
Honestly, I Want this Chapter to Be on Privacy, but If I Wrote It I'd Have to Blog About You

I got an e-mail in early 2009 from a good buddy of mine about an ad that showed up on Facebook that showed my profile picture and said, “Paul Greenberg is a friend of _____.” I’m leaving out the organization it referenced because I like them a lot and they aren’t the point here. I happened to be a member of a group on Facebook that supported them. But I didn’t give permission for my name to be used in an ad.

Also in early 2009, a friend of mine, Brent Leary, who you met in the small business e-chapter, put up a post on American Express Open Forum, a widely read business site/portal, called “Dale Carnegie Meets Barack Obama: Winning Friends and Influencing People in a Web 2.0 World.” Within a few weeks, a public relations firm called LaForce+Stevens plagiarized Brent’s article by changing a *very* few words and then repackaging it as a “pitch” to clients—without a single word of attribution to Brent.

What does all this mean? Are we facing a menace that can’t be stopped? Will Miss Manners prevail? What can be done about these violations of our privacy and our intellectual property?

The answer to this mystery is forthcoming, Holmes.

Privacy? What Is It About the Word “Social” You Don’t Understand?

Expecting privacy while participating in a social network is like expecting The One Above to help you win an Oscar or game seven of the World Series. The reality is that if you are filling out a personal profile as part of

your membership on a social network, the likelihood that part or all of it will be exposed in some way is pretty reasonable. This is a *social* network, which (as we saw in print edition Chapter 10) is designed to reproduce a representation of your actual life in a digital or cyber fashion. That means that you walking down the street wearing the clothes you wear (metaphorically of course) will make a fashion and style statement to both those you're friends with and to strangers or let's say, those who are loosely coupled with you. In other words, what you show about yourself publicly will affect what others think about you, regardless of what they know about you. That's how a social network works too. It's really no different. You're more likely to tell your trusted friends more about yourself than most strangers, unless it's a stranger you reveal intimacies with because you'll never see them again (I'm providing you with a delicate version of a one-night stand).

Where it differs markedly from a benign, noncommercial location is that most social networks are not noncommercial. They are a business. They are not there to provide you with a watering hole or "scene" or "neighborhood" for nothing. They want to monetize what they are doing and their assets are those very same profiles that you provide them.

If they are social networks associated with a particular company, they use the profiles of their customers to gain further insight into their customers—so they have an indirect benefit. But, for the purposes of privacy, they have a rightful expectation that they have access to that profile for their purposes. They also, depending on the terms and conditions you've agreed to, have a rightful expectation of exposure of that profile to someone beyond those you've chosen to expose it to.

That's outrageous, isn't it? Gets you furious or at least piqued, doesn't it? Aha! Gotcha!

For a few minutes you forgot that the reason you're reading this book, most likely, is that you are looking into contemporary customer models for your business. Meaning, you have your business casual clothes on (no one wears a suit anymore) and it's your business that you read this for. Yet you were mad about the violation of your privacy. Well, remember that feeling when you develop your business's social network or community. Especially if you have the intention of mining the data or exposing the profile of one or many of your members. You'll know how they're likely to feel.

But let's dig deeper into this privacy issue, because it affects more august institutions and directly affects—or not—how we spend.

Dealing with Identity Theft: We Kept on Spending

For good reason, we are increasingly worried about identity theft. We read stories about Lexis-Nexis and 310,000 stolen Social Security numbers or Bank of America “losing” 1.2 million customer records. The annual updates we get from companies on their privacy policies aren't really much of a comfort for those fears of stolen data, are they? Truthfully, do you even read them? I don't. What I expect of a company is that if I deal with them, I can trust them to protect whatever information I gave them in return for something they gave me. And that goes to the crux of the matter. Customer data privacy isn't really the concern of the population as much as trust in dealing with it is.

With all the concerns about privacy and its breaches you read of in the media, that hasn't stopped the 21st century customer from being forthcoming with enough personal information for someone else to establish a new identity complete with photos from what is publicly available online—and made public by the customer themselves. In fact, these neo-customers from Gen X and Y are surprisingly relaxed about providing tons of data well beyond the transactional and are also quite lax about its public exposure—as long as they are in control of the decisions for the exposure and feel that they can trust the institution they gave it to. Institutional trust is the primary concern of customers, not privacy per se. Even though there have been dozens of high profile customer data breaches and fear of being individually victimized by identity theft is running near 66 percent according to the 2009 annual Unisys security index, it doesn't stop customers from purchasing things with their credit cards online—at least didn't pre-recession—because they trust the means to do so. 2009 has seen (up to September) nearly \$132 billion spent online for retail sales—not exactly an indication of fear of cyber-theft as a whole. The overall level of “in the Internet and our business partners we trust” remains pretty high.

