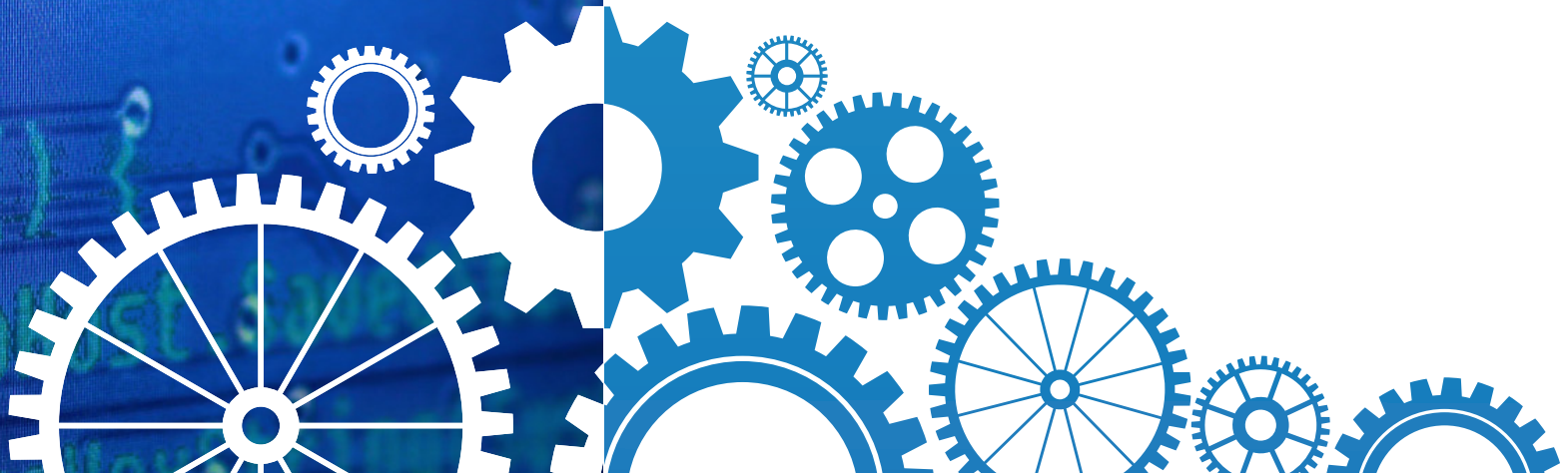


eBook

Watching the Watchmen: Earning and Keeping Your Customers' Trust in the Age of Big Data





Introduction

Are you doing enough to protect your customers' personal data? More importantly, do your customers think you're doing enough to protect the data with which they entrust you? Those are the two questions on which we want to focus this discussion.

The inherent difficulties of digital security and online privacy protection tend to hinder effective implementation. Some brands do only what they think they need to do for CYA purposes, while others do only what they feel they can afford and hope for the best. That said, however, other brands and companies adopt a nonchalant, even cavalier attitude toward data protection and their customers' sense of privacy, dismissing the risks of a breach or negative public sentiment. Our argument is that all these brands and companies take these varied attitudes at their own peril. Consumers are becoming increasingly conscious of online security, digital privacy, and corporate data practices. Brands that are aware of this and position themselves accordingly by becoming their customers' data advocates will distinguish themselves from their competitors and win their customers' loyalty and trust.

To answer the question to which our title alludes, "Who Watches the Watchmen?," increasingly that answer is everyone. While this is certainly true of the Millennial generation, who have grown up online and never lived in a world without online security and privacy concerns, these concerns are not isolated to them. As more of the world's population gets connected to the Internet, more of our lives and business are conducted online, and more of the objects on our persons and in our environments send and receive data, the natural result is increasing mindfulness of digital security on everyone's part. With every new day in the age of Big Data, more of your audience is watching you watching them, and their worries about their data and expectations for how you handle their data are increasing. Let's talk about those worries and expectations and what we can do to address them.



