1999

The Constitution and Encryption Regulation: Do We Need a "New Privacy"?

A. Michael Froomkin
University of Miami School of Law, froomkin@law.miami.edu

THE CONSTITUTION AND ENCRYPTION REGULATION: DO WE NEED A "NEW PRIVACY"?

*A. Michael Froomkin**

The regulation of cryptography is an issue that I personally believe is of great importance to our lives. I hope to persuade you over the next quarter hour that it will become increasingly important. I want to start, however, by briefly sketching the state of play regarding the legal and constitutional regulation of encryption, and then talk about the somewhat more speculative issues that really concern me the most.

The state of play right now is fairly simple. If you want to use encryption domestically to encrypt a stored file or a real-time communication, you can do so. Because this is peace time, there are, as has always been the case in this country in peace time, no limits whatsoever on your ability to use encryption technology—no legal limits, at any rate. There are export controls enforced for various kinds of cryptography that make it illegal to export various strong encryption products without a license. There are also certain categories of products for which certain categories of people do not and will not get licenses.

Those export control policies are being challenged in three court cases: *Bernstein v. United States Department of Justice*,[1] a California case, *Karn v. United States Department of State*,[2] a case out of Wash-

* © A. Michael Froomkin 1999. Professor, University of Miami School of Law. Internet: froomkin@law.tm. I have taken the liberty of tidying up the transcript of my talk, and breaking up or, on rare occasions, reorganizing sentences for clarity, but the text otherwise reflects my actual remarks. I have also added notes where I thought references might interest the reader or where there have been important developments since I delivered the talk on November 19, 1998.

1. 176 F.3d 1132 (9th Cir. 1999), *opinion withdrawn pending rehearing en banc*, ___ F.3d ___ (1999), *available in* No. 97-16686, 1999 WL 782073 (9th Cir. Sept. 30, 1999). Briefs and information on the progress of the case are available at *Challenging U.S. Export Controls on Encryption: Background to Bernstein v. U.S. Department of Justice*, ELECTRONIC FRONTIER FOUNDATION (visited Oct. 17, 1999) <http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoJ/>.

2. 925 F. Supp. 1 (D.D.C. 1996), *remanded by*, 107 F.3d 923 (D.C. Cir. 1997). Briefs and information on the progress of the case are available at *The Applied Cryp-*

ington, D.C., and *Junger v. Daley*,[3] an Ohio case. The *Bernstein* case was decided in favor of an academic who wanted a declaration that he could legally post source code from his Ph.D. dissertation on the Internet,[4] which under current law would result in an "export." Bernstein won in the district court, and the court said that source code is protected speech.[5] That decision was taken on expedited appeal to the Ninth Circuit, where it has languished for many, many months, verging on almost a year.[6] Maybe they are waiting for it to become moot, I do not know. Meanwhile, over in the D.C. district court, the cognate case, known as the *Karn* case, was decided against the person wishing to export encryption technology,[7] in what I have to say is one of the worst written decisions I have ever seen. You might agree with the bottom line, but the rationale, in which the court stated that this was a political question,[8] was, to my mind, extraordinarily unconvincing. On appeal, the D.C. Circuit vacated it as moot because the regulations had changed;[9] so, the case went back to district court in front of a new judge, the original judge unfortunately having died in the interim, and, there it remains waiting to be decided.

Meanwhile, on the regulatory side, the major statute that provides the legal underpinning for the export control rules lapsed. Congress had put in a sunset provision in the Export Administration Act and did not renew the statute when it lapsed.[10] You would think, perhaps, that

---

tography Case: Only Americans Can Type (visited Oct. 17, 1999) <http://people.qualcomm.com/karn/export/index.html>.

3. 8 F. Supp.2d 708 (N.D. Ohio 1998) (holding that export of encryption software is not expressive enough to merit First Amendment protection). The *Junger* case is currently being appealed. Briefs and information on the progress of the case are available at *Junger v. Daley* (visited Oct. 17, 1999) <http://samsara.law.cwru.edu/comp_law/jvd/>.

