

BIGGER BROTHER: THE EXPONENTIAL LAW OF PRIVACY LOSS

NICHOLAS THOMPSON

This past Tuesday, Facebook made a deal with the F.T.C.: from now on, the social-networking company can no longer humbug us about privacy. If we're told that something we post on the site will be private, it will stay that way, unless we give Facebook permission to make it public. Or at least sort of. For a while. Facebook has been relentless in its effort to make more of what it knows about us—the music we listen to, the photos we take, the friends we have—available to more people, and it will surely figure out creative ways, F.T.C. or no F.T.C., to further that campaign. The company's leadership sincerely believes that the more we share the better the world will be. Mark Zuckerberg, the C.E.O., has said that in ten years we'll share a thousand times as much as we do now. That seems to be both an observation and a goal.

Meanwhile, Zynga has announced that it's going to raise about a billion dollars in an impending I.P.O. Zynga makes social games like *FarmVille*, in which people harvest and sell virtual tomatoes. The games sound inane to non-players, and Zynga employees claim that their workplace is run like a labor camp; yet the company is worth perhaps ten billion dollars. Why? Partly because they collect and analyze fifteen terabytes of data a day from their users. They watch carefully in order to learn how to hook people and what enticements to offer someone frustrated about his slow-growing tomato crop. (There's a segment from *Bloomberg West* in which an analyst compares Zynga to a drug dealer.) According to Zynga's recent S.E.C. filings, its total

number of players is stagnant, but the amount of money it can extract from each one is growing. Data is the currency of the Web right now. Whoever has the most detailed data about you will get rich.

"Whoever has the most detailed data about you will get rich."

Zynga has great data, and Zynga is about to get very rich.

Last week also brought the news that a company called Carrier IQ has installed software on about a hundred and fifty million phones that lets it and its customers—such as Sprint, A.T. & T., and Apple—know an awful lot about you. It tracks location, stores the numbers you dial, and even records the Websites you browse when you're not connected to a cell network. The point of the software is to help the phone companies improve their networks and serve you better. But this is done in a mysterious (and perhaps nefarious) way. Most people don't know they have it, and it's not easy to remove. It's also not clear exactly what it's recording, though a bevy of new lawsuits and government investigations will now try to figure that out. At the very least, there's one more company that you've never heard of that knows a heck of a lot about you. "The excuse proffered thus far—improved service—is at best feeble when compared to the extent of the potential invasion of privacy," Stephen Wicker, a professor in electrical and computer engineering at Cornell, told me.

These are just three stories from the past seven days. There'll surely be more soon. Together, they've made me think of something I'll call The Exponential Law of Privacy Loss (or TELPL, pronounced "tell people"). The more we do online, the better companies get at tracking us, and the more accurate and detailed the data they glean from us becomes. The amount of data that they have grows exponentially over time.

It's impossible to exactly measure what percent of our time is spent connected to the Internet: texting, shopping, surfing, browsing, sleeping. But, my best estimation is that, a few years ago, we lived roughly ten percent of our lives online, and companies captured about ten percent of what we did. Now it's about thirty percent, and the companies capture thirty percent of that—which means roughly nine times as much as a few years ago. Eventually, when we live seventy percent of our lives online, digital companies will capture and store about seventy percent of that. I'm not sure what will happen to the formula when we spend our entire lives online. Ideally, we won't get there.

This tracking isn't all bad; it may not even be mostly bad. People keep letting Facebook broadcast more of their preferences and habits, and they love it. The more that advertisers know about you, the more willing they are to do things like buy advertisements on Websites, supporting journalism such as this. Carrier IQ makes our phones more efficient, and I have yet to hear of any specific harm done to any specific person by their system. Still, the Law is real. The F.T.C. can slow things down, but only a little. All of us are still becoming corporate data at an ever faster rate, for better and for worse.

TIME TO ENACT "DO NOT TRACK"

USA TODAY EDITORIAL BOARD

Facebook's 800 million users are probably feeling a little more secure since the social media giant agreed to privacy measures forced by the Federal Trade Commission (FTC) late last month. But they'd be wise to stay cautious. Plenty of incentive for mischief remains, and not only on Facebook.

The agreement requires Facebook to stop letting users mark their profile information as private and then making it public without their permission. Facebook also promised that it will warn users of privacy policy changes before enacting them.

But the agreement won't stop Facebook from monitoring and sharing users' Web-browsing habits, which is a way for the company and others like it to make money. It's an unsatisfying ending to a two-year investigation, but more important, it's a marker of how difficult it will be to maintain privacy in an increasingly wired world.

The weakness in the FTC's agreement is that it didn't establish any guidelines about Internet tracking, the method by which Facebook collects data about its users even when they're not on the network itself. As company representatives recently acknowledged to *USA Today*, Facebook automatically compiles a log of every Web page its users visit that has a Facebook plug-in, such as the ubiquitous "like" button.

Other online giants, such as Google and Yahoo, use similar methods to monitor users' Web-browsing. This lets them tailor their pages and advertisements to appeal to different visitors.

