Personal info can easily be used against you

By G.W. Schulz and Daniel Zwerdling, Center for Investigative Reporting

For some, revelations that the National Security Agency has been collecting vast amounts of personal information on U.S. citizens might seem as far removed as the city of Moscow.

But it’s not just an ultrasecret spy agency that can create a dossier on you.

Many Americans would be surprised by how easily local law enforcement, IRS investigators, the FBI and private attorneys can reach into the vast pool of personal information about their lives with little more than a subpoena, which no judge needs to review.

And it’s not just for selling you more products or services. It can be wielded against you.

“We used to have to rely on private investigators,” said Lee Rosen, a divorce attorney in North Carolina whose office averages dozens of subpoenas each month. “Now everything we need is more or less on the other side of the keyboard.”

Often, a simple form is all that’s required to access prescription histories, credit card purchases, monthly banking statements, ATM withdrawals, wire transfers, tax returns and, perhaps most importantly, the rich digital portraits we keep on our smartphones.

Law enforcement can create a map or timeline of a person’s whereabouts by accessing data from license-plate scanners, toll-bridge crossings and mobile phone carriers and, without much trouble, access records on your power consumption,

purchasing habits and even snail mail.

The more we leave heaps of digital detritus behind, privacy advocates say, the more we may have to answer for it to someone with an ax to grind, an investigation to close or a client to represent.

“The digital world has suddenly given us a wealth of information like we never had before,” Rosen said. “The floodgates of data have opened up.”

To illustrate this, the Center for Investigative Reporting teamed up with NPR to craft a typical day in the life of personal information. Along the way, we’ll explain how it is amassed and how it can be vacuumed up.

First, consider your IP address, a unique identifier used to connect your phone or laptop to the Web. Perusing the Internet before you shower in the morning, you might not know that the government or a private lawyer can start with your IP address and determine your name. Or, starting with your name, the government can determine your IP address.

Although precision can be limited, private lawyers have used IP addresses to unmask alleged movie and music pirates.

Voltage Pictures, makers of “The Hurt Locker,” subpoenaed the IP address of a 69-year-old woman believing it linked her to Internet downloads that infringed on the movie’s copyright. She and numerous others targeted in the suit said they weren’t guilty of piracy accusations. The lawsuit eventually died.

Say, however, you’re streaming Internet radio as you move about the house, listening to a shock jock or political talk show host considered obnoxious by some. Smartphone apps like TuneIn and Pandora will store data on their servers on the talk shows and music you enjoy.

If you’re like millions of other Americans, you might use

dating sites like JDate.com or OkCupid.com to find romantic matches. Many users rely on pseudonyms until they're comfortable giving out more personal information to a potential date, but digital anonymity is often an illusion.

In 2011, Google acquired facial recognition software company PittPatt, which has been used by researchers to link dating profiles with full identities on other social media sites. Google already uses "computer vision technology" to power its image searches, Picasa photo platform and Google Goggles.

"Any attempt to set up a dating profile – even if you're using a pseudonym and even if you're not uploading photos you put in other places – can result in (someone being able) to find you," said Rainey Reitman, activism director at the Electronic Frontier Foundation.

OkCupid's privacy policy says personal information could be disclosed "in response to a subpoena or similar investigative demand, a court order, or a request for cooperation from a law enforcement or other government agency."

Little-known third-party advertisers and marketers can observe your dating activity, too. Software privacy specialist Ashkan Soltani offered a recent demonstration using a tool called Collusion, which visualizes the array of companies that monitor our activity online, watching as we click from one place to the next in order to better understand consumer behavior.

Collusion can be downloaded to your browser – Firefox, Chrome or Safari. Clicking on an icon while visiting a site will display an interconnected web of bubbles that represent companies collecting information about your activities. The companies have names like Lotame and Criteo. The tracking is largely invisible without an add-on like Collusion.

Soltani offers this metaphor: a phone call in which you dial OkCupid.

“In responding to my phone call or connection to OkCupid, (the site) brought all of its friends on to listen to my phone call,” Soltani said. “I’m on speakerphone at OkCupid, and all of these other people are also listening to my conversation.”

While many tracking companies insist they don’t need personally identifying information in order for the data to be useful, Soltani and others say trackers know enough about your behavior from pseudonymous “cookies” to profile you and make decisions about you online, such as how to target ads or special deals.

Reading the network traffic – the language that exists behind Internet activity – Soltani showed how answers to sensitive profile questions on OkCupid’s site covering drug use, religious beliefs and more were transmitted to the data tracking company Lotame, along with the user’s IP address.

When you log in with a username and password to sites like Gmail, Amazon or OkCupid, your behavior can be linked to your real name or email address. Soltani said personally identifying information also can unintentionally “leak” to third parties, even if companies say they have no need for such data, and it’s not clear what happens to the information once it falls into their hands.

