Spring 2007

The Technology of Surveillance: Will the Supreme Court's Expectations Ever Resemble Society's?

Stephen E Henderson

The Technology of Surveillance: Will the Supreme Court's Expectations Ever Resemble Society's?

By Stephen E. Henderson, Associate Professor

For law students studying criminal procedure—or at least for those cramming for the exam—it becomes a mantra: government conduct only implicates the Fourth Amendment protection against unreasonable searches if it invades a "reasonable expectation of privacy." This is not the contemporary definition of the word "search," nor was it the definition at the time of the founding. But, via a well-intentioned concurrence by Justice Harlan in the famous 1967 case of *Katz v. United States,* it became the Court's definition.

This lack of fealty to the English language left some questions. For example, is determining whether someone has a "reasonable expectation of privacy" a normative inquiry (what *should* a person expect) or an empirical one (what *does* a person expect)? And why do we need to determine whether someone had a *reasonable* expectation of privacy when the next question is, to the consternation of law students, whether the search was *reasonable.* Remarkably, the High Court has never answered these questions, although Justice Scalia has complained about the latter. But there are even larger problems with what the Court has done with its "reasonable expectation of privacy" test, problems that became immediately apparent, but that are now becoming critical.

Consider some recent events and technologies, and the problem becomes clear. Why might Patricia Dunn soon be able to empathize with Martha Stewart? Because she has been indicted for her role in the Hewlett-Packard board-leak fiasco. In a nutshell, Dunn allegedly authorized and assisted in an investigation that relied upon an "information broker" to determine which board member or members were leaking confidential information to the press. How does an "information broker" obtain that information? She lies. But it isn't pleasant to have to tell new acquaintances at a cocktail party that one lies for a living, so instead "information brokers" engage in "pretexting," which means contacting phone companies, posing as customers, and thereby obtaining call records. HP also appears to have engaged in dumpster diving, shadowing, and other favorites in the snoop's arsenal, but for our purposes we want to focus on pretexting.

Naming aside, pretexting must be a pretty nasty business. Not only did it cost Dunn her chairman job, but the Attorney General of California charged her in a felony indictment and settled civil charges against the company for $14.5 million. The FBI investigated, the SEC instigated a review (admittedly for a tangentially related Sarbanes-Oxley issue), the House Committee on Energy and Commerce held hearings, the "governator" (Schwarzenegger) signed legislation explicitly criminalizing pretexting of telecommunications records, and the United States Congress considered—and might enact—the same. Whatever it takes to constitute a "reasonable expectation of privacy," it must be satisfied with respect to dialing

What if the government wants to plant a mole in your life who will remember, record, and transmit everything you say to him or her? There is no constitutional constraint. What if the government wants to place an electronic transponder on your vehicle to track your car? There is no constitutional constraint.

records. After all, *USA Today* created quite a stir when, on May 11, 2006, it reported that the National Security Agency had obtained and was parsing the records identifying millions, if not billions, of telephone calls placed by Americans. And there is, in fact, a federal statute, the Stored Communications Act, which forbids such access absent legal process. Apparently, a reasonable American both *should* and *would* expect dialing records to be confidential.

But according to the Supreme Court, there is *no* Fourth Amendment restriction on police accessing such records. They can be obtained for any reason, or for no reason. Mere curiosity will do. Why? Because to the Court, one who discloses information to a third party retains no reasonable expectation of privacy in that information (the "third party doctrine"). And we know we give those numbers to our phone company—how else are its switches to connect the call? So how about your bank records? As far as you are concerned, there is no constitutional constraint on government access. What if the government wants to plant a mole in your life who will remember, record, and transmit everything you say to him or her? There is no constitutional constraint. What if the government wants to place an electronic transponder on your vehicle to track your car? There is no constitutional constraint. What if the government wants to fly over your backyard to see what you do within that fence of yours? There is no constitutional constraint. And if the government wants to comb through your garbage, going so far as reconstructing shredded documents or testing a tampon for seminal fluid? There is no constitutional constraint.

These are the cases law students learn. But it gets worse. The human body is constantly radiating energy. This in itself sounds worrisome, but unless you are at a temperature of absolute zero (so chilly, atoms stop vibrating), you are going to emit energy. We don't see this energy because it isn't in the visible spectrum, but it turns out the body is much more emissive in the millimeter wave spectrum than most other objects, such as guns, knives, and particulates. And just as visible light transmits through glass, millimeter waves transmit through clothing. This allows police to carry what is in essence a video camera attuned to this spectrum and view what a person is carrying on his or her person from a distance. Does the Fourth Amendment restrict use of such a device? Not under the third party doctrine, because you knowingly (at least now you know) convey this information to others.

And there are more banal examples. Consider to whom you disclose your e-mail messages. And how about your physical location? If you carry a modern cellular phone, you typically convey a very accurate location to your service provider not only when you are placing or receiving a call, but anytime the phone is turned on. And what of querying the mammoth databases amalgamating different types of information that we tend to hear about when they suffer security breaches? This is the magnum opus of the Court's third party doctrine—the Court has removed all constitutional (legal) constraint, and technology has now removed any significant cost constraint.

So what should the Court do? Obviously the third party doctrine must go, but it is admittedly difficult to replace this wonderfully bright-line rule with anything administrable. I have crafted a proposal, and interested readers can peruse it via my page at Widener's Web site. But in the space I have here let me just say this: Last term the Supreme Court declared that "[t]he constant element in assessing Fourth Amendment reasonableness...is the great significance given to widely shared social expectations." As the HP debacle demonstrates, the Court's jurisprudence deviates sharply from actual expectations. Unless the Court changes course our Constitution will read like AT&T's recently modified privacy policy, which explains that "[w]hile your account information may be personal to you, these records constitute business records that are owned by AT&T." That might suffice for corporate America, but it shouldn't do for our Constitution. ■

So what should the Court do? Obviously the third party doctrine must go, but it is admittedly difficult to replace this wonderfully bright-line rule with anything administrable.

Stephen E. Henderson is associate professor on the Delaware campus, where he concentrates on intellectual property and criminal law. He received his JD from Yale Law School, where he co-founded the Yale Law and Technology Society.