

Privacy Goes Big

Forget the royal wedding—
2011 is all about privacy standards

Maybe it's bold to summarize a year before it starts, but we have strong feelings about this one: We predict that 2011 will be the year privacy is redefined—the year an extended public conversation on the topic produces a very different information landscape.

Why are we so certain privacy will take center stage? Consider the evidence: First, we're coming off a year in which there was a very public outcry—Google was trashed after collecting open Wi-Fi network information, and Facebook's slippery privacy policy was front-page news. Those concerns made their way to the dockets of legislators around the country, including New York Democratic Sen. Charles Schumer, who recently sponsored social-networking legislation. [Continued on page 3](#) ▶



What's Your Identity IQ?

Protecting your identity portfolio isn't rocket science

Quick—how much money is currently in your savings account? How are your investments faring today? What bank do you use? What's your broker's name?

You can probably answer all these questions—at least pretty closely, anyway—without much thought.

But what about these: Who knows your Social Security number? How many companies have access to your name, address, SSN—even a credit card number? How is your doctor collecting and storing your medical data, and who has access to it?

You're stumped, right? But you shouldn't be.

Every American's identity is made up of three things (no, none of them is football): financial data, medical records and public documents. We like to refer to this holy trinity as your identity portfolio. An identity is an asset—as valuable as cash in hand—that is easily compromised through theft or data breach. And if you can't answer every question about your identity portfolio, then you've made it a tempting—and viable—target for fraudsters who rely on a victim's lack of vigilance to keep them in business. [Continued on page 4](#) ▶





Out with the Old

In with the newer, safer and savvier

Everyone wants a clean slate in the new year—to start fresh with a revamped workout regimen, healthy eating habits, a neater house and a commitment to spending less, earning more.

It's also a good time to clean house identitywise, to start the year knowing what information about you is out there—who keeps your vital information on file (your Social Security number, credit card numbers and so on), who has access to it and whom they share it with. In "What's Your Identity IQ?" (page 1), we offer tips for protecting your identity portfolio with the same diligence that you apply to your investment portfolio. If your personal information falls into the wrong hands, it can be a time bomb for identity fraud.

With any luck, the powers-that-be also will put identity theft at the top of their to-do lists. It looks promising—in "Privacy Goes Big" (page 1), we recap the year in privacy and look forward to 2011. We consider how Congress, the Federal Trade Commission and the Department of Commerce have recognized privacy issues with a handful of proposals that could (finally!) put a thorn in the side of identity thieves, keep tech and finance industry giants from making major privacy missteps and even help the consumer.

Speaking of tech giants, there's another bit of news to keep you on your toes this year: Creditors have discovered how Facebook can work for them, in sneaky ways. "The Social Debtwork" (page 5) warns of "friends"—creditors, private investigators and lawyers in sheep's clothing—who poke around profile pages for information to help them collect money, whether that debt is fraudulent or not. We help you prevent your walk down memory lane from becoming someone else's trip to the bank.

The world may seem to be growing ever less secure, but with a little effort on our own behalf—and with our governing bodies bringing important issues to the public consciousness—we can make 2011 a safe and productive year.

Happy New Year from all of us at Identity Theft 911.

Matt Cullina
Chief Executive Officer
Identity Theft 911

In this issue...



Features

- 5 Just when you thought it was safe to "friend" a friend's friend. Don't let debt collectors harass you on Facebook—especially if the debt isn't yours.
- 6 **Case Study:** Her identity stolen by an aggressive thief, Adrienne Parker began to wonder if she would ever stop her evil twin.

Departments

- 7 **Hail & Hiss:** Who nailed it—and who flailed it—in the fight against identity theft and data breaches.
- 8 **Ask the Expert:** Identity Theft 911 fraud resolution center team leader Brett Montgomery weighs the pros and cons of credit monitoring.

Then, in December, the Federal Trade Commission and the Department of Commerce released groundbreaking reports on privacy in American business. The reports offer a new framework for possible legislation, a call for a national Privacy Bill of Rights, technical solutions for aggressive online advertisers and a proposal for a new federal office to monitor and enforce privacy rights. Even Congress joined in, signing off last month on the long-stalled Red Flags Rule, which requires creditors to implement identity theft detection and prevention plans when opening new credit accounts.

But why privacy now?

The FTC “needed to step back and look at the way consumer privacy has changed and how the discussion around it could be brought up-to-date,” said Peder Magee, a senior staff attorney with the agency.