Attitudes Toward Retailers' Use of Personal Data According to Digital Shoppers Worldwide, June 2014

% of respondents

Would like to be able to opt in and opt out from messages and offers from retailers



Trust my favorite retailers to use my personal data responsibly and for my benefit



Don't mind if my behavior in store is observed



Clear about the privacy policies of the retailers I interact with



Currently provided with clear notice, choice and control of how my personal data is collected, used and shared by retailers



Don't mind when a retailer uses my social media data



■ Agree ■ Neutral ■ Disagree ■ Don't know

Note: based on a 6-point scale where 1=strongly disagree, 5=strongly agree and 0=don't know; among those who have used digital channels and/or devices at least once in the shopping process in the past 3 months; numbers may not add up to 100% due to rounding
Source: Capgemini, "Digital Shopper Relevancy Report 2014" conducted by ORC International; eMarketer calculations, Sep 25, 2014

180313

www.eMarketer.com

Changes that Internet Users in Select Countries Have Made as a Result of Data Breaches at Major Retailers, Sep 2014

% of respondents

	UK	India	US	Australia
Changed one or more online passwords/PIN codes	55%	47%	45%	45%
Shopped less frequently at one or more of the retailers that experienced a breach	14%	29%	28%	10%
Started using cash more often than credit cards when shopping	14%	34%	23%	10%
Made fewer mobile purchases (e.g., via laptop, smartphone, tablet)	13%	33%	15%	15%
Made fewer online purchases (e.g., via desktop)	11%	31%	13%	12%
Other	1%	-	3%	2%
Haven't changed shopping behavior as a result of a data breach	32%	12%	30%	36%

Note: in the past year
Source: ISACA, "IT Risk/Reward Barometer" conducted by M/A/R/C Research, Nov 12, 2014

182312

www.eMarketer.com

Overview: The State of Affairs

If you were to listen to the news, you'd have to think there's a cybercrime wave under way and Big Brother is listening to every word we say. Every week seems to bring word of another major data breach, more revelations on how our privacy is being violated, and growing realization that the veneer of security around our online lives is thin and fragile. While reports of governmental privacy and security violations like those revealed by NSA leaker Edward Snowden grip the imagination with their similarities to *Nineteen Eighty-four*, the security and privacy lapses by companies and other private interests are drawing just as much scrutiny and have much greater impact on consumers' everyday lives. We've reached a point that, when brands and marketers think about our online audiences, we have to assume that everyone has personally been affected by data insecurity and/or knows someone who has. It is no longer the exception; concern over data security and privacy is the new normal.

Every year, the nonprofit Identity Theft Resource Center publishes its compiled statistics for data breaches for the past 12 months, and the picture painted in its 2014 report is not a pretty one. Along with the corporations whose breaches made headlines like Home Depot, Michael's, JP Morgan, and Sony, the ITRC reported nearly 800 significant data breaches last year, with a breach defined as a security failure resulting in data records containing personally identifiable information (PII) being exposed and put at risk. Those near-800 breaches, according to the ITRC, represent more than 85 million consumer data records being exposed. 2015 is already even worse, with the ITRC reporting 577 breaches exposing 156 million records as of September 29.¹

Given all these failures to secure consumers' information, it's not very surprising that many people have a lukewarm attitude toward companies handling their PII. In a recent eMarketer study, only half of respondents said they trusted retailers to use their data responsibly. Further, in a different eMarketer study, nearly 30% of respondents said they were shopping less frequently at retailers at which data breaches were reported. This means the damage inflicted by a breach can go far beyond the immediate exposure of customer PII and short-term financial losses. Once lost, your customers' trust can be difficult to regain, taking a toll on your brand's reputation and revenue for years to come.



PII and 5 Ways It Can Be Breached

PII, or personally identifiable information, is data that we use every day to peruse the Internet. It can include: first and last name, home address, email address, phone number, social security number & credit card info. This wealth of information can lead to big gains for anyone looking to resell this data. Here are five common methods used to trick you into giving up your PII:

1. Phishing – This common scheme attempts to trick a user by sending him or her a fake email newsletter to convince them to open and click on a link or create a user account on a fake website whose sole purpose is to steal the user's data. If you did not sign up for that email, then don't open it. Quarantine it to your junk mail and report it to your ISP.

2. Dumpster Diving – The push to recycle has created opportunities for thieves to hang out around homes and office buildings to get their hands on potentially sensitive material. A good shredder or trusted document destruction service should be included in the cost of doing business in today's security environment. Also, don't forget to secure the recycling of your IT hardware. Thoroughly research local computer hardware disposal and recycling services, and choose a reputable company that will make sure all your data is destroyed.

3. Skimming – We use our credit and debit cards every day, often trusting those swiping machines with little to no scrutiny. Let the buyer beware because this is a very easy way to steal your financial information.

