

# From Apps to Zeus:

## The year in privacy issues, 2010

Privacy is no longer the flavor of the month, but rather the issue of the decade. Growing concern over the risks inherent in the loss of control over personal information—either by unauthorized criminal access, business practice, governmental fiat or voluntary action—has brought the issue top-of-mind in 2010. People around the world finally began to recognize the reality and the dark side of global overexposure. We asked privacy experts from government, business and consumer rights organizations for their take on the message behind the headlines.

**Kristin Krause Cohen** is an attorney with the division of privacy and identity protection, Bureau of Consumer Protection, Federal Trade Commission. A former U.S. prosecutor, **Kimberly Peretti** is a director with PWC's U.S. Forensic Technology Solutions practice. **Paul Stephens** is the director of policy and advocacy with Privacy Rights Clearinghouse.

**Facebook**—The popular social networking site ignited a firestorm of controversy in May when it altered its privacy settings, changes that included the launch of social plug-ins that share profile information with other websites.

**Cohen:** "The FTC is certainly concerned that businesses, including social networking sites, live up to the privacy promises they make. For example, in our recent settlement with Twitter, we alleged that the company failed to live up to its promise to safeguard consumers' personal information." *Continued on page 3* ▶



## Fraud to the Maxx

### Lessons learned from *U.S. v. Albert Gonzalez*



When 29-year-old Albert Gonzalez (left) pleaded guilty early this year to the largest hacking and identity-theft case in U.S. history, he didn't have much to say. "I blame nobody but myself," he told the judge.

But Gonzalez could have talked about plenty: He masterminded the capture and exposure of more than 170 million credit and debit card numbers. He worked as an informant for the U.S. Secret Service on cybercrimes, while at the same time mounting some of the largest single-system data breaches anyone has ever seen. *Continued on page 4* ▶



# In Defense of Our Privacy

For several decades, other than a few shining moments, the concept of bipartisanship has been as elusive as the 10-cent cup of coffee. Our friends and colleagues in government have enough trouble coming to a consensus on the start and end dates for daylight saving time. But, as we transition from the era of TMI (too much information) into the age of EMI (ever more information), hundreds of millions of individuals are becoming members of Gen I (Generation Invincible). Sensitive personal information is being mandated, flung and sucked out of cyberspace by consumers, government and businesses alike. Leaders in the public and private sectors are beginning to agree that privacy is in danger of no longer “becoming the norm,” and its defense must become a top-of-agenda issue.

Our feature stories on the privacy policies of social networking sites and Google, colossal breaches of health care and banking databases—and the unprecedented identity-theft crimes of Albert Gonzalez—delve into how the Federal Trade Commission, as well as top consumer advocacy groups, are finally cracking down and developing a legal framework that takes steps to protect consumers.

Over the past two years, with the passage of landmark pieces of federal legislation—such as the Credit Card Accountability, Responsibility and Disclosure Act; the massive Dodd-Frank Wall Street Reform and Consumer Protection Act (FinREG); the HITECH Act and others—the American people have mandated that our institutions must become more transparent and accountable. All loopholes and unintended consequences to the contrary notwithstanding, institutional accountability is only part of the solution. It cannot fully succeed in the absence of individual accountability. Responsible institutional transparency is designed to protect; irresponsible individual transparency is a recipe for exploitation and potential ruin.

Every day, hundreds if not thousands of individuals and institutions (both public and private) access, gather, store and/or distribute information about us. Oftentimes we are either unaware of the number or frequency of these intrusions, or we are all too willing to accommodate them depending upon the scenario. Unfortunately, such information giveaways or takeaways don't necessarily empower us but rather expose our vulnerabilities.

