Ask CDT: Answers on Social Media Privacy

October 25, 2010

Last week, CDT Senior Resident Fellow and consumer privacy expert Justin Brookman took readers' questions for Ask CDT: Social Media Privacy [1].

At the bottom of this post, Justin answers some of the questions via video; written answers for all of the questions are also provided below.

Question: *How do you define social media? What do you consider to be trends in social media that privacy professionals should be cognizant of?*

Justin Brookman: For me, "social" means the ability for users to interact with other people — both real life friends and other computer users they've never met before and never will. When you think about it, this is how the Internet started out — a few isolated folks talking back and forth, and then eventually USENET message boards on a wide range of disparate topics. This was all social. In the 90s, companies began to publish on the web, and eventually came to monopolize it. For a while, the web became fairly passive, more like reading a newspaper.

But with the success of first MySpace, and then Facebook and Twitter, all Internet companies are looking to incorporate social aspects to their sites. Social sharing is a wonderful thing and has made the web a more democratic, open, and interesting place. But it also carries privacy risks, and an opportunity for consumers to share more information about themselves than they want to or even understand.

One of the trends we're most concerned about is merging of previously distinct personas and tying all social interact activity (or really all internet activity) to a person's real name identity. We've seen some of this with Facebook's Instant Personalization and with Google's Buzz, where what people had previously done online privately was linked to a real name and disclosed to contacts in that person's social network. We think people should be able to maintain different personas on line, and what I do on one message board or social media site shouldn't necessarily be published to the world under my real name. There's a real value to private pseudonymous or anonymous web participation, and I worry that some companies, and perhaps regulators, are trying to push the Internet to all real name, all the time.

Q: *What do you think about Facebook's new functionality to allow users to download all their data that they uploaded to Facebook?*

JB: We think this is fantastic. One of the things about Facebook is that their privacy improvements often come on the heels of a big privacy misstep, so their changes are often very reactive, and sometimes only fix a part of the problem they created. Here, Facebook came out of the blue with a really great tool to let consumers download their data from the site. This is something we've asked for for a long time from not just social networking sites, but from any cloud computing provider — any site you use to remotely store your data, be it a webmail provider, or a photo sharing site, or a utility that let's you back up your computer, or a service that offers enterprise level information processing to small businesses. Once a company gets hold of your data, it shouldn't be able to "hold you hostage" by making it hard for you to move your data to another provider. Not only do not enough companies fail to offer data portability tools, many make it a violation of their terms of service to use some sort of third party software to extract the data. Fortunately, we've seen some of the leading Internet companies like Google, with their Data Liberation product, and Facebook, with this recent announcement, hopefully set the standard for all cloud services in the future.

Q: *Scott McNeely famously said: "Privacy is dead, get over it." Given the rise of social media platforms, is McNeely right or wrong and why or why not?*

JB: No, privacy is not dead, and, perhaps counterintuitively, I think social media is a big reason why. Before the social web, ordinary users didn't really have any reason to know or think about how their personal information was being shared online. They browsed the web, from site to site, with little or no awareness of how those sites were tracking them, or using the limited information those users had input into the sites. In this way, the online world wasn't really much different from the offline world, where data brokers had aggregated information about consumers for years with very little consumer awareness. It was probably more efficient than offline, but let's remember that behavioral advertising was in its absolute infancy when McNealy made his remarks in 2000 (even today, it makes up only a small percentage of online advertising).

When people first got the chance to affirmatively share considerable amounts of personal information with the advent of social networking, they finally got it --- they finally started taking privacy seriously. They understood they were sharing detailed information about themselves and their families, and when they heard or read about social networks using that information in ways they didn't expect, they got upset! And in this way too the social web helped --- privacy stories went viral as users shared the stories with one other. Of course Facebook users were going to be interested in and want to post status updates about Facebook Beacon --- the stories rang true and meant something to them. In some ways, Facebook's privacy missteps were really important advances for consumer privacy, because they shone a light on information misuse that absolutely resonated with Internet users. Everyday consumers are a lot more aware of and concerned about privacy in 2010 than they were in 2000, and it's because of the social web.

Q: *I'm developing a privacy tool that will allow a user to post information in places such as social media sites and have it obscured in such a way that the casual reader cannot determine the content. The key that unlocks the content can be made available solely to those individuals that the poster wishes (or intends) to be able to read the content. It's a form of steganography so it's less encryption and more "cloaking".*

An example of the cloaked text might be:
[aaaaaccdeeeeffggghiiiiklllmmnnnnnooooooopprrrrsssssstttyy]

Are there any legal ramifications for (i) the user and/or (ii) the tool provider (probably me) for doing this?