4. Social Networks – This is a dead giveaway because we love to give away free content to these platforms - a *lot* of free content. Any malicious user could spend copious amounts of time styling and profiling other user's accounts/pages. All it takes is the first/last name of the newly wedded couple, their public wedding album, a search for them under public records, and voila! You have their home address and may know their possessions from the public thank-you messages sent out from their gift registry.

5. Friends & Family – “We're here having dinner @ 7:30pm. Tomorrow, we're jumping on a plane and will be gone for a week. We'll be sure to post lots of pictures!”

Does this sound familiar? That's because we've all done it. Let's try to save the most intimate of moments for our closest friends and families and not broadcast for the whole Internet to see. Settings => Privacy => Edit. Check!

Data, Data Everywhere...

It's easy to say that companies need to get their act together and secure their customers' data, but it's much harder to put into rigorous practice. Data security is hard for a number of reasons. It's a permanently defensive endeavor, it's easily seen as a burdensome cost rather than a profitable benefit, and it's extremely difficult for laypeople to understand. However, the main reason securing Big Data is hard is the “Big” part. The more data there is and the more it connects to other data, the harder it is to secure and the greater the chance of your data becoming “leaky,” putting your customers' privacy at risk.

Over the past 30 years, the Big Data world in which we now live can be seen as emerging in three waves. Each wave not only greatly expanded the role data plays in our lives, but also brought its own set of security and privacy problems:

- The first wave was the advent of the Web and eCommerce themselves, which marked the beginning of the Big Data era. Though large companies obviously had kept digital records of customer data for decades before (and security failures could and did occur), the Web both vastly increased the data stores of the big players already online and enabled smaller enterprises to get in on the action. Where it once took major companies and large data brokers to build and manipulate large sets of consumer data, the Web allows that data to be gathered and re-sold by small businesses or even individuals.
- The second wave came with the ubiquity of smartphones and their continual connection to the Internet, allowing both a greater volume and greater variety of data to be added to the mining mix. The greater volume is a natural result of being online more of the time, and the greater variety results from the galaxy of new applications that can all generate app-specific data for integrated analysis. A simple example of this is how the data from fitness apps, diet tracker apps, and your food purchasing history can be correlated to create a broad health profile for healthcare providers and insurance companies, as well as health-focused food and CPG brands. Dr. Iltifat Husain discusses some of the privacy implications of data collection by health apps in a post on the iMedicalApps blog.²



- The emerging third wave is being brought about by the combined effect of (1) the Internet of Things and (2) wearable computing. Taking the impetus of data and the Internet to its logical conclusion, every aspect of our persons and every object in our daily lives is now a potential information point; continually sending and receiving data, continually updating and expanding the global data environment. An added dimension of Big Data's third wave is the ubiquity and effectiveness of powerful algorithms to automatically score, categorize and rank target consumers based on their accumulated data and the algorithms' comparisons with other consumers' data. This algorithm-generated scoring data is an important part of the Big Data cloud in its own right. It is used to identify and target consumers as well as bundled and re-sold to other data brokers.

Obviously, the spread of information technology in general and Big Data specifically has brought enormous benefits. It is nonetheless foolish to lose sight of the problems inherent with the spread of these technologies, especially for brands and marketers who are reliant on the trust and goodwill of our customers and audiences. These problems will only get bigger as the data gets bigger. Indeed, one might be inclined to look at this and say, "More data, more problems."

We've understood and been dealing with the problems arising from the first wave of Big Data (breaches, fraud, malware) for over two decades now and have adjusted our online lives accordingly (no clicking links in strange email, no using "password" for our passwords, etc.). The discussion will now turn to the more recent issues surrounding the latter two waves and especially the emerging third. It is these nascent issues that will be gaining more attention as Big Data gets bigger, offering brands the best opportunities to distinguish themselves to their customers.



Case Studies: Big Data and Its Discontents

To take the temperature of our audience and get a good sense of their feelings about emerging data security and privacy issues, we'll take a look at two specific cases in the recent past to show how sensitive the public is to these issues. We'll then review two recent popular publications that both articulate current sentiment and even further heighten the issue of data security and privacy in the public consciousness. Taken together, these books and controversial cases show us what's at stake when we handle our customers' sensitive personal data.

1 The Case of the Facebook Emotional Experiment

Last summer, the Web was quite vocal on its feelings on the “emotional contagion through social networks” experiment conducted by Facebook. To briefly recap the issue, Facebook has experimentally demonstrated (with results published in the Proceedings of the National Academy of Sciences) the ability to shift the emotional states of its users by changing the emotions expressed in the posts seen in their News Feeds.³ The experiment's test subjects were active Facebook users who had their News Feeds filtered based on the broad emotional state being measured (“positive” or “negative”) without any acknowledgment from Facebook. The “positive” or “negative” emotional quality of these users' own posts were then measured and logged by Facebook – again, without these users' awareness or consent.


