

'Privacy paradox' poses problems for marketers

WHILE CONSUMERS BECOME MORE WARY OF COMPANIES COLLECTING THEIR PRIVATE INFORMATION, THEY ARE HAPPIER THAN EVER TO SHARE IT ONLINE.

JENNIFER BARRETT, GLOBAL PRIVACY OFFICER FOR ACXION, EXPLORES THE PRIVACY PARADOX.

Every day we are surrounded by technology that collects data about who we are and what we do. As marketers who are privy to more and more of this data, we need our customers to respect us as worthy custodians of that knowledge. It is in our own best interests to maintain that trust if we intend to continue to conduct business.

Companies of all sizes use powerful tools to capture, search, link and analyse data as it becomes consistently more affordable. Marketers are eager for more granular



The less people think about privacy, the more they lower their guard.

behavioural intelligence to better target their messages. Unfortunately, the risks to consumers are often not considered carefully. If they can do it and make a profit, some companies will. Though the majority of organisations may operate reputedly, one bad experience can create an aura of surveillance for the consumer that negatively impacts their confidence in the online space.

Ever more sophisticated mobile devices can now furnish user location information. This is a new type of data over which some concern regarding appropriate usage is being generated. Some say the consumer should be offered the choice of how the data is treated, but consumers may not understand what they are signing up for or refusing.

Consumers themselves now have access to inexpensive remote storage and processing, migrating email, pictures, video and documents from their personal computer to third party servers. Sometimes referred to as *cloud computing*, this trend, while offering great flexibility, also puts personal

data further outside the control of individuals who may not understand the inherent risks. In addition, the choices individuals are given about how to protect our data get more complex and unintelligible every day.

As we accept and adapt to these new technologies, altering what we do, what we say, and with whom we share information, the behaviour of our government agencies and businesses evolves accordingly. Governments embrace the same technologies and processes as other businesses, collecting more and more data, mining it extensively and sharing it with other agencies, often in the name of greater security. In the UK for example, a national network of roadside cameras will be able to read license plates, enabling officers to reconstruct journeys of motorists for investigations ranging from counter-terrorism to low-level crime.

Wobbly privacy on the web

Given this, and general anxiety concerning behavioural scrutiny in the private sector, it is ironic how much personal data is often volunteered by individuals.

While we all claim to care about our privacy, we reveal embarrassing moments on Facebook and other social networking sites, provide our credit card details freely on the internet or over the phone, and purchase those devices that track our activities, such as GPS navigators and mobile phones. In such cases, rules are not always in place to properly protect it. Researchers have labeled this the *privacy paradox*, where normally rational people do totally inconsistent things when it comes to the information they provide.

George Loewenstein, a Carnegie Mellon behavioral economist, conducted a research study and found that, "our privacy principles are wobbly. We are more or less likely to open up depending on who is asking, how they ask and in what context."

But you might be surprised at what



While we all claim to care about our privacy, we reveal embarrassing moments on Facebook and other social networking sites...

caused people to open up.

In one of Loewenstein's experiments, a group of students was given strong assurances that none of the information they divulged would be revealed. Though one might speculate that this would make them more comfortable and open, the opposite was true. When given a strong assurance of confidentiality, 25 percent of the students admitted to having copied someone else's homework. When given no assurance of confidentiality, more than 50 percent admitted to copying. Assurances raise "issues of privacy that might not otherwise figure prominently in people's minds." In other words, the less people think about privacy, the more they lower their guard.

In another experiment, students were asked to complete a survey on an official university website about whether they had engaged in certain disreputable acts. Another set of students were given the same questions, but on an informal-looking site with a graphic of a smiling devil and the headline *How BAD are U??* People completing the survey on this site were significantly more likely to admit to illicit behaviours. Creating an informal online atmosphere seems to encourage more personal self-revelation, even though the environment poses more potential privacy problems than a professional site.

Loewenstein concludes that "the cues that we rely on through culture and evolution to tell us there is a privacy issue are not present on the internet." Meanwhile, "the same technology magnifies the risk."

Legislators play catch-up

In times past, information flowed fairly inefficiently to a relatively small circle of people. Today, information about one individual is created and shared with other parties by another, often without the knowledge of the individual. This can create problems with an individual's privacy, confidentiality and reputation.

Legal frameworks encompassing consumer and data protection laws tend to be dated and ill-equipped to respond to either new technology or our changed behaviour. Most are grounded in principles that go back to the '70s and '80s and just don't work in today's reality. While there is a growing acknowledgement of this problem, no new model exists to fix our current regimes.

"Technology will outpace in its capacity the imagination of even the most clever law makers." Justice Michael Kirby

The concept of consumer consent is all we have to educate consumers and offer a level of control over how personal information is used. With technologies that don't necessarily lend themselves to notices, such as cookies, it is very difficult for consumers to make informed choices. This problem compounds as we move more of our online activity to our mobile devices.

The definitions of personal information versus anonymous information blur when technology allows information to be linked in ways not anticipated when the data was originally collected. With the legislation that protects and regulates the transfer of data between entities and across borders in flux, compliance nightmares are created when data moves or is viewed between multiple jurisdictions. Yet such transfers have become an integral part of the global economy.

Justice Michael Kirby, the Australian judge and chair of the group that drafted the OECD Privacy Guidelines said in *Four Parables and a Reflection on Regulating the Net* (2008), "technology will outpace in its capacity the imagination of even the most clever law makers."

Self-regulation is central

What does the future hold? If we are to succeed we should market with integrity and greater transparency. Second, by feverishly working on stronger self-regulation and conducting ourselves with integrity, we are less likely to find ourselves struggling within the confines of limiting legislation handed down by policy makers in the future. Granted, it may not be easy to move from where we are—being under tremendous pressures to simply make the quarter—to marketing with integrity... but doing the right thing will bring its own long-term rewards.

Like it or not, marketing has become increasingly regulated. Email and mobile messaging must follow the guidelines of the Spam Act, and telemarketing conform to the preferences recorded in the Do Not Call Register.

Most of the laws governing marketing have been enacted in the last five years, and we should expect more. The duration between consumer objections and the passing of legislation continues to shorten, but while policy makers concern themselves with how businesses handle data, companies expect more return on their marketing dollar than ever before.


As new technologies facilitate data collection and introduce new methods by which to employ it in marketing and advertising, we will see aggressive use of both. Eventually the right boundaries will be set, probably by trial and error. But today the adage *just because I can* doesn't mean you should. Not stopping to think about what you should do could make you tomorrow's headline.

I know what you clicked last summer...

The issue of how behavioural information should be used in online marketing is very important. Whether the tracked behaviour is the sites you visit, the keywords you search on, the content and attachments of your email, or the geographic location of your mobile phone, we can collect very granular information, act on it almost immediately and save it over long periods of time.

In the United States there have been calls for firms involved with behavioural targeting to impose self-regulatory guidelines on providing clear and concise notice about data collection. Regulators and lawmakers are expected to draft legislation this year.

Behavioural information is not new; marketers have inferred an interest in cooking or golf from a subscription to a certain magazine for years. However, today we are able to track very specific and detailed activities. We must tread carefully and conduct ourselves with integrity, particularly when dealing with sensitive behavioural issues involving finances, health or children.

What makes privacy challenging is that it is an abstraction...right up until your identity is stolen or your behaviour exploited. 

Jennifer Barrett is responsible for oversight of Acxiom Corporation's global public policy, privacy and information practices.