Who Will Watch the Watchers?

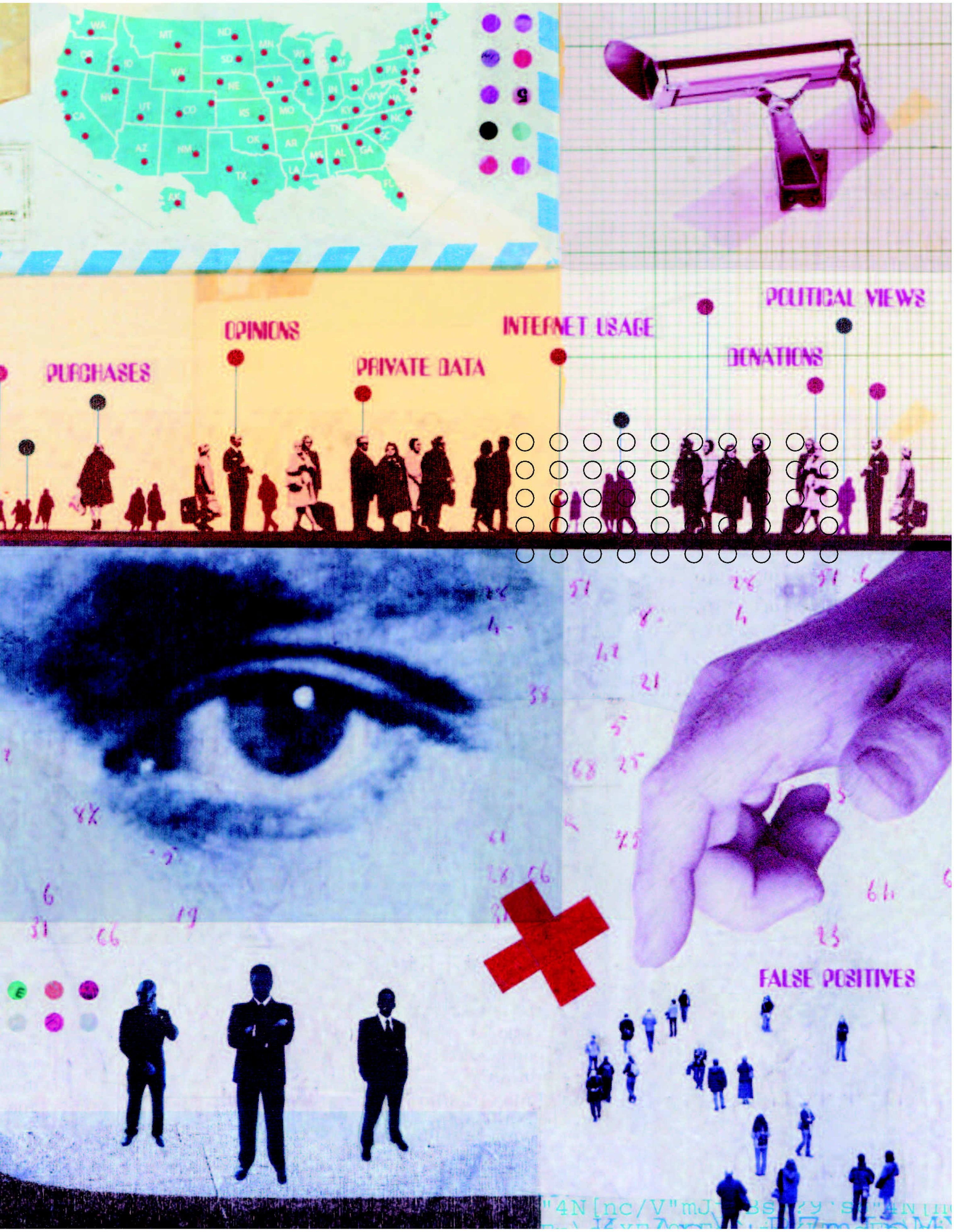
Securing Constitutional Rights in the Digital Age

By Mike Field
Illustration by Martin O'Neill

TRAFFIC IS TERRIBLE. Late for a meeting, your mind is working overtime on how to adjust your presentation. Suddenly, there's a clearing ahead. You hit the gas—and fly right into a speed trap. Blue lights flash in your rearview mirror.