4. *See Bernstein*, 176 F.3d at 1147.

5. *See* Bernstein v. United States Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996), *aff'd sub nom.* Bernstein v. United States Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *opinion withdrawn pending rehearing en banc*, ___ F.3d ___ (1999), *available in* No. 97-16686, 1999 WL 782073 (9th Cir. Sept. 30, 1999).

6. The expedited appeal was ordered on Sept. 22, 1997; oral argument was heard in December 1997. The Ninth Circuit ultimately issued its opinion on May 6, 1999. *See Bernstein*, 176 F.3d at 1132. As of this issue going to press, the United States had been granted a rehearing en banc. *See* Bernstein v. United States Dep't of Justice, No. 97-16686 (9th Cir. Sept. 30, 1999) (order granting rehearing en banc) (copy on file with author).

7. *See Karn*, 925 F. Supp. at 3.

8. *See id.* at 6.

9. *See* Karn v. United States Dep't of State, No. 96-5121, 1997 U.S. App. LEXIS 3123, at *1 (D.C. Cir. Jan. 21, 1997) (per curiam).

10. The statutory authority for Export Administration Regulations (EAR) is the Export Administration Act of 1979, 50 U.S.C. app. §§ 2401-2420 (1994). *See* 15 C.F.R. § 730.2 (1999) ("The EAR have been designed primarily to implement the Export

the rules which grew out of it would have lapsed as well. They did not. President Clinton signed an emergency order (as I might add, many of his predecessors had done when earlier versions of the law had lapsed for shorter periods of time) saying that the rules needed to be kept in force, and he has signed an extension of that order every six months.[11] It is only slightly cruel and barely unfair to say that the national emergency, which is being cited as a justification for keeping this statute in place, is that Congress has refused to pass a new bill. Some of us are very concerned about this.[12]

This is perhaps my main point for you today. Although the cases in the courts deal with the constitutionality of export controls, for my money, what really matters are the domestic rules and the domestic effects of the export control rules: export controls being used as a tool to try to limit the options available to Americans in practical terms. This was not the original intent of those statutes, and it is probably not the way they ought to be used. The emergency is being used in a way that I think is more appropriate for a banana republic than for a strong constitutional democracy. If Congress does not choose to re-pass a bill that it sunsetted, that failure to act ought to have some consequences. When it does not, the nature and quality of our democracy is undermined.

Now we are seeing proposals in Congress—and I am referring specifically to one of the bills mentioned in the materials handed out today,[13]—bills which are endorsed by the FBI as being the closest to giving them what they want. These would impose rather strong controls on the type of encryption that could legally be sold or distributed

---

Administration Act of 1979 . . . ."). The Export Administration Act of 1979 lapsed on August 20, 1994. *See* 50 U.S.C. app. § 2419 (1994). President Clinton issued an executive order requiring that the Export Administration Act be kept in force to "the extent permitted by law" under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706 (1994). Exec. Order No. 12,924, 3 C.F.R. 918 (1994), *reprinted in* 50 U.S.C. § 1701 (1994).

11. The Export Administration Act expired on August 20, 1994. *See* U.S.C. § 2419 (1994). Exec. Order No. 12,924 of August 19, 1994, 3 C.F.R. 918 (1994), extended by the Presidential Notices of August 15, 1995, 3 C.F.R. 501 (1995); August 14, 1996, 3 C.F.R. 298 (1996); August 13, 1997, 3 C.F.R. 306 (1997); and August 13, 1998, 3 C.F.R. 294 (1998), continued almost all of the Export Administration Regulations in effect under the IEEPA.

12. *See* A. Michael Froomkin, *It Came From Planet Clipper*, 1996 U. CHI. LEGAL F. 15, 71-75, *available in* <http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm> [hereinafter Froomkin, *Planet Clipper*].