Stanford University’s Center for Internet and Society showed in a 2012 paper how usernames or IDs leaked to third parties on 113 popular websites out of 185 tested.

Jonathan Mayer, a graduate student at Stanford who worked on the study, offered another demonstration. He first logged in to the video-sharing site Dailymotion with the username “jonathanmayer” and showed how a unique ID number assigned to him by the data tracker Criteo followed him to another site about sexually transmitted diseases.

Even a generic name like “stanfordguy” used to log in on multiple sites could be used to determine one’s real identity

and theoretically be exploited by law enforcement, Soltani and Mayer said.

Officials with OkCupid declined an interview, and Lotame did not respond to phone calls and emails.

Alexandra Pelissero, a spokeswoman for Criteo, said the company wouldn't know that "jonathanmayer" or "stanfordguy" correspond to the same technology researcher at Stanford. She also said Criteo does not store IP addresses.

"Criteo's cookie-based technology recognizes events, i.e., products viewed, and does not create individual user profiles based on them," Pelissero wrote. "It assigns Criteo IDs, which are based on a user's interests, i.e., online browsing behavior, and (doesn't) allow us to identify the individual user, so that we can serve more personalized ads that correspond to those interests."

Jules Polonetsky, executive director of the Future of Privacy Forum, said many such companies have good intentions and wish only to better-tailor advertising for products consumers want.

The forum bills itself as a "think tank that seeks to advance responsible data practices" and is supported by Amazon, Facebook, Netflix, Bank of America and a host of other major companies.

"I think companies haven't figured out how to talk to people about data or privacy," Polonetsky said. " … There's nothing to be ashamed of if what they're doing is fair and honest."

Accessing personal information

Logs of seemingly innocuous everyday activities – like your power usage – can be obtained and used against you.

There are typically three ways the government and civil attorneys can try to access personal information. A search warrant is the toughest standard and requires the government

to convince a judge there's probable cause of a crime. Next is a court order, and the easiest to obtain is a subpoena.

"A subpoena, unlike a warrant, doesn't come from a court," said Kevin Bankston, senior counsel at the Center for Democracy & Technology, a nonprofit organization that advocates for Internet freedoms. "No one has to go to court. No one has to make a showing to a judge. A subpoena in the criminal context is issued directly by a prosecutor."

Bankston said all investigators must do for a subpoena is state that the information is relevant to an ongoing investigation.

Law enforcement agencies often argue all they need is a subpoena. Drug agents issued a subpoena in 2010 demanding that the Golden Valley Electric Association turn over the power consumption records, customer names, telephone numbers and credit card numbers for three addresses. For drug investigators, big power surges in a private house could mean the resident is cultivating marijuana with grow lights.

But the Alaska energy cooperative balked at the subpoena, citing its customer privacy policy. A federal court decision overruled the company's position and directed it to give up the records.

"It's kind of like looking at you through an open window and seeing what you do in your home," said Cory Borgeson, president of the company. Borgeson said that if the government wants your power records, it should have to show probable cause of a crime and get a search warrant.

When you head to work, your data portrait will continue expanding. Surveillance cameras in subway stations and on city buses watch you board and depart.

Chicago police for the first time successfully nabbed a suspect in May using facial recognition software known as

NeoFace that connected a surveillance image of the man from the city's train system to a massive database of booking photos.

To automatically identify celebrities and regular customers when they enter a store, some retailers reportedly are using another facial recognition technology originally developed in the U.K. for spotting terrorists and criminals.

Meanwhile, smart cards log when and where you travel using public transportation.

Police departments in the Bay Area and elsewhere around the country have used license-plate scanners to identify stolen cars and outstanding warrants. But the devices are designed to photograph vehicles and record the location, date and time of everyone who passes by without discriminating between criminals and innocent people.

The American Civil Liberties Union recently found that departments have widely ranging guidelines for how long they'll store this data, from 48 hours to five years to indefinitely.

Toll records remember when you crossed a bridge or used a particular interstate, and divorce attorneys are fond of them for that reason.

E-ZPass records, for example, will tell divorce attorney Jacalyn Barnett when someone has driven from the island of Manhattan, and paying cash makes her more suspicious that a spouse has something to hide. Another sign is odd departures from routine.

"People are very, very ritualistic," Barnett said. "Most people go to the same bank (branch) to do their transactions. If all of a sudden they're going to a different area, that tells you something."

Gray area around technology

One of the most powerful sources of information is your mobile device, which creates a rough approximation of your whereabouts by checking in with nearby cell towers or a more precise pinpoint when the GPS function is enabled.

The government doesn’t believe it needs a warrant for historical tracking with a mobile device. Instead, investigators have said the law requires only a court order, which is slightly more demanding than a subpoena but still less protection than the Constitution affords under a warrant.

