

Customers stay despite high-profile data breaches

May 1 2011, By JORDAN ROBERTSON , AP Technology Writer



In this Jan. 27, 2011 file photo, Sony Computer Entertainment President and CEO Kazuo Hirai speaks how to use its new PlayStation Portable "NGP" at PlayStation Meeting 2011 in Tokyo. People are turning over personal information to online retailers, social networks and others in growing numbers, even as concerns about privacy mount. (AP Photo/Shizuo Kambayashi, file)

(AP) -- Week after week, thieves break into corporate computer systems to steal customer lists, email addresses and credit card numbers. Large data breaches get overshadowed by even larger ones.

Yet people are turning over personal information to online retailers, social networks and other services in growing numbers. The point at which people lose trust in the websites they deal with appears further away than ever before, if it exists at all, as [shopping](#), socializing and gaming online becomes deeply embedded in modern life.

People have come to accept that sharing information is the price of a meaningful, connected life online - even if they don't like it.

"We are clearly schizophrenic about this technology," said Jim Dempsey, an expert on [Internet privacy](#) at the Center for Democracy & Technology. "We love it, we use it, we expect it to work, and we've woven it into our daily lives, professionally, socially and personally. But we really don't trust it, and we do get upset when our data is lost or stolen."

Companies collecting the personal details have little incentive to offer the best privacy protections. So far, people haven't demanded that companies do better by walking away from their gadgets, online retailers or social networks.

"I know I take the risk," said Lance Locurto, 44. "It's more convenient."

The South Florida banker said he buys almost everything online, despite the fact that hackers got into both his iTunes and Amazon accounts in the past few months.

Jim Pachetti, 47, a laid-off carpenter looking at an iPhone at an Apple store outside Buffalo, N.Y., said he's resigned to the fact that breaches happen.

"I've accepted the fact that all my information is out there and someone has it, and that's just the way it is," he said.

James McCartney, an identity theft expert, said his smartphone has become an integral part of his life and business, despite the security concerns.

"The velocity of business precludes me from going without it," he said.

"It's the rules of the game. It's not something I can change."

It may take government regulation to force companies to do better.

The Federal Trade Commission is urging Web browser makers to build "Do Not Track" tools to let consumers stop advertisers from studying their online activity in order to target pitches. The Commerce Department has called on Congress to adopt ground rules for companies that collect consumer data online for marketing. Several lawmakers have introduced privacy bills.

"For many companies, it's easier and cheaper to deal with the repercussions of a data breach that's already occurred, rather than taking steps to prevent it," said Ioana Rusu, regulatory counsel for Consumers Union, publisher of Consumer Reports. "Companies need to be held accountable so they protect your data up front."

Information that distinguishes one faceless Internet surfer from another is so valuable that companies have been hurt when they limit what they collect.

Yahoo Inc., for example, will soon keep logs on people's searches for 18 months, the same amount of time as Google Inc. That's a reversal of its vow in late 2008 to strip out personally identifiable details after 90 days. In making an industry-leading privacy pledge, Yahoo said it became less competitive in offering personalized services enabled by long-term tracking.

Companies also face lawsuits and penalties by promising more than they can deliver. If companies are vague, their biggest risk is bad publicity when a hacking attack or a technical error exposes customers' information.

"The lack of meaningful liability for breaches reduces the incentive for making sure that they don't happen," said Susan Grant, director of consumer protection for the Consumer Federation of America.

Businesses only have to be as good as their competitors. They know customers have nowhere else to go as long as everyone sets the bar low.

"Choice becomes meaningless in this context," said Ashkan Soltani, a security researcher.

The number of records exposed in [data breaches](#) is staggering - more than half a billion in the past six years, according to the Privacy Rights Clearinghouse.

At the same time, people are sharing more online. More than half a billion people are on Facebook, and billions of people search Google and Yahoo each month and accept tracking data files known as cookies. The Pew Internet & American Life Project found that 61 percent of adult Internet users in the U.S. have used social networks, up from less than a third in 2008.

When they aren't sharing on social networks, they are leaving their marks with online gaming services, shopping sites and retail loyalty programs.

The dependence on technology explains why the reputations of technology companies are remarkably resilient, even after embarrassing breaches.

For example, hackers last year uncovered a security hole on AT&T Inc.'s website and exposed the email addresses of more than 100,000 iPad owners who had signed up for AT&T's wireless Internet service. At that point, Apple had sold more than 2 million iPads. Despite the breach, the

company sold some 17 million more iPads since then.

Smartphones have added a new dimension to the debate about online privacy because they also record their owners' location.

Apple CEO Steve Jobs emerged Thursday from medical leave to try to quash a controversy over secret recordings of location information by iPhones. Apple denied directly tracking people, but said it is building a database of known Wi-Fi hot spots and cell towers to improve location-based services. Google Inc.'s Android phones do something similar.

To quiet privacy critics, Apple is changing the iPhone's software to keep data for a week instead of indefinitely. Google says its phones only store data for a short time.

Apple's disclosure came a day after Sony Corp. said a hacker may have stolen [credit card numbers](#) and other valuable information on the 77 million players using its PlayStation online gaming network. That would make it one of the biggest known credit card breaches.

A few weeks ago, a little-known company behind the email campaigns of Chase, Best Buy, Hilton, Walgreens and other big brands revealed that potentially millions of names and email addresses of consumers were stolen. Epsilon sends more than 40 billion emails a year on behalf of those brands for services such as customer loyalty programs.

Other big attacks included some 130 million card numbers stolen from payment processor Heartland Payment Systems in 2008 and as many as 100 million accounts lifted in a break-in at TJX Cos. in 2005 and 2006. Many smaller ones go unpublicized.

Consumers are at a disadvantage because companies often leave their privacy policies intentionally vague, yet lengthy with legalese.

In any case, few people bother to read them at all. Carnegie Mellon University researchers found it would take the average person 40 minutes per day to read through all the privacy policies that person encounters online.

"Sadly, the consumer can do absolutely nothing to protect themselves," said Bruce Schneier, a prominent security blogger and chief security technology officer at the British telecommunications operator BT. "When you give your data to someone else, you are forced to trust them."

If you say no, he said, "that'll mean living in a cave in the woods."

©2011 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Customers stay despite high-profile data breaches (2011, May 1) retrieved 2 May 2024 from <https://phys.org/news/2011-05-customers-high-profile-breaches.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--