“...the industry needs to do a better job of making data-collection practices more transparent.... Businesses need to build privacy into their designs from the beginning.” — Peder Magee, FTC senior staff attorney

“Dramatically increased computer power, the lower cost of data storage, new business models that rely on the collection and use of user data, such as behavioral marketing, and data brokers” have all been privacy game-changers, he said.

The FTC report is open for public comment until Jan. 31. Then the FTC will review the responses and draft a final “best practices” report. The Department of Commerce report’s public comment period is open until Jan. 28.

That’s all great—but what do the higher-ups hope will come of this discussion?

“It’s clear the industry needs to do a better job of making data-collection practices more transparent, and they need to simplify consumer choice surrounding those policies. Businesses need to build privacy into their designs from the beginning—privacy-by-design,” Magee said.

Ideally, consumers will benefit in tangible ways: For example, the FTC’s much-discussed Do Not Track proposal could go a long way toward quieting concern about overzealous websites. Do Not Track would function like an off-switch for web users who want to prevent companies from gleaning their web-browsing habits and pushing targeted advertising onto them.

We’d like to see these changes in action, and apparently we’re not alone: The

“What’s the likelihood of legislation on privacy, on identity theft, at a federal level? There are lots of different possibilities as they relate to financial and health care reform. We could be near the moment when a uniform standard of practices is established: a consistent security breach notification rule, established privacy rights online.... Harmonization could make compliance possible,” Kosmala said.

And as it turns out, the U.S. is not the only country invested in improving privacy policy. More than 15 percent of the IAPP’s membership is from countries outside the United States.

“Over the next year, the European Union is looking at its privacy and data relationship with the U.S., as well as within the EU countries themselves,” said Eduard Goodman, chief privacy officer at Identity Theft 911. “It’s doubtful any international treaties will be inked, but we’ll start hearing a lot more talk about it.”

At home and abroad, the need for substantive debate and thoughtful legislation about the protection of personal information has never been more pressing, and—you can quote us on this—2011 looks to be the moment. •

International Association of Privacy Professionals (IAPP) reports a 30 percent growth over the last two years.

“The more attention that corporate boards and government agencies give to privacy issues, the more of an interest we’re seeing in membership and the media,” said Peter Kosmala, vice president of the IAPP.

He sees a good chance that legislation could drive interest in 2011.



Just as we scrutinize our investment portfolios for inconsistencies, we must pore over our identity portfolio with the same care—and be an active participant in protecting it. Reams of legislation have recently been passed to fight identity theft and force corporate accountability—the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Fair and Accurate Credit Transactions Act, the HITECH Act. While these are great steps, they won't keep tabs on your credit score and stash away your Social Security card for you.

If you fail your own identity quiz, there's no law on the books that can protect you. Follow these steps to safeguard yourself—today.

Financial Data

Guard your Social Security number—Simply go to ssa.gov/onlineservices and create an account. From there you can check your records for fraud. Also, carefully read your annual statement from the Social Security Administration, since this could indicate misuse.

Check your accounts—Review your bank and credit card statements regularly to make sure that no one has made unlawful charges.

Wallet woes—Never carry your Social Security card or all your credit cards in your wallet. Keep reserves at home. If your wallet is stolen, you'll be thankful for the backups.

Get a free credit report—The three major credit-reporting agencies are required by law to provide you with a free copy of your credit report once every 12 months. Visit: annualcreditreport.com.

Medical Records

Review bills closely—Open and carefully review each medical document you receive, checking the itemized costs. If something looks suspicious, investigate by calling right away.

Regularly check your medical and pharmaceutical records—Keep a list of the names and contacts for doctors, pharmacies and other health care providers you have visited in the past

and refer back to this list in the event a problem arises. Check your pharmacy records and be sure all prescriptions are really yours.

Check every medical insurance

Explanation of Benefits (EOB)—When your insurance provider sends an EOB, check the services charged against your own list of doctors visited, treatments received and dates of service.

searches of government databases for possible identifying information. In most cases, the company will alert you by email if your information has been made public.

If all this sounds too time-consuming, Identity Theft 911 Chairman Adam Levin has a few questions of his own for you: "How much time each day do you spend on your Facebook wall? How much time

Keep Your Computer Svelte

Whether you're on a Mac or PC, these regular maintenance tips will keep your system slim, trim and speedy—and block miscreants from your machine.