But it is a fragile high. The Ponemon Institute, what I consider the world's best privacy management firm, did a significant study released in June 2008 on the “Most Trusted Retail Banks.” They came to some very significant conclusions. First, it takes two breaches of privacy at a banking institution to destroy trust and lose the customer. Second, that 71 percent of the customers believe that the bank will protect their

customer data and privacy and will inform them should there be a breach. Only 19 percent weren't sure that their bank would. The study found that immediate response to a breach is important via phone or written notice (less electronically, oddly enough). They trust their banks to protect their information, but 85 percent would transfer to another bank if they didn't. So what kind of conclusions can we draw from all this? Privacy, while a significant issue, is actually less of an issue when it comes to 21st century customer/company relationships. The real issue is trust in the handling of that data, not the fear of its revelation. Most customers are willing to give the data if they can trust the institution they give it to. That is the true distinction between a meaningful privacy policy and a privacy policy that people will ignore or gloss over.

That said, expectations of privacy when it comes to everything ranging from traditional business transactions and the associated data to contemporary social networking business and mores, becomes a lot more complicated than it seems to be. A little later, we'll get into the rules that members of a social network and community need to expect and the rules that the community owners need to abide by.

Expecting Trust? Now THAT, You Should Be

What should you as a business and as a customer expect, if privacy is as elusive as it might seem to be? An expectation of trust from your customers is not unreasonable, even in the world of the community/social network. This means acting with integrity in how the assets that the customer provides you with—more often than not, information in a profile or transactional data—are handled with concern for the customer's well-being.

Yet that is often not the case, despite the obvious "Shoot, of course, we'll be that way" implied in how the assets should be used. Sometimes trust isn't so easy to gain from customers, when your business objectives conflict with that expectation of trust.

The continuous missteps of Facebook are an instructive example of what not to do to your customers.

Facebook and Profiles: Trust vs. Privacy

I think Facebook is valuable to me as a businessperson and, honestly, is just outright cool. It's an incredibly useful and easy way to communicate

with CRM and other business professionals, stay up with my nieces and nephews, and act immature with people of all ages. I can play, flirt, check out moods, look at photos, and do all the things that social networks are there for from a personal standpoint. I get nearly instantaneous response to Facebook messages—sometimes within minutes from business scions—that would take days in e-mail. In fact, only IM chats with business colleagues may be faster and that is when mutually connected. I don't need to do that in Facebook. My friends are paying attention to what's going on with their online buds.

I find it valuable for crowdsourcing (as I do LinkedIn, which may even be more valuable to me with the Ask a Question feature) and for developing and participating in groups that are of real interest. The groups can be esoteric or they can be of exceptional importance. But they are there for the picking. I can play with applications that involve everything from updating my calendar to exposing (with my delighted permission) my love for specific music or the Yankees or to revealing my likes and dislikes and political proclivity. I can take IQ tests designed by people who failed real ones. I have access to thousands of applications and can choose to use whichever I want and provide them to whomever I've befriended—who then can choose to accept or reject the request to join.

In return, I understand that my profile, when it's set to public, will be used by the application for whatever benefit that my personal details have for them. That's a risk I *choose* to take by setting my profile to public. I expect that the profile will be exposed to some degree. I also recognize that as a member, I have no inherent right to be one, and there is an expectation that my membership requires something in return to the social network *business* that is providing me with the tools that I'm using, including the location. That costs them money and requires value from me.

But Facebook's lack of business acumen or at least experience showed up continually in the period from 2005 to 2009, from the time they opened up Facebook to more than just college students, and particularly after they made the one great move of their business existence beyond its creation—the creation of their application programming interface and toolkits to provide to developers. They provided a Facebook platform that allowed developers to write applications that could potentially be profitable in some way.

But despite these very smart moves, the Facebook equation of “profiles + advertising = massive revenue jump” just might include a

new element “minus lots of Facebook members” if they miss the fundamental reason why Facebook and social networks in general have been the phenomenon they are—and continue to keep screwing up in the very vital area of trust and customer control.

I want to be clear on something before I go on and rant away—there is nothing wrong with Facebook exposing its members to advertising (without their individual permissions) when it comes to viewing ads. Facebook is a business that needs to generate revenue, social network for play or not. Advertising is probably going to be the core revenue generation engine for it. Facebook’s assets are its members. So you advertise to the assets. That’s part of the deal that a member signs up for in the two-way street. This isn’t a nonprofit.

But Facebook repeated its mistakes, using the members in the ads without their permission, as Jay Z and Tim McGraw articulated in 2002 “over and over again” (fans of Bill Murray and *Groundhog Day* take note). In 2009, Facebook had a near revolt on its hands with its terms of service trust violations, after having done the same thing several times over.

The Beacon Light Goes Out, Turns On, Goes Out Again, Turns On Again

The Beacon controversy of 2006 is where Facebook started to falter. At the time, they had no business model to speak of. Charitable folks would say that a sense of some urgency bordering on panic set in and they decided that advertising was the way to go. Early on this seemed to be justified (and still is to a large extent) with the 2007 Microsoft \$240 million investment, inflating the Facebook valuation to \$15 billion—making them even more panic-stricken—though Microsoft got an exclusive advertising partnership out of the deal.

But there were other factors that Facebook either was blindly not cognizant of or blithely ignoring. Foremost, their members trusted them. They thought that the information they gave freely to Facebook was treated pretty similarly to Las Vegas: “What happens on Facebook, stays on Facebook.”

Ain’t so, Joe.