On the side of the road the police officer takes your license and registration, returns to his car, and feeds them through an optical scanner. While you sit fuming, your name is being checked at a remote government computer center that keeps track of the websites you visit, the books you buy online, your long-distance phone bills, and hundreds of other pieces of both public and private information. Something in your past suggests behavior that authorities deem suspicious: Perhaps your name was included on a suspicious activity report for using binoculars and taking pictures "with no apparent esthetic value" in Los Angeles, as police policy there now dictates. As you wait, two more squad cars appear, their lights flashing, and the officer—now sounding a little nervous—says, "Please step slowly out of your car and spread your arms."

It may sound like a futuristic dystopian nightmare, but the possibility of this kind of scenario is closer to reality than many people imagine. Government run or sponsored data clearing houses are now active in nearly every state. Known as fusion centers, they are funded by the federal government as part of the national response to the 9-11 terrorist attacks. Originally envisioned as a means of sharing anti-terrorism intelligence among federal, state, and local law enforcement agencies, fusion centers are generally unknown to the


OPINIONS
PURCHASES
PRIVATE DATA
INTERNET USAGE
POLITICAL VIEWS
DONATIONS
FALSE POSITIVES

Professor of Law Danielle Citron says, "I'm a privacy person." She is also a national leader in studying legal issues surrounding government reliance on information technologies.

public. Even legal scholars are unsure how they fit within the country's legal framework. And no one seems to be quite sure what they do.

"There is this concept that computers can create a personal profile of individuals that will predict if they are a potential security risk, but the reliability of these models is unknown," says Professor of Law Danielle Citron of the methods employed by fusion centers to sift through vast quantities of seemingly innocuous —but often private—data to try to identify potential terrorists. "We are talking about it but it is not yet in the public eye." In order to advance the discussion and further explore legal issues surrounding government collection and analysis of information about private citizens, Citron helped organize one of the nation's first gatherings of legal scholars and privacy experts focusing on fusion centers. The Technology and Privacy Roundtable, which was hosted by the School of Law during the spring 2009 semester, brought together two dozen experts from across the country for a day of discussion and debate.

From the start it became apparent that it is what is *not known* about fusion centers that raises the greatest legal and privacy concerns. "People say, 'Oh, you worry too much.' I think now is the time to be considering these issues," said Roundtable co-leader Frank Pasquale, a visiting professor of law at Yale, and the Loftus Professor of Law at Seton Hall University, at the session opening.

But identifying the issues means knowing what, exactly, fusion centers are doing. Beyond bland generalities, most centers refuse to say. And the task is made all the more difficult by the fact that no two fusion centers are quite alike. The Department of Homeland Security reports that as of February 2009 there were 58 fusion centers around the country. To date, the Department has provided more than $380 million to state and local governments to build and equip the centers, but does not directly operate or control them. For the most part, fusion centers evolved locally on an ad hoc basis beginning around 2003. Each fusion center is run by a unique set of state and regional partners and, beyond having a general mandate of information and intelligence sharing, they often have widely differing approaches to what information they collect, and with whom and for what reasons they share it.

Fusion centers use powerful computers and sophisticated programming techniques to scan huge quantities of data, looking for anomalies that may indicate terrorist threats. But in addition to public records such as court appearances and tax records, the centers can "fuse" private information such as phone bills and credit reports and even secret information provided by other government agencies. This is what happened when Baltimore peace activists and antiwar demonstrators found themselves on federal terrorist watch lists after the Maryland State Police infiltrated their organizations and compiled extensive dossiers on the protesters in 2005 and 2006. The Baltimore Sun reported in 2008 that the undercover state police reports failed to identify any criminal or even potentially criminal acts on the part of the protesters, yet nonetheless entered their names on a database of potential terrorists or drug traffickers. "If you get put on a watch list, that means airlines can deny your ability to fly. You can potentially lose your employment if you are deemed a security risk, or perhaps be unable to get a job, depending on who gets to see these lists," notes Citron. "You're talking about real concrete harm."