How does swiftness equal security? Hacker intrusions, viruses and malware most likely will slow down your computer. This can go undetected in a sluggish system. Get your computer running fast and clean and you'll be in a better position to notice trouble—and respond to it.

1. **Turn on automatic updates.** This will make sure you have the latest software patches for your operating system and web browser, which are usually published to fix known bugs and security flaws.
2. **Must-haves: antivirus, antim malware.** Make sure you have both an antivirus and anti-malware program installed. There are several good free options for personal use from companies such as AVG and Malware Bytes.
3. **Drive power. Uninstall programs and apps you don't use.** Run a disk cleanup and defragmenter in Windows or use an application such as AppCleaner or AppZapper in Mac OS.
4. **Turn on your firewall.** This will prevent intruders from entering your system via the Internet—a must-have in these cybertimes.
5. **Manage your startups.** This is as easy as running "msconfig.exe" in Windows or finding "Login Items" in your Mac System Preferences. The fewer programs that automatically load, the more system resources available, the faster your computer.

For more on computer fitness, read Identity Theft 911 Chief Security Officer Ondrej Krehel's blogs at credit.com/blog/author/ondrej.

Ask your doctor if he or she has a privacy policy and how it's enforced—Find out if that policy applies to their vendors, such as third-party billing companies.

Public Documents

Search government websites—A look at your local court records can make sure that no one has committed a crime or obtained a lien in your name. Check your county assessor's office to make sure there are no errors in their records.

Consider a private service—There are private companies that will run regular

do you spend on gossip websites or checking sports scores?"

The commitment of a few hours to tracking your identity portfolio the way you would your stocks and bonds pays very real dividends. "Just ask the thousands wrongly put on no-fly lists, or with ruined credit or in life-threatening situations because their medical records were compromised by crooks," Levin said.

Millions of Americans discover every year just how real the risk is and just how much the damage costs. Don't be one of them: Know the answers. •



The Social Debtwork

With 'friends' like these, who needs collection agencies?

Social networking can make you feel all warm and fuzzy—until a bounty hunter comes knocking on your door. Sure, it's great to reconnect with your long-lost college roommate, and even better that Aunt Nan can check out family photos on your profile page instead of pestering you for pics. But if you happen to be in arrears, your warm fuzzies can quickly turn cold.

Whether you owe \$20,000 on a credit card or \$500 on a car, debt collectors can now track you down through your social networking profiles. These collectors are getting hip to how Facebook can work for them: By "friending" acquaintances of a debtor, or even friends of friends, they've been able to pinpoint where someone lives, works, even parties, and pursue collections using that information.

"Facebook is nothing more than a condensed version of alternate contact lists—phone, email, instant messaging, website—it's a cocktail of them all," said Eduard Goodman, chief privacy officer for Identity Theft 911.

While this practice might be effective for nabbing true debt dodgers, it's unclear whether it's legal or ethical—and there's no way to ensure that it's a power used only for good. "There's not a whole lot

tested on this and whether it's ethically kosher or not," Goodman said.

The main problem with it, he continued, is that there's "an expectation of privacy" on Facebook, and that, even with a discreet profile with fewer than 100 friends and the maximum privacy limitations, "all you need is for one friend

By "friending" acquaintances of a debtor, or even friends of friends, [debt collectors have] been able to pinpoint where someone lives, works, even parties, and pursue collections using that information.

of a friend to let [a debt collector] in that door." And, of course, there is usually no disclosure that they are attempting to collect debts—though collectors are required by law to identify themselves.

This is a particularly sticky point for victims of fraud—who are often chased by creditors pursuing false debt in the victim's name. In some cases, a fraud victim can clear the blemish on a credit report, but the creditor—rather than closing the account—can sell the debt to another agency, which slightly changes the amount and goes after the victim again. That debt has been cleared,

Goodman said, and the new collectors "don't have the right to contact friends, family members or alumni associations."

In addition to the Wild West mentality of social networking, said Goodman, creditors have the advantage of pursuing people who often are out of work and struggling financially, and who have little

legal recourse. "You walk into a free legal clinic and tell them you have an issue that's not life threatening and they won't be equipped to help you," he said, adding that the FTC is a good place to lodge a complaint.

Facebook also was used recently in civil litigation—in the issuing of warrants and subpoenas and for tracking witnesses and investigating jury tampering, Goodman said. "This is an always-changing technology, and it's still very unclear how it's going to play out," he added. "But it's going to get worse before it gets better." •

One Identity, Two Very Different Lives

An illicit impersonator denies an Arizona woman her due

When the woman who stole Adrienne Parker's* identity was arrested in Florida recently, she could produce more official identification than the *real* Adrienne Parker.