Institutions and criminals have determined that our personal information is an asset, yet for some reason millions of us never received that memo. When we hear the word “asset,” our Pavlovian response is “portfolio of investments.” Most of us never think of our credit or identity as portfolios, yet they are, and they are perhaps even more valuable to our security—and just as vulnerable. As we seek the right professional financial planner to intelligently and protectively manage our investment portfolio, we must be the professional managers of our credit and identity portfolios, for they too must be properly built, nurtured, managed and protected. And, while you can always find another professional to run your financial portfolio, no one has a greater stake in your personal protection—or is in a better position to know more about you—than you.

It doesn't matter how many laws exist on the books or how vigorously those laws are enforced. At the end of the day, the ultimate guardian of the consumer is the consumer. And while the privacy debate in Washington and other nations evolves, and the limits to our tolerance to unwanted intrusions are tested, we shouldn't add to the information glut by being irresponsible on the issue of individual transparency.

As always, we hope that you find this offering profound and provocative. Have a happy, healthy holiday season.

Adam Levin  
Chairman and Cofounder  
Identity Theft 911

## In this issue...



### Features

- 5 **Don't let airport security clip your wings** this holiday season. Follow these tips to sail through scans and searches without losing your cool.
- 6 **Case Closed:** Amy McCall's driver's license was stolen at a local copy shop, leaving her to travel a long and difficult road.

### Departments

- 7 **Hail & Hiss:** A roundup of who's getting it right and wrong in the fight against identity theft and data breaches.
- 8 **Ask the Expert:** Kimberly Peretti, a director in PWC's forensic services practice, helps keep your company's security practices up to snuff.

**Stephens:** “The real problem with Facebook is that so many people consider it socially indispensable. Facebook, in a sense, has a monopoly on social networking, and many people—app developers and the like—are taking advantage of this. Another key problem that makes Facebook very unfriendly to the consumer is that the privacy policy changes so often. Facebook has created this situation in which consumers feel they need to use it, yet they have a privacy policy that is incomprehensible and consistently changing.”

**Google**—Growing concerns over Google and privacy were amplified in 2010 when it was revealed that the Google Maps Street View team, which photographs city streets for the Street View feature, gathered more than just the occasional

**“The real problem with Facebook is that so many people consider it socially indispensable. Facebook, in a sense, has a monopoly on social networking, and many people—app developers and the like—are taking advantage of this.” — Paul Stephens, Privacy Rights Clearinghouse**

image of a naked person—they also nabbed personal data from unprotected Wi-Fi networks. Google called the collection “accidental” and is reportedly deleting the information, but not before privacy watchdogs showed their teeth.

**Cohen:** “The FTC certainly had concerns about Google’s internal policies that led to this inadvertent data collection. We’ve received assurances that they have improved their procedures, including incorporating a formal privacy review process into all their new initiatives. They have also said that they have not used the data and will delete it.”

**Stephens:** “There’s blame to go around here. One of the problems is that the typical default configuration of a wireless router does not maintain adequate security. It’s an extremely difficult task to properly configure a Wi-Fi router and

keep it secure. That doesn’t take any of the blame away from Google, but there are two parts to this story. It should serve as a wake-up call to consumers.”

**Health care**—Data breaches cost the health care industry \$6 billion per year—a systemic ailment if ever there was one—yet 70 percent of health care providers don’t see securing data as a priority, according to a November Ponemon Institute study with 65 survey respondents. Providers are apparently a soft target for cybercriminals: Over a two-year period, the average organization had 2.4 “data breach incidents” and lost approximately \$2 million.

**Cohen:** “With the push for electronic health records, we also need to start pushing data security. But it’s important,

too, that paper records not be ignored. [The FTC] and U.S. Department of Health and Human Services recently reached settlements with CVS and Rite Aid, in which we alleged the companies’ inadequate data disposal policies led to sensitive personal health and employee information being found in publicly accessible dumpsters.”

**Stephens:** “What’s unique with respect to the health care industry isn’t the number of breaches, but the nature of the data. Whereas typical data compromised in a breach tends to be financial and can contribute to identity theft, health care also has medical records that are sensitive in a different way. That information won’t help identity thieves but can cause embarrassment or issues with employers or in finding insurance.”

