Keeping Consumers Safe, Secure, and Satisfied

BY THOMAS HAIRE

As consumers continue to expand their technological literacy thanks to what seems like constant innovation — smart phones and their associated app technologies, the burgeoning Internet of Things (IoT), and more — they seem to have two options to maintain their privacy while taking advantage of these advances: become voracious readers of "terms and conditions" or remain ignorant to those sometimes lengthy documents and hope that the companies they do business with are doing their best to serve their privacy needs.

As a consumer, neither option feels that enticing, which means that marketers' jobs become that much more difficult. Industry associations, private attorneys, and state and federal regulators are in constant flux regarding how consumer privacy and data security are best respected and protected. At the same time, marketers have become enthralled by the expanding scope of data available to use in their efforts.

"Big data availability introduces a key managerial challenge: data is exceptionally distracting to marketing departments," says Doug Garnett, founder and CEO of Portland, Ore.-based Atomic Direct. "I've seen teams lose their power chasing ghosts in the data — ghosts without profit potential. Quite often, they get lost in the microscopic details that are unimportant to your business needs … we must remember the vast expanses of business truth that will never show in the data."

Read on to find out what Garnett and other members of the *Response* Advisory Board have to say about the power of big data, the challenge of data security, and the privacy that consumers desire even more than the technologies they enjoy.

In January, the Federal Trade Commission (FTC) held its annual PrivacyCon event, touching on many issues in consumer privacy and data security. What are the greatest risks facing marketers in these areas?

Tony Besasie, Cannella Media: Safeguarding data from hackers. With more personally identifiable information (PII) comes more responsibility and higher liability. In 2013, 40 million credit card numbers were stolen from the Target Corp. database, a company that invests millions of dollars annually in information technology (IT) security. That resulted in more than 90 lawsuits, $61 million in disaster recovery, $10 million in claim settlements, damaged brand equity — and the CEO was sacked. Like any criminal, hackers prey on the vulnerable and unprotected.

Peter Feinstein, Higher Power Media: As marketers, the greatest risks are facing our own profit motives and ever-present human greed. These two motivations are tightly related and can, if not vigilantly disarmed, forever sabotage our relationships with our clients and partners in the media. Our industry is based on mutual trust; if we violate that trust just to make a buck, we endanger our industry's reputation, put our companies at risk, and make consumers susceptible to the myriad dangers associated with securing data and maintaining their rights to privacy. We have to live above the battle and coach our clients to use data wisely, instead of purely for monetary gain.

Doug Garnett, Atomic Direct: The serious risk is that we can't control the risks. Generally, in business, risks are quantifiable and plans can be made to control them. But in

Members of the *Response* Advisory Board take on some of the questions swirling around consumer privacy and data security.

this case, it's not a question of whether you'll have a problem, but when — and how big.

It's more complicated in that there is a wide range of liabilities for a data or privacy breach. In many cases, it's reasonable and manageable. However, there's always a potential for the risk to be far bigger than your company can manage. It is impossible to achieve perfect privacy controls. So two keys for any company's success are: finding that place with the most protection but at a cost that is achievable; and having a reasonable plan in the event of breach.

Kevin Lyons, Opportunity Media: When consumer personal data is breached, the consequences for a marketer can be markedly sharp — in image and in revenue. Recent examples — such as Target, Home Depot, Yahoo, and MAPCO — demonstrate the vulnerability of marketers. The exact cost of those occurrences will be felt longer term.

How can marketers best utilize the growing trove of data to better target consumers while also staying on the right side of expanding consumer privacy laws?

Peter Koeppel, Koeppel Direct: Transparency is the key; that is, the consumer understanding exactly how their information is going to be used versus having those details buried in some fine print that nobody understands. Consumers will trade some measure of privacy for relevancy as long as it does not feel overtly Orwellian to them. But the balance of trust is clearly a fragile line.

Fern Lee, THOR Associates: Marketers can best use the data on cross-device retargeting. Although privacy has become an issue, the opportunity to capture the consumer journey — specifically and strategically — has arrived. The key is defining what the "right side of expanding consumer privacy laws" actually means. It goes without saying that cross-device usage is a hacker's dream come true. Consumers are ignorant about the opportunities made available for identify theft and malware.

What is interesting is that the FTC has asked that "sensitive" data (financial, health, children's information) be given greater protection. Taken into the context of lead-generation marketing, the 800-pound gorilla that begs for attention is in the execution of retargeting and contacting consumers that "ask" for follow up.

