NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2009/061109-how-facebook-and-twitter-are.html

How Facebook and Twitter Are Changing Data Privacy Rules

By Michael Fitzgerald , CIO , 06/11/2009

CIOs think about privacy the way some people think about
exercise: with a sigh and a sense of impending pain. Outside
of regulated industries like health care--where patient
privacy is paramount--privacy affects CIOs as a corollary of
security when, say, a laptop holding millions of people's
records is lost or hackers siphon off customer data.

"CIOs generally don't care about privacy," says Peter Milla,
former CIO and chief privacy officer at Survey Sampling
International (SSI). Milla says most CIOs either focus on
technology, or regard privacy as outside their domain, the
province of a chief privacy or chief security officer. He
finds both attitudes wrongheaded. CIOs, Milla says, should
"want to be ahead of the curve" on privacy.

The reasons, Milla adds, will become more obvious as
business goes increasingly digital. Web 2.0 applications connect like Legos, creating opportunities for companies
to gather incredible amounts of data. On social networks and blogs, people post vast amounts of information
about themselves. Marketers, meanwhile, are developing ever-better tools to exploit information about what
individuals do online. Companies routinely unlock sensitive data for business partners. As businesses enter into
cloud computing, they will give custody of their data to service providers. These trends create the potential for
unprecedented insight into people's behavior and open new ways to do business. But they also create challenging
questions about privacy, questions for which the answers are unclear.

To read more on this topic, see Privacy Is Your Business **and** Sears Settles Online Tracking Complaint From
FTC

Milla says he recently worked to modify a request from a big-box retailer who wanted information about the
people surveyed by his company on their behalf. "They were bewildered and frustrated that we wouldn't give it
to them," says Milla. The retailer already collects plenty of data on its customers and didn't see what the problem
was with a bit more. But Milla saw a breach of privacy, a contractual violation. If it leaked out that SSI shared
personal data about its panelists, it could devastate its business.

Milla says the big-box retailer's attitude is endemic. Companies think the data they gather belongs to them. Not

true, he says, but is he right?

The very question might strike CIOs as strange. Ten years ago, then-Sun Microsystems CEO Scott McNealy told us, "You have zero privacy anyway. Get over it." Since then, we collectively got in touch with our inner exhibitionist. People talk about their antidepressants on Facebook or post videos of themselves violating work policies on YouTube (two Domino's workers were fired for such a stunt). Teenagers are sending naked or semi-clad pictures of themselves over their cell phones.

But people also ask for photos or videos to be removed from social networking sites, says Deirdre Mulligan, a lawyer and former law professor who is now assistant professor at the University of California at Berkeley School of Information. Individuals and communities have balked at the way Google Maps' Street View exposes location information. Meanwhile, a 2008 Harris Interactive poll found that 60 percent of Americans were uneasy about having Web content customized for them based on their usage patterns.

Maybe privacy isn't dead. In fact, says Michael Blum, a partner at Fenwick & West and chair of the firm's privacy and information security practice, privacy should trigger all sorts of alarms for CIOs who must protect trade secrets, prevent security breaches or clean up after incidents that lead to bad public relations, lawsuits and expensive records repairs. It won't be long, Blum says, before some company has to deal with employees harassing each other in public via Facebook. Welcome to privacy 3.0.

Beacon of Trouble

Facebook and other social media sites are on the front line of the privacy wars. And because of their size-- Facebook has more than 200 million users--what these sites do with user data will influence what consumers expect from other companies. The early lessons from Facebook show that consumers increasingly expect to control their data. Tens of thousands of Facebook users revolted against its Beacon application, a targeted advertising tool that broadcast what they were buying by posting "stories" about it on their status feeds. There were plenty of Facebook users who wanted to know what their friends were buying. But there were also plenty who didn't want that information public (one poor fellow bought a very nice ring as a surprise for his wife, who subsequently saw it on his Facebook page and asked him who it was for).

There is a lawsuit unfolding against Facebook and some of its major advertisers for the privacy breach. Separately, Viacom went after Google's logs as part of its billion-dollar lawsuit against the search giant's YouTube unit, earning Viacom lots of bad publicity even though it said it wanted the log data anonymized. After California's Proposition 8 failed, angry gay rights advocates mashed up Google Maps with a public donations database and revealed home addresses for people who contributed money to defeat it. Some of those people were targeted by activists, raising questions about whether small donations should be made public.