**Albert Gonzalez**—In August 2008, then-U.S. Attorney General Michael Mukasey called the indictment of hacker Albert Gonzalez “the single largest and most complex identity-theft case ever charged in this country.” In March, the hacker smackdown continued when Gonzalez pleaded guilty to all counts and was sentenced to 20 years in federal prison. (See full story on page 1.)

**Cohen:** “Obviously, we’re extremely happy he’s been brought to justice, though we think it’s important to note that companies that collect sensitive data must remember that they have an obligation to protect information from hackers like Gonzalez. The burden is not solely on law enforcement.”

**Peretti:** “Our adversaries, the people who can attack our system, do not require a great amount of experience, resources or training. This isn’t a mafia. It’s kids meeting in high school or meeting in the shopping mall with the self-taught computer skills to get into hundreds of systems.”

**Zeus Banking Scam**—In case you needed more reasons not to open email attachments from unknown senders: More than 80 people were arrested worldwide in September and October in a banking scam that targeted midsize businesses and municipalities—siphoning off more than \$70 million.

**Cohen:** “Educate yourself. The FTC has an online security site, [OnGuard Online](#), to help consumers learn how to protect against Internet fraud and secure their personal information.”

**Peretti:** “Cybercriminals are constantly changing their attack. In this case we saw them using malware to steal credentials, but they also constantly changed their attack based on the financial institution’s particular security practices. It demonstrates the need for an active and ongoing incident response approach to cyberincidents.” •

Gonzalez and his team breached several major retail enterprises, including TJX Companies, the parent corporation of T.J.Maxx, OfficeMax, Barnes & Noble and Sports Authority, gaining direct access to the stores' point-of-sale terminals. When a card was swiped, Gonzalez's software automatically sent him a message, like an email, with the card information attached. All told he cost companies such as TJX and others more than \$400 million in damages, reimbursements and legal fees.

So what motivates Gonzalez and hackers like him? Is it more than money?

It's "a combination of challenge, ego and greed—in that order," said Kimberly Peretti, who, as the lead prosecutor in the case against Gonzalez, is uniquely qualified to know. Described by *The New York Times* in a November story as the person who "knows Gonzalez as well as almost anyone in government," Peretti now works for PWC as a director in the U.S. Forensic Technology Solutions practice.

"Hacking was Gonzalez's area of expertise, so it gave him this large sense of accomplishment to get into systems that have security in place and work around it," she said.

"We learned about the ease with which cybercriminals can hide their tracks on the Internet, but they do leave tracks and it's possible to investigate, identify, apprehend and convict them," Peretti continued. "Now the hacking community knows the stakes. The 20-year sentence for Gonzalez is the most significant ever issued to a cybercriminal. It equals the most severe punishments handed down to major white-collar criminals."