Both the theory and technologies that undergird the fusion systems are new—and, say many experts, unproven—and little legal framework exists to regulate or direct the

"The horse is out of the barn. Fusion centers are not going away. So what do they do? We are very concerned that because there are ambiguous lines of authority there is no policing mechanism in place to prevent abuse."

—Michael German, ACLU policy counsel

centers' activities. The possible misuse of such extensive new information collection and analysis capabilities first drew attention in December 2007, when the American Civil Liberties Union published a white paper titled "What's Wrong with Fusion Centers?" The report identified several areas of general concern, citing ambiguous lines of authority; participation by both private sector subcontractors and military personnel; the likelihood of "data mining" in which centers go looking for suspicious individuals without probable cause; and the aura of excessive secrecy that surrounds the centers. It went on to suggest a number of legal and political safeguards that could prevent misuse of the centers' unprecedented information gathering ability, dryly observing that the best solution might be to abandon the concept entirely, and "return to traditional law enforcement techniques based upon reasonable suspicion that have kept America safe and free for over 230 years."

Many observers—including report co-author and ACLU policy counsel Michael German—believe there is no turning back. "The horse is out of the barn," he said at the Roundtable. "Fusion centers are not going away. So what do they do? Are they being used to collect information on lawful dissent? Are these places where information on innocent activity is collected and shared? We are very concerned that because there are ambiguous lines of authority there is no policing mechanism in place to prevent abuse."

Throughout the day's discussion, participants repeatedly expressed frustration at how little public information is available about fusion centers, even after six years. There was a sense among the legal scholars and privacy experts that they were steering without a compass into uncharted territory. Consequently, the Roundtable at times seemed not so much policy debate as reconnaissance mission, with everyone putting their heads together trying to understand what's out there. It seemed a fitting venture for Danielle Citron, a self-described "cyber law geek" who has gained a national following writing about automated systems like e-voting machines, cyber security, and cyber harassment in scholarly journals and the online forum Concurring Opinions [see essay on p. 32]. The Roundtable, she says, was the natural extension of her interests: "All of my work is part of a broader story about how information about us can be used and misused." She considers a moment and adds, "I'm a privacy person, obviously."

Citron says her involvement in the cutting-edge field of cyber privacy rights "was pretty serendipitous," evolving from her first law article, published in 2006 in the *UC Davis Law Review,* concerning the relatively new technology of Voice Over Internet Protocol and its likely effect on personal jurisdiction theory. That investigation led her to contemplate the legal ramifications of other novel electronic technologies. The following year the *Southern California Law Review* published her article "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age," in which Citron drew an intriguing legal analogy between the collection of personal information in large unregulated databases and the early industrial age creations of large reservoirs of water to power mills. The water was harmless in repose but could wreak havoc if the dams gave way—though it took many years and several tragedies before the law evolved to protect those downstream. By the same token, in the cyber world any one of us could be living downstream of a data dam without under-

standing the risk. "The reservoir metaphor suggests we underestimate the dangers inherent in damming up and collecting data," Citron says, reflecting her article's central premise that new economic eras bring about new concepts of personal harm.

If large uncontrolled databases pose risks—as recurring stories of identity theft and wide scale security breaches would seem to indicate—then the danger becomes even more acute, says Citron, when the scope of information collected is hidden behind veils of national security. "What we are seeing with fusion centers is mission creep. They started out as anti-terrorism tools, but now we are seeing their mission changed to the protection of all infrastructure from all risk. The danger is that they are combining unproved theories of data mining with use of private databases that may or may not be accurate. If the data used is incorrect then the results are going to reflect that. It's the old story of garbage in, garbage out."

But the centers are not without their defenders. According to Sean Kates '07, a law and policy analyst in the Law School's Center for Health and Homeland Security, first responders such as police, fire fighters, and other emergency personnel are especially likely to see benefits in the centers. "What falls apart first in a large scale emergency is communications," he says. "First responders look upon fusion centers as a positive because they provide a reliable central source of good information. "I have had police officers verify to me that fusion centers have been helpful to them in looking across county lines, and across differing criminal records systems, to aid in investigations. From that perspective it's a good concept," says Kates.