Judges so far have handed down a patchwork of rulings on locational privacy, and the issue is far from resolved. In a Baltimore case that has civil liberties groups worried, police were able to obtain more than seven months’ worth of location data without a warrant from two cellphones belonging to robbery suspects. Most people would applaud catching robbers, but the advocacy groups argue that such prolonged tracking violates a reasonable expectation of privacy.

By the time you reach work, a mound of unopened emails awaits. Those, too, are part of a fierce debate over what requires a warrant. As its name suggests, the Electronic Communications Privacy Act of 1986 was designed to protect Americans who at the time were using the Internet increasingly to communicate. But the government has interpreted the law to mean that once your emails are opened or older than 180 days, no warrant is required.

Even if an investigator faces some hurdles with your inbox, such as Google insisting on a warrant, email is not entirely protected. With a court order that doesn’t reach probable cause, Google will give up your name, IP address, the dates and times you’re signing in and out, and with whom you’re exchanging emails.

Google said in a statement: “We are committed to keeping

people’s information safe and helping them control their personal data. Google Dashboard shows what’s stored in your Google Account. From one central location, you can easily view and update your settings for services such as Blogger, Calendar, Docs, Gmail, Google+ and more.”

Email nevertheless is at the center of a long-simmering legal dispute between environmentalists and Chevron over drilling in Ecuador. A federal judge this year granted Chevron’s subpoena seeking metadata from Microsoft email accounts of activists, including names, dates and possible locations. The company also has requested access to accounts on Google and Yahoo.

Last year, Twitter fought a subpoena from prosecutors in New York who were seeking information about a user charged with disorderly conduct among hundreds arrested by police during Occupy Wall Street protests in 2011. A judge threatened Twitter with fines if it didn’t give up the information, and the company handed over the data.

Digging into medical records

While many Americans are under the impression that their medical records are protected by privacy laws, investigators and private attorneys enjoy special access there, too.

The USA Patriot Act, passed shortly after the Sept. 11, 2001, hijackings, prohibits medical professionals from telling you if the FBI seeks your medical records as part of a national security or intelligence-related probe.

In some states like North Carolina, attorneys are considered officers of the court and issue subpoenas on their own as long as the information is connected to an ongoing dispute.

Divorce attorney Rosen tells the story of one client in a child custody case. The woman suspected that the father had mental health problems, so a subpoena was issued directing his psychiatrist to turn over notes about the man’s treatment,

relationship with his child and prescription medications.

“Medical records are very private and need to be protected, but there’s a balance,” Rosen said. “Sometimes, your medical records need to be made public in order to do what’s best for a child.”

Credit card purchases are similarly illuminating. Rosen calls them a “table of contents” for your life. Your financial records enjoy some amount of protection that requires the government to notify you when it seeks information about your purchasing habits.

That is, unless the FBI uses a so-called national security letter – which the Congressional Research Service calls “roughly comparable to administrative subpoenas” – to demand details about your financial transactions. Then the bank is barred from notifying you.

The FBI’s authority to issue such letters was expanded by the Patriot Act, and the letters’ use has exploded to the tens of thousands each year, targeting telephone billing records, bank transactions, credit reports, names of employers and more.

Perspective on privacy

Many Americans still might ask why they should care, following the recent news of NSA snooping. After all, asks Paul Rosenzweig, a former deputy assistant secretary at the Department of Homeland Security, why would we fear giving personal information to the government if we’re willing to give police the power to kill and arrest?

“I tend to think that this is a manageable problem along the lines of cops with guns,” he said. “Anybody who denies the U.S. government has made mistakes in the past is a moron. My own sense, however, is that our system is wonderfully self-correcting.”

Former President Richard Nixon and former FBI Director J. Edgar Hoover were known for their widely documented eavesdropping abuses. But even Nixon became angry when his daughters' privacy was violated, according to John Dean, a lawyer for the former president.

"If Richard Nixon were alive today, I'd have a lot of concern about the data that's being collected, because I don't think Nixon would have any reservations about going into anything that was available to pursue his enemies," Dean said.

One such "enemy" of Nixon was Morton Halperin, a senior policy official in the administrations of Nixon, Bill Clinton and Lyndon B. Johnson. Halperin eventually fell out of favor with the Nixon White House, so much so that his phone was bugged for two years.

During a recent interview, transcripts and summaries of the intercepted calls rested on a table in front of Halperin. But all these years later, he still was reluctant to read aloud from the personal communications.

"There were many conversations between me and my then-wife," Halperin said, "none of which I would have wanted to be made public and some of which would have been a little embarrassing."

G.W. Schulz works for the Center for Investigative Reporting and Daniel Zwerdling is a correspondent for NPR's Investigations Unit.