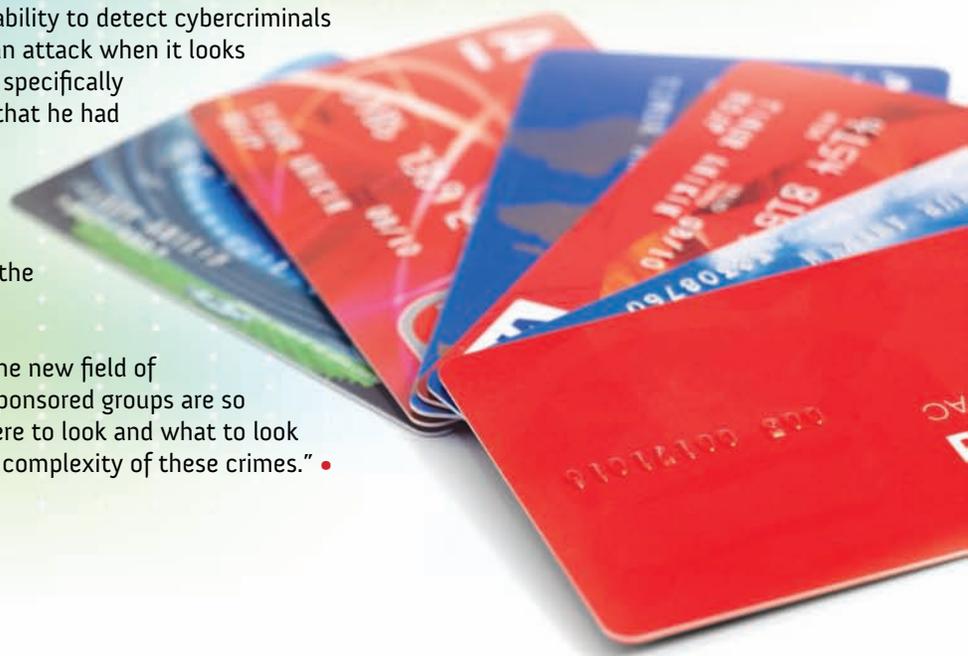
Reasonable security practices will prevent most types of cybercrime, yet Gonzalez and hackers like him operate on a different level, Peretti said.

"Businesses need to heighten their awareness and ability to detect cybercriminals in their system. Oftentimes a company only spots an attack when it looks through old logs and other indicators, when they're specifically looking for evidence. We saw in the Gonzalez case that he had unfettered access for months and even years."

The new security approach needs to be detection-based, she said, stopping hackers on their way in the door, rather than after they've left the system with stolen money or information.

"That detection is really what we're developing in the new field of cyberforensics. A lot of criminal groups and state-sponsored groups are so sophisticated that you need experts who know where to look and what to look for. It's essential now, because of the difficulty and complexity of these crimes." •

**"Businesses need to heighten their awareness and ability to detect cybercriminals in their system. Oftentimes a company only spots an attack ... when they're specifically looking for evidence. We saw in the Gonzalez case that he had unfettered access for months and even years."** — *Kim Peretti, former U.S. prosecutor*



# Happy travels...

## Here's looking at you, kid

Airport pat downs? Full-body scans? Fuhgeddaboutit.

With the holidays thundering toward us like Rudolph on Red Bull®, the last thing you want to worry about is the little gift you'll get from the TSA on your next trip to the airport.

Airport security is an inescapable part of travel. At Identity Theft 911, we watch the wrestling match between security and convenience play out every day as we help fraud victims reclaim their lives. And here's what we've learned so far:

You can have great convenience.  
You can have great security.  
But you rarely can have both.

While we can't relieve your angst about which option to choose at the security gate, we can offer you a few pithy thoughts to mitigate your agita during holiday travels and into the new year.

### Our Unofficial Guide to Which Folks to Avoid When Picking Your Screening Line *(aka, Don't Be Any of These People)*

1. **Ms. 12 Bottles of Perfume at the Bottom of Her Carry-on.** She obviously missed the memo: No liquids over 3 oz., and always pack them in a quart-size plastic bag.
2. **Alpine Hiking Boots Guy.** Yep, those things have to come off. All 36 eyelets and the double-knots in the laces. Better you should follow Mr. Loves His Slip-Ons, instead.
3. **Mr. "My Driver's License Is in My Checked Bag."** After an apoplectic moment when the TSA agent asks for his photo ID, he'll realize he can be pulled aside, searched and interviewed and hopefully still board the plane.
4. **Mrs. Pockets Bulging Like Squirrel's Cheeks.** Her watch, keys, cell phone and pen will set the metal detector atwitter. She won't be the only who wishes she'd stowed them in an empty pocket on her carry-on and sent them through the X-ray machine.
5. **Little "Mommy, the Scary Lady Is Touching Me!"** Too bad Mommy didn't have her own pat down first and explain that this touch is safe, just like the doctor's.
6. **Mr. "OMG, Where's My Boarding Pass?"** He could have saved a few gray hairs had he downloaded his boarding pass onto the Web-enabled mobile phone that never leaves his sight or—at the very least—shoved a paper copy into his shirt pocket.

