Extending the Principles to the Internet: A Way to Restore Trust

By Julie Gable, CRM, CDIA, FAI

Almost from its inception, the Internet has spawned thorny, complex issues that are not easily resolved. Matters such as online piracy of copyrighted material, theft of trade secrets, cybersecurity, and trans-border data transfer issues constantly confront governments, Internet service providers, businesses, individuals, and watchdog groups.

In recent weeks, the balance of personal privacy and the need for national security have been the subject of high-profile news coverage. With revelations about the U.S. National Security Administration's (NSA) electronic surveillance program called PRISM, the parallels of data mining for marketing purposes and for surveillance purposes came into sharp focus.

Technology has given us the ability to store vast amounts of data cheaply. Now, with highly sophisticated data analytics tools, it is possible to exploit stored personal data not only for more effective marketing, but also for more effective detection of potential security threats.

The key difference is that while users freely give personal information to social media sites, e-mail services, marketers, and other Internet presences, they don't necessarily suspect that this personal data can then be handed over to federal investigators. That's because many people don't realize that the background architecture for storing such data is the cloud.

A Battle in the Cloud

According to *The State of Cloud Storage 2013 Industry Report* from storage vendor Nasuni, cloud storage providers put more than one exabyte of information – that's more than 1 billion gigabytes – under contract in the previous year.

With surprising revelations about how large providers such as Amazon, Microsoft, and Google, have responded to federal warrants has come a public outcry. According to reports in *The New York Times*, some providers have had teams of in-house experts charged with finding ways to cooperate with the NSA, a strategy aimed to keep the information-mining process under the company's control rather than the federal agency's control.

Cloud service providers – and the companies that use them via Internet connections to provide flexible processing for transactions, communications, and storage – have suffered huge reputational damage. Internationally, some countries have exploited the NSA revelations to maintain that those who fear their communications are being intercepted should not use services that go through American servers.

In short, an atmosphere of deep mistrust has arisen that could prove damaging and costly to cloud service providers as well as to any entity that collects customer information in business-to-business or business-to-consumer transactions.

Principles Show Way Forward

Into this maelstrom steps Michael Geist, J.S.D., who believes that issues associated with cybermistrust are going to put pressure points on the Generally Accepted Recordkeeping Principles® (Principles) and extend them in ways

that people may not have been thinking about up to now.

Evaluating Service Providers

In addition to using the Principles to measure the effectiveness of in-house records programs, organizations may come to use them as a means to judge the information management maturity of their service providers. Going further, Geist believes the Principles and the Information Governance Maturity Model (Maturity Model) may also provide a template for devising solutions to restore trust.

Geist believes that companies offering cloud-based services – whether e-mail, social media, voice over Internet protocol, applications, or storage – will face some hard times in the wake of the U.S. surveillance scandals. Recent surveys have shown that U.S. cloud providers could lose as much as 20% of the international market for these services over the next three years.

Why? "Public trust is crucial for service providers," says Geist. "The providers were functioning in the hope that there wouldn't be a Snowden," he says, referring to NSA contract worker Edward Snowden, who leaked classified information about NSA surveillance activities.

Records and information managers will recognize this mind-set as similar to the one that believed (or wished) that electronic discovery would never be part of litigation and that a gentleman's agreement that implied "if you don't ask for our electronic records, we won't ask for yours" would prevail.

"Google's 'don't be evil' mantra is increasingly hard to reconcile," Geist contends, when, "as a service provider organization, it becomes difficult to promise your customer that their data isn't being disclosed to agencies that are actually collecting it with your knowledge and permission."

Michael Geist, J.S.D.: A Career Overview

Michael Geist, J.S.D., is a law professor at the University of Ottawa, where he holds the Canada Research Chair in Internet and E-commerce Law. He earned his doctorate in the science of law degree from Columbia Law School in New York.

Geist is an internationally syndicated columnist on technology law issues, has edited two books on Canadian copyright law, is the editor of several monthly technology law publications, and is the author of a popular blog on Internet and intellectual property law issues.

He serves on boards for CANARIE, the Canadian Legal Information Institute, the Privacy Commissioner of Canada, the Electronic Frontier Foundation, and the Open Society Institute. He has received numerous awards and recognition for his work in the areas of intellectual freedom, policy leadership, and public leadership.