Several media outlets were quick to condemn Facebook and government investigations both here and in Europe were opened to examine the issue.⁴ *Slate.com*'s reporting details the questions of research ethics raised, especially those of informed consent.⁵ Facebook's position was that it had consent; the published results in PNAS state that the experiment “was consistent with Facebook's Data Use Policy, to which all users agree prior to creating an account on Facebook, constituting informed consent for this research.”⁶ Said Data Use Policy states that Facebook uses its (our) information “for internal operations, including troubleshooting, data analysis, **testing, research** and service improvement” (emphasis added).

In contrast to the many naysayers, Farhad Manjoo in *The New York Times* defended Facebook in the name of testing and research, pointing out how “(m)ost web companies perform



My Facebook
made me sad





extensive experiments on users for product testing and other business purposes.”⁷ Manjoo further warned against a possible chilling effect the anti-Facebook backlash might have on social science and marketing research in the future. Along similar lines, Kate Kaye in Ad Age reality-checked those denouncing Facebook, citing both the ubiquity of this kind of testing in the online marketplace and the outdatedness of “traditional standards for obtaining consent” that “may not transfer well...to research involving data gathered on thousands of people online”.⁸

2 The Case of OKCupid

The discussion on the ubiquity of user testing fueled by the Facebook debate set things up nicely for OkCupid’s revelations that it manipulated its users’ compatibility reports without their knowledge as part of its own experiment.⁹ As the broader media dialogue on the Facebook experiment indicated (and as digital marketers have long known), these are perennial issues of the online world. Facebook’s and OkCupid’s actions are nothing new, but are merely casting light on well-established practices and opening them up to public debate.

What made the OkCupid case interesting as the next phase of this debate is how it chose to defend its actions. In the days following the initial story, OkCupid’s president Christian Rudder made the media rounds, giving interviews and presenting their defense, as summarized in a post on OkCupid’s company blog.¹⁰ The gist is:

- The purpose of the experiment was to gauge the effectiveness of OkCupid’s compatibility system, and without such behind-the-scenes tests they have no real idea how effective it really is or isn’t.
- Their experiment really isn’t a big deal because such testing is so commonplace in the online world. Rudder’s choice of words speaks volumes:

(G)uess what, everybody: if you use the Internet, you’re the subject of hundreds of experiments at any given time, on every site. That’s how websites work.

Rudder’s tone is markedly different than Facebook’s conciliatory non-apology, indicating that he’s comfortable with the curtain being fully pulled back and the public knowing how these practices really work.¹¹ One must imagine Rudder was betting the disclosure of this experiment

would be greeted with indifference or perhaps draw out those with similar views on data privacy who might be interested in buying his book, which happened to be published a few weeks after this story broke.¹²

3 Critique: Bruce Schneier's *Data and Goliath*


Right at the start of *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, Bruce Schneier¹³ goes to the heart of our current dilemma regarding Big Data by asking us to look at our phones:

(E)very morning when you put your cell phone in your pocket, you're making an implicit bargain with the carrier: "I want to make and receive mobile calls; in exchange, I allow this company to know where I am at all times." The bargain isn't specified in any contract, but it's inherent in how the service works.

Schneier's description of the nature of this "implicit bargain" (specifically, how it seems balanced against individual citizens/consumers in favor of governmental and corporate interests) takes up the bulk of the book. Even leaving aside the chapters where Schneier deals exclusively with government surveillance and focusing solely on his description of corporate data practices, it makes for sad reading. His account is disheartening both from the perspective of an everyday person and as a digital marketer, with many of the industry's most questionable practices spelled out in detail. From apps transmitting data from our phones without our knowledge or consent (which the app developers then re-sell), to shady data brokers using data correlation to de-anonymize PII, Schneier paints a grim picture of "the Stalker economy" brought into being by Big Data. However, rather than "Big Surveillance" (as Schneier calls it) being a monolithic single entity, he likens it to being "less Big Brother, and more hundreds of tattletale little brothers," as the new generation of information middlemen stake claims on their customers' data.