In the wake of its privacy faux pas with Beacon, Facebook has moved to asking its users their opinions on its privacy policies. It has also created more ways for its users to control who sees their data. To Fenwick's CTO, Matt Kesner, this creates an expectation about control over data that will ripple through the IT world.

You may disagree with Kesner that this is a problem, particularly if your company doesn't maintain sensitive information in its logs or doesn't run a social network. Alissa Cooper, chief computer scientist at the Center for Democracy and Technology, says that's misreading the tea leaves. "The more we have incidents like these, the more it's going to reveal that each of them isn't a one-off," she says.

One ongoing privacy controversy involves Webwise, a behavioral advertising technology from Phorm, a London-based startup. Webwise uses "deep packet inspection," which lets it see the content of Web traffic so that it may better track consumer Web behavior and create profiles that let it serve up more targeted ads (NebuAd is another company that uses similar technology). Phorm claims it uses technology to anonymize the data it gathers, helping protect individual privacy. Several British Internet service providers say they would use Webwise to serve up ads more effectively. But at least one antivirus firm has suggested that Phorm's profiling technology is akin to spyware.

Meanwhile, one of the British ISPs, BT, acknowledged piloting the program using actual consumer data, without asking for permission. That has landed BT in hot water. The European Commission has initiated legal action against the United Kingdom over its refusal to stop companies like BT from using live customer data without permission. Meanwhile, Amazon and Wikimedia have said they will block Phorm from accessing traffic on their sites, and in late April, the U.S. Congress began holding hearings on deep-packet inspection.

Fenwick's Kesner thinks it's up to CIOs to help their companies understand what this Web 2.0 world means for data control. As a first step, he thinks more CIOs should establish a social media presence. It's essential, he believes, for IT leaders to understand how these tools work and how people use them.

CIOs, then, may not decide on their own what their companies do with customer data, but they will have to weigh in on--and support--whatever decisions business leaders make. That includes any technologies that companies deploy to mine customer information as well as protect it from unauthorized use.

Loss of Control

But it's not only your customers who want to control data about themselves. Social media is blurring employees' personal information with business information, which presents a challenge for corporate privacy policies. Companies can't ban employees from using Facebook and Twitter. In many cases, notes Kesner, even though these are technically not work-related sites, they are increasingly critical for engaging with clients and customers. Yet companies want to be able to control information about themselves.

Fenwick has found, for example, that potential clients expect to be able to check out its attorneys on Facebook rather than in traditional sources like the Martindale-Hubbell Law Directory. "If there are pictures of a CEO at a beer bash 20 years ago, it really does change things," says Kesner. "Our job as CIOs is to educate people about how what they're doing today can be searched across the world today or tomorrow."

Furthermore, CIOs face the specter of routine business records leaking out. "We've had whole mergers done via instant messaging," Kesner says. He worries that it's a short step from using corporate instant messaging tools to mistakenly sharing proprietary corporate data on a service like Twitter.

One solution to protecting corporate data may be to broadly adopt encryption technology for e-mail correspondence and other important business data. Encryption won't stop employees from "tweeting" inside information (as New York Times reporters recently did after a staff meeting concerning ideas for charging for online content). But it can give companies legal cover in case of a privacy breach, Kesner notes. Such controls may be much more important now that social media makes it possible to quickly spread information to large groups of people--information that potentially lives online forever.

Then there's cloud computing. While companies may save money and gain efficiency by shifting to cloud environments, they also lose physical control over their data. For example, says the CDT's Cooper, putting data in the cloud makes it much easier for the government to get access to it. "If I have my personal diary, they would need a search warrant to get it in my house," says Al Gidari, chair of the privacy and security practice at the Seattle law firm Perkins Coie. "If it's on Google Docs, they can get it with a subpoena."

Complicating this scenario, however, is a potential upside to the cloud. Kesner's colleague Blum says cloud computing could reduce corporate exposure for maintaining data privacy by shifting that responsibility to the vendors. "It can be a way for CIOs to offload risk," says Blum.

Alex "Sandy" Pentland, an MIT professor and cofounder of Sense Networks, which uses location data to find business trends, argues that in the future, most companies will not gather data directly from customers the way they do now. Instead, they'll access it from the cloud via aggregators who operate much in the way banks do, delivering data to companies only when authorized by individuals. Early examples of this model include Google Health and Microsoft Health--data banks operated by Google and Microsoft, respectively, through which patients can share only such healthcare data they are comfortable disclosing. They can also share different kinds

of data with different healthcare professionals.

Much Ado About Nothing?