Online tracking companies, which help sites compile these browsing records, claim that your personal details are not connected to your name, meaning your privacy is not compromised when they share information with advertisers or others. But as the *Wall Street Journal* discovered last year, at least one tracking company collected Web surfers' names and other personally identifiable information and passed it on to clients.

The implication is that tracking companies and advertisers could know your name, e-mail address, hometown, medical history, political affiliation, and more. Such information could be used in troubling ways. A health insurance company, for example, could guess your medical conditions. Or a potential employer could find out whether you spend your time gambling online.

"Such information could be used in troubling ways."

If you don't like that prospect, your only option is to use a Web browser that offers a "Do Not Track" mechanism, such as Mozilla Firefox or Internet Explorer 9. Once you activate the feature, it signals websites you visit indicating that you do not want your data tracked by third parties. But existing Do Not Track mechanisms can't control what websites do; they can only communicate your preference.

That's why the FTC has called for a tougher and more universal version of Do Not Track, a move that the online advertising industry argues would hamper Internet innovation. These fears are overblown. Behavioral advertising, which targets viewers based on their Web-browsing history, is large and growing, but it still accounts for less than 5% of all online advertising. So ads that rely on tracking are hardly the Internet's only revenue stream.

Measures that would create a legally enforceable Do Not Track mechanism or otherwise address privacy concerns are languishing in Congress. Lawmakers should give Web users more tools to control their personal information. Until that happens, your online habits will reveal much more about you than just what you put on your Facebook profile.

This essay is from MacKinnon's book *Consent of the Networked* (2012).



PRIVACY AND FACEBOOK

REBECCA MACKINNON

As protests mounted in reaction to Iran's presidential elections on June 12, 2009, Facebook actively encouraged members of the pro-opposition Green Movement to use the social networking platform. By mid-June, more than four hundred members of Facebook's fast-growing Farsi-speaking community volunteered their time to create a Farsi version of Facebook. Thanks to efforts by Facebook enthusiasts all around the world, the platform has been made accessible in seventy languages—including many languages spoken in countries where regimes are known not to tolerate dissent.

Then in December 2009, Facebook made a sudden and unexpected alteration of its privacy settings. On December 9, to be precise, people who logged in got an automatic pop-up message announcing major changes. Until that day, it was possible to keep one's list of Facebook "friends" hidden not only from the general Internet-surfing public but also from one another. That changed overnight without warning. An array of information that Facebook previously had treated as private, suddenly and without warning became publicly available information by default. This included a user's profile picture, name, gender, current city, what professional and regional "networks" one belonged to within Facebook, the "causes" one had signed on to support, and one's entire list of Facebook friends.

The changes were driven by Facebook's need to monetize the service but were also consistent with founder Mark Zuckerberg's strong personal

conviction that people everywhere should be open about their lives and actions. In Iran, where authorities were known to be using information and contacts obtained from people's Facebook accounts while interrogating Green Movement activists detained from the summer of 2009 onward, the implications of the new privacy settings were truly frightening. Soon after the changes were made, an anonymous commenter on the technology news site ZDNet confirmed that Iranian users were deleting their accounts in horror:

A number of my friends in Iran are active student protesters of the government. They use Facebook extensively to organize protests and meetings, but they had no choice but to delete their Facebook accounts today. They are terrified that their once private lists of friends are now available to "everyone" that wants to know. When that "everyone" happens to include the Iranian Revolutionary Guard and members of the Basij militia, willing to kidnap, arrest, or murder to stifle dissent, the consequences seem just a bit more serious than those faced from silly pictures and status updates. I realize this may not be an issue for the vast majority of American Facebook users, but it's just plain irresponsible to do this without first asking consent. It's even more egregious because Facebook threw out the original preference (the one that requested Facebook keep the list of friends private) and replaced it with a mandate, publicizing what was once private information—with no explicit consent. If given the choice to remain a Facebook user with those settings, or quit, my friends would have quit rather than risk that information being seen by the wrong people. Instead, Facebook published it anyways. It's a betrayal of trust for the sake of better targeted advertising.

The global outcry over the exposure of people's friend lists in December 4 2009 was so strong that within roughly a day after the dramatic change, Facebook made an adjustment so that users could once again hide their friend lists from public view. People's friends could still see one another, however, and there was no way to hide them. Everybody's "causes" and "pages" were still publicly exposed by default, another serious vulnerability for activists. People kept complaining—many by creating protest groups within Facebook itself, where hundreds of thousands of people from all around the world posted angry messages. The groups had names like "Facebook! Fix the Privacy Settings!" and "Hide Friend List and Fan Pages! We Need Better Privacy Controls!" and "We Want Our Old Privacy Settings Back!" Scrolling through these pages, you see people posting from all over the world, with large numbers of Arab, Persian, Turkish, Eastern European, and Chinese names.

"People's friends could still see one another, however, and there was no way to hide them."

Eventually Facebook fixed this problem as well, adjusting the privacy 5 options so that information about what pages users follow, or groups they

have joined, can be made private. Meanwhile, however, lives of people around the world had been endangered unnecessarily—not because any government pressured Facebook to make changes, but because Facebook had its own reasons and did not fully consider the implications for the service's most vulnerable users, in democratic and authoritarian countries alike.