Many of Schneier's recommendations to companies and individuals to address the security and privacy problems posed by Big Data are sensible (though admittedly with added cost to brands and marketers), such as improving encryption, giving customers access to their data, and only collecting the minimum amount of data required for effective customer service. However, some of Schneier's other recommended remedies are extreme, to say the least. They run the





gamut from making vendors liable for data breaches in the same way polluters are liable for the cost of environmental cleanup, to sweeping policy changes like classifying companies who maintain large stores of consumer data as “information fiduciaries” subject to “special legal restrictions and protections”, to the outright illegal like vandalizing security cameras and destroying surveillance databases.

While perhaps some of these recommendations should be taken with a grain of salt, they do represent the pervasive public sentiment around digital privacy and security issues. In terms of customer trust in a brand and subsequently that brand’s long-term health, it compounds the harm done by a security or privacy breach when the breached company treats the cost bore by its customers as an externality. Both Schneier’s diagnosis and prescription for this problem hit the main nerve of the difficulties both companies and consumers face in the age of Big Data. Those of us who care about our customers and our brands’ long-term relationships with them would be wise to take Schneier’s analysis to heart.

4 Critique: Brian Krebs’ *Spam Nation*

As riveting as stories about the creeping influence companies have over their customers via their data, the big-name data breaches, and the Snowden NSA revelations are, the far greater threat to online security is much more pervasive while seemingly having a far less dramatic impact. Indeed, this threat has become so commonplace that we now almost ignore it, considering it part of the cost of being online at all: spam email.

Those annoying emails in your Junk Mail folder are the subject of Brian Krebs’ book *Spam Nation: The Inside Story of Organized Cybercrime - from Global Epidemic to Your Front Door*. In this book, Krebs identifies spam as “the primary impetus for the development of malicious software,” and describes in detail the interrelated networks of malware developers, spammers, and the shady businesses that utilize them. Krebs’ coverage of the dark underbelly of our email and online commerce is both detailed and broad and isn’t confined to just the organized crime organizations running the show. It ranges from describing the motivations of those who buy medicines advertised via spam to the rogue pharmaceutical companies who manufacture the drugs themselves (often ignoring safety protocols) to the “antis”: the anti-spam organizations

who track and try to block the spam-generating botnets, putting them at the front line of the struggle to keep our online commerce safe and secure. As Krebs points out, these very same botnets that were originally created for spam can (and are) also used for other nefarious purposes such as click fraud, malware delivery, dedicated denial-of-service (DDoS) attacks, and brute force attacks to gain access to systems and networks.¹⁴ In fact, one of the key spammers of Krebs' account, Pavel Vrublevsky, was convicted for using his botnet to run a DDoS attack against the Russian airline Aeroflot and its payment processor.

Far from being just a nuisance, the spam we regularly receive and immediately delete is the iceberg tip of a vast network of criminal enterprises - a long line of hacked PC's, malware developers, botnet administrators, and illicit payment processors that starts with organized crime and ends in your Junk Mail folder. What's more, this all starts from just one piece of PII: your email address.

Summary

You don't need to agree with Schneier's politics to see which way the wind is blowing. As stated earlier, the general public is already keenly aware of issues surrounding data security and privacy thanks to whistleblowers like Edward Snowden and numerous data breaches of ever-increasing scale and impact. It's also worth noting that Schneier is a long-established and respected expert in his field, and his book was a *New York Times* bestseller.¹⁵ Krebs' investigative analysis also shows the other kind of direct harm that can arise from poor security practice: the increased likelihood that your customers' data will wind up in the hand of criminals. Further, the reaction to Facebook's and OkCupid's utilizing their customer base as experiment subjects shows how sensitive the public can be to these issues even when there is no "real harm" done at all. A recent research poll conducted by On Device Research confirms this, showing that 2/3 of respondents say that it is important to know that a mobile app is collecting/sharing PII.¹⁶

Caring about who has access to your data and how they use it isn't just for crackpots with tin-foil hats. With everyone connected to the Internet in multiple ways all the time, everyone has skin in this game. If your customers don't feel like you respect them or their privacy, how likely are they to trust you and give you their business? The question then becomes how brands address their customers' growing concerns about their data practices.





Recommendations: Taking the Steps to Become Your Customers' Data Advocates

As public awareness and scrutiny mount over how companies treat their customers' data, the demand for a shift away from the status quo will only increase. Right now, businesses seem trapped in the cycle of hoping for the best, suffering a breach, cleaning up the mess, repeat. This not only means substantial losses for your company and your customers, but also a continuing loss of credibility and long-term trust.