For example, in a study done in October 2005 by Ralph Gross and Alessandro Acquisti of Carnegie Mellon Institute on “Information Revelation and Privacy in Online Social Networks,” they found that Facebook members (who were then primarily college students) chose

to reveal enormous amounts of personal information, such as their home addresses, IP addresses, data related to their personal relationships, including partner data, political preferences, hobbies, music, books, movies, you name it. At the time of the study, this data was available to any member of Facebook, most of whom were strangers to the other members. (Controls on who can see what data granularly are now in place. They learned the lessons of failure.) Even so, 50 percent of the member-respondents worried more about the data being seen by someone they actually knew who wasn't on Facebook, than those on Facebook. In virtual (but not actual) anonymity there was trust. Be intimate about the details of your life with the nameless faceless (not Facebookless) stranger.

In 2005, Facebook's privacy policy stated that they were allowed to continue to collect personal data from other non-Facebook sources, such as Instant Messenger conversations and newspapers, "regardless of use of the website." Additionally, they could use that data to supplement the personal profiles of the members and to give it to Facebook service providers. But because of the rather naïve trust the Facebook members had in Facebook, this incredibly fast and loose privacy policy was simply "not believed" by 60 to 85 percent of the respondents, according to the Carnegie Mellon survey. They chose to believe what they wanted based on their innate trust in Facebook, their cyber-home and digital hearth.

Beacon changed that.

For those of you who don't know what Beacon was, it was a partnership arrangement that consisted of 44 companies (including Overstock.com, eBay, Travelocity, and Blockbuster) who were "enabled" to use a specific cookie that Facebook provided to publicly expose, *without member permission*, the purchases of Facebook members logged into Facebook. Not just without their permission, but oftentimes without even the knowledge they'd been exposed with their name as purchaser, the item purchased, and even who it was bought for if that was part of the equation.

What made Beacon particularly onerous is that this wasn't opt-in, it was opt-out, meaning that if you bought anything from the 44 merchants, you were exposed unless you chose to not be exposed. So your fate as a customer was in the hands of the company you purchased from, not exactly the 21st century model for creation of advocates or even the cementing of loyal customers.

The outcry was, as you could expect, huge. Fifty thousand people signed a Facebook petition to stop exposing these particular “stories” (Facebook cutely included them in the routine exposure of activity that goes on without fanfare or complaint) without permission. The Center for Digital Democracy and the U.S. Public Interest Research Group asked the Federal Trade Commission to investigate whether Facebook and MySpace, who also had plans to do this, were using deceptive practices to violate privacy.

The result? Facebook caved, at least seemingly, and added a feature that required opting in to this public exposure, transaction by transaction—an awkward step forward in reducing the clamor and fixing the mistake. There was no universal shut-off of this and similar practices until 2009 after another outburst. But with Beacon, you were subjected to the inconvenience of having to respond to each transaction to protect your privacy.

After Beacon There Was . . .

Unfortunately, things didn’t stop there and the violation of trust continued, though not always associated with the issues of privacy. Facebook screw-ups became so commonplace that we wouldn’t just see newspaper (digital or print) headlines all the time—*way* too ordinary an occurrence—but also ongoing discussions inside of social networks and forums like, “Hey dude, Facebook f---ed up again, ja hear?” “NO WAY!” “Way.”

Or this text message:

U hr Fbk f-ed up? K. TTUL.

It was that frequent.

Even after the Beacon fiasco, they seemed to have not learned anything. In February 2008, an op-ed appeared in the *Washington Post* by staffer Catherine Rampell called “What Facebook Knows that You Don’t.” The piece highlighted the coverage of another major trust snafu by Facebook that went something like this:

Even if you deactivated your account (meaning, you quit Facebook), they maintained your profile data. The privacy policy and terms of service (TOS) were disturbingly cryptic on this issue. It said the company “usually keeps[s] a backup copy of the prior version [of updated profile information] for a reasonable period of time to enable reversion to the prior version of that information.” Facebook declined to enumerate how many days (or centuries)

constitute a “reasonable period of time.” Facebook users do not have access to this information, so it’s unclear who exactly would be doing the proposed “reversion.”

How incredibly stupid was the Facebook leadership here? I wondered at the time why the entire legal team there hadn’t been fired. This was even worse than Beacon.

Basically, what they were doing was insidious. It took control of the member profile, removing any controls members had over it from their hands. If you decided that you didn’t want to be a member of Facebook—no problem. But as far as Facebook was concerned, they still owned your profile.

If you decided that you made a mistake and revealed something you shouldn’t have or needed to get past something that you had done and recorded, that’s fine as far as Facebook was concerned. They still owned your history. So delete away, they could always “revert.”

One of the key psychological benefits of a social network is not just the peer-to-peer communications that it fosters. It is control of the parts of a life that is being exposed by the owner of that life. That gets translated to a profile when it comes to a social network or community and the actions on that profile. What made Facebook particularly nasty in its February 2008 iteration was that it said to the member, “Your ownership is an illusion. Once you commit—you commit. And then, heh heh heh, the data is mine, mine, I tell you, mine! I am Facebook, lord of this universe, master of this social domain.” Or to put it in little kids’ terms: What’s mine is mine. And what’s yours is mine.