13. *See H.R. 695 – The "SAFE" Bill, Amendment to H.R. 695 Offered by Mr. Oxley of Ohio*, CENTER FOR DEMOCRACY AND TECHNOLOGY (visited Sept. 29, 1999) <http://www.cdt.org/crypto/legis_105/SAFE/Oxley_Manton_rev.html> (referred to as Oxley/Manton Amendment to Security and Freedom Through Encryption (SAFE) bill).

to American citizens; they are de facto, broad, encryption controls in America. We have reason to be concerned about these proposals, and I want to talk about these reasons.

But before I do that, let me play lawyer for just a couple of minutes and talk to you about this wonderful document which I came upon just a couple of days ago: the Department of Justice FAQ (frequently asked questions) on encryption.[14] This is, by the way, I think, an example of first-class public service. It is really clear, it is written in terms that make the policies accessible and understandable, and it does a good job of advocating for its cause. The fact that I am going to beat up on it a bit, because I disagree with it, should not in any way be taken to suggest anything but my admiration for the quality of the work, because I really think they do a public service in government when they clearly state what it is they are about. We should all be grateful for that.

So here it is. The Department of Justice FAQ on encryption policy, issued and dated November 16, 1998, just a couple of days ago, says that:

> The Framers of our Constitution determined that individuals would not have an absolute right of privacy. The Constitution recognizes that there are certain circumstances in which it is appropriate for law enforcement to obtain information that an individual wants to keep private: for example, when a judge finds probable cause to believe that such information is *** evidence of a crime. Decisions as to where that line should be drawn are political and legal ones, not scientific or business ones; they should be made by the Congress, the Executive, and the courts, not by programmers or marketers. Policy should regulate technology; technology should not regulate policy. Just as in the first part of the twentieth century, when the law had to take account of the changes in society brought about by the automobile, the law will have to take account of the changes brought about by encryption.[15]

Now, here I take it that the Department of Justice makes two claims: (1) policy should drive technology and not the other way around, and (2) the U.S. Constitution does not create an absolute right to privacy. I agree with both of those claims. That may make me the middle of the road on this panel, but I agree with both of those claims. However, they go on to say "[c]ourt-authorized wire-taps have proven to be one of the most successful law-enforcement tools" and that the

14. *See Department of Justice FAQ on Encryption Policy*, U.S. DEPARTMENT OF JUSTICE (last modified Sept. 17, 1999) <http://www.usdoj.gov/criminal/cybercrime/cryptfaq.htm> [hereinafter *Department of Justice FAQ*].

15. *Id.* at Question 6.

loss of those wiretaps would be just a disaster for law enforcement.[16] As society is becoming increasingly reliant on wire communications, they argue, law enforcement's need to access the contents of those communications, in appropriate circumstances, has also increased.[17] Then they go on to tell us by now somewhat-familiar stories about the high-profile espionage, terrorists, and criminal cases where electronic surveillance has detected groups that planned to do terrible things.[18] One group by itself planned to bomb the U.N. building, the Lincoln and Holland tunnels, the main federal building of New York City, and also assassinate political figures, and all this was foiled just by one little wiretap.[19] We are all better off for those successes I am sure, and it is no doubt good to be reminded not to underestimate the potential value of wiretaps.

Whether or not wiretaps are as essential to the work of law enforcement as the Department of Justice claims, I am probably not competent to tell you for certain. I have to confess, though, to having met enough people in law enforcement to suspect that they have the resources to work around whatever limitations we might impose on them, at least up to a point. So, my suspicion is things might not be quite as dire as they say, but I cannot prove that to you. I think, therefore, that we need to accept, at least for the sake of the argument, that all other things being equal, strong encryption will make law enforcement's job harder. Thus, law enforcement is going to have to spend more money, or do less, or do things differently. Change is always difficult, so there is a potential impediment to law enforcement here.