This unacceptable status quo cannot continue. One way or the other, changes are coming for how companies are expected to treat consumer data. We're now going to discuss what those changes might look like and how brands can use this crisis as an opportunity. The key will be to face the impending changes not just as burdens or added costs but rather as a way to show your customers you have their best interests at heart.

Prepare for the Regulation of Big Data

As previously described, Bruce Schneier devotes a large portion of *Data and Goliath* to recommendations for various levels of society to address the inherent problems of the current Big Data regime, including advice for individuals, companies, and government. Many of these recommendations involve significant changes in public policy, presenting the possibility of significant new regulations on how companies collect and use consumer data. While no such overarching regulations have yet been introduced in the United States, the Federal Trade Commission has been looking into such changes, holding public workshops and publishing reports on the harm done to consumers by the current state of Big Data.¹⁷

The precedent for such changes has already been set in Europe, with the European Commission's unification of EU members' data protection laws into the umbrella General Data Protection Regulation (GDPR). Here's a summary of what GDPR imposes on companies who do business in the EU (from Lexology.com):¹⁸

- **Data Breach Notification:** All businesses are required to notify data protection authorities

Protecting Travelers' Data: An Opportunity to Build Trust with Our Customers

Cyrus Farivar's report last year in Ars Technica on the United States Customs and Border Protection's (CBP) retention of Passenger Name Record (PNR) data both raises concerns about how personal information is being collected and used and offers a glimpse at how the travel industry might address those concerns.²⁰

PNRs are created by airlines, cruise lines, and hotels when travel or lodging reservations are made and are routinely collected by CBP en masse. Farivar gained access to his collected PNRs through a Freedom of Information Act request to CBP and in the process learning that CBP had retained detailed information on him for several years after his original travel dates. The data collected included his mailing and email addresses, phone numbers, the IP addresses from which he'd made his reservations, and his full credit card numbers.

This might not be so concerning, due to the obvious national security interests in monitoring travel information, were it not for the fact that most airlines, hotel chains, and online travel agencies don't host their own PNR databases or handle the data transfers to CBP themselves. Instead, like many large companies, they outsource these tasks to undisclosed third-party firms whose security practices aren't available for scrutiny, leaving travelers' data vulnerable to hackers or other irresponsible individuals.

Compounding this risk is the fact that the United States, unlike Canada and the European Union, lacks both a general consumer privacy law and any sector-specific consumer privacy laws regarding travel information. In a joint letter to the U.S. Department of Transportation's Advisory Committee for Aviation Consumer Protection, a group of consumer and industry advocates urges the committee to take action to make traveler privacy and data protection a higher priority.

Response Media takes handling PII very seriously. We have many tools at our disposal to ensure that our customers' data are collected, processed, retained, and transmitted using the most secure methods available. Given the increasing concern with protecting digital privacy and security, there is an opportunity here for our partners in the travel industry to work with us to help make our customers' privacy an explicit concern and take open steps to protect it, even while we wait for the public sector to catch up. If we're asking our customers to trust us with their travel arrangements, it only makes sense that we be worthy of their trust regarding their data.

and data subjects in the event of a data breach. Notice of data breaches must be provided to the data protection authority "where feasible" within 24 hours, and to affected data subjects "without undue delay."

- **Consent:** Consent to use customers' data must be given explicitly and unambiguously.
- **Data Portability:** Individuals have a defined right of data portability, designed to facilitate an individual's access to personal data. This requires organizations to permit customers to move their data to new organizations offering similar products or services.
- **The "Right to be Forgotten":** Individuals also have the defined "right to be forgotten" allowing an individual to require an organization to delete personal data where there is no longer any legitimate reason for keeping it.
- **International Transfer of Data:** GDPR mandates that if EU citizen data is being collected and processed, then GDRP applies to that collection and processing regardless of where in the world the servers in question might be located. This is obviously of major concern to cloud providers
- **Data protection by design and by default:** GDPR requires data controllers to collect and retain personal data only to the minimum extent necessary in relation to the purposes for which they are intended by design to be processed.
- **Accountability and Data Protection Officers:** GDPR increases the accountability of data controllers and data processors, including by requiring that they carry out data protection impact assessments prior to risky data processing activities. Organizations with over 250 full time employees are required to have a Data Protection Officer.
- **Fines:** Data protection authorities will be allowed to impose fines of up to 2% of the worldwide gross revenue of an organization.