Peripherally, it was even a bit worse than that. Facebook was also giving developers access to the open profiles of the members and access to the profiles of friends of the users of the application. Meaning if you gave permission, *de facto* so did your friends.

Does that mean that Facebook is a horrible group whose intention is to snatch your digital soul? Hardly. They were making bad business decisions based on urgency to produce revenue with an unclear business model and they forgot some of the fundamental reasons why members associated with them.

Facebook is a business, not a hangout, and thus they rightfully treat the profiles as assets. This is no different on the surface of it than the salesperson who is treating his contact database as his asset and leverage (in that case, to protect his livelihood). But there is a different protocol that governs social networks. Peer-to-peer trust is one major facet of that governance.

The Facebook Terms of Service Outcry, 2009

It never seems to stop, does it? When it rains, it pours—or becomes ark-ready in the Facebook case.

In 2009, what may have been the final—though with Facebook it's always a challenge to say that—outrage occurred with the commensurate hue and cry. Facebook changed their terms of service, revealed in January 2009, to (once again, without member consent) keep all the content you ever provided from profiles to messages, even if you quit. Again.

Here were the terms of service (TOS) that Facebook presented as an apparent *fait accompli*:

You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof.

They removed:

You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.

The termination clause made ownership rights crystalline:

The following sections will survive any termination of your use of the Facebook Service: Prohibited Conduct, User Content, Your Privacy Practices, Gift Credits, Ownership; Proprietary Rights, Licenses, Submissions, User Disputes; Complaints, Indemnity, General Disclaimers, Limitation on Liability, Termination and Changes to the Facebook Service, Arbitration, Governing Law; Venue and Jurisdiction and Other.

Here's the way Mashable's Stan Schroeder described it in an article on February 16, 2009:

In short, all of the content you've ever uploaded on Facebook can be used, modified or even sublicensed by Facebook in every possible way—even if you quit the service . . . Looking at it globally, millions

of people are uploading bits of information on everyone and everything, to a huge online database, and by doing so they're automatically giving away the rights to use or modify this information to a private corporation. And not only that; they now also waiver the right to ever take it back from it.

This continued the imperious heritage of Facebook assuming that they controlled—no, make that owned—all your content, whether or not you were continuing the relationship. That would be the equivalent of a factory owner assuming a unionized worker will continue to work for free at the plant even if he got another job.

That sense of entitlement, or perhaps desperation, led to a weird incident with me directly in February 2009. A friend of mine sent me a note that went to an ad on Facebook that showed my profile picture and said, “Paul Greenberg is a friend of _____.” As I said at the beginning of this, I’m leaving out the company because I like them and they weren’t responsible for it. But what it amounted to is that Facebook ran an ad without my permission, even though there was nothing in the ad that was wrong. The Facebook TOS actually allowed them to do that. I’d have to opt out to prevent it—a decidedly non-customer friendly approach. This ad was just indicative of Facebook’s continued violation of, not privacy, but trust. Which they codified in those early 2009 terms of service.

But once again there was an outcry. It was exposed by the *Consumerist* blog with a post entitled “We Can Do Anything We Want with Your Content. Forever.” The furor began. Within 24 hours, Facebook returned to their less onerous previous TOS and within a week, opened the discussion on the TOS to their “constituents.”

Lesson learned finally? Hopefully, but we’ll see. I did notice that in September 2009, Facebook (very) quietly announced the demise of Beacon.

The Lessons of Facebook and the Expectation of Trust

The value of this story is that Facebook provides a great set of lessons and practices on what not to do to deal with your 21 century customers—that apply well beyond a social network—when it comes to trust.

Facebook’s mistakes are just that. Mistakes. I understand that by having my profile public, it is subject to being seen. Fine. But I’m not consenting to commercial use of the information. Giving information

to advertisers might be infuriating but isn't remotely illegal. But it does forget that as their customer, I have to have control over my activity—in fact, I demand it. There is a compact between Facebook and me that provides for Facebook as a commercial property and for me as a customer. Additionally, the value proposition has to be mutually beneficial or I have no reason to be on the site nor does Facebook have any reason to want me.

Social networks, if they work right, are giving me, the member/customer, the means to control my activity and to personalize the way I want to act and the level at which I want to expose my information. In return, I am giving the environment that I chose to be in the limited right to use me as an asset of that environment. If they are for profit, that means I am giving them the right to make money from me—the asset, as long they don't impinge on my control of my activity. In other words, Facebook and other social networks I choose to use have the general right to earn revenue from me, but only in ways I am willing to let them do so. They can't presume that assent from me without permission.

If contemporary businesses that are considering communities, whether for profit or for branding, think of the inherent rights the business has and the inherent rights the members have, then peace and harmony will rule the land and mutually beneficial value will be derived.

In order to achieve that commonwealth of value, here are some rules and lessons that businesses need to keep in mind when developing social networks that will reach out to customers and some rules for the members to abide by—or to at least think about.