JB: Let me start out by saying I am not your lawyer, nor am I the lawyer of anyone who uses your product. This is not legal advice! I think what you're proposing is an interesting tool, and CDT generally believes offering consumers more privacy choices is a good thing. At first blush, I don't see any inherent legal problem with doing this. One thing to keep in mind is that this sort of thing might violate a social network's terms of service — they may not want user profiles to be a mishmash of gobbledy-gook that only certain users can deencrypt. In extremely rare instances, prosecutors have tried to allege that violating a website's terms of service constituted a Computer Fraud and Abuse Act criminal violation, but those cases have all eventually failed. As a tool provider, in theory, you should generally be protected from liability by just being a neutral intermediary (you're not encrypting data on social networking pages, you're just offering users a means). On the other hand, notwithstanding the law, regulators or private parties might see you as the most logical party to go after since you're the source of the code and the party with the most power to stop the practice.

One additional thing to keep in mind is that the government is considering how to revise CALEA, which is the law that implements the government's power to wiretap communications. They're considering expanding its mandate to encompass a broad new range of communication services, and to effectively require a government backdoor for all internet communication technologies. I'm not sure if the law that eventually gets passed would apply to something like you're considering, but it's worth keeping an eye on.

Q: *Hi Justin,*

The media has recently reported on a few cases in which individuals have sued social media services (namely YouTube) to uncover the identities of anonymous Internet posters. In one of these cases, the person bringing the suit against YouTube was arguably a public figure.

What legal precedent do these cases have under U.S. law, and what long-term implications do you think these cases could have for people who use social media to voice controversial opinions?

JB: I agree with you that this is a huge potential privacy concern, and I worry about the precedent that some of these cases might set. Now fortunately, the United States has a pretty strong legal foundation to address these issues. First of all, the Supreme Court has long held that there is a First Amendment right to anonymous speech; that right applies to the Internet just as it does to the public square. Second, and relatedly, we have relatively weak defamation laws here in the United States, certainly as opposed to the United Kingdom and other countries, and here at least, a plaintiff has a very high burden of evidence in order to win this kind of case.

That said, we have seen American cases where courts have unmasked bloggers and commenters for allegations of intellectual property violations and libel, and I worry that some of these decisions have gone too far and do infringe upon our free speech rights. If the rule was that you lose your anonymity anytime you say something absurd and insulting in YouTube comments, that could well be enforced against approximately 95% of the site! I don't necessarily want to endorse YouTube comments as the model of Socratic debate, but by and large, people should feel comfortable expressing novel and potentially embarrassing ideas online without being worried that their real identity is going to be revealed. As a society, we benefit from pure ideas that don't have to pass through the lens of how a speaker fears (correctly or mistakenly) that his or her comments will be judged by society.

Q: *Seems to me that there is a fundamentaly wrong assumption on the fact that "social media" is primarily "social".. It is mainly (only??) done by companies willing to do business with their members' data.. Not at all to provide a "social service", which is in reality a "by product" of their first objective which is cash generation, without providing full transparency on their intent and the way they use personal data.*
Don't you think that this fundamental issue has to be clarified and maybe the use of data has to be restricted in a very strict way.
Isn't the social media buzz a sign of a more fundamental societal issue?? The current uncontrolled situation is only worsening the perception of social media which may, in reality, provide tremendous benefits to our societies which have lost some references and the practice of true "human to human" communication..

Seen this way it is even worse to let some companies use and abuse it without a minimum control and ethical practices..

JB: Well, what you're saying is really true for all websites and even offline services: Google offers search, but obviously the underlying corporate goal is to make money. The Gap sells you a shirt, but their fundamental goal too is to get paid.

I think this truism is slightly different in the social media context (as well as for any site powered by behavioral or profile advertising) because the cost isn't entirely clear. When you buy a shirt, you know you're paying $20. When you're paying with your privacy, it's not always clear — you have to dig through complex privacy policies to see what's happening, and even then, the company may just reserve all rights and not actually tell you what they're doing.

That's one of the biggest reasons we've been aggressively pushing for consumer privacy legislation, to give consumers more clear information and more control over their data. Many social networking sites and others make a value proposition to consumers about how they're proposing to use their data, and if the consumer thinks it's a good deal, he or she can make the informed decision to use the service.

Q: *I think privacy is also a perception issue on the part of individual participants. There is a tendancy to think that "everbody is out there viewing my profile page." Would it not be better to advocate that social media sites be able to provide metrics reporting to individuals using these sites? LinkedIn already has this feature and I can see who views my profile and how often I turn up in their search results. These features might go a long way towards alleviating a lot of perceptions around privacy,*

access and choice. And I think many people would be surprised at just how much (or more likely how little) their information is viewed.

JB: This is an interesting idea and there may well be some value in providing aggregate metrics to consumers about how often their profile page is being viewed. I would be a little leery about a product that tells Facebook users who has looked at their profiles. I think in that case the looker might well consider that a privacy violation — telling everyone whose page he or she looked at that this specific person viewed your profile — because that's not the way the site worked in the past. And that's always one of the biggest privacy challenges for social networks — when the network changes the rules for what is revealed about you and under what circumstances. A site that made such a change should be really careful to message to its users that there are new rules for looking at people's profile pages, and to make sure that users fully understand before telling the world where they had been surfing.