Homeland Security's Robert Riegle, who directs the state and local program office of the Office of Intelligence and Analysis, pointed to two recent success stories involving law enforcement, in testimony last April before a subcommittee of the Committee on Homeland Security. In one, a DHS operational specialist coordinated with federal officials on an Amber Alert for a 3-year-old girl being taken out of the country by a suspect wanted for rape and murder. Using information and contacts gathered through a California fusion center, he was able to track the youngster to a flight bound for the Netherlands; she was ultimately recovered unharmed. In the second case, the Denver fire and police departments worked with a Colorado fusion center to track and apprehend a suspect wanted for seven different fire-bombings of SUVs.

Skeptics note, however, that a good concept does not always translate into good practice. In order to truly understand the dangers posed by fusion centers that operate with virtually no public awareness or oversight, we must first invent new ways of describing our rights, says Professor of Law and Government Mark Graber. "The great danger is that very often we think of constitutional rights purely in traditional paradigms that don't reflect current reality. For example, we think that freedom of speech means an individual can stand on the corner and denounce the government without fear of interference. But today free speech often involves someone on the Internet. How do we ensure free speech is not inhibited in this environment?" Fusion centers, he says, pose a special challenge in this new world. "In the old days the concept of privacy meant that there was information that the government couldn't learn about you without going to court to obtain a warrant. And then they had to go look. In the past if a government official asked me, 'What have you been reading?' I would say, 'None of your business.' Now they

Professor of Law and Government Mark Graber: "We very often think of constitutional rights purely in traditional paradigms that don't reflect current reality."

> Since most fusion centers involve at least some participation from commercial data brokers, there is, practically speaking, **no limit and no quality control on the kinds of information** that might be sifted in search of unusual patterns that indicate a threat.

don't need to go look, they already have the information. From the patterns on Amazon they know your reading habits. So it becomes crucial that they can't use that information."

But that may require entirely different legislation than the current regulatory structure concerning individual privacy and electronic data. Congress passed the Privacy Act of 1974 after numerous hearings and a number of reports on such topics as national data banks, commercial credit bureaus, and the effect of computers on personal privacy. In many ways it is a bill very much of its time, reflecting an era before the Internet, when only the government could have the kind of massive concentration of computers needed to keep and search enormous databases of private information. When signed into law, the bill established a code of fair information practices governing the collection, use, and dissemination of personal information maintained in systems by federal agencies. Information about an individual could not be disclosed from these systems without that person's written consent, or by specific statutory exception; and individuals were enabled to access and amend their records in the case of faulty information.

In theory, at least, the Privacy Act protects citizens from an intrusive, all-seeing government sticking its proverbial nose in people's private business. But what the Act does not do—and the reason it offers little in the way of protection today—is in any way regulate or control private interests from intrusively collecting, analyzing, and selling data about individuals.

Since most fusion centers involve at least some participation from commercial data brokers, there is, practically speaking, no limit and no quality control on the kinds of information that might be sifted in search of unusual patterns that indicate a threat. An individual whose purchases, opinions, Internet use, political donations, or general activities are deemed potentially subversive—by whom or by what standards to be determined by fusion center operators and not shared publicly—could be flagged for questioning, monitoring, or observation. Since private databases are often error-prone and not subject to consumer control or review, Citron's "garbage in/garbage out" dictum means the system would generate a relatively high number of "false positives"—flagging innocent individuals for further scrutiny or surveillance based on faulty information. The ACLU report points out that even if fusion centers obtain the unrealistically high accuracy rate of 99 percent, in the U.S. population of 300 million citizens with a hypothetical 1,000 terrorists at large, 990 of the terrorists will be "caught"—as will *3 million* innocent Americans. "We have decided we want to live with more false positives than negatives," says Citron. "This approach relies on crude algorithms which mean that, for a large number of people, you're going to be pulled aside."

If, as most Roundtable panelists agreed, "the horse is out of the barn" for fusion centers, then the need for effective legal oversight and vigilant public scrutiny is compelling. The Roman poet Juvenal once asked, "Who will guard the guardians?" Ultimately, the experts concluded, there will need to be some kind of online presence "watching the watchers."