Rules for the Business

As a social network there are four things that should be remembered:

- ▶ The social network is responsible for providing a reasonable expectation of privacy for each and every member of the network. That means that the individual who provides the profile retains ownership of the profile and is, in effect, licensing the use of that profile in a limited way.
- ▶ That the terms of the “license” must be mutually agreeable and always transparent. There are no hidden or undue uses of the profile by the social network.

- ▶ The member must feel that they have control over their profile at all times. This one is mission-critical. It is no different from a customer feeling that they have control over their relationship to your company.
- ▶ The social network must do whatever is necessary so that it is trusted *as a peer* by the individual members of the social network. This one is critical to all businesses, whether a social network is involved or not. Suffice it to say, the individual members can't see the social network as an abstract entity. It *must* be seen as a trusted peer to be successful.

Rules for the Members

The members don't get off scot-free either. They are involved with a commercial property more often than not and they don't own that commercial property. So they have to abide by some rules too:

- ▶ They have no inherent right to be a member.
- ▶ There are risks associated because there is no complete privacy that can be guaranteed—even if there is a guarantee. (What is it about the word “social” members don't understand?)
- ▶ While they retain ownership of their profile, by signing up they are providing a limited license to the social network to use that profile as an asset, as defined by the terms of the agreement.
- ▶ That profile may well be used commercially, with their permission.
- ▶ There is no permission needed for the social network to carry ads that the members will most likely view. That is the prerogative of the social network.

Okay, enough of me for the moment. I'll be back later. Now, I'd like to introduce Karl Wabst, who will run our nitty-gritty discussion on privacy. I thought it important to get with an expert who can actually give you the tools you need to establish a privacy policy that both supports the expectation of trust that the social customer has of you and, at the same time, protects your company from legal issues.

Karl, a seriously great security and privacy strategist and an advisor to my company for years, was even the interim chief information security

officer at Boeing in one of his incarnations. He is one of the foremost experts on privacy and trust in the United States. Not only does he have years of practical experience, he is certified in all areas of privacy and security known to the human species. He is a long-time associate and friend whom I trust completely to give you what you need to know to develop an appropriate framework for your privacy policies.

KARL WABST ON ENTERPRISE-LEVEL PRIVACY

Whatever one's personal viewpoint, privacy is becoming a hot business and legal topic. Governments in many large markets regard privacy as a human right. The force of law backs complex enforcement systems. Fines are growing larger each year. Ignore local attitudes and legislation at your own peril. On a more positive note, information privacy programs can actually save money and add to the bottom line.

Embracing the new global economy by expanding into international markets to take advantage of the soft U.S. dollar to gain a wider audience, or increased usage of customer, partner, third-party, and employee data to provide targeted services, has led to unexpected discussions between board members and executive management. Legal risk forces consideration of information privacy as a corporate and governmental discipline.

Preliminary investigations of European markets have exposed some U.S. corporations to the different attitudes, practices, and legislation surrounding sharing of information and its constituent datum. European society tends to be less blatantly commercial than the Americans are. That is not to say that EU citizens are not stalwart consumers. They simply approach the process differently.

The European Convention adopted formal privacy principles, partly in response to the horrible lessons learned from the misuse of private information during WWII. Many countries, including the United States, subscribe to privacy principles formulated by the OECD.

Around the world, varying attitudes, alliances, and legislation related to privacy are in evidence. The sectoral or patchwork approach taken by the United States has not inspired trust in nations that view privacy as a human right. Approaches to privacy as a discipline, in the U.S. and around the world, continue to evolve toward stricter interpretation and enforcement.

The first impulse in the U.S. has been to merge information privacy strategy and concerns with those of information security. There are fundamental differences between information privacy and security that boards and senior management ought to consider before making costly errors in resource allocation. With little exposure to the discipline of privacy, it is easy to miss the fact that privacy protection is not limited to computer security.

The discipline of security tends to focus on defending corporate borders against intrusion. Firewalls to protect bits of data, the systems, cables, and other devices that transport data, and the applications that process those bits draw more attention than how these assets are used to create value. The business value of security, as well as the reputation value, market value, and replacement costs of data go overlooked in many corporations.

Privacy professionals collaborate with business functions, partners, vendors, and customers to focus on the legitimate uses of information, within the boundaries prescribed by U.S. and international law regulation in concert with corporate policy. Privacy involves formulation of strategy and response to issues in both computerized and paper-based systems. Many privacy professionals are lawyers or business people with international experience developing services and collaborating across corporate boundaries.

Rather than defending network borders, privacy professionals focus on education of senior management and boards regarding benefits and risk of the commodification of information held by companies, such as behavioral targeting or procedures to ensure that customer preferences are recorded and respected.

Privacy professionals collaborate within the company and externally regarding legal and reputation risks, damage to clients, obtaining business value from information collection, storage, processing, and sharing with vendors, partners, and employees.

By acting as liaison between customer, vendor, and the corporation, the mission of information privacy is to facilitate competitive advantage through responsible management and usage of sensitive data. Working to maintain client trust ultimately provides more information to target services and potential gain in market share.