Geist warns that "once the NSA has the information, the line up of other agencies that want to use it runs right out the door. Drug enforcement, copyright infringement, and other uses suddenly appear. The highest level national security purposes become a slippery slope of something far different."

Restoring Trust

According to Geist, the biggest collectors of personal information in the private sector are scrutinized by non-governmental organizations (NGOs) who bring citizen concerns to governments, advocate and monitor policies, and encourage political participation through provision of information.

One example is the Electronic Frontier Foundation. While NGOs may be the guardians of individual legal rights in a digital world, these watchdogs may not have the tools needed to measure good stewardship of information.

Principles to Apply

Geist offers, "It is useful to begin looking at what is important from the perspective of ARMA's Principles for recordkeeping performance and to see how Amazon, Google, Microsoft and other providers could be judged in terms of information governance maturity."

Transparency

The Principle of Transparency will be essential to restoring trust. According to Geist, "It will no longer be enough for these providers to say 'here's what we do,' but rather, 'here is what we have done.' Policies might include requiring a warrant for surveillance or law enforcement requests, telling users about government requests for data, publishing guidelines for law enforcement, and being ready to stand up and fight for their customers' privacy rights."

Geist is a proponent of transparency reports that disclose requests for user data and tell how the company has complied with these requests. "Up to now," he says, "most transparency has been about the processes involved with complying with data requests rather than with the actual actions themselves."

Geist believes that transparency reports foster public confidence in service providers. Steps will also

likely have to be taken to demonstrate that the provider functions at a transformational level of transparency, including a continuous improvement program to ensure that transparency is maintained over time.

referred to at level five of the Maturity Model, the idea that retention is perceived holistically and is applied to all information in the organization, not just to official records. Will consumers have the right to request that their data

"Businesses that are regulated and have a high priority on information security are under threat if they move to the cloud," Geist says.

Accountability

Accountability is another key element that has sometimes been lacking, particularly where the provider's stated goals related to accountability have not been met. "Greater oversight is a start," says Geist. "Many people think that accountability is not what it should be, particularly when elected officials are not told the truth. This means that NGOs – people invested in watching the watchers – are not able to do so."

Greater accountability would likely have to be at the board level to have a truly transformational effect. The Principles recommend a chief records or information governance officer who reports at the senior management level.

Retention

"Retention is another issue that is interesting," notes Geist. "The ongoing ping-ponging of 'how long a retention period is enough' will get new momentum. The longer data is kept, the more susceptible it is to breaches or to government requests."

This is the aspect of retention

is not kept very long? Will it be possible to actually comply with this request? The answers remain to be seen.

Protection

Protection for records and information that are private, confidential, privileged, or secret, of course, is a huge concern. While general businesses can have legal frameworks built on the privacy of their own systems, moving to the cloud provides another source of access with lower safeguards.

"Businesses that are regulated and have a high priority on information security are under threat if they move to the cloud," Geist says. "Cloud-based models are based on public confidence in the level of security in the cloud vs. the level of security on network servers. With the new revelations, cloud providers just can't make those claims anymore."

Clearly, there is much work to be done.

The Need to Collaborate

"Within normal businesses, the answer to security varies by

the type of business, the data collected, and the context in which it is used," says Geist. "National governments must insure that the Internet functions the way its users expect, and many countries work together on how to do this."

As a global phenomenon, the Internet transcends geographic borders but is not necessarily free of political or cultural restrictions. Following the scandals, some have questioned whether the US-led Internet Corporation for Assigned Names and Numbers, more often referred to as ICANN, should continue as the governing model for the Internet. A year ago, there was debate on whether a government-led, United Nations-style model that would include countries such as Russia and China should have control.

No doubt the line between national security and Internet freedom will continue to be debated. In a post-9/11 world, the emphasis has been on security rather than on privacy.

But Geist believes that the pendulum may swing back after Snowden, with Amazon, Google, and Microsoft becoming far more vocal and trying to build on public concern for more privacy.

Meanwhile, proposed laws, such as the U.S. Cyber Intelligence Sharing and Protection Act (CISPA), seek to allow more sharing of Internet traffic information between the U.S. government and technology companies.

How service companies deal with issues of balancing cybersecurity and Internet freedom going forward will be key. Geist contends that they will do best by confronting the issues and using the Principles to guide information governance policies. **END**

Julie Gable, CRM, CDIA, FAI, can be contacted at juliegable@verizon.net. *See her bio on page 47.*