-wired phone calls. *Id.* § 3:19. Continued improvements in cordless technology make cordless phone transmissions somewhat less vulnerable to scanner monitoring. *See* Margaret Bernstein, *Here's the Bottom Line on Cordless Phones*, PLAIN DEALER (Cleveland), Mar. 24, 2002, at L3; David Colker, *New Digital Telephones Go the Distance*, L.A. TIMES, July 24, 2003, at F8. Cell telephone technology and the law's treatment of cell phones followed a similar path. *See* FISHMAN & MCKENNA, *supra* note 29, § 3:16.

72 John Schwartz, *Nanny-Cam May Leave a Home Exposed*, N.Y. TIMES, Apr. 14, 2002, at A1. It is not even clear whether the unauthorized monitoring of such transmissions violates federal law. A wireless camera transmission is an "electronic communication" and, therefore, is protected by the Wiretap Act only if its signal is "transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (2000). Whether a wireless camera that transmits an image a few hundred feet is a "system that affects interstate or foreign commerce" is far from clear.

73 The best known incident involved then–House Speaker Newt Gingrich. A Florida couple, the Martins, randomly (but illegally) scanned a phone call between Speaker Gingrich and three other Republican congressmen, including Representative Boehner (who participated via his cell phone). Boehner v. McDermott, 191 F.3d 463, 465 (D.C. Cir. 1999). Realizing that the conversation contained information that would prove embarrassing to the Speaker, the Martins taped it. *Id.* The couple, whose loyalty to the Democratic Party surpassed their respect for the rule of law, informed Florida Democratic Representative Thurman, whose respect for the law and the right to privacy did not prevent her from suggesting that they get the tape to Representative McDermott, the then-ranking member of the House Ethics Committee(!). *Id.* Representative Thurman also assured the Martins that they could expect immunity from prosecution for the unlawful interception and disclosure. *Id.* Representative Thurman was wrong; the Martins were prosecuted, pled guilty, and were fined $500, the maximum penalty at the time. *Id.* Representative McDermott, whose dedication to partisan advantage in turn surpassed his devotion to congressional ethics, gave copies of the tape to the *New York Times*, the *Atlanta Journal-Constitution*, and *Roll Call*. *Id.* Representative Boehner sued Representative McDermott, alleging unlawful disclosure of the intercepted call. *Id.* The D.C. Circuit held that McDermott's conduct was not protected by the First Amendment. *Id.* at 476. One judge concluded that the act of giving the tape to the newspapers, which constituted an unlawful disclosure under 18 U.S.C.A. § 2511, did not constitute "speech," *id.* at 477–78 (Randolph, J.), and another concluded that McDermott's conduct did constitute speech but was nevertheless unprotected, *id.* at 478 (Ginsburg, J., concurring). The third judge dissented. *Id.* at 480 (Sentelle, J., dissenting). While certiorari from the Supreme Court was pending, the Court decided *Bartnicki v. Vopper*, 532 U.S. 514 (2001), holding that the federal statute making it a crime to knowingly disclose the

The Internet also threatens privacy because it can be used in many ways to *acquire* information surreptitiously. Illicit computer hacking is a huge financial problem for businesses and leaves confidential records vulnerable to electronic intruders.[74] "WiFi,"[75] wireless access to the Internet, provides the considerable convenience of permitting a computer user to log on without having to plug in physically;[76] it may also leave the user extremely vulnerable

---

contents of an unlawfully intercepted communication could not constitutionally apply to someone who did not participate in the interception when the matter was one of public concern. *Bartnicki*, 532 U.S. at 535; *see also infra* notes 208–238 and accompanying text. On May 29, 2001, the Supreme Court granted certiorari in *McDermott*, vacated the judgment, and remanded to the D.C. Circuit for further consideration in light of *Bartnicki*. McDermott v. Boehner, 532 U.S. 1050 (2001). The D.C. Circuit, *per curiam*, remanded to the district court. Boehner v. McDermott, 22 Fed. Appx. 16, 16 (D.C. Cir. 2001). As this footnote is being written, the district court has each side's motions for summary judgment under consideration.

In a somewhat similar case, a Dallas couple intercepted cordless phone calls by a neighbor, a prominent school board official with whom they were feuding. Peavy v. WFAA-TV, Inc., 221 F.3d 158, 163–64 (5th Cir. 2000). The conversations revealed that the official was a bigot who, with other board members, was striving to marginalize nonwhite members of the school board and also was involved in some remarkably shady dealings with rather questionable people, including one who had done time for manslaughter. Peavy v. New Times, Inc., 976 F. Supp. 532, 533–34 (N.D. Tex. 1997). The couple informed the media, and several rounds of litigation ensued. *Id.* at 536–57. The key difference in the two cases is that in *Peavy*, the TV station, unaware that Congress had amended the Wiretap Act to protect cordless phone calls, actively encouraged the couple to continue to intercept Peavy's calls. *See* Peavy, 221 F.3d at 164. The Fifth Circuit held that the First Amendment did not protect the TV station from suit under the Wiretap Act. *Id.* at 193.

A third case, *Quigley v. Rosenthal*, 327 F.3d 1044 (10th Cir. 2003), bears several similarities to *Peavy*: it involved feuding neighbors, a cordless phone, and a supposedly media-savvy institution, the Anti-Defamation League ("ADL"), which, like the television station in *Peavy*, was unaware that the law regarding cordless phones had changed. *See Quigley*, 327 F.3d at 1047–53; *Peavy*, 221 F.3d at 163–64. The ADL ultimately used the illegally intercepted calls to publicize trumped-up allegations of anti-Semitism against the Quigleys. *Quigley*, 327 F.3d at 1051–55. Unlike the interceptions in *Peavy*, which clearly involved matters of public concern, however, the conversations in *Quigley* did not; thus the Tenth Circuit, post-*Bartnicki*, affirmed the Quigleys' judgment against the ADL. *Id.* at 1074.

For a more detailed discussion of *Boehner* and *Peavy*, see FISHMAN & MCKENNA, *supra* note 29, § 4:12.1–:12.2.

74 The *New York Times* has reported that "[t]he number of successful, and verifiable, worldwide hacker incidents for the month of January [2003] is likely to surpass 20,000," and that in a recent survey of 500 computer security practitioners, eighty percent acknowledged financial losses to computer breaches. Bob Tedeschi, *E-Commerce Report: Crime Is Soaring in Cyberspace, but Many Companies Keep It Quiet*, N.Y. TIMES, Jan. 27, 2003, at C4. "Of the 223 respondents who quantified the damage, the average loss was $2 million. Those who had sustained losses of proprietary company information said each incident cost an average of $6.5 million, while financial fraud averaged $4.5 million an incident." *Id.*

75 The term is short for "wireless fidelity."

76 *See, e.g.*, Scott Kirsner, *Wireless, Wireless, Everywhere*, BOSTON GLOBE, June 23, 2003, at C1; Jonathan Krim, *WiFi is Open, Free and Vulnerable to Hackers: Safeguarding Wireless Networks Too Much Trouble for Many Users*, WASH. POST, July 27, 2003, at A1. Wireless access can be obtained for as little as a $70 antenna. Kirsner, *supra*. Many retail establishments provide WiFi to attract business—coffee shops, sandwich shops, even some McDonald's restaurants have done so. Roy Furchgott, *A Tall Decaf Mocha Cappuccino and the Wi-Fi Selection of the Month, Please*, N.Y. TIMES, Dec. 8, 2003, at C4. Starbucks has begun to offer more, including free music videos or free streaming holiday stories from National Public Radio. *Id.* A number of truck stop companies now provide WiFi access to truckers and other motorists at rates ranging from $1 for

to someone who wants to access the Internet on a WiFi user's account or to someone seeking to "steal data, introduce viruses, launch spam or attack other computers."[77] In fact, the vulnerability of wireless systems has given rise to a hobby, called "war driving," in which hobbyists and hackers drive around with receiver-equipped computers, logging "hot spots"—areas where wireless transmitters allow Internet access over the air—and then compiling and comparing their information at conventions.[78]

The Internet also allows cookies,[79] spyware,[80] and snoopware[81] to be installed remotely. These programs permit the installer to monitor how the targeted computer is used.[82] These products may violate the law,[83] and even

---

fifteen minutes to $99 for an annual subscription (although the latter will soon be raised to $199 a year). Jeannette Borzo, *Roam the Web While at the Wheel*, N.Y. TIMES, Dec. 4, 2003, at G5; *see also* Jeanette Borzo, *Head Out (Wirelessly) on the Highway*, N.Y. TIMES, Dec. 4, 2003, at G5 (reporting that the number of WiFi users nationwide is expected to reach 4 million in 2003, up from 1.9 million in 2002). Homeowners can equip their homes for wireless access from any room in the house. Krim, *supra*, reports that in 2002, 3.1 million households had wireless networks. The number of households using wireless networks is likely to double in 2003. *Id.*

77 Krim, *supra* note 76; *see also* Kirsner, *supra* note 76. In thirty seconds, the president of a computer security consulting firm, walking all of forty-five feet down the Avenue of the Americas in Manhattan, located at least thirteen separate wireless networks that were vulnerable to hacking. Erik Sherman, *Walk-By Hacking*, N.Y. TIMES, July 13, 2003, § 6 (Magazine), at 22. Although WiFi comes equipped with an encryption system, it can be confusing to enter the encryption codes, and using it can prevent connected systems from functioning properly with each other. Krim, *supra* note 76. Thus, most people with WiFi do not use the encryption system. *Id.*

78 Krim, *supra* note 76 (reporting estimates that the number of "hot spots" in the world was roughly 20,000 in 2002 and will increase to approximately 150,000 by 2005). Products are now available that permit a network administrator to see who is on a wireless network and where they are and allow them to limit or deny access to certain individuals or locations. Kirsner, *supra* note 76.

79 *See infra* Part II.B.

80 *See* CTR. FOR DEMOCRACY & TECH., GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM (2003). The report defines "spyware" as "key stroke loggers and screen capture utilities, which are installed by a third party to monitor work habits, observe online behavior, or capture passwords and other information," and "'adware' and similar applications that install themselves surreptitiously through 'drive-by downloads' or by piggybacking on other applications and track users' behaviors and take advantage of their Internet connection." *Id.* at 2. Similarly:

> Spyware is installed surreptitiously as an add-on to other programs, and tracks your computer use for the benefit of Web advertisers. It often displays ads but, like any mischievous application set loose in Windows, can do much worse—potentially anything, including steal your confidential information or erase your hard drive.

Rob Pegoraro, *Cookies and Spyware*, WASH. POST, Nov. 2, 2003, at F6.

81 *See* John Schwartz, *When Free Isn't Really Free: That Song You Just Downloaded May Cost You Your Privacy*, N.Y. TIMES, Nov. 23, 2003, § 3, at 1 (reporting that many programs and services offered for free on the Internet surreptitiously implant "adware," "spyware," and "snoopware" on the hard drives of unwitting recipients).

The definitions are fuzzy, but the privacy-intrusive programs fall under three broad categories: "adware," which serves pop-up ads and banners, including some for pornography; true "spyware," which monitors Web wanderings for marketing purposes; and more insidious "snoopware," which can track everything users do on their computers, whether or not they are online. Some programs can even disable antivirus software and hijack the results of Web searches. *Id.*

82 *See* John Schwartz, *Snoop Software Is Generating Privacy Concerns*, N.Y. TIMES, Oct.

if they do not, the advertisements almost certainly do.[84] This fact has not deterred manufacturers of some of these products in the past,[85] however, and it is unlikely to do so now.[86]

The Internet has also given rise to a new specialty, which might be called "document reconstruction." When a document is posted on the Web with blacked-out material, that material now can be retrieved.[87] Where material was deleted to protect officials from appropriate criticism, the tendency is to rejoice that "they didn't get away with it." Nevertheless, use of the technique can also compromise legitimate privacy interests and imposes on someone seeking to post such a document the additional expense and effort of producing a new electronic version of the document with the confidential information deleted altogether, not merely blacked over.[88]

The victim of Internet-aided intrusions may lose more than his or her privacy; identity theft is also a growing problem, and misuse of the Internet is a significant contributor.[89] In August 2003, the *New York Times* reported a case that illustrates how a clever thief with sufficient skills can victimize the unwary.[90] The thief illicitly installed key loggers on computers available for

---

10, 2003, at C1 (reporting, among other things, that a company called LoverSpy "promises to let buyers '[s]py on anyone by sending them an e-mail greeting card!'").

83 It is a crime to manufacture, advertise, ship, or possess any device, "knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications." 18 U.S.C. § 2512 (2000).

84 It is a crime to advertise "any other electronic, mechanical, or other device [whether the device is "primarily useful" for unlawful interceptions or not], where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications." 18 U.S.C. § 2512(1)(c)(ii).

85 Defendants in § 2512 cases sometimes maintain that it is lawful to sell communications interception equipment so long as the salesperson tells the buyer that it would be against the law to use the equipment without the consent of a participant. *See* United States v. Wynn, 633 F. Supp. 595, 606 (C.D. Ill. 1986); *see also* United States v. Bast, 495 F.2d 138, 143 (D.C. Cir. 1974); United States v. Spy Factory, Inc., 951 F. Supp. 450, 474–75 (S.D.N.Y. 1997). This is a pseudo defense because the statute clearly states that if the equipment itself is "primarily useful" for unlawful interception of communications, its manufacture, advertisement, sale, shipment, or possession is *per se* unlawful. 18 U.S.C. § 2512(1)(c)(i); *see also* FISHMAN & MCKENNA, *supra* note 29, § 2:41.

86 It is no surprise that this pseudo defense is being asserted by the manufacturers of invasive software. *See* Schwartz, *supra* note 82.

