

Privacy: The Slow Tipping Point Transcript

Part 1: The Economics of Privacy Breaches

Stephanie Losi: Welcome to the CERT Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Show notes for today's conversation are available at the podcast website.

My name is Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon working with the CERT Program. I am pleased to introduce Alessandro Acquisti, a professor at Carnegie Mellon who specializes in economics and privacy. So, Alessandro, let's get started. Your research focuses on the intersection of privacy and economics. What are some of the interesting things happening right now in this space?

Alessandro Acquisti: Hi, Stephanie. I would say there are many interesting things, that there are more things happening than time to study them, because privacy is a hot topic and privacy ends up often being an issue of economics. Although the two terms may sound in contradiction—some people may believe that economics and privacy are almost an oxymoron—in fact, it turns out that often privacy invasions have economic roots because there are entities interested in somebody else's data because they can make profit or can use the data to their advantage, and there are costs involved in revealing, exposing, or losing the data.

Therefore, the economics of privacy today is very relevant and also a very exciting area to work on. It can involve anything from studying privacy breaches in a company—what are the costs for companies, as I said with those breaches, and what are the costs to consumers when their data is exposed or revealed by a company? And it can relate to studying individual behavior from an economic framework, trying to understand which are the incentives that drive people to reveal so much about themselves, and what are the incentives that may restrain this information revelation? And it can deal with issues such as social networks and the revelation of personal data on online social networks, for instance.

Stephanie Losi: Okay, and I know some of your research has focused on these topics lately, and I want to start talking about the stock market impact of privacy breaches since I know many of these have been in the news lately. We had ChoicePoint; in the government sphere we had the VA case with the stolen laptop. How do companies' stocks tend to be affected by disclosure of a privacy breach?

Alessandro Acquisti: So what we've found in a recent study with Rahul Telang, who is also a professor at CMU, and Allan Friedman, who is a Ph.D. candidate at Harvard, is that indeed there is a statistically significant negative reaction in the marketplace in terms of the stock market, and this is not completely surprising, although what we are looking for was to see whether the market reaction happens not only for the big famous cases such as ChoicePoint or Polo, Ralph Lauren or Playboy.com, but also for less publicized cases—and that happens to be case. However, it turns out also that the reaction is—although statistically significant and negative—is short-lived, meaning that when you do the kind of analysis that we did, which is called event study analysis, after a few days the market generally recovers from that loss, meaning that the stock market evaluation of the firm goes back to pre-breaches level in general, and also the total loss is kind of limited if you compare it to other studies done for, say, maybe security breaches or other forms of accidents or events which are not related to security. Which means, in short, that the market is not

putting too much weight on these data breaches—is not putting zero weight, but is not putting too much weight.

Stephanie Losi: Right, now did you find a difference between the big companies—you know, Polo, Ralph Lauren, Playboy.com—and the smaller companies that you studied? So were the smaller companies affected more or the larger?

Alessandro Acquisti: The larger. Definitely, yes, which makes sense because there are many more consumers, so it's going to be a bigger deal. That was not surprising, so there is a strong difference between small and large firms.

Part 2: The Evolution of User Attitudes

Stephanie Losi: So let's talk some more about your most recent research. That one focuses on the privacy aspects of online social networking, and I know you looked specifically at the Facebook. I know for example you found that the Facebook users are extremely willing to give away their private information. What do they gain in exchange, what are the incentives that make this transaction seem worthwhile, and what do you think business leaders really can take away from this and apply to their own businesses?

Alessandro Acquisti: In particular in online social networks, it's clear that there is a strong incentive to reveal information because that's the nature of the game, right? You are there to find maybe friends or mates or dates or a business partner and so on and so forth.

Now what is interesting is that sometimes this pushes people to reveal information which is surprisingly personal, that they would have not revealed, say, in a face-to-face conversation with a stranger. The information revealed sometimes may seem like it is being revealed to a bounded community, especially on networks like the Facebook in which there is—at least there's a perception of—a bounded community, the campus. For example, you are on the CMU (Carnegie Mellon University) Facebook and therefore only CMU students may see your profile.