Touching back on the issue of spam email, another ominous precedent for the kind of regulation on the horizon for Big Data is last year's Canada Anti-Spam Law (CASL). On July 1st 2014 Canada passed strict new legislation limiting marketers that send electronic messages for commercial purposes, with the stated intent of protecting consumers and businesses. The purpose



of CASL is to provide privacy protection as the internet grows and mobile marketing expands in Canada. Businesses and marketers sending CEM will have to clearly state a recipient's opt-in and opt-out options, and the messaging will need to be crystal clear in its purpose.

Hefty fines can be a result of an organization not complying with CASL. Recently the Canadian Radio-television and Telecommunications Commission (CRTC) fined Quebec-based Compu-Finder \$1.1 million after finding it guilty of sending bulk mail to addresses without proper consent and failing to provide functioning unsubscribe links.¹⁹ Though the CASL is a Canadian law meant to protect Canadian citizens, companies and organizations worldwide that do business and transmit data in Canada are subject to it.

Both the new European and Canadian regulations show what is inevitably coming down the road for businesses in the United States. Let's talk now about what you can do to not be caught flat-footed and be a champion for your customers at the same time.

Getting Out In Front

In order to win the trust (and business) of those concerned about the security of their personal data, what can businesses do to better protect their customers? Here are the highlights from a recent eMarketer study:²⁰

- **Partner with a security expert:** By working with a third-party security vendor, businesses can focus on increasing sales and making sure their customers leave happy and feeling safe. Security vendors will manage and execute the most suitable tactics to ensure private information is protected.
- **Increase budget for security:** This year, \$4.1 billion was spent to keep hackers away from hundreds of U.S. companies, according to a PricewaterhouseCoopers survey of 758 American companies. That survey suggests the amount spent could increase by \$2 billion in 2017. A substantial investment should be spent on security advisers, expansion of a data security division, and studying the newest malware hacking methods to stay ahead of any possible incident that could occur.

Actions that US Small-Business Owners Are Taking to Protect Against Security Risks, by Business Size, May 2014

% of respondents in each group

	20-99 employees	10-19 employees	0-9 employees
Working with third-party vendor(s) to help with security	45%	45%	29%
Plan to increase budget for security this year	24%	22%	18%
Currently running employee security awareness education programs	23%	14%	15%
Breach preparedness plan	22%	15%	13%
Plan to decrease budget for security this year	6%	4%	4%
Not currently taking measures to protect against security threats	23%	28%	42%

Note: n=505

Source: CSID, "Small Business Security" conducted by Research Now, June 9, 2014

174650

www.eMarketer.com



- **Run employee security awareness education programs:** To guarantee employees maintain and protect important business data, lay a foundation for a data protection training program. The program will help teach employees new procedures for creating strong passwords and educate them on how to steer clear of scams like phishing, the attempt to acquire sensitive information such as usernames, passwords, and credit card details by directing users to enter details at a fake website whose look and feel are almost identical to the legitimate site. Employees should also be made aware of how to properly document any data breach that took place.
- **Follow good data practices:** Ensure that you have express consent for anyone from whom you collect and store data. Implied consent is a lower standard and can only be used for a limited period (as short as a number of months from a transaction). Collect and preserve proof of opt-ins/agreements, version terms, and agreements. Proof of opt-in should include a written or digital record including a timestamp and some linkage to the process the consumer used to opt-in. Provide clearly written privacy statements accessible from any communication you have with your customers.

How Response Media Can Help

Response Media's practices and processes are already privacy compliant with the requirements of GDPR and CASL. Here are our measures taken to minimize risk and protect consumer privacy.

- Our standard contract/agreement includes standard IAB terms and compliance with current regulations.
- Data and privacy agreements include affirmative consent standard (to which any third party who handles data must agree)
- Transactions sent through us are logged and recorded using independent front- and back-end auditing, including automated snapshot of every agreement.
- Clients that follow our tracking guidelines have an audit trail for each record.
- Vendors are required to complete self-assessment addressing compliance with these guidelines.



After the Breach

In today's technological environment, brands must face an unpleasant truth: the only reasonable attitude to take is that it's not a matter of if you get breached but when. As such, your response plan needs to include how you mitigate the damage to your brand's reputation and regain your customers' trust. Writing for Forbes.com, Kate Vinton stresses the importance of being visible and active in response to a breach, and most of all maintaining the appearance of having all the facts and having them straight, citing Target's seeming confusion and uncertainty after its 2013 breach as a cautionary example.²¹ David Gianatasio at AdWeek goes further, saying that "breached companies are often their own worst enemies" thanks to a reluctance to take preventative IT steps to stop breaches from happening and then responding in a haphazard fashion when they do.²² He points out that appearing to respond with certainty and capability after a breach can "keep the spin cycle in high gear and trip up companies even as they strive to be good corporate citizens."