87 *See, e.g.*, Tom McNichol, *Peeking Behind the Curtain of Secrecy*, N.Y. TIMES, Nov. 13, 2003, at G7 (relating how a self-described "information archeologist" retrieved blacked-out portions of an internal Department of Justice report criticizing the Department's efforts toward diversity in hiring).

88 In 2000, the *New York Times* posted on its Web site portions of a classified CIA document discussing the 1953 coup in Iran that placed the current Shah on the throne in that country. *Unediting the Editing of a Report*, N.Y. TIMES, Oct. 31, 2003, at A19. Although the newspaper removed the names of Iranian agents from the document, a computer expert was able to delete the black boxes and read the names underneath. *Id.*

89 According to a Federal Trade Commission survey, more than 27 million people were victims of identity theft between 1998 and 2002, including 9.9 million in 2002 alone. *Identity Theft Hits 27 Million Since '98: More Awareness Slowing Growth*, CHI. TRIB., Sept. 4, 2003, § 3, at 3. All told, the crimes cost victims $5 billion, and businesses and financial institutions lost about $48 billion. *Id.*

90 Lisa Napoli, *The Kinko's Caper: Burglary by Modem*, N.Y. TIMES, Aug.7, 2003, at G1.

public use at several Kinko's copy shops in Manhattan.[91] When someone using one of these computers entered personal or financial data, the thief collected the data; when a user accessed a home computer (using a program called GoToMyPC), revealing his or her password in the process, the thief gleaned still more information from files on the home computer's hard drive.[92] The thief sold some of this information on the Internet and used other information to raid bank accounts, transfer assets, et cetera.[93] He was caught because one victim reported that while watching television, he heard his computer turn on and watched the intruder open various files.[94]

As to some of these activities, it is clear that the conduct is both wrong and unlawful. First, the private, unauthorized interception of communications is a crime.[95] The subsequent disclosure and use of such communications (except by the media!)[96] is also a crime, so long as the prosecutor can show that the person disclosing or using the information knew, or had reason to know, that the communication was intercepted unlawfully.[97] Unlawful interception, disclosure, and use also provide a basis for civil liability.[98] Second, unauthorized access to stored electronic communications is a crime[99] and is civilly actionable.[100] Finally, the same is true of unauthorized access of a "protected computer" and the information stored thereon,[101] although the civil remedy is limited because an act of unlawful access must result in costs or damages of at least $5,000 to be actionable.[102] And, of course, any criminal act committed with the use of such information is by definition also criminal. Such intrusions are easy to commit, while detection and apprehension is often difficult and sometimes impossible.[103] At least the legal status and moral implications of such activities are pretty clear.

---

91 *Id.*

92 *Id.*

93 *Id.*

94 *Id.*

95 18 U.S.C. § 2511(1)(a) (2000).

96 *See infra* note 301 and accompanying text.

97 18 U.S.C. § 2511(1)(c)–(d).

98 The victim of an unlawful interception or disclosure may be entitled to actual, liquidated, and punitive damages. 18 U.S.C. § 2520.

99 18 U.S.C. § 2701 (2000).

100 18 U.S.C. § 2707 (2000 & Supp. I 2001).

101 18 U.S.C. § 1030 (2000 & Supp. I 2001). "Protected computer" is defined as a computer:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
> (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States . . . .

Id. § 1030(e)(2).

102 18 U.S.C. § 1030(1)(4) (2000); *see infra* notes 167–68 and accompanying text.

103 Someone using a scanner to unlawfully monitor cordless and cell phone conversations leaves no electronic trail to follow; cases of such monitoring come to light only if the criminal is indiscreet enough to disclose or use the contents of the conversations in a way that allows the

Some forms of electronic snooping by private individuals, however, are unregulated by law, and the rightness or wrongness of the action is unclear. For example:

(1) It is perfectly lawful to search out information about someone from a variety of sources to accumulate a profile. Whether it is right or wrong to do so depends on why the profile is being accumulated and the use to which it will be put.

(2) It is perfectly legal to post lawfully obtained information, photographs, videos, and the like on the Internet—even if the underlying purpose is to embarrass someone and to undermine their public image. That it is not illegal, however, does not make it *right* to do so.

(3) Reconstruction of edited documents violates no law, except perhaps where state secrets are involved, even though in some instances it may deprive an author of the right to control the version of his or her work that is released to the public.

C. Spammers

Spam, whether seeking suckers to defraud,[104] offering pornography or various physical or performance enhancements,[105] or advertising from mainstream enterprises,[106] intrudes into privacy because it interferes with our ability to communicate with others and our ability to use our computers. Spam diverts time and attention away from more important matters. Despite measures that the law and Internet Service Providers ("ISPs") take to suppress spam,[107] it threatens to overwhelm efforts to control it,[108] particularly because spammers have now begun to employ Trojan horses that enable them to take over other computers and use other computers to send more spam. This procedure prevents investigators from tracing either rogue programs or spam back to its source.[109] Web sites now exist where hackers who have

---

victim of the monitoring to learn about it. A number of cases have been widely publicized. *See supra* note 73.

104 Is there anyone left who has not been given the opportunity to make a quick profit from a mysterious Nigerian bank account?

105 The "performances" in question do *not* involve the violin.

106 *See* Saul Hansell, *It Isn't Just the Peddlers of Pills: Big Companies Add to Spam Flow*, N.Y. TIMES, Oct. 28, 2003, at A1 (reporting that companies such as Palm, Bank of America, SBC Communications, and Sprint are trading customers' e-mail addresses and are sending the addressees advertisements for a wide range of goods and services).

107 *See* Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003, 15 U.S.C.A. § 7701 (West 2004) (creating penalties, in the form of fines and jail time, for individuals and companies that send out junk e-mails to recipients who have indicated that they wish to unsubscribe from mailing lists).

108 According to Brightmail, a developer of spam filters, forty-one percent of total Internet e-mail was identified as spam in December 2001, and that percentage has increased each month since. BRIGHTMAIL, SPAM STATISTICS, *at* http://www.brightmail.com/spamstats.html (last visited Aug. 12, 2004). In November 2003, spam was fifty-six percent of all e-mails. *Id.*

109 *See* John Schwartz, *Hackers Steal From Pirates, to No Good End*, N.Y. TIMES, Dec. 8, 2003, at C2. An "enormous rise in the volume of spam" occurred during the summer of 2003, when several versions of the SoBig virus began to circulate; it turned out that SoBig included a Trojan horse that directed infected computers to send spam. *Id.* A later virus, MiMail, "caused infected machines to attack the computers of organizations that fight spam." *Id.* The latest

developed a network of infected machines offer to rent out that network to spammers and scammers for fun and, with increasing regularity, profit.[110]

III. Corporate Information Gathering

Commercial enterprises intrude into privacy in many ways. One method is to force unwanted advertisements into our homes. Junk mail is ubiquitous. Unsolicited telemarketing has become so annoying that, when Congress recently enacted legislation allowing people to place their names on a national "do not call" list, irate recipients signed up more than 735,000 home, fax, and cell phone numbers on the list the first day.[111] At one point, numbers were being added to the list at a rate of 108 per second,[112] and 19.6 million numbers were signed onto the list in the first ten days.[113] While most e-mail spam is generated by businesses with questionable legitimacy, mainstream corporations also have used spam to advertise their products and services.[114]

This section of the Article focuses on a more-direct intrusion, corporate information gathering. When it comes to monitoring and information gathering by business enterprises, the law fails to protect privacy adequately. In the aggregate, corporate America has a more powerful motive and far greater resources to develop information about each of us than either the government or private snoops.

This section briefly addresses the threat to privacy posed by lawful business monitoring and information gathering in three contexts: (1) employer monitoring of employee communications and other activities; (2) corporate use of computer "cookies" to monitor a customer's online activities, and (3) corporate use of customer "bonus cards" to gather information about individual consumers.

A. Employer Monitoring of Employee Communications and Other Activities

Many businesses could not survive without providing telephones, computers, e-mail, and Internet access to their employees. Inevitably, employees will use such equipment for personal as well as business purposes. It is just as inevitable that an employer or supervisor may become curious as to how a particular employee, or employees in general, use the equipment. This curiosity might be prompted by simple nosiness, or it might be motivated by

---

Trojan horse, called Sinit, hijacks infected computers "to serve pop-up advertisements and to download 'porn dialers,' programs that cause the victim's machine to turn on the modem and place expensive pay-per-minute phone calls." *Id.*

110 *Id.* The founder of an Internet security company described the development of Trojan horse-created "peer-to-peer networks" as "scary," among other reasons, because it demonstrates that hackers, whose primary motive for breaking into systems was once the thrill of being able to do so, now increasingly are operating from a profit motive. *Id.*

111 Anitha Reddy, *108 People Per Second Tell FTC Hotline: "Do Not Call,"* WASH. POST, June 28, 2003, at A1.

112 *Id.*; Matt Richtel, *National Do-Not-Call Registry Overwhelmed by Eager Public*, N.Y. TIMES, June 28, 2003, at C2.

113 Don Oldenburg, *Millions Answer Yes to No-Call*, WASH. POST, July 8, 2003, at C9.

114 *See* Hansell, *supra* note 106.

legitimate business concerns. Whatever the reason, is it lawful for the employer to electronically monitor how one or more employees use such equipment?[115]

With regard to telephones, the answer is that it is lawful only sometimes for employers to monitor use of equipment, and then only under carefully limited circumstances. With regard to computers, e-mail, and Internet activities, the answer is yes, without qualification. It is lawful to monitor employees' use, regardless of motive or circumstances.

Employers, sometimes legitimately and sometimes not, place cameras that enable them to surveil employee activities. On this subject, the law is mostly a blank page.

1. Telephone Monitoring

The Wiretap Act states a basic rule: interception of a wire communication is a crime and is civilly actionable.[116] The statute contains several exceptions, and those that are relevant are outlined below. The law's basic assumption is that such interception is unlawful. If an employer has monitored telephone communications, the burden is on the employer to demonstrate that the circumstances fall within one of the exceptions.

a. The Consensual Interception Exception

The first exception is found at 18 U.S.C. § 2511(2)(d):

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.[117]

---

115 For a more detailed discussion, see FISHMAN & MCKENNA, *supra* note 29, §§ 7:5–:10.

116 18 U.S.C. § 2511(1)(a) (2000). The statute makes it a crime (exceptions aside) to intercept a wire, oral, or electronic communication. *Id.* The definition of "wire communication" includes telephone conversations; it includes use of cellular and cordless telephones, as well as hard-wired phones. *See id.* § 2510(1). *See generally* FISHMAN & MCKENNA, *supra* note 29, §§ 2:1–:8, 4:3.

117 18 U.S.C. § 2511(2)(d). Thirty-four states follow the federal approach: Alabama, Arizona, Colorado, Connecticut, Delaware, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, West Virginia, Wisconsin, and Wyoming. FISHMAN & MCKENNA, *supra* note 29, § 6:39; *see, e.g.*, ALA. CODE §§ 13A-11-30(1), 13A-11-31 (1994); S.D. CODIFIED LAWS § 23A-35A-20 (Michie 1998). In thirteen states, all participants must consent: Alaska, Arkansas, California (more or less), Florida, Georgia, Illinois, Maryland (does the name "Linda Tripp" ring a bell?—pun intended, see *infra* note 201), Massachusetts, Michigan, Montana, New Hampshire, Pennsylvania, and Washington. FISHMAN & MCKENNA, *supra* note 29, § 6:39. Nevada permits one-party consensual interceptions of face-to-face conversations, NEV. REV. STAT. 200.650 (2001), and requires one-party consent for telephone conversations, NEV. REV. STAT. 200.620 (2001). The law in New Mexico and Vermont is unclear. For a detailed discussion, see FISHMAN & MCKENNA, *supra* note 29, § 6:38.

The consent exception applies most often in a business context when an employer, for "quality control purposes," monitors (i.e., listens to or records) the phone conversations of employees who deal regularly with the public. The employer may invoke the consent defense only by showing that the employee knew, or at least had actual notice, that such monitoring would occur.[118] Of particular importance, "consent within the meaning of section 2511(2)(d) is not necessarily an all or nothing proposition; it can be limited."[119] Thus, that employees consented to the monitoring of their business-related calls does not mandate the conclusion that they also consented to the monitoring of personal calls.[120]

b. The "Ordinary Course of Business" Exception

A second defense is that no "interception" occurred as that term is defined in the Wiretap Act. "Intercept" is defined in 18 U.S.C. § 2510(4) as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any *electronic, mechanical, or other device*."[121] If the employer did not use "any . . . device," then no interception has occurred. "[D]evice," in turn, is defined, in pertinent part, as:

> (5) "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business . . . .[122]

---

118 Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (stating that the key issue in an implied consent inquiry is "whether the parties were given sufficient notice"); Griffin v. City of Milwaukee, 74 F.3d 824, 827 (7th Cir. 1996); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (distinguishing consent to monitoring of business calls with consent to monitoring of personal calls); Deal v. Spears, 780 F. Supp. 618, 622 (W.D. Ark. 1991) (rejecting defendant's implied consent defense); Jandak v. Brookfield, 520 F. Supp. 815, 824–25 (N.D. Ill. 1981) (upholding consent defense where plaintiff should have known his calls were monitored based on his "training and job situation"); Curley v. Bd. of Trs., 624 N.Y.S.2d 265, 265 (App. Div. 1995). *Cf.* Hart v. Clearfield City, 815 F. Supp. 1544, 1548 (D. Utah 1993) (finding that use of a telephone line that plaintiff knew was recorded defeated a 42 U.S.C. § 1983 action for violation of plaintiff's constitutional right to privacy). For a detailed discussion of this issue, see FISHMAN & MCKENNA, *supra* note 29, §§ 6:42, 7:6.

