THE FUTURE OF ONLINE PRIVACY

The coming years will make you more vulnerable than ever

What are the dangers of storing ever more e-mail, documents, photos and financial account information online? I first read interviews with experts and then designed several scenarios that depict what could happen in the next few years if technological innovation and public policy trends in three categories - online storage, location tracking and biometrics - remain on their current course.

Online Storage

The scenario: You receive a series of e-mail notes. The first attaches a compromising photo from your college days. The second excerpts an interoffice e-mail message containing confidential details of your company's merger negotiations. The third replicates a nostalgic letter that you recently sent to an ex-flame, whom you ran into at your high school reunion.

The fourth e-mail demands that you send $50,000 to an offshore account within 48 hours or your spouse, your kids and your boss will get copies of the other three messages. You have no idea how you were targeted, but someone with the keys to your online life is trying to use your past against you.

What began in 2005 with Google and Microsoft Windows Live suites of Web-based consumer applications evolved, toward the end of the decade, into online business applications that made having anything but a Web browser on an office workstation unnecessary.

Soon afterward, a multiplatform operating system appeared that synced to your TV, car, cell phone and digital video recorder. Its instant access and ease of use soon had you storing a lifetime's worth of messages, media, shopping lists, photos, notes and books on third-party servers.

Like countless others, you trusted big-name developers of new OS and Web apps to secure your data. But the volume of valuable information they house has attracted organized criminals who specialize in online data theft. They always seem to find a way to evade the latest security technologies.

You tell your company's chief security officer about the leaked merger e-mail, and she quickly initiates an FBI-led investigation.

The good news: The FBI will soon apprehend a low-level member of the gang, and your company's CTO will work on bringing hosted data services back inside the company firewall.

The bad news: Your toga party photos are destined to be a big hit on interoffice e-mail.

Why it might happen: "The biggest worry, which covers everything from Web mail to search to spreadsheets to Web OS, is how much of your data is in someone else's hands and therefore is not really yours," says PGP Corporation CTO Jon Callas. "The entire thing is running on their servers. How do you know what is going on? How much of it is yours? How much do you get to back up or delete? An awful lot of this is insecure."

Even if a company such as Google offers ironclad guarantees never to snoop into or sell your data, you're at risk from hackers, rogue coworkers, and even subpoenas or civil lawsuits filed against your company. Federal privacy laws afford less protection to data held on a third party's server than to data stored on a private hard drive.

"If [government investigators] need a warrant for your house but not your car, then certainly they don't need it for your Web mail," says Callas.

Tracking Your Location

The scenario: The police are at your house on official business, your inbox is flooded with pornographic ads - and all you did was drive to the mall to buy an anniversary gift. Welcome to wireless location tracking in the year 2020.

On Saturday morning, you jumped into your car and plugged in your new high-speed Internet phone. The phone downloaded data to the car's real-time holographic traffic map and guided you to the mall along the route with the least traffic. To find the jewelry store, you downloaded a map of the mall to your phone. The turn-by-turn directions took you past a new lingerie shop, so you wandered inside for a few seconds. Then you proceeded to the jewelry store, and in 15 minutes your shopping was done.

A little later, you started receiving raunchy multimedia messages hawking sex toys.

While you were inside the lingerie shop, the store's data reader pinged your phone via Bluetooth and then automatically bought your contact information from commercial data brokers. Now its affiliate, which sells novelty adult items, can legally market to you via e-mail, claiming an ongoing business relationship.

Next, two police officers show up at your home, explaining that your route to the mall took you past a liquor store at about the time of a holdup there. The culprit escaped in a white car, and in-road sensors flagged yours as one of ten such vehicles then in the area.

Though the police visit is for routine questioning only, and though you'll be able to unsubscribe from the adult-toy marketing list fairly easily, your wireless devices now seem less attractive than they did before.

You wish that, when purchasing them and their accompanying services, you had hunted for the opt-out privacy check boxes (required by law) that restrict or prohibit sharing of your sensitive data.

Why it might happen: Your visit to the lingerie shop could allow its owners to e-mail you. "Antispam, junk fax, and telemarketing laws all have established-business-relationship loopholes," says Chris Hoofnagle, a privacy expert at the University of California-Berkeley School of Law. "If you simply drive your car into the parking lot of Sports Authority, the company might argue that you have a business relationship."

The groundwork for tracking a car's location is already in place. Automatic toll-payment systems such as E-ZPass equip cars with RFID transponders that can transmit information about the vehicle, and in 2005 the UK began testing RFID-equipped license plates. Sensors collect only anonymous data right now, but what happens if - in the spirit of an Amber Alert - law enforcement is allowed access to vehicle data to investigate violent crimes?

The Dark Side of Biometrics

The scenario: You were trying to get a good deal on a 20-megapixel camera. Instead, you ended up with an empty bank account and a ruined credit history. The culprit was your biometric debit card, which was designed to thwart identity theft but instead let a thief impersonate you.

By 2010, after leaks of millions of credit card numbers, financial companies rolled out biometric credit and ATM check cards, which required that a card user's fingerprint (examined by a fingerprint reader) match the account holder's fingerprint (stored on the card).

The seemingly foolproof technology took off, and within a few years new PCs came equipped with software-enabled fingerprint readers that allowed users to authorize financial transactions over the Internet.

When you used your biometrically enabled ATM check card to purchase the camera, you sent your IP address, card number, and digital fingerprint over the Internet to a credit card server.

But your information got intercepted in transit and then sold on a message board. Now someone has depleted your checking account, and you can't prove it wasn't you because your fingerprint is all over the transactions.

Eventually the problem will be resolved in your favor. But for the time being, you'll have to rely on an almost extinct form of payment: cash.

Why it might happen: "It's the classic 'The computer can't be wrong' scenario," says PGP's Callas. "The opportunities for a criminal in the middle are huge, and the risk for the person who has the card is very high because people tend to believe what the biometric says."

Welcome to the future.

Dennis Turner