It's not just making things right after a data breach that matters but also making things right in the right way. Be consistent and transparent when speaking with your customers about what happened, as well as confident and personal in your response, and you can help keep a data breach from tarnishing your brand.

A FINAL NOTE

If recent events have taught us anything, it's that data security and consumer privacy concerns are an inescapable part of doing business in the 21st century. Even if the rate and severity of data breaches don't get any worse (unlikely, to say the least), the horse is already out of the barn as far as public perception and government oversight are concerned. Further, security experts writing in the public space such as Schneier and Krebs are constantly making consumers more knowledgeable and aware of who has their data and how it's being bought, sold, and used. In such a business environment, a brand's trustworthiness is directly proportional to the care with which it treats its customers' data. Your customers want and need you to be on their side and will repay you many times over for it.



References

- 1 **2014:** http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf
- 2 **2015:** http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf
- 3 <http://www.imedicalapps.com/2014/08/health-apps-insurance-companies/>
- 4 <http://www.pnas.org/content/111/24/8788.full.pdf>
- 5 <http://www.theverge.com/2014/7/9/5885351/senator-asks-ftc-to-investigate-facebook-news-feed-experiment>
- 6 <http://bits.blogs.nytimes.com/2014/07/02/facebooks-secret-manipulation-of-user-emotions-under-british-inquiry/>
- 7 http://www.slate.com/articles/health_and_science/science/2014/06/facebook_unethical_experiment_it_made_news_feeds_happier_or_sadder_to_manipulate.html
- 8 https://www.facebook.com/full_data_use_policy
- 9 <http://www.nytimes.com/2014/07/03/technology/personaltech/the-bright-side-of-facebooks-social-experiments-on-users.html>
- 10 <http://adage.com/article/digital/academics-head-facebook-controversy-back-burner/294050/>
- 11 <http://www.nytimes.com/2014/07/29/technology/okcupid-publishes-findings-of-user-experiments.html>
- 12 <http://blog.okcupid.com/index.php/we-experiment-on-human-beings/>
- 13 <https://www.facebook.com/akramer/posts/10152987150867796>
- 14 <http://www.newyorker.com/magazine/2014/08/25/2710913>
- 15 <https://www.schneier.com/about.html>
- 16 <http://www.responsemedia.com/online-marketings-four-letter-word-has-five-letters/>
- 17 <http://www.nytimes.com/best-sellers-books/2015-03-29/hardcover-nonfiction/list.html>
- 18 <https://ondeviceresearch.com/>
- 19 <https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion>
- 20 https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf
- 21 http://ec.europa.eu/justice/data-protection/index_en.htm
- 22 <http://www.lexology.com/library/detail.aspx?g=a30f8645-11cb-4c5c-b945-48f6787940f5>
- 23 <https://nakedsecurity.sophos.com/2015/03/09/canadas-anti-spam-law-gets-first-success-with-1-1m-fine/>
- 24 <http://totalaccess.emarketer.com/Article.aspx?R=1011483> (login required)
- 25 <http://www.forbes.com/sites/katevinton/2014/07/01/how-companies-can-rebuild-trust-after-a-security-breach/>
- 26 <http://www.adweek.com/news/advertising-branding/retailers-are-finding-data-vulnerability-can-undo-years-brand-equity-156459>



Authors



Quentin Blasingame

Account Manager

Quentin's work at Response Media includes managing email marketing programs as well as front-end development for both emails and landing pages. He also manages Response Media's content marketing efforts and administrates the agency web site. Prior to joining Response Media, Quentin was part of a major publisher's digital ad operations team and has been part of web development teams for various corporations, universities, and government agencies in both the United States and Canada.



Kevin Lassiter

Account Supervisor

Kevin is responsible for executing campaign media plans and optimizing campaigns to help generate high volume in a cost-effective manner. He engages in the ongoing monitoring of campaign progress and results to find insights to aid with campaign optimization. Kevin also liaises with the Response Media tech team and recruitment developers to devise and implement campaign tracking methods.





Josh Perlstein

CEO

joshp@responsemedia.com

(770) 220-5086

3155 Medlock Bridge Rd.,

Atlanta, GA 30071

P: 770.451.5478

responsemedia.com