119 *Watkins*, 704 F.2d at 582.

120 *Id.* at 581–82.

121 18 U.S.C. § 2510(4) (emphasis added).

122 *Id.* § 2510. Section 2510(5)(a)(ii) exempts devices "being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties." *Id.* § 2510(5)(a)(ii). Subsection (5)(b) also exempts from the definition "a hearing aid or similar device being used to correct subnormal hearing to not better than normal." *Id.* § 2510(5)(b).

This section has become known as both the "ordinary course of business" exception[123] and, somewhat less accurately, as the "extension phone exception."[124] The applicability of this defense depends on two factors: (1) the nature of the equipment used to overhear or record the phone call; and (2) the circumstances and purposes of the interception.

(1) *Equipment used.* Courts generally interpret 18 U.S.C. § 2510(5)(a)(i) to include standard telephone equipment provided by either the provider of telecommunication services or by the subscriber and not to include equipment specially designed or modified for wiretapping.[125] Courts are divided on whether this provision applies to standard telecommunications systems with built-in monitoring capacities.[126]

(2) *Purpose and circumstances.* The second element of the "no interception" defense is that the call was monitored in the "ordinary course" of the employer's business. The statute does not define "ordinary." As the courts have applied the provision, "ordinary" does not mean routine or regular. An employer cannot immunize itself from civil liability for unauthorized monitoring merely by conducting such monitoring as a matter of routine. On the other hand, the monitoring need not have been routine or in accordance with established policy to have been "in the ordinary course of [the employer's] business." Rather, to be "in the ordinary course," the monitoring must have a legitimate business purpose and be reasonable in scope and duration.[127]

Regardless of the ostensible purpose, indiscriminate monitoring is likely to be civilly actionable.[128]

In short, an employer may monitor an employee's phone calls made from the work place but must do so warily, taking care to consider the nature of the equipment used, the justification for the monitoring, how it is conducted, and how the information is used and disclosed. Upon learning of the monitoring, the employee may bring a civil action in federal court, placing the burden on the employer to establish its legality.

---

123 *See, e.g.*, Adams v. City of Battle Creek, 250 F.3d 980, 983 (6th Cir. 2001); Sheinbrot v. Pfeffer, No. 93 CV 5343, 1995 WL 432608, at *5 (E.D.N.Y. July 12, 1995); *see also* Bunnell v. Superior Court, 26 Cal. Rptr. 2d 819, 825 (Ct. App. 1994) (discussing "ordinary course of law enforcement duties").

124 *See, e.g.*, Stinson v. Larson, No. 2020918, 2004 WL 541826, at *2 (Ala. Civ. App. Mar. 19, 2004) (discussing "extension-telephone exception"); Britton v. Britton, 223 F. Supp. 2d 276, 281 (D. Me. 2002) (same); Commonwealth v. Barboza, 763 N.E.2d 547, 553 (Mass. App. Ct. 2002); Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home*, 2 J. HIGH TECH. L. 87, 90 (2003). The phrase "extension phone" is somewhat inaccurate because, although the exception does apply to the standard extension phone, it also applies to far more sophisticated equipment. *See generally* FISHMAN & MCKENNA, *supra* note 29, §§ 2:31–:35.

125 *See generally* FISHMAN & MCKENNA, *supra* note 29, § 7:4.

126 *See generally id.*

127 *Id.* § 7.5. Legitimate purposes may include monitoring employees' conversations with customers and other members of the public, *see id.* § 7:6; monitoring employees suspected of misconduct, *see id.* § 7:7; monitoring to determine whether an employee is violating a policy banning use of company phones for personal phone calls, *see id.* § 7:8; and various other purposes, *id.* § 7:9.

128 *Id.* § 7:10.

2. *Employee E-mail*[129]

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA").[130] That statute included the Stored Communications Act.[131] Section 2701 of the Stored Communications Act permits an employer who is also an e-mail service provider to lawfully access employees' stored or archived e-mail without the knowledge or permission of employees.[132]

Section 2701(a) makes it a crime, punishable by either one or five years in prison, depending on the circumstances, for a person to access stored electronic communications without proper authority.[133] An exception, however, is codified in § 2701(c): "Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—(1) by the person or entity providing a wire or electronic communications service . . . ."[134]

This provision gives the ISP the unrestricted right to sift all messages stored in its central computer. The legislative history contains no explicit explanation.[135] In theory, therefore, when individuals subscribe to a commercial ISP, they surrender all right to privacy in any communication they send or receive via that ISP.

In practice, however, most commercial ISPs respect and protect the privacy of their customers. They do so for a very good reason: enough of their subscribers insist on it. A commercial ISP with an inadequate privacy policy will lose business. Thus, although a commercial ISP's subscribers lack statutory protection against the ISP's examination of stored communications, they do have contractual protection.[136]

When employees use an Internet service provided by their employer, however, such contractual protection is lacking, and there is no legal impediment to the employer's post-transmission examination of employees' e-mails or Web browsing.[137] An employer may have a perfectly good reason to ex-

---

129 Aspects of this discussion are adapted from a prior publication. *See id.* § 3:22.

130 Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2000 & Supp. I 2001).

131 18 U.S.C. §§ 2701–2712 (2000 & Supp. I 2001) (Stored Communications Act).

132 *Id.* § 2701.

133 The full text of 18 U.S.C. § 2701(a) is set forth *infra* note 169.

134 18 U.S.C. § 2701(c)(1).

135 Neither congressional report on the ECPA contains any explanation as to why an ISP is given total freedom to access stored communications and fails to make any reference to the privacy implications of employer-provided e-mail and Internet access. *See* S. REP. No. 99-541, at 36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3590 (restating the language of the provision without further explanation or comment); H. REP. No. 99-647, at 64 (1986) (same).

136 *See, e.g.*, AOL.COM, PRIVACY POLICY, *at* http://www.aol.com/info/privacy.adp (last modified Apr. 8, 2003) (specifying what information AOL collects from its customers and those who visit its Web sites, how such information is collected, how a subscriber may opt out of certain services by declining to permit certain information from being accumulated, and assuring that no information about a user's visits to AOL.com or any of its Web sites will be used by AOL or shared with anyone except "in response to legal process, such as a court order or subpoena, or in special cases such as physical threat to you or others"); PEOPLEPC, PRIVACY POLICY, *at* http://www.peoplepc.com/online/legals.asp?locid=1&pageid=1 (last modified July 6, 2004); NETZERO, NETZERO, INC. PRIVACY STATEMENT, *at* http://www.netzero.net/legal/privacy.html (last updated Mar. 26, 2004).

137 An employer who monitors an employee's e-mails *as the employee sends or receives*

amine a particular employee's e-mails. If an employee uses company e-mail to harass or libel someone or to inflict trade disparagement, the employer may be held liable.[138] Likewise, an employer is entitled to take reasonable steps to assure that an employee does not spend inordinate time attending to personal e-mail, shopping online, or visiting pornographic Web sites while "on the clock."

But these legitimate employer concerns about employee use of the Internet apply equally to employees' use of the telephone. Still, while the Wiretap Act presumes all phone conversations are protected and obliges the employer to demonstrate a legitimate business purpose to justify monitoring, the Stored Communications Act gives the employer/ISP the unrestricted right to make a post-transmission examination of employees' every e-mail and Web-surf. There is no logical reason for this dichotomy. Indeed, one of the purposes of the ECPA was to protect the privacy of *phone calls* transmitted via private telephone networks on the same basis as those transmitted by telecommunications companies,[139] and nothing in the ECPA's legislative history suggests that Congress intended to create a dichotomy with regard to workplace Internet access.

The Wiretap Act's protection of employee phone calls should also apply to employee e-mails, whether monitored during transmission or examined as stored communications. Congress should amend § 2701(c)(1) to permit an employer/ISP to access an employee's stored electronic communications only with the consent of the employee or in the "ordinary course of [the ISP-employer's] business." This will ensure that the employer/ISP has the au-

---

them has "intercepted" those communications in violation of 18 U.S.C. §2511(1) and would be subject to the less permissive provisions of the Wiretap Act set forth *supra* note 116. *See* 18 U.S.C. § 2510(4) (2000) (defining "intercept"). A second provision provides that it is lawful for

> an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

18 U.S.C. § 2511(2)(a)(i) (2000 & Supp. I 2001). Except in such circumstances, the employer-as-provider-of-electronic-communication-services may not intercept an employee's e-mail during the brief instant that it is being transmitted. *Id.* Once transmission is complete, however, monitoring the *stored* copy of the communication is regulated by the Stored Communications Act—which gives the employer/ISP carte blanche. *See* 18 U.S.C. § 2511.

138 *See* Harley v. McCoach, 928 F. Supp. 533, 540 (E.D. Pa. 1996); Michael K. McChrystal, William C. Gleisner III & Michael J. Kuborn, *Coping with the Legal Perils of Employee Email*, 72 WIS. LAW. 10, 12 (1999); *see also* Strauss v. Microsoft Corp., 814 F. Supp. 1186, 1193 (S.D.N.Y. 1993).

139 "It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute." S. REP. NO. 99-541 (1986), at 3, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556; *see also* H.R. REP. NO. 99-647 (1986), at 18 (noting that "totally private systems are rapidly being developed by private companies for their own use" and that "these networks . . . are not covered by existing Federal law").

thority to access such communications when a legitimate need exists and at the same time provide a degree of privacy protection to the employee.[140]

Until Congress amends § 2701(c)(1), the only available stopgap is for employers to respect their employees' privacy voluntarily. An employer should ensure that employees know that copies of all their incoming and outgoing e-mail are accessible to supervisors even after the employee deletes it from his or her hard drive.[141] The employer should require that employees be informed that the employer reserves the right to review an employee's e-mails and other online activity for valid business purposes.[142]

3. *Video Surveillance*

Anecdotal evidence suggests that increasingly employers are subjecting employees to video surveillance, usually intentionally, but sometimes not.[143] Sometimes the surveillance is with advance notice and sometimes without.[144]

---

140 Of course, the employee has the option of using the employer-provided e-mail system strictly for business purposes and conducting his personal e-mail correspondence and Web-surfing on a home computer with a commercial ISP. But this is inconvenient, just as it would be to never use the office phone to speak to family members, make doctor's appointments, or conduct other personal business during working hours.

141 It is surprising and a little sad that many people are still unaware of this fact. Lt. Col. Oliver North, who was the central figure in the "Iran-Contra" affair in the late 1980s, is perhaps the best known individual to learn of this ongoing accessibility of deleted e-mails. *See* Karen Tumulty & Sara Fritz, *The Iran-Contra Hearings: Assumed Reagan Knew of Diversion—North*, L.A. TIMES, July 8, 1987, Part I, at 6; Lawrence J. Magid, *Computer File: As North Learned, Deleted Files are Retrievable*, L.A. TIMES, Aug. 10, 1987, Part IV, at 4. ("Wow, were we wrong" was how North described the unpleasant discovery. *Id.*) For a detailed discussion of the prosecution of North, see LAWRENCE E. WALSH, U.S. COURT OF APPEALS FOR THE D.C. CIRCUIT, 1 FINAL REPORT OF THE INDEPENDENT COUNSEL FOR IRAN/CONTRA MATTERS 105 (1993).

142 Where the employer is the government, the situation becomes somewhat more complicated because the Fourth Amendment regulates government searches and seizures even in contexts unrelated to traditional law enforcement. *See* O'Connor v. Ortega, 480 U.S. 709, 718 (1987) (holding that, in some situations, a public employee may have a reasonable expectation to privacy in his desk or in filing cabinets located in his office). In *United States v. Simons*, 29 F. Supp. 2d 324, 327 (E.D. Va. 1998), *aff'd in part*, 206 F.3d 392, 404 (4th Cir.), *remanded to* 107 F. Supp. 2d 703 (E.D. Va. 2000), a federal district court held that a government employee lacked a reasonable expectation of privacy in his Internet activities or his hard drive, where the agency's official policy informed employees that their use of government-owned computers was subject to review and that an automatic record was made and kept of Internet access from those computers. The court thus upheld a search which revealed numerous pornographic photographs downloaded onto Simons's computer. *Id.*

143 *See, e.g.*, Doe *ex rel.* Doe v. B.P.S. Guard Servs., Inc., 945 F.2d 1422, 1424–27 (8th Cir. 1991). Organizers of a fashion show at a convention center set up a curtained dressing area for the models, unaware that the area was visible on one of the convention center's security cameras. *Id.* at 1424. Guards in the security control room used the surveillance camera to watch and videotape the models changing clothes. *Id.* Although the curtained area was used by all of the models and presumably was accessible to the show's director and assistants, the court nevertheless (and correctly) held that the models had a cause of action for invasion of privacy predicated on the video surveillance. *Id.* at 1427.

144 *See, e.g.*, Roberts v. Houston Indep. Sch. Dist., 788 S.W.2d 107, 108, 111 (Tex. Ct. App. 1990) (holding that a school teacher had no legal complaint when school officials videotaped her classroom performance, with her knowledge but over her objection, because she had no reasonable expectation of privacy while teaching).

Sometimes it is with a legitimate business purpose and sometimes without.[145] Sometimes the surveillance is guided by discretion and common sense, and sometimes it is not.[146] In the absence of legislation regulating such surveillance, so long as the cameras capture only visual images and not sounds, only in rare instances would such surveillance be criminal.[147] Thus, whether the employee is liable for civil damages depends on general tort law, rather than specific legislation regulating video surveillance.