Now, the Department of Justice FAQ concludes that the world would just be a better place if everyone volunteered to use some sort of encryption system with government access to keys, which I will call "GAK" for short.[20] It might be key escrow, key recovery, the equivalent, whatever. The FAQ is careful to point out that the Justice Department does not advocate a mandatory approach.[21] I might ask, therefore, to what extent the Justice Department has been coordinating with the FBI, because it seems fairly clear to me that the FBI comes within about one hair of advocating a mandatory approach. When asked, the FBI says, "Anything that is not a mandatory approach does not satisfy our needs, and yes, things that are mandatory do satisfy our

16. *Id.* at Question 7.
17. *See id.*
18. *See id.* at Question 8.
19. *See id.*
20. *See generally id.* at Question 13.
21. *See id.* at Question 15.

needs. Of course, we are not advocating that because that would not be in keeping with the Administration's policy." Those are very subtle Washington distinctions.

The Justice Department likes to keep this discussion hypothetical and says that *if* faced with a hypothetical mandatory key escrow statute, it is the Justice Department's best judgment that a mandatory plaintext recovery regime, if properly structured, could comport with constitutional doctrine.[22] Here, I most emphatically disagree.[23] I mentioned one of the reasons before, in the question and answer: I do not read the Fourth Amendment as giving the federal government a right to an effective search. The Fourth Amendment is structured so that we have a basic right to be secure in our homes, et cetera. That right has a derogation in that, in certain circumstances, the government, with a court order, can conduct a search. That does not create any obligation on citizens who retain the sort of rights the Bill of Rights is designed to protect, to say, "Here it is! Here is the incriminating stuff!" or "Yes, here, let me help you understand my documents." That is just not the way the Constitution is supposed to work.

Another thing that I think the Department of Justice really glosses over in this FAQ is the way that reasonable expectations have been used in the case law. A great deal of Fourth Amendment law is based on some idea that a particular type of warrantless search is allowed because the person who is subjected to the search did not have a reasonable expectation of privacy. If you go through the cases, it is really quite an amazing catalog of circumstances under which we are told we did not have reasonable expectations: planes flying low over your house, the garbage in bags outside your curtilage, people standing on boxes to peek over high fences, people going inside fences with "No Trespassing" signs, all kinds of stuff.[24] In case after case, the so-called "drug exception" to the Constitution does its work,[25] and you

22. *See id.* at Questions 16 and 17.

23. *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PENN. L. REV. 709, 810-43 (1995) [hereinafter Froomkin, *Metaphor*], *available in* <http://www.law.miami.edu/~froomkin/articles/clipper1.htm>. *See generally* Froomkin, *Planet Clipper*, *supra* note 12.

24. *See generally* Laura B. Riley, Comment, *Concealed Weapon Detectors and the Fourth Amendment: The Constitutionality of Remote Sense-Enhanced Searches*, 45 UCLA L. REV. 281, 293-301 (1997); Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383 (1997).

25. *See generally* STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE, CASES AND COMMENTARY 285-88 (5th ed. 1996) ("If evidence will be destroyed in the time it takes to obtain a warrant, then the warrant requirement is

find that what you might have thought was a reasonable expectation of privacy is not reasonable.

Now comes a technology that proposes to change one's expectation of what privacy is reasonable, but for once would increase expectations instead of decreasing them, and here is the Justice Department saying, "No, no, we will design the system so that your expectations do not get out of control, so you do not expect too much, and that will be all right, because we will make what we are doing clear to you." They are honest about this: "We will make it clear to you that you must not expect too much, and you will not expect too much; it will be a self-fulfilling prophecy, and we will have access to plaintext."

I do not see why technology should be a one-way ratchet to reduce expectations of privacy. If we are going to talk about the relationship between social policy and technology, and argue that policy, not technology, should be the master, what are we to make of all this sense-enhanced searching, aerial surveillance, and all the rest, where it seems technology drove the policy? Why, all of a sudden, when a technology is going to increase privacy, do we suddenly reverse field and say technology must be limited? I do not get it. That may be more a policy issue than a constitutional law issue, but it seems to me a serious problem that ought to be considered.