Richard Stacey, Northern Response Intl. Ltd.: The age of big data is a new opportunity for marketers to reach their target audiences more efficiently and effectively. There are many ways to use this myriad of data depending on the objectives of the marketer. In addition to better audience targeting, the increasing availability of data allows marketers to test faster and more cost effectively — and then scale faster and more cost efficiently.

Garnett: A good friend of mine observed that the core problem with big data is that the mass of data that holds no meaning very quickly overwhelms those tiny areas of data that hold important meaning. We are facing this problem today — especially with the range of data being collected. It's important to remember, too, that this data has a highly significant weakness: it records only behavior. The risk with behavioral data is that while it says "what" someone did, it holds no evidence of "why" they did it. Without the "why," it leads to mis-spent marketing money.

How can marketers best align their product development, IT, and marketing teams to maximize both the effectiveness of marketing messages and the security of customer data?

Besasie: There are plenty of articles that say that a company's chief marketing officer (CMO) and its chief information officer (CIO)/chief technology officer (CTO) should be best of friends. I agree with this. Collaboration needs to start at the top.

Koeppel: There are three ways that come to mind. The first is to give the people what they want. We have more information about consumer behavior than at any other time and that behavior should help guide us. The second thing is to align offerings with the behaviors and values that consumers are already exhibiting. After all, marketers now have to meet the consumer at a time and place of the consumer's choosing. The third thing is to respect the rule of law, and that begins by having a clear understanding of it. Today's marketing landscape is ever changing, therefore consumer behaviors and the laws surrounding them are going to have to respond to those changes.

Stacey: Many firms are moving to a team-based organization from functional silos, as product development, marketing, sales, and IT now have to work more closely together. The other important change involves the consumer using data as a tool for dialog.

Consumer consent mechanisms can help ease the strain for marketers trying to walk the proper privacy line. What consumer consent mechanisms have you seen that have been most effective, and why?

Feinstein: Without naming names, the best consumer consent mechanism I've seen comes from a wearable device company. It's grown from a one-product wonder to six different devices, with a seventh readying for launch. The company's approach to consumer consent is to be in-your-face when you install its app, and it offers periodic reminders, and options to opt-in or out, based on certain milestones of activity, distance, sleep, or even your device's battery level. Instead of being product-centric, the company is consumer-centric. Instead of operating from fear, it brings privacy and data out of the shadows and puts it front and center, where it gives users clarity and ease of choice.

Lee: It's not only about consent. The privacy issue will be questioned because of tracking and shared information. It is the responsibility of the marketer to create policies of best practices and to adhere to the FTC barometer. That being said, with the changes in our political climate, there may be more leeway and less regulation with this new administration.

Lyons: Nielsen has an app you can download to your phone, where you consent to its data collection, providing the user with an incentive of up to $50 per year to do so. That is a good example of an effective consent and collection mechanism.

With security breaches and hacking making more headlines, what are the most effective data security measures that marketers and their agencies/vendors are using to ensure the safety of customer data?

Koeppel: With high-profile hacks — from Target to the Democratic National Committee — making big news, it's obvious that no individual or institution is invulnerable to this sort of sabotage. Given how this sort of problem is escalating, it's clear that security is a moving target and — with apologies to Mr. Popeil — there is no "set it and forget it." As some data security experts advise, it's "lather, rinse, and repeat."

Lee: The bigger issue is the truthfulness of what is being presented as news online. Aside from security breaches and hacking, as a marketer it is alarming how gullible and impressionable the consumer has become. It's just as important to educate the consumer on what is true, and how to fact check information, as it is to install measures to combat data hacking and breaches.

The key is not only for the marketer to ensure customer data safety but also consumers should update passwords, keep software up to date, and make sure Wi-Fi networks are protected. Where banks and financial institutions have addressed this issue and adhered to protection of consumer data, retail establishments, hospitals, and e-commerce sites need to step up their game.

Lyons: There is no silver bullet solution here, in terms of 100-percent protection against data breaches, as the tools hackers use evolve quickly. However, essential tools that marketers and their agencies must use to fight against this risk include sound IT infrastructure, continuous monitoring, and employee education on security measures. ■

For the complete and unabridged answers to these questions from our Advisory Board, find the March issue online now at *www.responsemagazine.com.*