B. Installation of "Cookies"

A "cookie" is a data file that is placed on a computer's hard drive when the user visits a particular Web site.[148] The cookie is used by the Web site to develop and store information about the user, including usernames, preferences, browsing habits, and online purchases. These memory files facilitate access to Web sites, allow for the use of targeted banner advertisements,[149] and enable features such as shopping carts.[150] Once a user has accessed a Web site that uses cookie technology or an affiliated site, the embedded

---

145 *See, e.g.*, United States v. Bissell, 954 F. Supp. 841, 864–67 (D.N.J. 1996), *aff'd*, 142 F.3d 429 (3d Cir. 1998). To investigate allegations that a part owner of a gasoline service station was defrauding a fellow investor, government officials, with the investor's permission, installed a camera overlooking a desk area of the service station in a room that was readily accessible to customers and visible through windows from the parking lot. *Id.* at 864. The camera videotaped the defendant pocketing a substantial portion of the receipts before depositing the rest in company bank accounts. *Id.* The court held that the videotaping was not a search because defendant lacked a reasonable expectation of privacy in the area. *Id.* at 866; *see also* Marrs v. Marriot Corp., 830 F. Supp. 274, 283 (D. Md. 1992). In *Marrs*, the court upheld an employer's use of a camera to monitor one employee's desk drawer after the employee had complained that someone had tampered with its contents. *Id.* at 277. The camera captured the plaintiff, a coworker, picking the lock. *Id.* The court held that the plaintiff had no "reasonable expectation of privacy in an open office." *Id.* at 833; *see also* Sacramento County Deputy Sheriffs' Ass'n v. County of Sacramento, 59 Cal. Rptr. 2d 834, 843–44 (Ct. App. 1996) (holding that deputy sheriffs lacked a reasonable expectation of privacy against being videotaped in a jail office in which inmates' property was stored, particularly because the office was accessible to other people, including inmates).

146 *See, e.g.*, Savo, *supra* note 11, at 174 (reporting that managers of the Sheraton Boston Hotel secretly videotaped employees in their locker room, supposedly in an attempt to catch a busboy suspected of selling cocaine; this invasion of privacy cost the hotel $200,000 in a settlement agreement).

147 As noted previously in this Article, there is no federal legislation regulating video surveillance, and only a few states have enacted such laws. *See supra* note 29.

148 Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502–03 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001).

149 *See DoubleClick*, 154 F. Supp. 2d at 502. In *DoubleClick*, the court described the renting of advertising space on a Web site as follows:

> Commercial Web sites often rent-out online advertising "space" to other Web sites. In the simplest type of arrangement, the host Web site (e.g., Lycos.com) rents space on its webpages to another Web site (e.g., TheGlobe.com) to place a "hotlink" banner advertisement . . . . When a user on the host Web site "clicks" on the banner advertisement, he is automatically connected to the advertiser's designated Web site.

Id.

150 This is the electronic equivalent of a supermarket shopping cart when one is shopping online—an electronic "place" to "store" various items the shopper has selected until, after the

cookie on the hard drive begins collecting data about the user's Web activities.

In four reported cases—*Chance v. Avenue A, Inc.*,[151] *In re Intuit Privacy Litigation*,[152] *In re DoubleClick, Inc. Privacy Litigation*,[153] and *In re Pharmatrak, Inc.*,[154] computer users have sued upon discovering that commercial Web sites have installed cookies on their computers. The suits were based on three federal statutes: the Wiretap Act,[155] the Stored Communications Act,[156] and the Computer Fraud and Abuse Act ("CFAA").[157]

1. The Wiretap Act

In *Chance*, *Intuit*, and *DoubleClick*, the courts correctly rejected Wiretap Act claims. In each case, the user communicated information to a commercial Web site, which installed a cookie on the user's hard drive; the cookie directed the user's computer to send the same information to a third party, which compiled such information to develop user profiles.[158] In each case, the court held that no unlawful interception had occurred because, even if the transmission to the third party constituted an "interception" of the user's communications with the Web site, this was done with the consent of the Web site, which was a party to the communication.[159] Thus, the interception was consensual under 18 U.S.C. § 2511(2)(d),[160] and, because it was not conducted for a tortious or illegal purpose, it was lawful.[161]

In *Pharmatrak*, however, the companies maintaining the Web sites specifically instructed the third party *not* to collect information that would identify the user, but the third-party's cookie did so anyway.[162] This action, the court correctly held, was not protected by the consent exception in § 2511(2)(d), because the Web site companies had not consented to interception of that information.[163]

---

shopping expedition is complete, the shopper is ready to pay for all of his or her purchases. *See* NEWTON'S TELECOM DICTIONARY, *supra* note 42, at 719.

151 *Chance*, 165 F. Supp. 2d at 1155.

152 *Intuit*, 138 F. Supp. 2d at 1274.

153 *DoubleClick*, 154 F. Supp. 2d at 502–03.

154 *In re* Pharmatrak, Inc., 329 F.3d 9, 12 (1st Cir. 2003).

155 18 U.S.C. §§ 2510–2522 (2000 & Supp. I 2001) (Wiretap Act).

156 18 U.S.C. §§ 2701–2712 (2000 & Supp. I 2001) (Stored Communications Act).

157 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000 & Supp. I 2001).

158 Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1156–57 (W.D. Wash. 2001); *DoubleClick*, 154 F. Supp. 2d at 503–04; *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001).

159 *Chance*, 165 F. Supp. 2d at 1163; *DoubleClick*, 154 F. Supp. 2d at 519; *Intuit*, 138 F. Supp. 2d at 1278.

160 *See supra* note 117 and accompanying text.

161 *Chance*, 165 F. Supp. 2d at 1163; *DoubleClick*, 154 F. Supp. 2d at 519; *Intuit*, 138 F. Supp. 2d at 1279.

162 *In re* Pharmatrak, Inc., 329 F.3d 9, 15 (1st Cir. 2003).

163 *Id.* at 20–21. In *Pharmatrak*, several pharmaceutical companies invited users to visit their Web sites to access information about their products and rebates. *Id.* at 12. Pharmatrak collected information about the Internet users who visited the pharmaceutical companies' Web sites and sold that information to the companies. *Id.* This information allowed each company to track the Web pages a user viewed within a Web site, how long the user spent on each Web page, the visitor's path through the site, including points of entry and exit, the visitor's IP address, and

2. *Computer Fraud and Abuse Act*

The CFAA makes it a crime to access a computer without authorization and states that whoever "intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication . . . shall be punished as provided in subsection (c) of this section."[164]

The CFAA also creates a civil cause of action for the victim of such unauthorized access.[165] The statute permits such a suit, however, only if a plaintiff suffers "damages" as defined in the statute. "[T]he term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information that—(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals . . . ."[166]

In *DoubleClick* and *Chance*, each court held that although plaintiffs could combine as a class to achieve the minimum threshold of $5,000 damages or economic loss, they had to prove that a single act of unauthorized access to a particular computer caused the plaintiffs to suffer an aggregate loss that met the threshold.[167] Apparently, if a single act of unauthorized access to a particular computer by the defendant cost each of 500 individuals $10, this would meet the threshold; but if the defendant, in 10,000 separate albeit identical acts, illicitly inserted a cookie on 10,000 separate computers, causing each computer user $1, or $10, or $100, or $4,999, in damages or loss, this would not meet the threshold.

In *DoubleClick*, the court also concluded that the damages asserted by plaintiffs—the inconvenience and time required to delete the cookie, the economic value of having plaintiffs view certain advertisements, and the value of

---

the Web page the user viewed immediately before arriving at the client's site (i.e., the "referrer URL"). *Id.* at 13. Pharmatrak also enabled each company to compare the traffic on its Web site to the traffic on the other companies' Web sites. *Id.* Pharmatrak accumulated the data by transmitting a persistent cookie to the user's computer that allowed it to track the user's access to the Web sites in question for ninety days. *Id.* at 13–14, 14 n.5. Users who visited the Web sites were not informed of this. *Id.* at 13–14. Although the companies insisted that the process must not collect any identifying data about who visited the Web sites, and Pharmatrak assured them that it did not, in fact such information (including date of birth and medical condition) entered by a small number of users who visited the Web sites was gathered. *Id.* at 15. The Court of Appeals for the First Circuit correctly held that such personal information qualifies as the "contents" of an electronic communication under the Electronic Communications Privacy Act, and that Pharmatrak "intercepted" such contents by acquiring the information contemporaneous with the transmission of that information. *Id.* at 18–19.

164 18 U.S.C. §§ 1030(a)(2), (a)(2)(C) (2000).

165 Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages.

Id. § 1030(g).

166 *Id.* § 1030(e)(8)(A). "Damages" can also be shown if the unauthorized access impairs medical care, *id.* § 1030(e)(8)(B); causes physical injury, *id.* § 1030(e)(8)(C); or threatens public health or safety, *id.* § 1030(e)(8)(D).

167 Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1157 (W.D. Wash. 2001); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 523–24 (S.D.N.Y. 2001).

the demographic data accumulated—did not have the requisite monetary value.[168]

3. Stored Communications Act

Three courts have considered whether installing a cookie on a computer's hard drive, and accessing the information gathered thereby, constitutes accessing a stored electronic communication in violation of 18 U.S.C. § 2701(a). This statute states as follows:

> (a) OFFENSE.—Except as provided in subsection (c) of this section whoever—
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[169]

At issue in each case was whether the defendant's activities came within an exception to § 2701(a) codified in § 2701(c):

> (c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—
> (1) by the person or entity providing a wire or electronic communications service;
> (2) by a user of that service with respect to a communication of or intended for that user . . . .[170]

In *Intuit*, a federal judge in California reached the emotionally satisfying conclusion that installation of a cookie on a computer's hard drive did violate the statute.[171] To do so, however, the court had to "rewrite" the statute. In the other two decisions, *DoubleClick* and *Chance*, the courts, applying the statute as written, concluded correctly, if disappointingly, that this conduct does not violate the Stored Communications Act.[172]

a. DoubleClick *and* Chance

DoubleClick is the leading case and is, therefore, worth a more detailed review than the other cases.

---

168 *DoubleClick*, 154 F. Supp. 2d at 524. The court refused to accept a monetary evaluation for the inconvenience and time required to delete the cookie because the defendant had provided a reasonable method for a computer user to opt out of having a cookie implanted in the first place. *Id.* at 524–25. It rejected the concept that the defendant's opportunity to present the plaintiffs with advertising constituted economic damages or loss to plaintiffs. *Id.* at 525. Lastly, "although demographic information is valued highly . . . the value if its collection has never been considered an economic loss to the subject." *Id.*

169 18 U.S.C. § 2701(a) (2000).

170 *Id.* § 2701(c)(1)–(2).

171 *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1276 (C.D. Cal. 2001).

172 *Chance*, 165 F. Supp. at 1162; *DoubleClick*, 154 F. Supp. 2d at 514.

DoubleClick, Inc. "acts as an intermediary between host Web sites and Web sites seeking to place banner advertisements" by placing a client Web site's banner advertisement on the screens of viewers who match the client's demographic target.[173] DoubleClick does so "by building detailed profiles of Internet users and using them to target clients' advertisements."[174] DoubleClick compiles the profiles by using its own technology to sift through information it obtains from thousands of affiliated Web sites.[175] The only information DoubleClick acquires is information that the user voluntarily discloses to a DoubleClick-affiliated Web site.[176]

The process begins when a computer user visits a Web site (e.g., "ABC.com") affiliated with DoubleClick.[177] To visit that Web site, the user's computer automatically communicates certain information to the Web site.[178] The Web site installs a cookie on the user's hard drive, instructing the user's computer to "send a communication automatically to DoubleClick's server."[179] This communication includes the cookie number, the name of the DoubleClick-affiliated Web site the user visited, the user's browser-type, and a request that DoubleClick send advertisements to fill the blank spaces in the ABC.com Web page.[180] DoubleClick technology automatically evaluates all of the information that has been accumulated about that user,[181] including information obtained as a result of the user's prior visits to other DoubleClick Web sites, and chooses the banner ads from other DoubleClick clients that fit the user's profile.[182] DoubleClick also updates its profile of that user by adding the fact that the user has visited the ABC.com Web page.[183] Likewise, the cookie collects information about anything the user does while visiting the ABC.com Web site.[184]

The court stressed three "clearly defined parameters" that limited the information the DoubleClick cookies collected.[185] First, the cookies only collected information concerning the user's activities on DoubleClick-affiliated Web sites.[186] Second, there was no allegation that DoubleClick ever attempted to obtain any information that the user did not voluntarily reveal to a DoubleClick affiliate, or that DoubleClick attempted to access files, pro-

---

173 *DoubleClick*, 154 F. Supp. 2d at 502.

174 *Id.*

175 *Id.* at 503.

176 *Id.* at 504.

177 *Id.* at 503.

178 *Id.*

179 *Id.*

180 *Id.*

181 As the court in *DoubleClick* noted, the cookie collects data about the user's computer and not about the user him or herself. *Id.* at 502 n.7. If several people use the same computer to visit DoubleClick-affiliated Web sites, DoubleClick has no way of isolating which user happens to be using the computer at any given time. *Id.* The converse is also true; "if one person uses multiple computers, DoubleClick would be unable to identify and aggregate the person's activity on different computers." *Id.*

182 *Id.* at 503–04.

183 *Id.* at 504.