The Department of Justice says that there are no Fifth Amendment issues in its hypothetical proposals. It argues that the advance deposit of decryption information—especially if done by the manufacturer before the product ever gets into a person's hand—does not create Fifth Amendment problems since disclosure by the manufacturer is neither compelled, testimonial, nor incriminating. Indeed, that is a conclusion that pretty well tracks the way that the law has developed in the past.[26] It is certainly the case that, as designed, current policies and current proposals, especially the House Intelligence Committee's substitute amendment for the SAFE Bill,[27] very cleverly sidestep all the Fifth Amendment issues by using technology. Why we should design a policy to take advantage of the back door to the Fifth Amendment that technology provides for us is not clear to me. I do not think that this is in keeping with the spirit of the Fifth Amendment, although I would be willing to accept that it might be in keeping with the letter of the law, as interpreted by prior precedent before the advances in

excused. . . . Not surprisingly, destruction of evidence issues often arise in drug cases.").

26. *See* Froomkin, *Metaphor*, *supra* note 23, at 836-38.

27. *See* Security and Freedom Through Encryption (SAFE) Act, H.R. 695, 105th Cong. (1997).

technology. Those precedents, however, did not have these social circumstances in mind.

The Department of Justice also says that there are no First Amendment issues. It identifies five types of First Amendment issues, some of which are only straw men, and says none is applicable.

First, the Justice Department says that encrypted speech is not like a foreign language because nobody "speaks" it without mechanical aids. "Ciphertext," the Department tells us,

> is not like a foreign language, the use of which can convey unique meaning and nuance to the listener or reader. Thus, ciphertext itself—as opposed to the underlying plain text—has none of the properties of protected "speech" that the Supreme Court has traditionally identified, and, accordingly, the dissemination of ciphertext should not be entitled to First Amendment protection.[28]

I do not really see how that argument can be right. I am willing to accept that ciphertext is not like a foreign language, but that seems to me to be asking the wrong questions. Speaking into a telephone turns speech into mechanical, digital, items that cannot be understood without a mechanical aid, namely a telephone that unscrambles the digital information into sounds. It has never been suggested that the digitization of the sounds removes the content of that telephone communication from protected speech, so I just cannot understand how the Department of Justice can make this argument. When one is playing law professor, one can spin wonderful hypotheticals about people who speak through prosthetic devices because they have lost their natural speech functions, for example, signaling Morse code with devices that track their eyebrows and whatnot, but we do not need to do that. Today, we are going to stick to the main things and avoid the straw men. We come not to praise Caesar, but to bury him.

The second argument that the Department of Justice puts up and knocks down is the claim that knowing the government is listening would have an impermissible chilling effect. The Justice Department points out, logically, that if this were the case then all wiretaps would be unconstitutional. I think that that is probably right as far as it goes. I am going to suggest to you, in my last couple of minutes, that the context in which speech may be chilled might need to be evaluated in the context of all the other things that are happening to people in society. Thus, the chilling effect problem might be larger when we do the individualized balancing that might be required in any individual case; but, as a rebuttal to a general proposition, the Justice Department is

28. *Department of Justice FAQ*, *supra* note 14, at Question 17.

correct that a chilling effect argument cannot be the basis for a First Amendment claim to a right to un-escrowed strong cryptography.

The third suggestion addressed is that some people say the distribution of object code is a protected First Amendment activity. At least for the sake of the argument, I would be willing to concede that here, the Department of Justice is correct, and that object code falls in the "Widget" category, rather than the "Speech" category. I would be willing to concede that, only for today, because it gets us to where we are going.

That brings us to whether source code is protected speech and whether its distribution is a protected First Amendment activity. These are precisely the questions at issue in the *Karn* and *Bernstein* cases, especially the *Bernstein* case. The Department of Justice's position on this is interestingly nuanced: "Some persons do disseminate source code for communicative purposes. Nevertheless, we believe that a restriction on the dissemination of certain encryption products could be constitutional . . . because such a restriction could satisfy the 'intermediate' scrutiny that the First Amendment provides for incidental restrictions on communicative conduct."[29] To make a long story short, while this has some elements of a close question, it does seem to me that, at least in a non-commercial context, the balance weighs pretty clearly in favor of saying that source code is a form of protected speech.[30] In the *Bernstein* facts, where you have an academic who wants to distribute work relating to his dissertation, it seems to me to be pretty close to a core protected speech situation. I think that the issue for a commercial product is somewhat tougher, but I do not think that it is as close as the Department of Justice would like you to think it is.