Wishing you safe skies, short lines and a joyous New Year, *Your Identity Theft 911 Team*

**Want more on TSA screening and other privacy issues?**  
Check out the Privacy & Security blog on [Credit.com](http://Credit.com).



## A Minnesota Crook Has License to Steal

### When a driver's license is left behind, there's trouble ahead

Amy McCall\* has wished a thousand times that she could take back the moment when she forgot her driver's license on the glass of a Kinko's copy machine.

Since that day in 2007, the Minnesota nurse's financial road has taken one twist after another.

Her license got into the hands of a woman who obtained credit cards, rented cars, opened checking accounts, wrote a slew of bad checks and got a pile of driving violations—all in McCall's name.

"It's just been such a mess," said the 25-year-old McCall.

She immediately got a new driver's license and had no inkling of a problem until, months later, she received a letter saying her license was going to be revoked due to an unpaid handicapped-parking violation.

Then, she was notified about an unpaid Las Vegas rental car bill and bad checks written in her name—more than 20 in all, for about \$100 to \$150 each.

McCall began working with Identity Theft 911 fraud specialist Mark Fullbright, but every time they took care of one problem,

a new one popped up: A second rental car was repossessed, McCall was banned from renting cars at major agencies, and at one point, a suspicious store clerk tried to take McCall's license from the perpetrator—but she got away.

This was one of Fullbright's most complex cases, he said, because the perpetrator was using someone else's Social Security number in conjunction with McCall's license, complicating matters greatly. And it wasn't in the past tense—the case was active and ongoing.

"We were discovering things as they were happening," he said. "We couldn't anticipate them, so the challenge was to get them taken care of quickly."

Fullbright worked with police in several counties—and in Wisconsin, where the perpetrator was given a ticket, but police missed a fraud warning in McCall's DMV file. He worked closely with a bank, two credit card agencies, two rental car agencies, several collection companies, a Wisconsin judge and, in the most dramatic moment of McCall's ordeal, a mortgage company.

McCall was poised to purchase a new home when fraudulent activity showed up on her credit file. With his client's mortgage in jeopardy, Fullbright shifted into overdrive, tracking down the debt, pleading with the lender and sorting it out in time. McCall closed on her house as scheduled.

**The perpetrator was using someone else's Social Security number in conjunction with McCall's license, complicating matters greatly.**

The perpetrator has never been caught, though Fullbright and McCall have presented documentation to law enforcement several times. "You talk to a thousand different people," McCall said, "and nobody puts it together."

The personal costs have been great and McCall's credit has been tarnished, but for the most part, she has recovered her life. Law enforcement officials and banks have dismissed or written off most charges.

And through it all, she has had Fullbright by her side. •

\* Victim's name changed to protect her privacy.

## Hail



### FBI Goes In on Trident Breach

Even the savviest high-tech thieves have a weak link, according to the **FBI**, which took down an international ring of cyberthieves through the syndicate's street-level money mules. While criminal computer wizards plundered U.S. and European businesses with sophisticated hacking and money transfers, Operation Trident Breach pinpointed numerous mules who set up shell accounts into which stolen money was transferred. A dozen criminal complaints from the bureau's New York office show many Eastern European immigrants established multiple accounts and received money in exchange for an 8 to 10 percent cut—a paltry price for taking the fall.



### Air Force: Don't Check In for the Enemy

Servicemen shouldn't run for "mayor" of their military base on Foursquare or other social networking sites with location applications, says the **U.S. Air Force**. A careless Facebook "Check-in" or use of Gowalla or Loopt, which reveal an airman's location, "can have devastating operations security and privacy implications," warns a recent posting on the internal USAF site. The U.S. Department of Defense, which does allow the use of Twitter on nonclassified military networks, has long been concerned about social media use—for good reason, apparently, as now we know that lax use of Loopt could hurt the troops.