184 *Id.*

185 *Id.*

186 *Id.*

grams, or other information on users' hard drives.[187] Third, DoubleClick provided users with an easy, no-cost way of preventing DoubleClick's tracking.[188]

Plaintiffs alleged that DoubleClick's placement of cookies on their computers' hard drives constituted unauthorized access to stored communications on their computers and, therefore, violated 18 U.S.C. § 2701(a) of the Stored Communications Act.[189] The court rejected this claim, holding that DoubleClick's activities fell within an exception in the statute set forth in § 2701(c)(2), exempting conduct authorized by a user of a wire or electronic communications service "with respect to a communication of or intended for that user."[190] The court concluded that the DoubleClick-affiliated Web sites were "users" of the Internet within the meaning of that term in § 2701(c)(2).[191] Because all the plaintiffs' communications with the DoubleClick-affiliated Web sites accessed by DoubleClick's cookies were either communications "of" those Web sites or communications "intended for" those Web sites, and the Web sites authorized DoubleClick to access those communications, DoubleClick's activities fell within the § 2701(c)(2) exception.[192]

Plaintiffs also argued that the information stored in the cookie on a computer's hard drive (i.e., the identification number) was an electronic communication in "electronic storage" because they were never sent to or through the Web sites.[193] The court rejected this contention.[194] First, even assuming the cookie identification number installed on the plaintiff's hard drive was an "electronic communication," it was not in "electronic storage," as that term is defined in 18 U.S.C. § 2510(17).[195] The statute defines "electronic storage" as:

> (A) any *temporary, intermediate storage* of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication *by an electronic communication service* for purposes of backup protection of such communication . . . .[196]

---

187 *Id.*

188 *Id.* at 504–05. As to the latter, the court noted that users had two options: "(1) visiting the DoubleClick Web site and requesting an 'opt-out' cookie; and (2) configuring their browsers to block any cookies from being deposited." *Id.*

189 *Id.* at 507.

190 18 U.S.C. § 2701(c)(2) (2000). This provision is the Stored Communications Act's equivalent of 18 U.S.C. § 2511(2)(d), the consensual interception provision of the Wiretap Act. *See supra* note 117 and accompanying text.

191 *DoubleClick*, 154 F. Supp. 2d at 508–09.

192 *Id.* at 513.

193 *Id.* at 511.

194 *Id.* at 511–13.

195 *Id.*

196 18 U.S.C. § 2510(17) (2000) (emphasis added). Section 2510 is the first section in the Wiretap Act. *See id.* § 2510. The Stored Communications Act specifically imports the definitions from the Wiretap Act. *See id.* § 2711(1) (2000) ("[T]he terms defined in section 2510 have . . . the definitions given such terms in that section . . . .").

The court correctly reasoned that a cookie did not qualify for statutory protection under § 2510(17) because a user's hard drive was not an "electronic communication service."[197] The court also found that a cookie did not qualify for statutory protection under § 2510(17)(A) because that provision only protects a communication that was "temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it."[198] Thus, the statute did not protect an electronic communication that was stored on the recipient's hard drive after it had been received.[199] The court also found that the cookie could not qualify under § 2510(17)(A) for another reason; that provision protects only communications in "temporary" storage, while the DoubleClick cookie remained on the user's hard drive for an indefinite period of time.[200] As the court stated, "[I]n plain language, 'indefinite' existence is the opposite of 'temporary,' and the DoubleClick cookie's residence on plaintiffs' hard drives is certainly not an 'intermediate' step in their transmission to another addressee."[201]

Finally, the court held that even if a DoubleClick-installed cookie *was* a stored electronic communication, it still fell within the § 2701(c)(2) exception, which exempts the act of accessing a stored communication "by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user" from the criminal provision.[202] Thus, DoubleClick's cookie was exempted because DoubleClick was a "user" of the service, and the cookie (if it was a "stored communication") was intended for itself.[203]

The facts in *Chance* are substantially identical to those in *DoubleClick*.[204] In *Chance*, Avenue A played the same intermediary role between the individual user and the commercial Web sites as DoubleClick.[205] The only factual difference was that Avenue A had a commercial agreement

---

197 *DoubleClick*, 154 F. Supp. 2d at 511.

198 *Id.* at 512. The statute's specific use of the terms "temporary" and "intermediate" makes it clear that the ECPA "only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it." *Id.*

199 *Id.*

200 *Id.*

201 *Id.* It takes only a slight twist of this reasoning to portray the court as holding that a computer owner is not protected by a statute designed to safeguard against "temporary" intrusion because in this case the intrusion is permanent.

202 *Id.* at 513–14; *see supra* note 170 and accompanying text.

203 *DoubleClick*, 154 F. Supp. 2d at 513. As the court observed:

> In every practical sense, the cookies' identification numbers are internal DoubleClick communications—both "of" and "intended for" DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs' hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. In contrast, virtually all plaintiffs are unaware that the cookies exist, that these cookies have identification numbers, that DoubleClick accesses these identification numbers and that these numbers are critical to DoubleClick's operations.

Id.

204 Chance v. Avenue A., Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001).

205 *Id.* at 1156–57.

with DoubleClick that allowed Avenue A to supply DoubleClick-affiliated Web sites with advertising even if those Web sites had no affiliation with Avenue A.[206] As the court in *Chance* noted:

> Although this is a significant factual difference from DoubleClick, it leads to the identical legal conclusion. DoubleClick still has the necessary authorization from the web site to escape liability under § 2701(c)(2) and the rerouting is irrelevant after that initial authorization. The statute only addresses the entity that "accesses" the communication, not any party to which the authorized accessor decides to route it, such as Avenue A in this case. Because the web site has in all cases authorized either Avenue A or DoubleClick to access the communication between the computer user and the web site, the § 2701(c)(2) exception applies, and the end result of no liability is the same.[207]

Although the judge in *Chance* differed somewhat on the question of whether the user's computer could be considered a "facility" as that term is used in § 2701(a),[208] the result was the same: the defendant was protected by the exception in § 2701(c)(2) and, therefore, was entitled to a directed verdict.[209]

---

206 *Id.* at 1157.

207 *Id.* at 1161.

208 "[I]t is possible to conclude that modern computers, which serve as a conduit for the web server's communication to Avenue A, are facilities covered under the Act." *Id.* at 1161; *see DoubleClick*, 154 F. Supp. 2d at 508–09.

209 *Chance*, 165 F. Supp. 2d at 1162; *see DoubleClick*, 154 F. Supp. 2d at 514 (holding that "all plaintiff's communications accessed by DoubleClick fall under § 2701(c)(2)'s exception . . . and, accordingly, are not actionable," and that plaintiffs' claim should be dismissed). Conceding "this rather strained interpretation of a 'facility through which an electronic communication service is provided,'" the *Chance* court held, did not avail the plaintiffs; the commercial Web sites that the user visits are "users" of the "electronic communication service." *Chance*, 165 F. Supp. 2d at 1161.

> It naturally follows that any communication between the individual computer and the web site is a communication "of or intended for" that user . . . [and if] web sites are "users" and the communications allegedly accessed by Avenue A are "of or intended for them," the § 2701(c)(2) exception only requires that the web site "authorize" Avenue A's conduct.

Id. The court found that this fact, too, was clearly established. *Id.*

> Any web site for which Avenue A provides advertisements must have written the programming code required to direct Plaintiffs' computers to Avenue A's server. Given the technological and commercial relationship between web sites and Avenue A, it is implausible to suggest that any such "access" by Avenue A was not intended or authorized by the web site. In fact, the opposite conclusion is inescapable: the very raison d'etre of Avenue A is to provide web sites with targeted advertising, and it cannot do so without the collaboration and consent of those sites.

Id. (citing *DoubleClick*, 154 F. Supp. 2d at 509).

b. Intuit

By contrast, the court in *Intuit* concluded that the type of cookie under discussion did in fact violate the Stored Communications Act.[210] It did so by the simple expedient of rewriting the statute to support that conclusion:

> Section 2701 does not require, nor has any court ever interpreted it to require, that a defendant accused of violating Section 2701 be a third-party to an electronic communication which eventually may be in electronic storage in a facility. More specifically, Section 2701 *does not require that there be a "communication" at all*, i.e. the existence or absence of communication is irrelevant. The primary act required for violation of Section 2701 is the act of accessing electronically stored data.[211]

The court could reach this remarkable conclusion only by ignoring the title of the statute, the title of the specific provision in question, and its contents. The statute is under the heading "Stored Wire and Electronic *Communications* and Transactional Records Access."[212] Section 2701 is entitled "Unlawful access to stored *communications*."[213] The provision makes it a crime if someone "intentionally accesses without authorization a facility through which an electronic *communication* service is provided" or "intentionally exceeds an authorization to access that facility . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic *communication* while it is in electronic storage in such system."[214] To read this to mean that § 2701 "does not require that there be a 'communication' at all" and that the statute's primary focus "is the act of accessing electronically stored data" is a truly remarkable example of judicial Humpty Dumptyism.[215]

The court went on in a footnote: "Hereinafter, the court uses the term 'data' interchangeably with the statutory term 'electronic communication.'"[216] But the Stored Communications Act, which the court was purportedly applying, does not consider "data" and "communication" to be "interchangeable." The statute defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature *transmitted in whole or in part* by a wire, radio, electromagnetic,

---

210 *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1275–76 (C.D. Cal 2001).

211 *Id.* at 1275–76 (emphasis added). The court continued: "For example a hypothetical 'hacker' who accesses data in a computer without the owner's knowledge would be guilty of violating Section 2701 even though the hacker had no 'communication' with the storing agency, i.e. the hacker is not a 'third-party' to a communication." *Id.* As is spelled out below, this is simply a gross misreading of the statute.

212 18 U.S.C. §§ 2701–2712 (2000) (Stored Communications Act) (emphasis added).

213 *Id.* § 2701 (emphasis added).

214 *Id.* § 2701(a) (emphasis added).

215 "When *I* use a word," Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean—neither more nor less."

"The question is," said Alice, "whether you *can* make words mean so many things."

"The question is," said Humpty Dumpty, "which is to be master—that's all."

LEWIS CARROLL, ALICE IN WONDERLAND AND THROUGH THE LOOKING GLASS 238 (Grosset & Dunlap 1996) (1872).

216 *Intuit*, 138 F. Supp. 2d at 1276 n.4.

photoelectronic or photooptical system that affects interstate or foreign commerce," with exceptions not germane to the current discussion.[217]

This definition confirms what was already plain and obvious. A statute entitled "Stored Wire and Electronic Communications" regulates access to stored wire and electronic communications and not to stored data generally.

c. Evaluation

DoubleClick and *Chance* interpreted § 2701 correctly. This conclusion is supported by the plain language of the statute (to the extent that any clause in any provision of any federal statute dealing with electronic surveillance can be said to have a "plain" meaning) and by its legislative history.[218] Additional support for the *DoubleClick* interpretation is the implication of the contrary holding. If *Intuit* is good law, then each use of commercial cookies is a federal felony.[219]

And yet, the result of a correct reading of the statute is appalling. A statute designed to protect the privacy of an individual's use of his or her computer winds up protecting the right of a commercial enterprise to install a program into a person's computer; to use that program to gather information about the users of that computer; to compile a profile of those users; and to enable businesses to target specific advertisements at the users with that information. All of this legally can take place without the computer user's informed consent.

The result is directly attributable to the relative antiquity of the Stored Communications Act, which is now a bit more than eighteen years old—adequate perhaps for the technology of 1986 but as antiquated today as, say, legislation enacted in the 1920s regulating the manufacture and operation of automobiles.[220]

The threat to privacy posed by cookies is not particularly egregious. But the idea that an advertising company can install an electronic bug on my home or office computer and accumulate information about me, assemble a profile of my buying habits (which may or may not be accurate),[221] and in

---

217 18 U.S.C. § 2510(12) (2000) (emphasis added). For a discussion on the relationship of the definitions to the Stored Communications Act, see *supra* note 196.

218 *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001) (discussing the text of the statute and its legislative history as support for the proposition that "Congress' intent was to protect communications held in interim storage by electronic communication service providers").

219 In *DoubleClick*, the court commented:

> [I]f § 2510(17) were interpreted in the manner plaintiffs advocate, Web sites would commit federal felonies every time they accessed cookies on users' hard drives, regardless of whether those cookies contained any sensitive information. This expansive reading of a criminal statute runs contrary to the canons of statutory interpretation and Congress' evident intent.

Id. at 512–13.

220 "Although the Act was intended to cover such mid-1980s technological facilities as telephone companies, email servers, and bulletin boards, modern technology has placed the personal computer at a focal point of Internet communications." Chance v. Avenue A., Inc., 165 F. Supp. 2d 1153, 1160 (W.D. Wash. 2001).

221 See *supra* note 181. Even if I am the only person using the computer, my cookie "profile" may be grossly inaccurate. For example, if I went online to buy a canned ham as a gift for a

essence "rent out" that profile to advertisers, all without my knowledge or consent, and without any legal remedy or recourse,[222] is infuriating.

I am not arguing that cookies should be outlawed. People have the right to share information about themselves with commercial enterprises. Indeed, some consumers might appreciate the convenience that may follow when merchants have a clearer idea of what kinds of goods and services are likely to interest them. But this should be a matter of choice, not stealth. Legislation should be enacted requiring companies like DoubleClick and its affiliates to explain, in plain language, what kinds of information it will acquire, how it will acquire the information, how it will use the information, and with whom it will share it. Such companies should be required, also, to provide a user-friendly opt-out option or, even better, to collect information only on computer users who affirmatively opt *in*.[223] These requirements would give each user the ability to make an informed choice about whether or not to consent to the accumulation of a user profile. It would also provide a firm basis on which to claim damages if a cookie installer exceeds the limits spelled out in the notice.

C. *"Shopper Discount" or "Bonus" Cards*

Anyone who has ever shopped in a supermarket knows that some percentage of the store's wares are almost always specially priced because the manufacturer is seeking to entice new consumers, the store overstocked certain items, or the store wants a loss-leader. In the past few years, however, more and more stores make these bargains available only to customers who have store "shopper discount" or "bonus" cards. Some pharmacy chains have begun instituting the same practice. The store compiles a profile of purchases made with the card number, which is used to target the named card holders with specific ads and discount coupons. (The enrollment or application forms permit the customer to opt out of receiving such mailings.) Some stores also award periodic "bonus points" that entitle the customer to additional discounts.