Finally, and perhaps most importantly, the Department of Justice says—and here I think it is an accurate statement of the law as it stands today, but not, I hope, as it stands tomorrow—that there is not a general constitutional right to encryption. It concludes from this fact that, therefore, prohibition of the manufacture or distribution of nonrecoverable encryption products would be okay. Legislation could be drafted, the Department says, "as a permissible time, place, and

29. *Id.* at Question 17.

30. *See* Bernstein v. United States Dep't of Justice, 176 F.3d 1132, 1145 (9th Cir. 1999) ("To the extent the government's efforts are aimed at interdicting the flow of scientific *ideas* (whether expressed in source code or otherwise), as distinguished from encryption *products*, these efforts [, specifically Export Administration Regulations,] would appear to strike deep into the heartland of the First Amendment."), *opinion withdrawn pending rehearing en banc*, ___ F.3d ___ (1999), *available in* No. 97-16686, 1999 WL 782073 (9th Cir. Sept. 30, 1999).

manner restriction—particularly since any such restriction on the 'tools' of speech would be unrelated to any communicative impact of the underlying plaintext."[31] Well this, it seems to me, really is the fundamental issue because of the spillover effects on other parts of our lives; and I think, in talking about this, while we can play technical games and work through each of the individual constitutional amendments and find good arguments there as well, there is something to be said for also hitting the issue head-on. It may be time to think about deriving a new jurisprudence we might call, somewhat grandly, "the new privacy," which I hope has echoes of "the new property," because I think it is just as fundamental to our future as "the new property" was in the period in which it developed.

Now, what would "the new privacy" look like? First off, it would change the assumption that facts about us tend to be public property. We would personalize ownership of facts about us in transactions, perhaps even sometimes in public, and we would try to use the property regime and the intellectual property regime to take back some control over personal data. The First Amendment imposes limits on the extent to which one can limit the appropriation of public facts, so this is in no way a complete solution; but, it is a way, I think, of dealing with this problem of how technical change affects social policy if you do not confront it squarely.

Here are some of the technical changes that concern me, which I think "new privacy" has to address. We have now an enormous number of new techniques of high-tech searches, many of which do not, apparently, require warrants. Courts in this country have held, for example, that technologies which detect heat from a house can be used without a warrant; indeed, if you find a lot of heat coming out of the house, that is probable cause for a search because somebody must be doing something inside they should not be doing.[32] If you find no

31. *Department of Justice FAQ*, *supra* note 14, at Question 17.

32. *See, e.g.*, United States v. Robinson, 62 F.3d 1325 (11th Cir. 1995) (holding that aerial surveillance of occupied, private residence with infrared thermal detection was not unconstitutional search), *cert. denied*, 517 U.S. 1220 (1996); United States v. Ishmael, 48 F.3d 850, 857 (5th Cir. 1995) (finding that warrantless use of thermal imager in "open field" does not violate Fourth Amendment because such use is passive and non-intrusive), *cert. denied*, 516 U.S. 818 (1995); United States v. Myers, 46 F.3d 668, 669 (7th Cir. 1995) (holding that thermal imaging scanning is not "search" within meaning of Fourth Amendment), *cert. denied*, 516 U.S. 879 (1995); United States v. Pinson, 24 F.3d 1056 (8th Cir. 1994) (holding that Fourth Amendment rights were not violated by government's warrantless use of forward looking infrared device (FLIR) to detect differences in surface temperature of house because defendant's subjective expectation of privacy in heat emanating from his house was not one that society would find objectively reasonable), *cert. denied*, 513 U.S. 1057 (1994); La-

heat coming out, that also is probable cause because they must be using a lot of shielding.[33] Not every court has gone that way,[34] but some have.