Well, it turns out to be that the communities on these online social networks are mostly imaginary, meaning that they're virtually boundless, because it's very easy to see other profiles even if in theory you may not access them. There are both legal and illegal ways to do that, and the first example that comes to mind was debated this summer, when it turned out that employers of some corporations were actually using Facebook to check out the Facebook profile of some of the applicants that were applying to those companies. These companies were maybe using other students, maybe alumni or other people who were part of a certain social network, in order to see the profiles of that network. The point being that these communities—their boundaries are very permeable, so it's very easy to enter online communities, and therefore the information you provide there can be effectively considered public data, even if it has an appearance of being a secluded network.

Stephanie Losi: Okay, interesting, so you found that corporations were using this to kind of get advance information on potential employees. So do you think that online social networking sites fall short in any way in protecting users' privacies in terms of the default preferences assigned to accounts, or do you think they're all right on that count?

Alessandro Acquisti: I feel that there is an incentive to have poor privacy and poor security almost by design, and I don't try to make this as an attack or purely negative terms, but I'm just trying to explain this from an economic perspective. Which means that also the social network itself benefits from, clearly, the size of the membership, which also means two things. That: A.) you

don't want to have too strict security, in terms of, say, registration, authentication, and login. You don't want to put too many controls to make sure that you, Stephanie, are really Stephanie logging in, and I am really the person who is authorized to create the profile for Alessandro, because you want to make it easy for people to join the network.

B.) Also, you don't want too much privacy, because the more information revelation you elicit, so the more incentives you create for people to share data, the more valuable is the network—to you if you are the manager of the network because you have data that you can resell or study for marketing trends, and for the users because the more data they see about other users, the more points of contact they find with those other users.

The problem becomes to find the balance where you put little security and little privacy without making *too* little, because you don't want to end up on the front page of The New York Times because some hacker penetrated your system and downloaded the private data of millions of users and so forth. So the issue is how much you can push the envelope and how much the users are willing to accept, and what happened with Facebook was very interesting in this regard.

Stephanie Losi: Can you talk a little bit about that?

Alessandro Acquisti: Yeah, there was this new initiative out there, the Newsfeed, in which your profile would show to visitors a kind of chronology and history of the actions you had recently taken on the system. For example, you had just made a new friend three days ago, you have uploaded some new information one day ago, and so on and so forth. And these trigger very, very strong reactions among Facebook users, which forced the company itself, including its founder, to publically address the issues and somewhat step back by making the feature not a default but an option.

What is interesting to me is that this information was available before, but it was not so easy to access. By making it so easily available, you have a change which is a quantitative change in the system, which makes a qualitative change in the perception of the privacy of the users, because now the users realize—they have a very visible, very clear way to realize how little privacy they get. It's kind of a stalking machine. So what I find interesting is how at that moment it's a moment of awareness, of waking up. To show—they can show the users what really can be done with the data and how visible and exposed the data can be.

Part 3: Lessons Learned and the Future

Stephanie Losi: Okay, so this was about aggregation really. I mean, the data was available before, but now it was available in a form that was easily accessible to anybody, and so this seems like a case where, you know, the company found that the users reacted because it had crossed a certain threshold. And so I guess I would ask you, what can business leaders—how can they apply the findings of this research to their own customer-facing operations, you know, convincing customers to disclose information while also ensuring customer data security and privacy? How can a company know where it should draw the line?

Alessandro Acquisti: It turns out to be, I believe, that it's pretty easy to convince users to provide information. In general, it's much better to be up-front and tell the user, "We would like this data," and maybe even offer something back, because studies have shown that users give away that for very small rewards, so you don't have to offer gold. You just offer a few cents, and users will be happy. Or you can just offer the option to reveal or not to reveal, and many users will end up revealing.