This sounds fairly benign until you consider that using such a card permits the store to keep a detailed record of each transaction the customer makes: the date, store location, time, and items purchased, including not only food and drink but also over-the-counter health products—birth control products, pregnancy test kits, and various other items that suggest a great deal about a customer's physical and emotional condition and intimate behavior. If the store is also a pharmacy, the profile may also include prescrip-

---

Christian friend, a couple of romance novels for my aunt, and a kung fu movie for my nephew, the ads the cookie would send me would probably be a bit off, given that I keep kosher, do not read bodice rippers, and have no idea which end of a chukka-stick is supposed to stir the soup.

222 *But see* Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*, 76 S. CAL. L. REV. 893 (2003) (arguing that insertion of cookies into computers constitutes the common law tort of trespass to chattels).

223 DoubleClick, in fact, agreed to a procedure much along these lines when it settled a suit brought by several state attorneys general. Press Release, DoubleClick, Attorneys General End Investigation into DoubleClick's Ad Serving Practices (Aug. 26, 2002); Stephanie Miles, *DoubleClick Settles Investigation*, WALL. ST. J. (Europe), Aug. 28, 2002, at A6.

tions filled at the store.[224] Marketers are smugly delighted at how easy it has been to get customers to provide such information.[225]

In researching this Article, I obtained three application forms: one from Giant Foods (which in some states does business as "Super-G"), one from Safeway (both Giant and Safeway are multistate supermarket chains), and one from CVS Pharmacy. Each form has a space for the applicant to provide his or her name, address, home phone number,[226] and e-mail address.[227] The Safeway and CVS forms contain space for the applicant's date of birth; Giant does not. None requests the applicant's social security number.[228] Directly above where the applicant is to sign, each contains a statement explaining how the information will be used and assuring the applicant that the information gathered will not be sold or leased. Presumably a disclosure in violation of this agreement would subject the store to a suit for breach of contract.

---

224 The CVS/pharmacy ExtraCare enrollment form privacy agreement states in pertinent part, "As an extra service to our valued customers, we can send you offers and information that are customized based on your prescription and non-prescription purchases." *See infra* note 229. By contrast, the Giant Foods privacy statement on its Web site states in bold-face type:

> This privacy policy does not include Giant/Super G pharmacy records. Pharmacy records are kept separate from other Customer Information and maintained in accordance with the privacy and other requirements of Federal and state law. Please speak to your pharmacist for additional information.

GIANT, GIANT PRIVACY STATEMENT, *at* http://www.giantfood.com/Privacy.htm (last modified July 11, 2003).

225 *See* Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534, 536 (2002) (quoting statements from a trade publication and an industry executive). The article is unabashedly an advocacy piece. Albrecht describes herself in the author profile:

> Katherine Albrecht is the founder and director of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), a national grass-roots consumer group dedicated to fighting supermarket "loyalty" or frequent shopper cards. CASPIAN's efforts are dedicated to educating consumers, condemning marketing practices that invade customers' privacy, and encouraging privacy-conscious shopping habits across the retail spectrum. Formed in 1999, CASPIAN has since reached millions of American consumers with its pro-privacy message.

Id. at 565.

226 The home phone number is used as an alternate identification device in case the customer forgets his or her card. It is worth noting, however, that the federal "do not call" legislation, *see supra* notes 111–14 and accompanying text, exempts from the telemarketing ban companies with which the telephone subscriber has done business in the past eighteen months. *See* 16 C.F.R. § 310.4(b)(1)(iii)(B)(ii) (2004) (exempting seller who has an "established business relationship" with the target of the call); 16 C.F.R. § 310.2(n) (defining "established business relationship" as "a relationship between a seller and a consumer based on" a business transaction between the seller and the consumer taking place within the eighteen months preceding the date of the telemarketing call). Thus, applying for a card exempts the store from telemarketing restrictions and frees the store or its parent company to make telemarketing calls to the cardholder's home phone.

227 Friends who have obtained such cards tell me that stores do not insist that e-mail addresses be provided, although the application does not inform the applicant of this.

228 A different section of the Safeway form can be used to apply for a Safety Smartcheck card; that section does ask for the applicant's social security number. *See* SAFEWAY, SAFEWAY CLUB CARD APPLICATION, *available at* http://www.safeway.com/app.pdf (last visited August 12, 2004).

Still, there are differences in the three privacy provisions. The CVS statement unequivocally states that it "NEVER" gives or sells "any specific information about you to any manufacturers or direct marketers."[229] The *Safeway Club Card Customer Agreement Statement*, by contrast, reads, in pertinent part, as follows: "We respect your privacy. Safeway does not sell or lease personally identifying information (i.e., your name, address, telephone number, and bank and credit card numbers) to *non-affiliated* companies or entities."[230]

An attempt to learn the identities of "affiliated companies" was unavailing.[231]

Giant's *Privacy Statement* provides the greatest detail of the three as to how the company will acquire information, to whom it will disclose it (it, too, states that information may be disclosed to affiliated companies, without naming them), and the circumstances. It is, for example, the only one of the

---

229 CVS/PHARMACY, CVS/PHARMACY EXTRACARE CARD ENROLLMENT FORM, *available at* https://www.cvs.com/CVSApp/cvs/gateway/registerextracare?LOGINMSG=XFRACAREMSG (last visited August 12, 2004). The CVS/pharmacy ExtraCare Card enrollment form privacy statement is as follows:

> PRIVACY AGREEMENT As an extra service to our valued customers, we can send you offers and information that are customized based on your prescription and non-prescription purchases. We may at times use an outside processing company as CVS's agent to help print and send mailings; beyond your name and address, these agents do not receive any personal information and are bound to strict confidentiality. We value your privacy and NEVER give or sell any specific information about you to any manufacturers or direct marketers.

Id.

230 SAFEWAY, *supra* note 228. The *Safeway Club Card Customer Agreement Statement* reads as follows:

> We respect your privacy. Safeway does not sell or lease personally identifying information (i.e., your name, address, telephone number, and bank and credit card account numbers) to *non-affiliated* companies or entities. We do record information regarding the purchases made with your Safeway Club Card to help us provide you with special offers and other information. Safeway also may use this information to provide you with *personally tailored* coupons, offers or other information that may be provided to Safeway by other companies. If you do not wish to receive personally tailored coupons, offers or other information, please check the box below. Must be at least 18 years of age.

Id.

231 On December 10, 2003, I called the regional Safeway office for the Maryland suburbs of Washington, D.C. The recording directed that for any inquires about the Club Card program, I should dial, toll-free, 1-877-723-3929. The recording at that number directed that, to enable the company to "access your account more fully," I should enter either my Club Card number or my phone number. I did nothing. After a pause, the automated system responded, "I'm sorry, I did not recognize that number." I entered my office phone number. Same response. I entered my cell phone number. Same response. In other words, unless you are a "member" already, no apparent means are offered to get past the machine to ask questions about the program. On my fourth try, when asked for my card or phone number, I entered "0"—not an option given by the recording. After a brief musical interlude—as it happened, Billy Joel's recording *You May Be Right (I May Be Crazy)*—I spoke to "Helen," who told me she is located in Phoenix. When I asked her the identity of "affiliated" companies, she said she "imagined" that they would only share the information with other Safeway stores. I asked who could give me a more precise answer. After another reasonably short interlude on hold, Helen said she would send an e-mail to corporate headquarters in California asking someone there to call or write to me. Is anyone surprised to learn that no one ever got back to me?

three to mention that the information could be subpoenaed. Giant's statement invites those seeking additional information to visit its Web site.[232]

The question of "affiliated companies" aside, the privacy statements are reasonably reassuring on their face. But there may be much less to privacy promises than meets the eye. Consider again the Safeway promise: "Safeway does not sell or lease personally identifying information (i.e., your name, address, telephone number, and bank and credit card numbers) to *non-affiliated* companies or entities."[233] According to an activist who seeks to warn consumers against using such cards, even if companies delete such "personally identifying information" from customer profiles before those profiles are shared or sold, "[a] computer process called 'reidentification' can allow marketers to re-attach names and addresses to 'anonymous' records" quite easily by combining the remaining information with information available from other databases.[234] And even if the store shares the information with no one, incidents have occurred where companies do so accidentally, or corrupt employees sell the information illicitly.[235] Moreover, the privacy agreements do not preclude the *store* from combining its own profile of a customer with the vast amounts of other information likely to be available about most people from various databases.[236]

Nor does the privacy policy preclude the store from using its information against a customer if a dispute arises between the two, as allegedly happened in one case.[237] A private litigant may subpoena such information.[238] Other

---

232 GIANT FOODS, INC., GIANT BONUSCARD APPLICATION AND CHANGE FORM, Form 810120 (2003). The application form contains the following:

> We will not disclose customer names, home or e-mail addresses, or phone numbers to any company, other than those affiliated with Giant, without your permission. We may provide information to unaffiliated companies who perform a service on our behalf, such as mail houses who process mailings for us. In such cases, our vendors sign a strict confidentiality agreement and cannot use this information for any other purpose. Giant may disclose customer identifiable information as required by law in response to a subpoena or court order.
>
> Purchases made with your BonusCard will be automatically recorded. The BonusCard is our primary means of collecting information that helps us to target benefits and services to our customers. For your protection, Giant has developed a set of privacy policies for the use and handling of this data. (For detailed information, visit our website at www.giantfood.com).
>
> One of the most exciting aspects of this program is the opportunity to provide offers targeted to specific customer needs. This means we can provide baby offers to families with babies, and pet offers to families with pets.

Id. The form offers an "opt out" box for "[c]ustomers who do not want to receive targeted offers in the mail," with the caveat that selecting that option leaves the customer ineligible for the company's electronic sweepstakes program. *Id.*

233 SAFEWAY, *supra* note 228.

234 Albrecht, *supra* note 225, at 536–37, 565 (reporting that most people can be reidentified merely by combining zip code and date of birth). Although the Safeway form promises not to reveal a customer's name, address, phone number, or bank and credit card numbers, it does not promise to withhold a customer's date of birth from those to whom it sells or leases the data. SAFEWAY, *supra* note 228.

235 Albrecht, *supra* note 225, at 537.

236 *Id.*

237 A shopper sued a supermarket, claiming he slipped on a yogurt spill in the store and fractured his kneecap. *Id.* A mediator allegedly told the plaintiff's attorney that the store

grim possibilities for use of such information include a supermarket chain sharing customer purchase records with health insurance companies, which might then refuse to cover the customer or restrict coverage for certain conditions;[239] use of such information by the Internal Revenue Service[240] or prosecutors;[241] and store use of driver's licenses or biometrically secure identification techniques to prevent shoppers from falsely identifying themselves when they obtain or use the card.[242]

At least two states have enacted legislation prohibiting stores from requiring customers to disclose certain information to obtain such cards and prohibiting stores from selling or sharing cardholders' personal information.[243]

IV. The Media

A. In General

"Ethical journalism" has always been a somewhat fluid concept.[244] The willingness of mainstream media companies to use surveillance technology to intrude upon individual privacy in pursuit of a story is not a twenty-first century phenomenon.[245] In the past several years, however, restraints on what is

---

planned to introduce the plaintiff's liquor purchase records at trial to paint him as an alcoholic. *Id.*

238 *Id.* (relating that in a divorce action, the wife used the husband's supermarket card records indicating purchases of expensive wine as a basis to argue that he could afford to pay more alimony than he claimed he could pay). Of the three membership applications I examined, only the Giant BonusCard application mentions that the information is subject to subpoena. *See* GIANT, *supra* note 232.

239 Albrecht, *supra* note 225, at 538.

240 *Id.* at 539 (reporting that such practices are already used by British tax enforcement authorities "to investigate whether shoppers' spending habits match the lifestyles indicated by their tax returns").

241 *Id.* (relating an incident in which Drug Enforcement Agency agents obtained supermarket card data of individuals in Arizona who had purchased large quantities of plastic bags, which are often used to package illicit drugs, as well as more benign substances (such as brownies for a bake sale)).

242 *Id.* at 558–59.

243 CAL. CIV. CODE §§ 1749.61–.66 (West 2000) (prohibiting stores from requiring driver's license or social security numbers to obtain a discount card and prohibiting stores from selling or sharing cardholders' personal information); CONN. GEN. STAT. § 42-371 (2003). For an analysis and critique of these provisions, see Allison Kidd, Note, *A Penny Saved, A Lifetime Learned? The California and Connecticut Approaches to Supermarket Privacy*, 4 N.C. J.L. & TECH. 143 (2002).

