

## Data Trail



# It's 11 o'clock

## Do you know where your data is?

AS YOUR DAY TICKS BY, IT SEEMS THAT EVERYTHING YOU DO can leave a data trail. From your purchases online to the resumes you post, to health-care transactions made with your insurance cards, you probably are exposing your own personal data to possible snooping, fraud, or identify theft.

“Having so much sensitive information available makes it even more difficult for other organizations to release information that is effectively anonymous,” says Latanya Sweeney, associate professor of computer science, technology, and policy and director of Carnegie Mellon’s Data Privacy Lab. Sweeney demonstrated that birth date, gender, and 5-digit ZIP code is enough to identify 87 percent of people in the United States.

One year ago, Sweeney started to pull together a group of faculty who were looking at issues relating to privacy and security and working toward possible solutions. In the Internet age, few areas of our private lives—and what U.S. Supreme Court Justice Louis Brandeis called “the right to be left alone”—remain untouched by technology.

Lorrie Cranor, associate research professor in the School of Computer Science and director of Carnegie Mellon’s Usable Privacy and Security Laboratory, describes Carnegie Mellon as “the place to be for privacy research.” She explains, “There’s a concentration of researchers and experts here that you just don’t find at any other university.”

So how do these Carnegie Mellon experts suggest you protect yourself when you find the information technology that drives your everyday life to be more sophisticated than you are?

Here is a sample of some of their creative solutions—your wake-up call for keeping your data “self” both private and secure.

**6:01 a.m.**

You wake up to a ringing Blackberry—urgent email alerts you that your kids’ field trip has been canceled. You start calling around for an after-school sitter.



Percentage of adults who’ve been “phished”—that is, had online bandits try to get to their personal data.



Percentage of adults who fell for such scams.

**7:30 a.m.**

You’re on the road, tied up in traffic again. You try your car’s GPS feature, but it’s developed a glitch. Your cell phone won’t work when you try to call the office. You sit.



**Spam and other**

privacy compromises to your cell phone and handheld devices, such as personal digital assistants (PDAs), are rampant. These programs burrow into embedded systems in our cars and cell phones, wreaking all sorts of havoc and running up enormous bills. Carnegie Mellon CyLab member Adrian Perrig’s research team is developing new software designed to detect remote malicious attacks, such as worms and viruses. Dubbed SWATT, short for SoftWare-based ATtestation, this new cyber-cop can root out the worst offenders by alerting users that an unwanted rogue virus has invaded their cell phone or car computer.

**8:59 a.m.**

You arrive at the office and get coffee.



**Cyber stores allow** you to store your credit card information so you don’t have to enter it for each transaction. You don’t have to think: All you have to do is click.

One-click shopping is convenient and instantly gratifying, but there is a downside that few of us think about, although we should. The same technology that allows you to store your credit card information online for quick purchasing also tracks your purchases. If you knew that storing your credit card information online could compromise your privacy, would you do it?

Many consumers don’t realize the trade-off made for convenience sake. Alessandro Acquisti, assistant professor of information technology and public policy at the H. John Heinz III School of Public Policy and Management, studies privacy through economic models, including the economics of immediate gratification. He finds that people compromise their privacy for convenience and perks in the short run without considering what it could mean in the long run.

Think before you click. Sometimes protecting your privacy is a choice you can make for yourself.

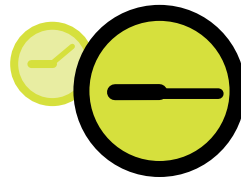
**9:03 a.m.**

You realize tomorrow is your secretary’s birthday. You get online to order flowers—pronto! You click “yes,” “yes,” “I agree,” “confirm,” and log off before anyone notices you scrambling.



**9:15 a.m.**

You log onto your email—76 new messages. “IMPORTANT: Security Breach,” jumps out at you. You scan: You need to change your online banking password. Better make it fast, 75 emails to go.



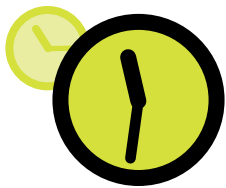
**Web phishing is**

an attack that forges legitimate Web sites to trick users into revealing sensitive information. Phishers send emails that can lure us into disclosing all sorts of personal information. The emails include links to sites that are virtually identical to Web sites you trust, such as your bank. But, in reality, the sites belong to the phisher, who, with a simple form, can get your user name, password, account number, credit card information, mother’s maiden name, and other sensitive information that can lead to identity theft.

Perrig and a group of researchers are developing a Web phishing detection tool that checks for a number of indicators that a Web site is forged and alerts users to sites that are not secure.

**11:32 a.m.**

You head over to the local medical lab to take a blood test for your annual physical—part of your company’s health insurance requirements.



**12:58 p.m.**

You walk by a construction site on the way back to your office. You wave to the Webcam. Cool, you’re famous!



Percentage of all spam that comes from “zombie” networks—online viruses that turn infected computers into spam-making machines. Some estimates are as high as 80 percent.

**We often are** told that our medical information is confidential, but the Data Privacy Lab shows it is possible to link specific DNA data with an individual by using algorithms to search through a variety of other lists of available data. Sample lists of data are provided to researchers by medical facilities, who take measures to conceal the identity of their patients. The Data Privacy Lab discovered that while many organizations sincerely believe they have protected people’s identities, they have unknowingly released information that can identify them and link them with their DNA data, revealing confidential medical information.