Behavioral advertising, also known as behavioral marketing or behavioral targeting, used by an increasing number of corporations to gather data by observing the actions of Internet users, is pushing

corporate America into uncharted waters while enriching the relationship with our customers. Privacy professionals can help bridge business, legal, and technical realms to advise and oversee such efforts.

Technologies invisible to consumers are able to track online activities with the goal of presenting advertising targeted toward that consumer, or at least one fitting the profile created by analysis of the types of sites users visit. Tracked actions may include searches conducted, web pages visited, and content viewed. Combining cookies and web beacons—also referred to as web bugs, web tags, clear GIFs, action tags, and pixel tags—provides marketers with the ability to identify groups, sometimes individuals, depending upon data collected or combined with information from site registrations.

Partnerships have formed between marketers, ISPs, and websites. Services that track users across seemingly unrelated sites produce advertisements and e-mails targeted to the assumed interests of the consumer. This process is not limited to computer users. The same principles extended to mobile devices provide marketers with the opportunity for more granular targeting, since shared mobile phones are less common than shared computers. An abundance of data points available from extended Internet usage combined with the GPS included in most phones allow targeting of advertisements to physical location.

Not to be outdone, television companies are testing targeting technology on 500,000 subscriber homes in New York City and New Jersey. Cablevision plans to route advertisements to specific homes based on data, gathered by Experian, including income, ethnicity, gender, and presence of children or pets. The result? Your next-door neighbor may see different advertisements than appear on your TV set.

As the quality of the data collected improves, so does the precision of advertisement targeting. The experience of just the right ad to just the right place to be seen by the right person may be in reach. Instead of appreciating the level of sophistication and innovation required to achieve such a feat, many consumers decry the “creepiness factor” of behavioral targeting. Practitioners of behavioral targeting claim that information is not retained.

Unfortunately, corporate trust is at an all-time low. At the same time, millions of layoffs, blamed on the economic crisis, has dropped employee morale. Recent studies have found that many terminated employees are taking unknown amounts of corporate data with them,

largely unchallenged. Only a cursory understanding of probability is required to see that eventually sensitive customer data, potentially worth millions of dollars, will resurface in an embarrassing place and lawmakers are likely to respond with reactionary legislation.

Concerns about behavioral targeting inspired reexamination of FTC advertising rules, likely to move the U.S. closer to opt-in rules, already law in the EU. The increase of FTC activity around privacy promises made by companies is a signal of increased risk for corporations that do not follow through on promises to customers related to sensitive information handling. Privacy cases prosecuted under Section 5 of the FTC Act send a clear message of change. It is likely, however, that the possibility of increased profits is a more palatable stimulus for change in business practices.

The self-regulatory privacy rules for behavioral advertising are similar to those found in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. It is reasonable to expect development of similar rules for non-Internet environments that use behavioral targeting to create consumer profiles. A basic understanding and incorporation of these privacy principles may save some angst later.

- ▶ **Transparency** Monitoring of user activity and collection of data for use in providing tailored product and services advertising would require a posted statement, outlining such practices in consumer-friendly language.
- ▶ **Consumer control** The statement should provide consumers with information to decide whether they wish to have their information collected for such purposes. The site should also provide a clear, easy-to-use, and accessible method for exercising this option.
- ▶ **Reasonable security** Risk-based security protection is required. Protection is employed based on the sensitivity of the data, the nature of the company's business operations, types of risks the company faces, and the reasonable forms of protection available to the company.
- ▶ **Limited data retention** Prohibits retaining consumer data longer than is necessary to fulfill a legitimate business or law enforcement need.

- ▶ **Affirmative express consent for material changes to existing privacy promises** The consumer must expressly provide permission for use of their data for a purpose other than that for which data was collected.
- ▶ **Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising** Permits collection of sensitive data for behavioral advertising only with affirmative express consent from the consumer to receive such advertising.

With no overarching federal privacy law, more than 40 states have enacted privacy or breach reporting legislation extending the morass of corporate compliance. California's privacy law, recently expanded to include medical and insurance data, acted as the template for many U.S. laws. The EU is currently debating adopting some form of breach notification modeled on U.S. laws.

Understanding the role of information privacy in terms of a contributor to the bottom line also differentiates its role from that of information security. Examining privacy methodologies from the board room instead of the server room may reveal ways that data can further understanding of customers and save money in other information-related areas. Motivating employees and customers to view data as an asset, rather than a cost, may spur interest in new ways to utilize assets already in-house.

Some final thoughts about the benefits of implementing a proactive approach to privacy:

- ▶ Proactively identifying sensitive data allows marketing, sales, and other business functions to collaborate in development of more personalized services for customers.
- ▶ It provides a reduction in security costs, by targeting preventive and detective control mechanisms on areas hosting valued assets.
- ▶ It also provides a reduction in audit costs and response time to e-discovery requests, since an inventory of data assets exists and risk scores are built into existing assessments.
- ▶ Demonstration of due diligence related to sensitive information may yield reductions in insurance premiums and enhance business continuity and disaster recovery abilities.

Three Takeaways

So what can you do about all this? Here are three things that will support a bullet-proof privacy policy.