244 The same can probably said of the ethical standards of many professions, including the legal profession.

245 *See, e.g.*, Quentin Burrows, Note, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1107–08 (1997) (noting the regularity with which "camera crews follow police and emergency personnel as well as use video surveillance cameras mounted on poles and buildings"); Howard Kurtz, *Hidden Network Cameras: A Troubling Trend? Critics Complain of Deception as Dramatic Footage Yields High Ratings*, WASH. POST, Nov. 30, 1992, at A1. For example, Group W Productions did a television story about a traffic accident and the resulting rescue operation, including footage of plaintiffs' extrication from the wreck and conversations between plaintiffs and members of the rescue crew. Shulman v. Group W Prods., Inc., 955 P.2d 469, 475–76 (Cal. 1998). The court held that aspects of the situation that could be seen and heard by passers-by and onlookers were newsworthy and not protected by any

(to borrow a phrase) "fit to print" or broadcast have pretty much disintegrated.[246] The decline might have begun when Senator Gary Hart challenged reporters to catch him in adultery if they could, and, taking up the challenge, they did.[247] The antics of Bill Clinton as governor and president, and the equally offensive extremes to which his political enemies went in their attempt to destroy him, gave the media the perfect excuse to abandon whatever limitations remained.[248]

Consider, for example, Monica Lewinsky's infamous blue dress from The Gap. The passage of time has perhaps permitted us to forget some of the details we never cared to know, but it is worth reviewing how the existence of the damning evidence first became public. On January 21, 1998, gossip and sleazemonger Matt Drudge first reported on his Internet *Drudge Report* that Lewinsky possessed a "black cocktail dress" with presidential DNA on it.[249] Responsible institutions in the mainstream media presumably had heard similar rumors but had not published them because they had not been properly sourced. Yet, the next day, NBC's *Today* show interviewed Drudge, who repeated the story while admitting that he had no confirmation besides his single source.[250] Once *The Today Show* "broke" the story, a typical media feeding frenzy took place, each mainstream media outlet striving to outdo the others.[251] On Friday evening, January 23, ABC's *World News Tonight*

---

right to privacy. *See id.* at 490–91. Other items shown or played, however, were actionable. *See id.* The nurse who participated in extricating plaintiffs from their car wore a microphone to enable the corporate defendant to tape her conversations with one plaintiff. *Id.* at 475. Regardless of whether the cameraman could have heard this conversation with his unaided ear, the court held, it was a triable issue whether, by persuading the nurse to wear the microphone, the cameraman listened in on a conversation that plaintiff could reasonably have expected to be private. *Id.* at 491. Moreover, after they were extricated, a cameraman accompanied the victims in the helicopter to the hospital. *Id.* The court stated that "we are aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent." *Id.* at 490; *see also* Sanders v. Am. Broad. Cos., 978 P.2d 67, 71 (Cal. 1999) (holding that a worker for a telepsychic marketing company, whose employees gave psychic readings to customers over the telephone, had a cause of action for tortious intrusion because a television news reporter, working undercover as an employee with the same company, had covertly recorded her conversations with the plaintiff by wearing a small video camera in her hat and a microphone in her bra).

246 I am modifying the slogan that appears as the upper left hand slug on the front page of the *New York Times*: "All the News That's Fit to Print."

247 *See* Jim Savage, *Gary Hart Affair Turned Spotlight on Paper*, MIAMI HERALD, Sept. 15, 2002, at 9MH (reporting how the author and another reporter "broke" the story of Senator Hart's dalliance with Donna Rice). Savage notes the coincidence that the *Miami Herald*'s story "was published on the same Sunday that The New York Times published a story that contained Hart's denial of womanizing allegations and his famous challenge to the press to 'follow me around[,] . . . it will be boring.'" *Id.* That statement can indeed be found in *The New York Times Magazine* profile of Hart. *See* E.J. Dionne, Jr., *Gary Hart: The Elusive Front Runner*, N.Y. TIMES, May 3, 1987, § 6 (Magazine), at 37 ("'Follow me around. I don't care,' he says firmly, about the womanizing question. 'I'm serious. If anybody wants to put a tail on me, go ahead. They'd be very bored.'").

248 For a description of these excesses, see McClurg, *supra* note 67, at 1010–13.

249 Adam Cohen, *The Press and the Dress*, TIME, Feb. 16, 1998, at 52.

250 *Id.*

251 *See generally id.*

was the first mainstream news outlet to report the story based on its own sources, rather than on Drudge's story.[252]

That the media competes to publish salacious details about people who become "news" is nothing new,[253] but the "Drudgification" of journalism—the fact that it is now "news" that someone with little credibility publishes a rumor on the Internet—demonstrates the danger the media pose to the privacy of those who fall into its maw.

B. Bartnicki v. Vopper

In 2001, the United States Supreme Court, in *Bartnicki v. Vopper*, considerably increased the media's destructive power when it held that the media are immune from civil damages suits brought under 18 U.S.C.

---

252 *Id.*; Lawrence K. Grossman, *Spot News: The Press and the Dress*, COLUM. JOURNALISM REV., Nov.–Dec. 1998, at 34, 34. In all candor, gentle readers, I must confess to a personal resentment about all this. That week in January, the red-hot story was that Monica Lewinsky had called her friend Linda Tripp numerous times in the preceding months describing her encounters with President Clinton, and that Tripp had taped many of those conversations. On the morning of January 22, I was interviewed by ABC-TV News about the legality of taping telephone conversations and the admissibility of such evidence at trial at their downtown Washington studio. I was clear, I was concise, I was witty; in short, I was brilliant, and the producer told me that the interview would be prominently featured on that night's show.

I drove back to the law school, where I immediately e-mailed my faculty colleagues, my friends and relatives, and my synagogue listserv about my impending media stardom. Some time between my interview and air time, however, someone at ABC decided that the hot story, to which about fifteen minutes of the show was devoted, was about rumors—*mere rumors!*—about the dress. Thus, my five minutes of fame gave way to a rumor of presidential proportions.

253 The most dramatic examples involve media coverage of criminal, and occasionally civil, litigation. For a short overview of previous trials which also became media circuses, see Laurie L. Levinson, *Cases of the Century*, 33 LOY. L.A. L. REV. 585, 587–92 (2000), briefly discussing, among others, the trials of Ted Kaczynski (the "Unabomber"), Harry Thaw (for the 1907 murder of architect Sanford White), the McNamara brothers (for terrorist bombs that killed numerous people in Los Angeles in 1910), Sacco and Venzetti, Bruno Richard Hauptmann (for kidnapping and killing Charles and Anne Morrow Lindbergh's baby), the Nuremberg War Crime trials of 1945 to 1946, O.J. Simpson, the trial in 1911 arising out of the Triangle Shirtwaist Company fire (where wholesale violation of safety regulations resulted in the death of more than a hundred employees when a fire broke out in its factory), the Scopes "monkey" trial of 1925, the 1975 to 1976 robbery trial of Patty Hearst (the newspaper heiress who in 1974 was kidnapped by a radical group and then joined her abductors in the commission of several crimes), the Scottsboro rape trials of 1931, the rape trial of William Kennedy Smith, the securities fraud trial of Charles Keating, and the assault trials arising from the beating of Rodney King. Subsequent articles in the issue cover specific trials or trial lawyers in greater depth. *See generally id. See also* THE PRESS ON TRIAL—CRIMES AND TRIALS AS MEDIA EVENTS (Lloyd Chiasson, Jr., ed., 1991) (including chapters on the 1735 trial of John Peter Zenger; the 1770 trial arising out of the Boston Massacre, in which, by the way, John Adams defended the British soldiers charged with murder; the 1859 trial of John Brown; the Haymarket Riot trial of 1886; the trial of Lizzie Borden in 1893 for chopping up her parents; the Harry Thaw murder trial; the case of the Chicago "Black Sox," who were accused of fixing the 1921 World Series; the Scopes, Scottsboro, and Hauptmann trials; the espionage trials of Alger Hiss and the Rosenbergs; the 1969 "Chicago Seven" trial arising out of protests against the Vietnam War; the Charles Manson murder trial; the trial of Lt. William Calley for the murder of Vietnamese civilians; and the O.J. Simpson case).

Some media organizations, it should be noted, occasionally refuse to participate in salacious reporting. *See, e.g.*, Tracey, *supra* note 62 (relating that one Colorado newspaper has announced it will not cover frivolous details of the trial of L.A. Lakers basketball star Kobe Bryant for rape).

§ 2511(1)(c) of the Wiretap Act.[254] The Court held that the media may publish or broadcast with impunity the contents of intercepted communications that they know or have reason to know were unlawfully intercepted, so long as the media company that published or broadcasted the communication did not participate in the unlawful interception and the contents of the communication were of "public interest."[255] A concurring opinion signed by two members of the six-justice majority opinion offered some hope that the damage may be limited.[256] Nevertheless, the decision has ominous implications for anyone in public life or anyone who becomes embroiled in a publicized controversy. Although the decision does not directly involve the Internet, those implications, when combined with the way the Internet and more traditional arms of the media interact, merit discussion here.

Bartnicki arose out of a situation that comes to every community from time to time, a wage dispute between county school officials and the teachers union.[257] During the dispute, Kane, the president of the union, vented his frustration in a phone conversation with Bartnicki, the union's chief negotiator, by suggesting that they "blow off the front porches" of some school board members.[258] Someone, identity unknown, intercepted the call.[259] Eventually the union won a favorable tentative agreement.[260] Well after the strike had been settled, and some four months after the phone conversation, someone anonymously delivered the tape to a community activist who opposed the union's demands.[261] The activist gave copies of the tape to two local radio stations, which played excerpts on the air.[262] Television stations and newspapers picked up the story thereafter.[263]

---

254 *See* Bartnicki v. Vopper, 532 U.S. 514, 525 (2001).

255 *Id.*

256 *Id.* at 541 (Breyer, J., concurring).

257 *Id.* at 518.

258 *Id.* at 518–19.

259 *Id.* at 518. Bartnicki used a cellular phone; Kane presumably used a hard-wired phone. *Id.* The call probably was intercepted at random by someone using a scanner equipped to scan the frequencies at which cellular calls are transmitted. *See supra* note 103. Such scanners cannot target a particular cell phone, because a cellular phone does not have a particular frequency dedicated to it. *See* S. REP. NO. 99-541, at 9 (1986) (explaining cellular telephone services operation). Rather, the cell phone company switching station computer randomly assigns a frequency to each call it receives. *Id.* If the cell phone moves from one cell to another during the call, the call is automatically handed from one switching station to the next, and each switching station randomly assigns a new frequency to it. *Id.* The other possibility is that someone unlawfully tapped Kane's hard-wired phone. However the call was intercepted, the interception was unlawful under 18 U.S.C. § 2511(1)(a). *See* 18 U.S.C. § 2511(1)(a) (2000).

260 *Bartnicki*, 532 U.S. at 519.

261 *Id.*

262 *Id.*

263 *Id.*

The union officials sued the activist and radio stations[264] under 18 U.S.C § 2520,[265] alleging a violation of 18 U.S.C. § 2511(1)(c), which provides:

> (1) Except as otherwise specifically provided in this chapter any person who—
>
> . . . .
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> . . . .
>
> (4) shall be fined under this article or imprisoned not more than five years, or both.[266]

Defendants moved for summary judgment on First Amendment grounds.[267] The trial judge denied the motion but certified the First Amendment issue to the U.S. Court of Appeals for the Third Circuit.[268] The government intervened to defend the statute.[269] The Third Circuit reversed, granting defendants' motion for summary judgment on the First Amendment issues.[270] The Supreme Court, dividing six to three, held that the First Amendment precluded imposition of civil damages for the disclosure because the tape recording containing information of (supposed)[271] public significance and the defendants (two radio stations, their reporter, and the activist who gave the tape recording to the radio stations) played no role, direct or indirect, in the unlawful interception.[272]

The decision has been analyzed extensively,[273] so I offer only a brief overview here. The majority acknowledged that the Wiretap Act provision

---

264 Presumably no suit was brought against the television stations and newspapers that reported the matter thereafter because, once it was aired on the radio, any privacy interests the speakers had in the conversation were already destroyed. Commenting on 18 U.S.C. §§ 2511(1)(c) and (d), the Senate Judiciary Committee stated, "The disclosure of the contents of an intercepted communication that had already become 'public information' or 'common knowledge' would not be prohibited." S. REP. NO. 90-1097, at 93 (1968), *reprinted in* 1968 U.S.C.C.A.N 2112, 2181.

265 18 U.S.C. § 2520. Recovery of civil damages authorized

> (a) IN GENERAL.—[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520(a) (Supp. I 2001). Relief may include a preliminary injunction, other equitable or declaratory relief; actual, punitive, or liquidated damages; and reasonable attorneys' fees and other litigation costs. 18 U.S.C. § 2520(b) (2000). For a detailed discussion of civil actions based on this provision, see FISHMAN & MCKENNA, *supra* note 29, §§ 4:31–:40.

266 18 U.S.C. §§ 2511(1), (4).

267 *Bartnicki*, 532 U.S. at 520.

268 *Id.* at 521.

269 *Id.*

270 *Id.* at 522.

271 As explained briefly below, I do not believe there was any public significance to the contents of the tape.

272 *Id.* at 525.

273 *See, e.g.*, Daniel P. Paradis, Comment, Bartnicki v. Vopper*: Cell Phones and Throwing*

was content-neutral, as applied to defendants, but held that it nevertheless constituted "a regulation of pure speech."[274] Thus, the provision was subject to the general rules that "state action to punish the publication of truthful information seldom can satisfy constitutional standards,"[275] and that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order."[276]

The government argued that the statute served two interests: "[F]irst, the interest in removing an incentive for parties to intercept private conversations, and second, the interest in minimizing the harm to persons whose conversations have been illegally intercepted."[277] The Court dismissed the first as speculative and unsupported by empirical data.[278]

The majority acknowledged, however, that the government's second interest, minimizing the harm to the victims of illegal interception, "is considerably stronger" than the first asserted interest,[279] that "the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself,"[280] and that "the fear of public disclosure of private conversations might well have a chilling effect on private speech."[281] But "privacy concerns give way when balanced against the interest in publishing matters of public importance."[282] Such was the situation, the majority concluded, in the case at hand.[283] The Supreme Court stated: "The months of negotiations over the proper level of compensation for teachers at the Wyoming Valley West High School were unquestionably a matter of public con-

---

Stones, 37 NEW. ENG. L. REV. 1117 (2003); Jennifer Nichole Hunt, Note, Bartnicki v. Vopper: *Another Media Victory or Ominous Warning of a Potential Change in Supreme Court First Amendment Jurisprudence?*, 30 PEPP. L. REV. 367 (2003). A somewhat more detailed version of my own analysis and criticism of the decision may be found in FISHMAN & MCKENNA, *supra* note 29, § 4:12.1.

274 *Bartnicki*, 532 U.S. at 526.

275 *Id.* at 527 (quoting Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 102 (1979)). Although *Bartnicki* was a civil suit brought by a private litigant, the case indirectly involved "state action" because it was a federal criminal statute, 18 U.S.C. § 2511(1)(c), that created the cause of action.

