Your Digital Trail: Data Fuels Political And Legal Agendas

By Daniel Zwerdling

Fri October 4, 2013

Here's a question for the digital age: If you are one of those people who say, "I've done nothing wrong; I've got nothing to hide," do you have any reason to worry that someone might try to use your digital records against you?

We posed that question to John Dean, a man who has become immortalized in U.S. history books as President Richard Nixon's White House lawyer. His answer: "Think about the Nixon Enemies List."

"If Richard Nixon were alive today and in office," Dean says, "I'd have great concern about the data that's being collected."

Dean says the history of Nixon's Enemies List, which surfaced during the Watergate scandal, shows that even when people have done nothing wrong and think they have nothing to hide, unscrupulous government officials can still dig up personal information and use it to try to smear people.

The main Watergate scandal revealed that top government officials committed crimes to help Nixon politically, and Nixon himself took part in the cover-up. But one bombshell that exploded during the Senate's investigation of Watergate was that Nixon's aides had plotted a smear campaign during his first term, and ordered Dean to take part. In a memo for White House staff titled "Dealing with our Political Enemies," Dean wrote: "Stated a bit more bluntly — how can we use the available federal machinery to screw our political enemies."

The full list, which included more than 600 people, included journalists whose reporting Nixon didn't like. Others were on it because they had criticized the president or supported liberal causes. According to the White House strategy, government officials would dig up embarrassing information about them, and then administration officials would figure out how to take revenge on them with tactics such as sparking IRS audits and investigations by prosecutors, and messing with federal contracts or grants they might have.

Nixon and his aides were caught before the plot could take off. But in 1975, only a year after Nixon resigned in disgrace, investigations revealed that other administrations, both Republican and Democratic, had tried to smear their enemies, too. The Senate intelligence committee reported that the FBI had "conducted almost a million investigations of so-called subversives and extremists over the past 20 years," as the committee's chairman, Sen. Frank Church, D- Idaho, summarized it. "We know that marriages were destroyed, violence was encouraged, and the mass media were manipulated."

Of course, all that happened before computers were easily accessible. You don't need computers to dig up dirt on people. But Nixon's former lawyer warns that digital records make it far easier to do. "This digital information is out there," Dean says, "and it is getting collected in enormous heaps that can be mined electronically and digitally, and politically twisted."

Julian Sanchez, a research fellow at the libertarian CATO Institute, calls this era "a golden age of surveillance." Before computers, it took a huge amount of time and work to try to find dirt on somebody. For instance, the FBI tried to discredit Martin Luther King Jr. They wiretapped his phones, bugged his hotel rooms, and then had to listen to hundreds of hours of recordings. The Watergate scandal started unraveling after operatives physically broke into the Democratic Committee's headquarters to plant bugs and photograph documents — and got caught. But Sanchez says the computer age lets you find intimate parts of a person's life right in front of you, on a screen. And you can search and analyze it almost instantly, with a few clicks.

"There has never been so much data about so many of us so easily available to law enforcement and intelligence agencies," Sanchez says. "Even if it's being used properly now, we are constructing an architecture of surveillance, an architecture that will be in place if and when there comes someone holding power who wants to use that against those he regards as enemies of the country."

But analysts like Paul Rosenzweig, former deputy assistant secretary of the Department of Homeland Security, dismiss those fears. After all, he says, why should people fear that the government might misuse their digital records any more than they fear police — whom society has granted the power to arrest and kill?

History suggests that government officials will indeed misuse digital records, Rosenzweig says, just as some police have abused their power. "Anybody who denies the U.S. government has made mistakes in the past is a moron," Rosenzweig says. But he says Congress and the courts will figure out how to minimize and punish digital abuses, just as they have handled rogue cops. "Yeah, inevitably somebody's going to do something that we're all going to look [at], and hit ourselves on the forehead, and say, 'My God, how could they possibly do that?' " he says. "And they'll get caught. And we'll fix it."

Private Attorneys Use 'Floodgates' Of Data

There's another reason besides history to anticipate that your digital records could be used against you: Private attorneys are already getting access to them. They're getting the digital footprints of ordinary people to dig up evidence against defendants, such as cheating spouses.

"It's, like, literally the floodgates of data have opened up to us," says Lee Rosen, owner of the Rosen Law Firm, based in Raleigh, N.C.

Rosen says North Carolina and some other states consider private lawyers to be "officers of the court." So attorneys like Rosen and his staff are authorized to issue subpoenas much like prosecutors can. Rosen's employees simply fill out blank subpoena forms on their office computers, print them off and sign them.

Rosen says his staff issues "dozens" of subpoenas in a typical month for digital files, including cellphone location logs, bank records, credit card statements, travel reservations, and — Rosen says this is one of his favorite sources of evidence — text messages. He says nothing proves adultery as easily.

"Everything is right there in the text messages," says Rosen, "everything from what time we're going to meet and where we're going to meet, to how much we love one another, to what we're going to do or what we did do in a hotel room or in somebody's apartment or the back seat of a car."

And if you're thinking that none of this could apply to you, imagine other potential scenarios: a legal battle with your employer, or with an irascible neighbor, or with an insurance company that refuses to pay your claim. Rosen warns that even medical records are fair game for his subpoenas, despite HIPAA (the Health Insurance Portability and Accountability Act), which helps keep medical records private. Under the law, health care providers "may disclose protected health information" in response to a subpoena from an officer of the court — like Rosen — or from law enforcement.

"When it comes to family law cases," Rosen says, "everything is relevant."

Consider a child custody case he fought last year, in which he represented the mother. She suspected her former husband, the child's father, was having mental health problems. So Rosen subpoenaed all of the man's medical records from his internist and psychiatrist. Those records showed that the father was taking medication commonly prescribed for bipolar disorder, and that he had made negative comments in therapy about his son. Of course, Rosen says, lawyers like him subpoenaed medical and other records, when those files were 8-by-10-inch pieces of paper in manila folders. But he says he can get immeasurably more detailed information, spanning many more years, now that they are in digital form.

Spokesmen for Internet giants such as Google and AOL say their companies have sometimes tried to block subpoenas for users' personal information — although they acknowledge that they have turned over digital files in response to many, if not most, requests. But Rosen and other lawyers say executives of smaller companies that receive subpoenas often do not fight them.

"The companies generally want to comply with the law in the way that's least expensive to them," says Rosen. "They don't want to have to hire lawyers; they don't want to have to send doctors or other representatives to depositions or court hearings. They just want to give you the records and move on."

The Senate Judiciary Committee passed a bill earlier this year that would lay out tougher rules for this new world. Under current law, for example, police and government agencies like the IRS can sometimes get your emails, content and all, with only a subpoena — as long as you've already opened the emails or they're more than 6 months old. The new bill would require probable cause of a crime and a search warrant. So far, the full Senate has not scheduled a vote.

Research for this story by NPR's Emma Anderson.