- 1. Recommendation:** Develop a holistic business process–focused approach to privacy management. Approach privacy as an enterprise-level business process requiring input from legal, audit, sales, marketing, HR, accounting, and technology departments. Identify all processes that require collection or incidentally collect, manipulate, or transmit sensitive data. Maintain the right to audit vendors' and partners' policies and practices since legal responsibility may remain with your organization. Assign responsibility for information privacy within senior management. **Note:** Privacy is often confused with IT security or compliance. An important distinction is that information privacy is more encompassing than IT. Do not overlook non-IT data, such as records storage, contracts, or voice records. Protect the physical perimeter. In the United States, compliance regulation has followed a sectoral approach. This is not true internationally. Privacy requirements transcend international borders (e.g., transborder flow), industry type, (e.g., financial services, health care, retail), application type, (e.g., CRM, ERP, desktop applications), data format, and storage or delivery method (e.g., electronic, written, printed, spoken). Be prepared to prove that you do what you say in your privacy, security, and business policies.
- 2. Recommendation:** Integrate internationally recognized standards frameworks, such as ISO 27002, ISO 38500, and OECD privacy principles into business and technology processes. Standardizing on international frameworks increases your ability to operate successfully in globalized markets. Implementing international standards helps support evidence of due diligence and due care. Simply put, if you do not know what or where your data assets are, you cannot protect your company, client, and employee data properly. Best practices: Inventory and document types of data assets held, how data flows into, out of, through the company, especially to vendors or suppliers. Document: A) Data types that legally, contractually, or ethically require special handling. B) Business need, purpose, sensitivity level, protection requirements. C) Data owner, custodian, user roles and responsibilities. D)

Method of data acquisition, changes, protection and flow. E) Opt-in/opt-out, requests for removal. F) Data retention schedules, secure destruction. G) Partner, vendor, and auditor policy compliance. H) Use in development, sanitization, marketing. I) Breach reporting and monitoring. **Note:** Many companies do not follow recommendations in privacy and security frameworks and fail to reap the benefits of a privacy program. Worse, they miss opportunities to gain competitive advantage through insight to customer needs and process efficiencies while still accepting legal and reputational risk. Benefits to implementing information privacy program: Output will significantly augment governance, CRM, business intelligence, e-discovery, security, metrics, audit, incident response, physical security, breach reports, , outsourcing, and systems development lifecycle.

- 3. Recommendation:** Design a privacy program to be adaptable. Expect change as globalization drives standardization. **Note:** The EU is creating strategy for adoption of U.S.-style breach-reporting laws to augment robust privacy controls in the next year or two. Expect this move to reignite the push for U.S. federal privacy law. Such laws will likely set a minimum standard, rather than attempt unification of the 45-plus state privacy/breach laws in existence.

I told you he knows what he's talking about.

Intellectual Property, Transparency, and Theft

There is another area that should be briefly discussed in the era of the social customer, and that's the way that intellectual property (IP) should be considered.

We clearly live in a time when the demand for transparency and honesty has been paramount. If your company isn't transparent enough—meaning you are unwilling to reveal enough information about yourself to allow the customer to make an intelligent decision on how he or she is going to deal with you—then you should simply close up shop, give me your IP, and I'll make good use of it.

Simply exposing your IP—some of which you might consider trade secrets—isn't the answer, either. However, there is some benefit to loosening the ropes surrounding your intellectual property when it

has a beneficial result for you. For example, there is a group of 125,000 scientists and engineers who are organized around a social network called Innocentive that solves problems. The way it works is that the member companies, who pay an annual membership fee of roughly \$100,000, are presented with a problem—could be an R&D problem, an engineering problem, but always a scientific problem of some sort. Often they are corporate conundrums—problems that are not resolvable by the R&D departments of the companies that present them. The Innocentive members go to work and usually, at a significant cost savings, they solve the problem and are paid for their effort, though a fraction of the cost of the solution under normal conditions.

As cool as this is, the reason I bring it up is not the neat-o social network or the focus around crowdsourced innovation. I bring it up because in order to get the problems solved, companies have to expose their intellectual property appropriately to the individuals who are attempting to solve it. Samsung, Procter & Gamble, and companies of a similar ilk all do exactly that.

But there is also the opposite problem. What about those who abuse the more open environment? Just because information is given freely, it doesn't mean it's there to be taken freely.

Brent Leary, LaForce+Stevens, and Social Plagiarism

In New York City, there is a public relations firm (which, as you will see, makes this an all the more astonishing story) that pretty much did something that no self-respecting public relations firm would ever do. They plagiarized something.

The plagiarizer is the New York-based public relations firm LaForce+Stevens (that would be “LaForce and Stevens” with the little plus sign their cutesy affectation). They have a seriously upscale clientele that includes Nautica, Perry Ellis, Piaget, and the *Wall Street Journal* among many others, who would be shocked—and should be concerned—if they heard what LaFarce-Stevens (that would be “LaFarce minus Stevens,” which is what they'll be called for the rest of this section) actually did.

The plagiarized was Brent Leary, the very same CRM guru you heard from in the web chapter on small business. Here are the facts of the case, judge and jury.