276 *Bartnicki*, 532 U.S. at 528.

277 *Id.* at 529.

278 *Id.* at 530–32. The Court concluded:

> Although this suit demonstrates that there may be an occasional situation in which an anonymous scanner will risk criminal prosecution by passing on information without any expectation of financial reward or public praise, surely this is the exceptional case. Moreover, there is no basis for assuming that imposing sanctions upon respondents will deter the unidentified scanner from continuing to engage in surreptitious interceptions. Unusual cases fall far short of a showing that there is a "need . . . of the highest order" for a rule supplementing the traditional means of deterring antisocial conduct. The justification for any such novel burden on expression must be far stronger than mere speculation about serious harms. Accordingly, the Government's first suggested justification for applying § 2511(1)(c) to an otherwise innocent disclosure of public information is plainly insufficient.

Id. at 531–32 (citations, footnotes, and internal quotation marks omitted).

279 *Id.* at 532.

280 *Id.* at 533.

281 *Id.*

282 *Id.* at 534.

283 *Id.* at 535.

cern, and respondents were clearly engaged in debate about that concern. That debate . . . is . . . worthy of constitutional protection."[284]

Well, yes. But Kane and Bartnicki were not "engaged in debate about that concern" during the unlawfully intercepted phone call. They were having a private conversation about their frustrations and problems.[285]

The Supreme Court attempted to limit its decision in several ways. First, it left open the question whether, if a newspaper or other public medium *unlawfully* acquired information of "public concern," the government could punish disclosure as well as the unlawful acquisition.[286] It also held out the possibility that the prohibition against disclosure might be upheld with regard to matters not of "public concern" such as "trade secrets or domestic gossip."[287] But a trade secret—which, after all, enables a company to charge more for its product or services—can easily be made a matter of "public concern" by politicians, agitators, and their allies in the media. And, given current journalistic standards, query whether there is any distinction between "public concern" and "gossip," at least as it relates to anyone who ever has attracted media attention.[288]

Justice Breyer, joined by Justice O'Connor, filed a concurring opinion "to explain why . . . the Court's holding does not imply a significantly broader constitutional immunity for the media."[289] The concurrence may be of considerable significance, because, although Justices Breyer and O'Connor signed Justice Stevens's majority opinion rather than concurring separately, without their votes, Justice Stevens's opinion would not have attracted a majority of the Court.

Justice Breyer emphasized that, although 18 U.S.C. § 2511(1)(c) and the corresponding provision of Pennsylvania's law "restrict public speech" and "media publication" and do so "directly, deliberately, and of necessity . . . not simply as a means, say, to deter interception, but also as an end," they also "directly enhance private speech" and, therefore, promote First Amendment and privacy rights.[290] Thus, "[a]s a general matter . . . the Federal Constitution must tolerate laws of this kind because of the importance of these privacy and speech-related objectives."[291]

Under the facts, however, as Justice Stevens wrote, the statutes in question "disproportionately interfere with media freedom."[292] Justice Stevens cited two reasons supporting this conclusion. First, the broadcasters had in

---

284 *Id.*

285 *Id.* at 518.

286 *Id.* at 528.

287 *Id.* at 533.

288 Suppose, for example, a scanner intercepted a participant in the teachers' salary dispute having an angry cell phone conversation with his or her spouse and leaked it to a local newspaper. Is it too difficult to imagine the paper running an article entitled, say, "Pressures of Salary Dispute Hit Home," including excerpts of the conversation to illustrate the "newsworthy" fact that being caught in an angry public debate has its effects on participants' home life, too?

289 *Id.* at 536 (Breyer, J., concurring).

290 *Id.* at 537.

291 *Id.* at 537–38.

292 *Id.*

no way participated in or actively encouraged the unlawful interception.[293] Second, "the speakers had little or no *legitimate* interest in maintaining the privacy of the particular conversation" because it "involved a suggestion about 'blow[ing] off . . . front porches' and 'do[ing] some work on some of those guys,' . . . thereby raising a significant concern for the safety of others."[294]

Oh, please. The excerpt of the conversation reproduced in the opinion strongly suggests that the only "blowing off" that did or would occur was Bartnicki and Kane blowing off steam. This is confirmed by the fact that no porches in the county had been damaged between the phone call and its disclosure[295]—a disclosure which came, significantly, *after* the dispute had been resolved mostly to the teachers' satisfaction.[296] Clearly there was no longer any need, assuming there ever was a need, for the local authorities to form a special Porch Protection Unit.[297]

If the four-month old fact that allies in a since-settled public controversy used hyperbole while venting to each other in a private conversation is of sufficient "public concern" to trump privacy legislation enacted by Congress, it is difficult to discern how any information about those in public life would escape such a classification. Consider the following hypothetical situations:

- Suppose a hacker broke into stored e-mails and discovered that a candidate for public office had been treated for depression a

---

293 *Id.*

294 *Id.* at 539 (alterations in original). Justice Breyer cited several situations in which "the law recognizes a privilege allowing the reporting of threats to public safety" where the act of reporting would otherwise be actionable. *Id.* For example, there is a general privilege against privacy actions to report "that another intends to kill or rob or commit some other serious crime against a third person." *Id.* (citing RESTATEMENT (SECOND) OF TORTS § 595 cmt. G (1977)). There is a privilege that is likely permitted in trade secret law to disclose information "relevant to public health or safety, or to the commission of a crime or tort, or to other matters of substantial public concern." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995). *See also* Lachman v. Sperry-Sun Well Surveying Co., 457 F.2d 850, 853 (10th Cir. 1972) (stating that a nondisclosure agreement is not binding with respect to criminal activity); Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 343–44 (Cal. 1976) (noting that the psychiatric privilege is not binding in the presence of danger to oneself or others).

295 I assume that the respondents would have introduced evidence of any otherwise unexplained epidemic of porch explosions in the intervening period.

296 Apparently, whoever recorded the conversation never presented the tape to the police, as a civic-minded citizen might be expected to do if the conversation could reasonably be interpreted to indicate any serious intent to harm another physically.

297 That the supposed threat was uttered in May 1993, and the tape was not delivered to the broadcasters until four months later, after the dispute had been settled, did not, in Justice Breyer's view, alter the outcome. *Bartnicki*, 532 U.S. at 539 (Breyer, J., concurring). "Even where the danger may have passed by the time of publication, that fact cannot legitimize the speaker's earlier privacy expectation. Nor should editors, who must make a publication decision quickly, have to determine present or continued danger before publishing this kind of threat." *Id.* The Court found this particularly true because petitioners were "limited public figures," who "voluntarily engaged in a public controversy." *Id.* But if the "editors" (i.e., radio station personnel) were truly concerned about a "present or continuing danger," they would have notified the police. Instead, they aired the tapes. The facts strongly suggest that the only danger the editors feared was the risk of losing a juicy story (and the resultant publicity for the radio stations), with perhaps the added "benefit" of reigniting the rancor in the community that only recently had begun to subside.

few years earlier. Or suppose the candidate's former employer, reviewing the e-mails sent to or by the candidate on the company's system, made the same discovery. The snoop or the former employer leaks the information to the media. Is this arguably of "public concern"? It is not very difficult to imagine an argument that the public has a "right" to decide whether such information is relevant in assessing the candidate's fitness for office.

- Suppose instead that the information discovered is that the candidate refills a prescription for Viagra each month. Presumably all nine of the Justices would agree that this is not a matter of "public concern." But once information was posted anonymously on the Internet, there would be no privacy in the information left to preserve, which would free the media to report about the information's availability on the Web.[298]

Justice Breyer concluded his concurrence with the following:

> [T]he Constitution permits legislatures to respond flexibly to the challenges future technology may pose to the individual's interest in basic personal privacy. Clandestine and pervasive invasions of privacy, unlike the simple theft of documents from a bedroom, are genuine possibilities as a result of continuously advancing technologies. Eavesdropping on ordinary cellular phone conversations in the street (which many callers seem to tolerate) is a very different matter from eavesdropping on encrypted cellular phone conversations or those carried on in the bedroom. But the technologies that allow the former may come to permit the latter. And statutes that may seem less important in the former context may turn out to have greater importance in the latter. Legislatures also may decide to revisit statutes such as those before us, creating better tailored provisions designed to encourage, for example, more effective privacy-protecting technologies.[299]

This passage is encouraging, until the reader seriously attempts to figure out what it means. First, there is nothing in the record to suggest that either participant in the Kane–Bartnicki phone conversation used his cell phone "in the street" where passers-by could overhear. Second, nothing in Justice Breyer's concurring opinion prior to this paragraph suggests that his position would have changed if the cell phone had been encrypted. Finally, technologies already exist that enable a snoop to intrude into the mundane *and* the most intimate activities, thoughts, and words of those targeted for the surveillance. *Legislation* is not needed "to encourage . . . more effective privacy-

298 *See supra* note 63 (where the "agony aunt" photograph lawsuit was dismissed because the "aunt" no longer had an expectation of privacy in the posted photos).

299 *Bartnicki*, 532 U.S. at 541 (Breyer, J., concurring). The Court, therefore, must "avoid adopting overly broad or rigid constitutional rules, which would unnecessarily restrict legislative flexibility. I consequently agree with the Court's holding that the statutes as applied here violate the Constitution, but I would not extend that holding beyond these present circumstances." *Id.*

protecting *technologies*";[300] the marketplace will provide encouragement enough. But if the technological revolution of the past several decades proves anything, it proves that technological innovation will protect privacy for only a short period at best before snoops develop techniques to overcome it.

What is needed is *legal* protection against both the seizure of private information and its dissemination. The statutory provision at 18 U.S.C. § 2511(1)(c) is well crafted, designed to deter unlawful interception of communications not only by punishing those who intercept it, but by frustrating those who might hope to use the media to disseminate the information. Additional legislation similarly protecting stored communications and other data would expand such protection. Instead, the Court, in *Bartnicki v. Vopper*, interprets existing legislation such that the damage a private snoop can do to his target's privacy is greatly multiplied. A snoop can guarantee that unlawfully obtained information will be disseminated to the public by anonymously passing such information on to media outlets. The media can lawfully publish information obtained by unlawful interception of communications, by unauthorized access to stored communications, and, presumably, by unlawful hacking into private files and records, so long as it played no direct part in the prior illegality, and the target's words, actions, or thoughts can be said to have been "of public concern."[301]

Conclusion

Privacy long has been a deeply held value. The law has played a part in protecting privacy, but that part is necessarily limited. Until the past few decades, privacy was protected from individual and commercial snooping primarily by the limitations of technology available to acquire, store, or retrieve information. Privacy was also protected by an informal social contract, often breached but never formally disputed, that certain matters were nobody's business or, at least, had no place in the mainstream organs of communication.

Advances in surveillance technology and data storage and retrieval have stripped away most of the practical safeguards to privacy, and the situation will get only worse.[302] At the same time, the "social contract" that often limited the dissemination of private information has been effectively revoked. It is not at all clear that the law could make up for these losses. Unfortunately, gaps in federal legislation and a most unfortunate Supreme Court decision may render the law impotent to protect privacy in a wide range of circumstances.

Current debate has focused primarily on restricting and regulating the government's ability to use the Internet to intrude upon individual privacy.

---

300 *Id.* (Breyer, J., concurring) (emphasis added).

301 *See id.* at 535.

302 It is possible that techniques such as encryption will provide adequate protection to some forms of communication and data storage. But the need to give legitimate recipients quick and ready access to information will likely preclude encryption from becoming a broadly effective remedy.

The far greater threat to privacy, however, comes from private individuals and businesses. The Internet and related technologies have given anyone with a mind to do so the ability to snoop on and betray others and to disseminate hurtful and embarrassing information. Add in the profits to be made from identity theft, and the aggregate risk to privacy from individual betrayers, grudgers, and snoops far outstrips anything the government is likely to do or even to try to do.

Similarly, commercial enterprises have the resources and the motive to acquire detailed profiles about both the public and intimate aspects of our lives—where and when we travel, where and what we eat, what we do for entertainment, the personal hygiene products we buy. Employers may with impunity review every e-mail an employee sends or receives and every Web-browse an employee makes on company computers and Internet-access systems. Anyone who is brave, foolish, or unlucky enough to attract public attention is likely to be targeted for such lawful or unlawful attention by private snoops.[303] For those who become even "limited public figures,"[304] the real possibility exists that the mass media, which has cast off its own standards of restraint and has been licensed by the Supreme Court to knowingly publish the contents of unlawfully intercepted communications so long as they relate to matters of "public concern," will make private information a matter of local, regional, national, or even international common knowledge.

Symposia such as this one are valuable and important because a close study of the situation, generally and in its particulars, is a crucial step toward rectifying it. Still, I cannot escape the melancholy conviction that, in striving to preserve our traditional concepts of privacy, we are desperately trying to restore to health a beloved friend, who, despite our efforts, is dying.

---

303 Consider, for example, Monica Lewinsky, Linda Tripp, and Private Jessica Lynch. Private Lynch was an innocent victim of circumstance. Ms. Lewinsky acted foolishly, then indiscreetly (most of us did so one way or another when we were in our twenties, or thirties, or forties, or . . .). Ms. Tripp found herself caught up in a situation she did not seek and was unable to control. None of these women sought public attention; yet each, in varying degrees, found themselves targeted, examined, scrutinized, betrayed, and misrepresented by friends, strangers, and large, impersonal institutions. The same has been and is likely to be true of any woman who is sexually assaulted by a prominent man and reports it to the authorities. (Men as well as women can be and have been the victims of unsought public attention, but, for whatever reason, the public appetite for female victims is apparently far greater than that for male victims.)

304 *See supra* note 297.