The contradictions, understandably, make some CIOs skeptical that privacy needs to be an overarching concern. "It's not a nightmare situation," says Gerard McCartney, vice president of information technology and CIO at Purdue University. Not that he ignores privacy--the university spends half a day during orientations discussing privacy and security issues with incoming students. But McCartney thinks most people can and do manage their own privacy fairly well through common sense.

But here again, there are multiple points of view. There are questions, for instance, about how far common sense goes in the online world. "There is a sense of anonymity for people when they sit in front of a computer screen that I don't fully understand," says Leon Goldman, chief compliance and privacy officer at Beth Israel Deaconess Medical Center. "They say things to a computer they wouldn't to a real person."

Gidari, with Perkins Coie, says our values about privacy may be changing: "I wonder whether we are 10 years behind in our views of privacy, and this next generation may not be much concerned about the things this generation is screaming about." He points to behavioral ad targeting, which the U.S. Federal Trade Commission and especially the European Union are attempting to regulate. It's "a joke to kids," who expect targeted advertising, he observes.

Jim M. Swartz, CIO at Sybase, says privacy worries aren't keeping him awake right now. He notes, however, that technology shifts can quickly rewrite the rules for CIOs. More mobile workforces, for instance, create challenges and situations "that we wouldn't even have thought about five or six years ago," he says. For instance, it's easier for people to download attachments on their handheld devices, making it much harder for companies to control where sensitive data goes.

Swartz also notes potential challenges emerging from the way individuals and organizations share information. It's easier than ever to pull together disparate bits of information, develop opinions about it and present those opinions publicly. "Maybe you've lost three jobs, or filed for bankruptcy or have a DUI. Do the pieces of information available about you on the Web over a period of time tell a story you would rather not have told?" he muses. "It could be a concern. We won't know how big of a concern it is until there is a benchmark incident of some sort."

Pressure from Consumers

If such an incident occurs--a privacy breach that causes a public backlash against companies--what might happen?

Privacy experts believe that under the Obama administration, public pressure could push policymakers to take the side of consumers and demand more controls on companies. As a candidate, President Obama posted a position statement on his website that included a promise to strengthen consumer privacy protections. "That's what consumers are really worried about," says Milla, the former SSI CIO.

Milla fears that a major privacy incident could spark Congress to slap together an onerous regulation and race it through, a la Sarbanes-Oxley.

Remember ChoicePoint? The company collects and sells consumer data, and in late 2004, it had to reveal that it had sold such data to an identity-theft ring. One of the first big data breaches, the thefts sparked calls for a national identity theft law. ChoicePoint paid tens of millions of dollars in legal settlements and fines. Rep. Rick Boucher (D-Va.), chairman of the House Subcommittee on Communications, Networks and Consumer Privacy (who convened the April hearings on behavioral advertising), says he will introduce legislation in the fall that would strengthen privacy protection. But such legislation has gone nowhere in the past.

The Obama administration could go back to the privacy activism of the Clinton Administration's FTC, worries Jim Harper, director of information policy studies at the Cato Institute in Washington, D.C. Under Robert Pitofsky, the Clinton FTC pushed for a uniform regulatory regime for privacy. Harper thinks today's policymakers should take their cues from consumers, and especially from the dialogue between Google, Facebook and their users.

From a regulatory perspective, therefore, privacy and data control questions are by and large open. In fact, right now German courts are considering whether an IP address is personally identifiable information that needs to be protected. No matter what the court decides, Milla thinks companies will eventually find that consumers do think their IP address is akin to their Social Security number. That will at the least force many companies to rethink their marketing strategies.

Whether or not legal prescriptions for privacy change, the cultural shift toward consumer control of personal data seems to be gaining steam. At the World Economic Forum earlier this year, MIT's Pentland called for a "New Deal for Data." He wants companies to acknowledge the power of consumers by acknowledging:

* Consumers have the right to possess their own data.

* Consumers can control the use of that data.

* Consumers can dispose of or distribute that data as they choose.

He says a number of companies have expressed support for his principles, which he argues really aren't that different from the way financial institutions handle data already. Ultimately, companies need to decide whether the data they manage is their data or not.

"The 'privacy is dead' thing is just clearly wrong," says Pentland. "Yes, different people have different attitudes about privacy. But the part they care about is control. They're willing to put something up on Facebook but they want to control who sees it."

The ultimate privacy question for CIOs, then, is what it means for their companies to cede that control.

Michael Fitzgerald is a freelance writer based in Massachusetts.