On November 26, 2008, Brent wrote an article for the American Express Open Forum called “Dale Carnegie Meets Barack Obama: Winning Friends and Influencing People in a Web 2.0 World.”

In January 2009, Brent received an e-mail from a friend who was the recipient of a pitch via e-mail from the aforementioned LaFarce-Stevens. The pitch was pretty much the same as Brent’s article with about perhaps ten words different and no attribution whatever, though even attribution wouldn’t have been a palliative for this egregious theft. Table 1 is one excerpt from Brent’s article, side by side with the LaFarce-Stevens pitch.

Table 1: A Comparison Example between Brent Leary’s American Express Open Forum Article and LaFarce-Stevens Pitch

Brent Leary’s American Express Open Forum Article	LaFarce-Stevens Pitch
<p>Dale Carnegie 2.0</p> <p>President-elect Obama’s campaign is a living testament to the longevity of the teachings and concepts of Dale Carnegie. But they are also a testament to the power social media can have on building meaningful relationships with people we may have never met—and might not ever meet. Now it’s not likely that we as small business people will ever reach the scale and scope the Obama campaign operated on. But we don’t need to reach millions of people and raise hundreds of millions of dollars to be successful. We just need to figure out how we can use blogs, podcasts, social networks and other tools to make it easier for people to find us when they are searching for help. We can thank Dale Carnegie and Barack Obama for showing us how we can do it.</p>	<p>Dale Carnegie 2.0</p> <p>President-elect Obama’s campaign is a living testament to the longevity of the teachings and concepts of Dale Carnegie. But they are also a testament to the power social media can have on building meaningful relationships with people we may have never met—and might not ever meet. Now it’s not likely that we as small business people will ever reach the scale and scope the Obama campaign operated on. But we don’t need to reach millions of people and raise hundreds of millions of dollars to be successful. We just need to figure out how we can use blogs, podcasts, social networks and other tools to make it easier for people to find us when they are searching for help.</p>

What is incredibly galling is that as of September 2009, LaFarce-Stevens hasn’t apologized, hasn’t offered that they will, and made an offer to Brent that anyone would find insulting. They abused the public nature of information and were found out through the interconnectedness of networks in combination with the real-time availability of communications channels. A 21st century tale of a company that doesn’t belong in business due to their unethical behavior. This is where the open nature of intellectual property and its easy accessibility was violated when a company crossed the line.

Oh yeah, to show you the courage of this intrepid PR firm, they literally blamed it on a newbie underling who “didn’t know” that this was wrong! That seems to tell you something about their training methodology.

The Lessons

Intellectual property is more freely shared than it has ever been before. But it is still owned by its creator unless that creator has given away or sold the rights to that property. One solution to the conundrum of how to share IP freely without exposing the rights to the public is Creative Commons licenses, which are licensing agreements (not legally binding) that allow the use of materials under circumstances dictated by the owner of the materials. So, for example, I use a number of Creative Commons licensed musical pieces for podcasts, especially those from Podsafe Music and IODA Promonet. I have permission from the artists based on particular permutations of Creative Commons licenses to use particular musical works in my podcasts under specific conditions regarding attribution and context. There are some 70 licenses like this that are open source, and several CRM software companies, notably SugarCRM, operate under some version of this kind of license.

There are real-world consequences to screwing up the version of the Creative Commons license you use. Seth Godin is one of the handful of marketing gurus out there who is not only right about what he writes but a true thought-leader in the space and beloved by many. In 2005, Seth Godin wrote an e-book entitled *Everyone's an Expert*, which he gave away and put under a Creative Commons Attribution 2.5 license (now 3.0), which, with attribution, doesn't prevent commercial repackaging and sale of the book—which, in 2007, a publishing company did. Godin was informed of this by a friend (just like Brent found out about his violation) who had gotten a notice from Amazon that the book was available for the south side of ten bucks. Godin issued the following in his February 10, 2007, blog posting: "I didn't authorize this book to be published, I have no idea who the publisher is, and I certainly didn't ask Amazon to e-mail anyone."

Godin didn't have a royalty issue—it was a free book—but what he wasn't cool about was that the original cover was missing the following: "This is a reprint of a free 2005 EBook under Creative Commons License." It now has that and he's happy.

This parallels Brent's case, but where the publisher fixed the problem when it came to attribution with Seth Godin—despite the questionable nature of their publishing practices—LaFarce-Stevens, as mentioned above, hadn't done anything close to the ballpark when it comes to attribution or acknowledgment of their "mistake."

What this means all in all is that when you are using social media with your company to reach out to your customers, it's likely that the

reason you're doing it is to enhance your brand reputation. That means you need to protect your materials—even in the age of freely available information. By being transparent, you're also more vulnerable to the things that happened to Seth Godin and Brent Leary, which if done improperly can damage your brand. Trademark your name, copyright any material that you think needs it, use Creative Commons licenses for other materials, and determine what you are willing to allow as fair use before you need to take action. Freely available doesn't mean free to take.

Of course, as always with me, this subject went longer than expected. But I hope that it's now clear that we are negotiating new territory when it comes to how we deal with trust, privacy, and intellectual property—something that you have to consider when it comes to how you're going to engage your customer and capture knowledge.