So users get angry when something is done without their consent, and this may be explained for different reasons—one of them, I feel, is the sense of entitlement that all of us feel for our personal information. So that if we put very private data on the Facebook, we are okay with that. If CMU or the institution where we work or study or live puts the same data on a website which has a comparable level of audience and accessibility than the Facebook, we will get angry because we have not authorized that. So the feeling of entitlement explains why people react nastily when they've not been contacted.

Another interesting thing which we found out in our studies is the importance of default settings. So, if we stick to the Facebook, the Facebook is very interesting because actually it's pretty good in terms of how much control it gives to its users in terms of their privacy. In fact, it's very good, it's better than many other social networks. If you're a Facebook user, you can basically control almost everything about your data—who can see each single piece of data and who cannot.

Well, that's really great. The problem, however, is that, as other studies in HCI (Human Computer Interaction) as well as in behavioral economics have shown, is that users tend to like the status quo, the default settings, the way a system starts. It's rare that they change those settings. Which means that even though you may offer the options of setting your preferences, effectively when you choose certain default settings, you, the operator or the manager of the social network, you are basically almost dictating what kind of privacy your consumer will or will not have.

Stephanie Losi: Okay, interesting, so basically—and this I assume would apply to businesses as well, you know, in terms of what you provide to your customers as the default, you're saying as long as you are telling them what you're doing, probably they're okay with it, and it's when you don't tell the customer that then it becomes a problem?

Alessandro Acquisti: Yeah, but I'm saying definitely that companies have a much safer route for using customer data, which is be up-front and be open rather than do it sneakily.

Stephanie Losi: So what do you think are the long-term effects for all businesses of users' increased willingness to disclose private data to sites like this in exchange for prestige or access or service? I mean, do you think that users—at some point there will be a backlash among users, or do you think that that will be more of an isolated per-user occurrence, you know, a user might say, "Oh, I didn't realize, you know, how much information I was giving away, I should back off"? So, I mean, how much do you think companies can collect from customers without triggering any kind of backlash?

Alessandro Acquisti: It seems that they can collect a lot, and they can collect more and more because what I'm noticing—and here I am kind of making an hypothesis—is that privacy invasions trigger a desensitization towards privacy rather than an increase in sensitivity toward privacy. What I mean is that in an environment in which there is continuous information revelation from this sharing of personal data, then the more we live in that, the more we get used to that.

You know, there are these studies in the social psychology literature which focus on how it is behavior which influences attitude, even more sometimes than attitude influences behavior, right? So it's what you do that changes the way you think about things rather than how you think about things that impacts the way you act. So the more you live in an environment in which it's normal to reveal—you grow up with mobile phones, and you continuously are on some kind of system which leaves a data trail, an electronic dossier about what you're doing in every single moment of your day—well, the more we see that, the more we are probably going to assume that that is in fact normal and adequate, and therefore the less sensitive we probably become to further information revelation. Which means that—and again, these are just hypotheses—it could be that in the long

term our sensitivity towards privacy will get more and more reduced, which means that we'll see even further information revelation or information appropriation by companies or organizations.

Stephanie Losi: So what do you think is the biggest threat right now to online privacy?

Alessandro Acquisti: What are the great threats to privacy? One is this: the fact that we are giving personal information which can be used to decrease the trust online and to increase the probability that you fall for attacks by scammers. And the second threat is the one I was mentioning earlier: the fact that as a society we are going to change our perspective on the value of our personal data. A few years ago you would go to privacy conferences and people would talk about, "Well, sooner or later people will understand when there is a privacy Chernobyl how important their information is." I'm afraid that this may never happen because rather than a privacy Chernobyl, what we will see is a slow but continuous erosion of the balance of power between you and other entities which can have information about you that you don't even know they have. So rather than one big boom scandal which will wake up everybody, it's more like a continuous progressive erosion that may not even wake you up.

Stephanie Losi: Okay. Thank you very much, Alessandro. I appreciate your time.

Alessandro Acquisti: Thank you.