Parker, 38, has waged war with her larcenous alter ego since 2005, when the IRS notified her that she owed back taxes for a job she'd never had. Next, she went to the DMV to find out why she hadn't received registration renewal paperwork and discovered that someone had changed the address in her file—and that someone else's photograph was in there too.

Parker repeatedly told the agencies it was a mistake. But the thief, who had likely ransacked her mailbox for her Social Security number, was already entrenched as Adrienne Parker.

In 2006, Parker's credit union referred her to Identity Theft 911, where fraud resolution specialist Mark Fullbright uncovered a labyrinth of credit, medical and employment

"I'm not a criminal. I've never been arrested, never been in jail, never even had a parking ticket." — Adrienne Parker

fraud totaling tens of thousands of dollars—among other crimes—spanning several states.

The thief, Parker said, had been charged with "shoplifting, burglary, abuse of a minor, everything. She'd gotten a gas bill in my name, opened bank accounts, gotten medical care and even started collecting Social Security benefits."

Fullbright spent hundreds of hours working with law enforcement and state agencies, clearing 90 percent of Parker's records. Despite the culprit's arrest, however, Parker cannot dispute out-of-state criminal records without appearing before a judge in each state—and she can't afford to make those trips because her erroneous criminal history has hindered her job search.

"I'm not a criminal," Parker said. "I've never been arrested, never been in jail, never even had a parking ticket. She walked into the DMV and got a driver's license [in my name], and now I have a criminal background."

Fullbright says Parker's case is among the worst he's seen in 18 years in the business, particularly since she did everything right. His advice for anyone facing similar circumstances:

- Immediately place a fraud alert in your file at all three credit-reporting agencies.
- Order credit reports and identify the fraud.
- Notify creditors affected by the fraud.
- File a detailed police report.
- Document every attempt to notify police and creditors, and put all communication in writing.
- Follow up. Don't assume the agencies or police you talk to will handle the problem.
- Contact an identity theft resolution company at the first sign of trouble.

Fullbright is now helping Parker obtain a new SSN, and he keeps tabs on her case as it wends through the criminal justice system. They talk a few times a month, rather than every day like they used to. Fullbright is also helping Parker find free legal counsel—a step he believes may offer her the best chance to get the happy ending she deserves.

"I have lived with this every day," she said. "She has ruined my life for the last six years, out there living as me. I just want my name cleared."

Until that day, Parker is grateful for Mark Fullbright and Identity Theft 911. And she has some advice for others: "I wouldn't wish this on anyone. Shred everything, check your credit report. Because if you're not looking, you won't know there's a problem." •

* Identifying details have been changed to protect the victim's privacy.

Hail



Breaking News: Pigs Fly as Data Miners Dig Consumer Concerns

Wonders, apparently, still haven't ceased: In January, the **Open Data Partnership**, comprising eight data-mining companies, will launch a site letting consumers specify what profile information the companies can disclose online. Scott Meyer (left), CEO of Better Advertising, which spearheads the project, says more transparency is needed in the \$25 billion industry. The self-regulatory step could blunt possible federal curbs on data collecting, though major companies like Google and Yahoo aren't on board. According to *The Wall Street Journal*, initial participants include BlueKai Inc., Lotame Solutions Inc. and eXelate Inc., which, combined, reach at least 80 percent of U.S. Internet users. When consumers are done gawking at all those soaring swine, they'll be able to better control what advertisers know about them.



Security Soars as Top Priority for Indian Outsourcers

The **Data Security Council of India** and **KPMG** highlighted data protection as the major concern of the country's \$15 billion business processing industry. Companies agreed that privacy and data security issues lead their list of challenges, though many are trying to limit their liabilities with contracts that make clients responsible for any data vulnerability. The recent joint study said 70 percent of respondents feel they've addressed their own security issues adequately. This won't be the last time the issue is raised, as forecasts suggest the Indian processing industry will expand to \$225 billion by 2020. Here's hoping they continue to value security as much as they do growth.



Snark Site Sincere After Data Breach

Gawker Media, parent of nine popular websites, including Gawker.com, acted with speed and sincerity after its comment boards were hacked. It promptly told 1.3 million registered commenters to reset their passwords to protect themselves and included an uncharacteristically earnest apology. "We understand how important trust is on the Internet, and we're deeply sorry for and embarrassed about this breach of security—and of trust." The digital mea culpa transcended the realm of snark, as sites from Yahoo!, LinkedIn and Blizzard's "World of Warcraft" then urged password resets, elevating the often-ignored issue of password security.