Q: *I know that CDT advocates the need for an overall bill (one bill... one privacy bill to rule them all...) that protects our privacy. If the bill that CDT wants passed becomes law, what would happen to companies caught in privacy mishaps like those we've seen over the last couple of days?*

JB: The first thing a privacy bill would do is to make the privacy mishaps less likely to happen. It would put into effect substantive and enforceable baseline legal protections, as opposed to what we have now which is only that companies cannot lie about how they use your data. So many just put incredibly broad terms into rarely read privacy policies, to ensure that from a legal perspective, they don't get into trouble. A law would also require companies to have internal accountability measures and corporate controls to ensure that companies design products with privacy in mind. Also, most companies who do a lot with consumer data would be strongly incentivized to join a safe harbor coregulatory program, which would set forward greater, industry-specific privacy requirements, along with periodic monitoring and compliance checks.

If that doesn't work, FTC and state Attorneys General would have enforcement authority, backed up by significant penalty authority. The FTC has already interpreted its legal mandate under Section 5 of the FTC Act to require companies to have reasonable security practices in place — targeted enforcement has been very effective there in setting a strong standard for companies to follow. In the absence of privacy legislation, or at least while we're waiting for it, we would like to see more aggressive enforcement from the FTC on unfair privacy practices as well as security. Even after a privacy law is in place, the FTC and states will still need to bring enforcement cases against wrongdoers to put some teeth behind the rules.

Q: *Facebook is the slow moving target of social media and their privacy screw ups make the headlines. I doubt these guys are the only ones affected by privacy problems. My question then is this: Do users of these various social media sites have any legal recourse if they find their privacy is violated? Is there some federal agency (I don't think it would be the FCC) that has the authority to fine a company for a privacy violation?*

JB: So the right authority is the FTC, the Federal Trade Commission. To date they have brought some important privacy cases, notably against Sears for secretly installing monitoring software, and recently against the online data broker USSearch.com. David Vladeck, head of consumer protection, said last month that they're looking to do more aggressive privacy cases, and I know that a lot of their cases come directly from complaints they receive. Unfortunately, except where a few industry-specific laws govern, they by and large don't have the ability to get fines or penalties from companies who violate users' privacy. CDT has long asked that the FTC be given general penalty powers, but so far it hasn't happened.

Also, you could submit a complaint to your state Attorney General — I used to work for the New York AG's office, and we were always looking for new and interesting ideas for consumer protection cases. A lot of our cases came out of consumer complaints as well. Most state enforcers do have the ability to get significant statutory penalties from violators.

There might be a personal cause of action depending on the exact violation. Class action attorneys have brought some really important cases in recent years, including some of the first spyware cases,

and recently against companies who seemingly utilized Flash local storage (or Flash cookies) to deceptively track consumers. Class action attorneys have gotten some pretty impressive multi-million dollar settlements in the past few months from companies like Facebook and Google, but by and large these cases are hard to bring, because you have to demonstrate actual harm, which can be challenging for a privacy case. Fortunately, regulators don't have to make such a showing to bring an action — the fact of a deceptive or unfair practice is enough.

Q: *Facebook just had another privacy "incident." I like the service because I can keep in touch with old friends. Why can't they control these privacy breaches? Isn't it ultimately their responsibility to keep the place clean, so to speak?*

JB: It's certainly the case that Facebook has had a number of high-profile privacy incidents over the past couple of years. And I think they really are grappling as a company with balancing their fundamental mission, which is to help consumers share data, with consumers' privacy interests. One of the problems is that their first big privacy hullabahoo was over the News Feed product, which a lot of people complained about at the time, but which eventually became an integral feature to the site (Facebook did make some privacy improvements around News Feed, but they were at the margins). I think from that point on, their assumption with some of these privacy issues would be that consumers would eventually come around to their point of view and that the company should stick to their guns. Over time, I think Facebook has realized that the overall privacy issue isn't going away, and I really do believe they are doing a better job thinking in advance about user privacy, proactively and not reactively. Certainly, I think they have become more responsive to their users, so when something you think is bad for privacy happens on Facebook — or any other site for that matter — be vocal. Blog, and tweet, and post, and tell your friends about it. One thing we've seen over and over again is that user pressure on privacy is an extremely powerful tool. If you're interested in learning more about just how to be vocal on privacy, you should drop by our Take Back Your Privacy campaign page [2] for ideas.

- social media privacy
- Social Networking
- social networks
-
- social media
- privacy
- Consumer Privacy
- Justin Brookman
- online privacy
- ask CDT

Source URL: https://www.cdt.org/blogs/cdt/ask-cdt-answers-social-media-privacy

Links:
[1] http://www.cdt.org/ask
[2] http://www.cdt.org/takebackyourprivacy