### Alarm Bells on Smartphone Security

Independent technology analyst **Ovum** and the **European Association for e-Identity and Security (EEMA)** say widespread smartphone use dials up data-security worries for businesses. The blurring of personal and business use on work-issued devices, such as the ever-present BlackBerry, heightens the vulnerability of corporate information. It's "the elephant in the boardroom," according to eWeek Europe. Only half the organizations surveyed use some form of authentication for mobile users, and only 9 percent of that group use the highly secure two-factor authentication protocol with one-time passwords. That leaves an open line for data breaches.

## Hiss



### Hospitals' Ailing Data Protection

The **health care field** lags behind all other sectors in data security as one-third of all related businesses report at least one instance of medical identity theft, according to a national study by the Healthcare Information and Management Systems Society. Leading the list, six California hospitals were recently fined a total of \$842,500 by the California Department of Public Health—mostly for unauthorized employee access of patient records, which in one case were used to open fraudulent accounts, according to the Los Angeles Times. Seems like medical practices and hospitals have a bad case of seriously lousy security procedures.



### Adler Seeks Red Flag Bill Restrictions

**New Jersey Democratic Congressman John Adler** introduced a bill to narrow the scope of the Federal Trade Commission's groundbreaking identity theft legislation. As reported on a blog by the law firm Hunton & Williams, Adler wants to revise the Identity Theft Red Flags Rule—which requires creditors and financial institutions with "covered accounts" to create identity theft protection programs—to exclude attorneys, law firms and health providers. Why? Because these groups only "advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person." Adler's act might cut down on the paperwork but could also cut down on identity theft safeguards.



### Higher Ed's Failing Grades for Data Security

A **University of Hawaii** alumnus sued his alma mater after finding out his student data was used to generate four other Social Security numbers. It's just the latest example of remedial-level data protection at U.S. colleges and universities, where students' personal information routinely winds up in the public eye. Hundreds of thousands of current and former students at state universities in Nebraska had their information exposed by the state treasurer's office, which failed to "scrub" the data. The Hawaii suit, by Philippe Gross, wants the state to put data protection plans in place and seeks financial damages. Compliance would be an easy A.



## Q&A with Kim Peretti

### Reducing your company's vulnerability to cyberattack and breaches

**Question:** I own a medium-size business with extensive customer files and billing records. How can I stay informed about emerging threats and make sure my security practices are up-to-date and effective?

#### Answer:

When I was at the Department of Justice, I talked with a lot of companies, and one of the responses I always heard was, "If we only knew this kind of attack was happening 18 months ago, we would have been able to respond and stay safe." What they learned the hard way is that security is a lot more than checking off compliance boxes.

First you must identify, within your industry, what attacks could most likely happen. Staying compliant isn't enough, because criminals always outpace regulators. We've seen a sea change in the last 18 months to two years. Law enforcement groups, academics and nonprofits are all pushing out information on cyberattacks. Find the groups following attacks in your industry and stay abreast. For example, if you have credit card data and are PCI compliant, the Secret Service Electronic Crimes Task Force regularly puts out payment card data information. InfraGuard at the FBI regularly puts out information on recent attacks, as do the big credit card companies like VISA. There are also consumer-based incident response groups, some specific to particular industries. You want to get on those listservs.

It's important to remember that compliance does not mean you're secure. Smart businesses take a risk-based approach. Security is only effective if it's tailored to the types of attacks that are most likely to happen on your system.

**Kim Peretti** was the lead prosecutor in *U.S. v. Albert Gonzalez*, the largest identity theft case in U.S. history, and now serves as a director in PWC's U.S. Forensic Technology Solutions practice.