To combat this potential misuse of information, Sweeney and fellow researchers invented the Datafly System to guarantee anonymity while sharing medical data. Their Scrub System replaces personal identifying data in medical records.

**Today, in the** United Kingdom, there are more than 200,000 cameras monitoring public spaces, housing estates, car parks, and public facilities. But closed-circuit television (CCTV) is not just hot in the U.K. Publicly available, online Web cameras are everywhere in the United States too—on our roadways, monitoring construction sites, on college campuses, and at tourism sites.

What do all these cameras see? Camera Watch, another project of the Data Privacy Lab, is a searchable database of approximately 6,000 Web cameras monitoring public spaces. The database offers direct links to the cameras and user access to both real-time and cached images. The goals of Camera Watch are to assess the number and nature of publicly available cameras, to explore potential uses, and to analyze and propose related policies and best practices, especially in relation to privacy concerns. By providing concrete data, the debate about benefits and drawbacks of Webcams is better informed.

Want to know if you’re being watched?  
> <http://privacy.cs.cmu.edu/dataprivacy/projects/camwatch/>

**The solution is** simple. Visit the MySecureCyberspace portal at [www.mysecurecyberspace.com](http://www.mysecurecyberspace.com) and let CyLab help you customize your safety measures. Click “secure my cyberspace” and answer a couple of questions about your Internet activity and the environment from which you’re accessing the Internet. MySecureCyberspace will offer a summary of threats to your security, and tell you how you can protect your data.

MySecureCyberspace also has articles and updates to help you stay informed on hot topics, an encyclopedia of terms so thorough it could make an expert out of you, and a section for kids and teens that includes articles and games that teach Web safety the fun way, so they don’t have to learn it the hard way.

Securing your cyberspace is the smart thing to do and makes the Web a safer place to be.

“If computer users would follow a few simple and safe practices, they’d solve a large percentage of the cyber problems that plague us today,” says Dena Tsamitis, director of education, training, and outreach for Carnegie Mellon CyLab and director of the Information Networking Institute.  
> <http://www.mysecurecyberspace.com/>

Doing lunch? Back up your hard drive. Backing up your hard drive is relatively simple, can take place while you are away from your computer, and can be a lifesaver. There are a number of commercially available backup applications that are easy to use and affordable.

### 5:35 p.m.

You use the automatic checkout lane at a food mart to get home quicker with tonight's dinner and family movie. You pick up a bottle of wine for later.



**The automatic grocery** store, toward which many large food suppliers in the Western world are moving, will be designed to note every item you purchase every time you purchase it. The data collected for marketing purposes is meant to inform the merchant about the customer—and ensure you get your discount perks for purchases. However, collecting data through automatic and online transactions also allows for marketers to analyze buying behaviors on a very personal level, which can be a serious intrusion of your privacy.

Perhaps no one else will care how much broccoli your family buys. But the insurance company, employers, police, and even the government may be interested in how much tobacco, liquor, pharmaceuticals, and painkillers you buy and what kind of videos or magazines you take home.

Acquisti finds that even people who worry about their privacy may fail to take steps to protect personal data because doing so has immediate costs and uncertain long-term benefits. Shoppers who decline to use the automatic checkout know they have to wait longer in line but can't be sure what they'll gain over time.

### 8:04 p.m.

You walk past your 10th-grader typing away on the family computer. He's finally applying for a summer job. Good thing so many companies take job applications electronically these days.



**Identity theft** is a costly crime that has been abetted by information technology. Because stealing someone's identity can be as easy as doing a Google search, Sweeney's research team has created an Internet Angel that warns thousands of Americans who are at risk for identity theft. Identity Angel scans information available on the World Wide Web and notifies people that there is sufficient information available online to allow criminals to impersonate them in financial and other transactions.

The team came up with the idea after using Google to search for and find files containing names and Social Security numbers. The search turned up a number of resumes that included the information, leaving job applicants vulnerable to identity theft.

### 11:09 p.m.

Browsing online for vacation possibilities, you find a new travel site with a great deal on airfares. Prices go back up at midnight, so you sign up quick to snap up the bargain rates.



**When making an** online purchase, how often do you stop to read the overwhelmingly long privacy policy before clicking "I Agree"? Believe it or not, each policy is different, and each organization protects your privacy in different ways to different degrees. So how do you know which policies meet your needs without attempting to decipher all of them?

Cranor is building a search engine that will read and decipher privacy policies for you. This search engine uses a standard called the Platform for Privacy Preferences (P3P) and a tool called Privacy Bird to find Web sites that match your personal privacy preferences.

Here's how it works: You tell the search engine what you want in a privacy policy. You only have to do this once. Then you search for a book you want to buy on Google. Privacy Bird ranks the cyber stores that carry the book according to their compliance with your privacy preferences. If a retailer does not meet your privacy standards, you can click on an icon to learn which aspects of the privacy policy are not met.

Privacy Bird provides you with the information. All you have to do is make an informed decision. The result is privacy and security for you, and an incentive for sellers to provide better privacy policies to consumers, so they can be first on the list.

Try out the Privacy Bird software and search engine yourself.

> <http://privacybird.com/>

### Midnight

You turn off the light and hit the pillow. Your glowing laptop goes to "sleep," too, but your data trail is still ticking....



>> For more information visit [www.carnegiemellontoday.com/cybersecurity](http://www.carnegiemellontoday.com/cybersecurity)