Hiss



McData Breach for Promo Campaigns

Customers aren't lovin' it: Burger fans who took part in recent **McDonald's** promotions, including the Monopoly game, also signed on for potential identity theft. **McDonald's warned customers of a data breach** by a third-party vendor—hired by a different third-party vendor—which exposed customers' ages, phone numbers and email and physical addresses. The company stated that it doesn't collect Social Security or credit card data but asked customers to report any emails purporting to be from McDonald's requesting financial information. In related news, **Walgreens recently notified customers** that a crook had nabbed its email marketing list—and went phishing with it—but assured them that prescription information was not disclosed. Want some fries with that lousy security?



Sniffing Raises a Stink

Hundreds of websites can track your web surfing past, **eWeek reports**, and dozens of them are already taking that data to their own networks, say researchers at the University of California, San Diego. "History sniffing" exploits web browser properties and sends invisible links to web pages, then tracks them to determine if the user has visited specific URLs. **Two California residents are suing Midstream Media International**, the Netherlands-based parent of an adult website, for illegally taking data that could be sold to marketing firms. It's the first legal counterattack on sniffing, but, by the smell of it, surely not the last.



Fed Med Database Stirs Staff Wrath

Eight million federal employees can't be wrong: Plans to put their medical claims data in a research database caused an outcry among privacy activists. **The Office of Personnel Management (OPM)** wants to analyze medical claims filed by participants in the Federal Employees Health Benefits Program, but critics say concentrating that data raises the possibility of its being breached. The American Civil Liberties Union, the Consumers Union and the American Federation of Government Employees called for more disclosure about the database. In response, according to the Washington Post, OPM said it has a strong security track record, but one breach could be devastating. Hmmm ... 8 million to 1. Not odds we'd take.



Q&A with Brett Montgomery

Double down for credit safety

Question: I've been hearing a lot about credit monitoring, but I'm not sure it's worth paying a service for this. Should I spend the money? Can't I do this for free?

Answer:

The short answer is yes, there are free options, and yes, credit monitoring is worth the investment. In fact, for those who feel their identity or personal information may be at risk, I always recommend a two-pronged approach: a credit-monitoring service combined with a free fraud alert placed on your credit file (go to annualcreditreport.com for more information on how to do this).

Credit monitoring is a good thing—it's fairly inexpensive and serves its purpose. Basically, if there's any change in your credit profile, you're notified by email. You have the freedom of not having to check your credit all the time—the service is working for you. It's not always instantaneous, though. You may not learn of a change in your file for about a week. So if you're away on vacation and unable to check your email, the damage has been done.

That's why, for those who think their personal information may somehow have been exposed, using both methods is best. If you place a fraud alert on your credit file and a creditor checks your credit, they're instantly alerted to contact you by telephone. They should not extend credit unless they reach you and authenticate you. The fraud alert lasts for 90 days, so you must extend it regularly.

But realize, the purpose of a fraud alert is to make it more difficult to extend credit, and this might affect your ability to "instantly qualify" for an in-store credit card or auto loan. This is also why you'll need to set up your monitoring product first. If you place a fraud alert first, it may prevent the monitoring company from accessing your credit information. If you already have a fraud alert in place, it's best to wait until the alert has expired. Once it has, you can register for your monitoring products, then reactivate the alert.

When shopping for a monitoring service, check with your insurance carrier, bank or credit union. Many sell and back up products with fraud resolution. An annual service is easier and less expensive than a monthly one, but both are fine. What's most important is choosing a product that covers all three credit bureaus. Many services will give you access to all three credit reports but will only monitor one bureau.

Also, find out how the monitoring company backs up their services. If your credit is compromised, are resolution services included? What else are you paying for? Do they also include public and court records or Social Security trace monitoring? And do they share or sell your information with third parties to market to you later?

None of these methods is 100 percent fraud-proof. Occasionally creditors don't adhere to the fraud alert. But with both a credit-monitoring program and a fraud alert in place, you've increased the likelihood of catching fraud early and decreased the chances of human or systems error allowing an identity thief to slip through the cracks. •

Brett Montgomery is a team leader in Identity Theft 911's fraud resolution center. He has more than 15 years' experience in financial fraud and advocating for identity theft victims.