We have enormous possibilities for tracking and identifying people coming on-line—not just the things you may have seen in the movies with Global Positioning Systems (GPS)[35] and cell phones, not just data mining that allows a corporation to find all of your reading and transacting on the Internet and correlate it to build up a profile about you. We have DNA databases;[36] we have databases of addresses of people who have had brushes with the government, felony convictions, or other things. We have the motor vehicle and DMV databases, which can be cross-referenced with all of the above.[37] We have child support databases;[38] we have databases about workers;[39]

Follette v. Commonwealth, 915 S.W.2d 747, 749 (Ky. 1996) (finding that use of FLIR unit during overhead flight to survey dwelling's heat emissions did not constitute search); State v. McKee, 510 N.W.2d 807, 810 (Wis. Ct. App. 1993) (holding that use of infrared sensing device to detect heat emanating from defendant's residence did not constitute "search" within meaning of Fourth Amendment), *review denied*, 515 N.W.2d 715 (Wis. 1994).

33. *See, e.g.*, United States v. Kerr, 876 F.2d 1440, 1443-44 (9th Cir. 1989) (considering absence of heat to be sign of suspiciously good insulation).

34. *See, e.g.*, United States v. Field, 855 F. Supp. 1518, 1533 (W.D. Wis. 1994) (holding that use of thermal imager is search that does not fall into exception of warrant clause); People v. Deutsch, 52 Cal. Rptr. 2d 366 (Ct. App. 1996) (holding that society has reasonable expectation that heat generated from within home may not be measured without warrant); State v. Siegal, 934 P.2d 176, 192 (Mont. 1997) (thermal imaging scan is search that implicates state constitutional right to privacy), *overruled on other grounds by* State v. Kuneff, 970 P.2d 556 (Mont. 1998) (finding that overruling *Siegal* on standard of review of search warrant applications); Commonwealth v. Gindlesperger, 706 A.2d 1216, 1223-24 (Pa. Super. Ct. 1997) (holding warrantless use of thermal imaging device unconstitutional search under Fourth Amendment), *appeal granted*, 724 A.2d 933 (Pa. 1998); State v. Young, 867 P.2d 593, 604 (Wash. 1994) (holding that warrantless use of thermal imaging violates both Fourth Amendment and rights to privacy in Washington Constitution).

35. *See, e.g.*, Joseph Rose, *Satellite Offenders*, WIRED (Jan. 13, 1999) <http://www.wired.com/news/news/technology/story/17296.html> (describing use of Global Positioning System technology to track probationers, prisoners on work release, and others).

36. *See Reno Proposes National DNS Database*, EPIC ALERT VOLUME 6.04 (Electronic Privacy Information Center, Washington, D.C.) (Mar. 4, 1999) <http://www.epic.org./alert/EPIC_Alert_6.04.html> (noting that FBI Combined Index DNA Indexing System (CODIS) currently contains information on 38,000 people with another 450,000 samples awaiting processing).

37. The 1996 Illegal Immigration Reform and Immigrant Responsibility Act, Pub. L. No. 104-208, 110 Stat. 3009-716 (codified as amended at 5 U.S.C. § 301 (Supp. 1994)), prohibits the use of state drivers' licenses after October 1, 2000 unless they contain Social Security numbers as the unique numeric identifier "that can be read visually or by electronic means."

38. *See* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*,

we have databases about people who do not have proper immigration status to be allowed to work, and so on and so on and so on.[40] We have all kinds of observation technology: keystroke monitoring[41] in the workplace, cameras in public places, speed cameras that take pictures of license plates and that can be used to track an individual's movement.[42] We have road pricing schemes,[43] which are designed not only to debit an anonymous account, but also to keep track of the car and, incidentally, how fast it was going as it goes from point to point. Currently, in one neighborhood in England, the government is doing an experiment where they are using facial recognition technologies along with cameras mounted on telephone poles.[44] (It happens to be one of the poorest areas in the country—I wonder why they chose that to be the place where they test this new social control technology.)

---

16 J. MARSHALL J. COMPUTER, 529, 546-47 (1998) (discussing federal statute that requires creation of database containing names and social security numbers of all persons who owe or are owed child support).

39. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996, part of the 1996 welfare reform, Pub. L. No. 104-193, 110 Stat. 2209 (codified as amended at 42 U.S.C. § 653a (Supp. III 1994)), set up a "State Directory of New Hires," under which employers are now required to send the government the name, address and Social Security number of every new employee. *See id.* § 653a(b)(1)(A).

40. For example, the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 2024 (codified as amended at 42 U.S.C. § 1320d-2(b)(1) (Supp. III 1994)), gives the Department of Health and Human Services (HHS) the power to create "unique health identifier[s]" so that the government can electronically tag, track and monitor every citizen's personal medical records. *See also* Phyllis Schlafly, *Stealth Assault on Medical Records*, WASH. TIMES, Aug. 13, 1998, at A19 (discussing contention that federal government plans to assign personal identification number to every medical patient). The 1993 Comprehensive Child Immunization Act would have authorized the HHS "to establish state registry systems to monitor the immunization status of all children." S. 732, 103d Cong. § 2145 (1993).

41. *See* Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 942 (1996) ("[K]eystroke monitoring . . . tracks the user's every keystroke and the computer's response. . . . [It] indicate[s] who signed on, at what time, for how long, and even the nature of their activities while logged on.").

42. *See Controlling Speeds on Limited Access Highways: Surface Transportation Safety Hearing Before the Subcomm. on Transp. and Related Agencies of the House Comm. on Appropriations*, 106th Cong. (1999) (statement of Brian O'Neill, President, Insurance Institute for Highway Safety) ("[Speed cameras] photograph motor vehicles going a specified amount above the posted speed limit, and violators are ticketed by mail. . . . The time, date, location, and speed of the vehicle are recorded on the film.").

43. *See generally* Margaret M. Russell, *Privacy and IVHS: A Diversity of Viewpoints*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 145 (1995) (examining differing views on Intelligent Vehicle-Highway Systems).

44. *See* Nick Taylor, *Closed Circuit Television: The British Experience*, 1999 STAN. TECH. L. REV. VS 11 <http://stlr.stanford.edu/STLR/Symposia/Privacy/index.htm>.

In the United States, we have economic tracking capabilities, which grow out of anti-money laundering projects[45] designed to combat various types of financial fraud or the use of money in other kinds of transactions you do not like, especially drugs. We are looking at a potential world—not that it is guaranteed to happen—where we are going to be facing a new level of perfection in law enforcement. I see Professor Moglen shaking his head because he thinks everyone will encrypt their way out of it. But that is, in fact, my point. My point is that it is important to safeguard the countermeasures that people will use. It is not my point that the government will have a perfect success rate in stamping out those countermeasures. It is just going to make life very unpleasant—and needlessly so—for lots of people as we fight our way to the end. And, it is better to get to that end on the high principle which it deserves, the principle that people are entitled to private space. We should focus on the high principle that the United States government should, as a matter of policy and decency and human rights, encourage people to create private space for themselves and help people to find the tools to do so. We should insist that this right derives not only from the right of privacy, but also from the right of freedom of association, and remind opponents that without these rights and these tools everything you do is non-anonymous.

If you cannot be anonymous, then everything you do can potentially be tracked.[46] Furthermore, your right to private associational activities in cyberspace, which are going to increasingly become indistinct from regular 'meeting space' activities, will be infringed if you cannot use the Internet in real privacy. Every time you use a computer to speak, to publish something, to chat with people, to transact, to read something, if that is all becoming part of a dossier about you, that is going to change your life in a way that I do not think it ought to be changed. I think it is appropriate to invoke the Constitution to protect a citizen's abilities to employ technical countermeasures against the new technologies that are likely to be deployed against us all.

45. *See* Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Policy Technology?*, 34 JURIMETRICS J. 383, 386-91 (1994).

46. *See generally* A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 U. PITT. J.L. & COMM. 395 (1996), *available in* <http://www.law.miami.edu/~froomkin/articles/ocean.htm>.