# CERT's PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

## Privacy: The Slow Tipping Point

**Key Message**: A trend toward more and more data disclosure, as seen in online social networks, may be causing users to become desensitized to privacy breaches in general.

**Executive Summary**

Corporations have long feared privacy breaches — inadvertent disclosure of customers' or employees' personal data. They worry that such breaches could harm their reputation and the bottom line. However, a surprising paradox is that if individuals are asked up-front to reveal the same data, they likely will do it with few qualms.

In this podcast, Alessandro Acquisti, a Carnegie Mellon professor whose research focuses on the intersection of privacy and economics, discusses some of his findings and hypothesizes about how the trend toward more and more data disclosure may desensitize people to the loss of their privacy.

---

**PART 1: THE ECONOMICS OF PRIVACY BREACHES**

**Privacy versus Economics?**

Privacy and economics are not mutually exclusive concepts. Often, privacy invasions have economic roots.

For example:

- What are the costs to companies of breaches?
- What are the costs to consumers?
- What are the incentives that drive people to reveal so much about themselves?
- Conversely, what are the incentives that may prevent people from revealing information?

**Some Cost Surprises**

In terms of costs to companies, a recent study found a statistically significant negative reaction by the marketplace to privacy breaches.

However, this reaction is short-lived.

After a few days, the market value of the company returns to pre-breach levels.

This is interesting when combined with the trend we'll talk about next: the increasing willingness of users to reveal their own private information.

---

**PART 2: THE EVOLUTION OF USER ATTITUDES**

**The Illusion of Privacy**

Users are increasingly willing to reveal their private information. This is especially true in online social networks, such as Facebook, where data revelation is the name of the game.

Users may be willing to reveal their privacy because social networks feel like bounded communities; however, they

are really not.

In fact, they are virtually boundless.

For example, in Summer 2006, it came to light that employers at some corporations were checking the Facebook profiles of some applicants. They were doing this through alumni or other students who were members of the Facebook community.

Information provided in online social networks can effectively be considered public data.

**A Delicate Balance for Data Collectors**

From an economic perspective, in online social networks, there appears to be an incentive to have poor privacy and security almost by design. Why?

**a.)** You don't want overly strict security in terms of registration, for example in identity checking, because you want it to be easy for people to join the network.

**b.)** You don't want too much privacy, because the more people share data, the more valuable the network becomes. Network owners can resell or study the data. And users of the network can use the information to find more points of contact with other users.

The problem is finding a balance. You don't want to end up on the front page of *The New York Times* as a hacker attack victim, with millions of users' personal data disclosed.

So the issue is twofold:

- how much you can push the envelope
- how much users are willing to accept

**When the Balance Tips**

For example, in Fall 2006 Facebook introduced the Newsfeed, which listed on a user's profile actions that user had taken recently, such as adding friends or uploading information.

This sparked a strong reaction among users that forced the company founder to address the issue publicly and make the feature not a default but an option.

One interesting point is that this information was available before, but it was not **easily** available.

When the information became easily available, users realized how little privacy they had.

That moment was a moment of awareness, of waking up, for many users.

---

**PART 3: LESSONS LEARNED AND THE FUTURE**

**Learning from Facebook**

How can business leaders apply these findings to their own businesses, convincing customers to disclose information while also ensuring customer data security and privacy?

It's pretty easy to convince users to provide information. The important thing is to do it up-front. Perhaps even offer something in return. Studies have shown users will give away their data for very small rewards.

The key is: Give users the option to reveal or not — many will choose to reveal their data.

Users get angry when something is done *without* their consent.

**Mind the Default**

It's also helpful to recognize the importance of default settings.

For example, Facebook actually gives users a lot of control with regard to their privacy — but users often stick to the default settings.

Effectively, when you as an operator or manager choose the default settings for users, you are dictating the level of privacy most of them will have.

**A Desensitized Future?**

Companies can collect more and more data than ever before.

Hypothesis: It may be that privacy invasions trigger a **desensitization** toward privacy rather than an increased sensitivity.

The more we spend time in an environment where there is continuous information sharing:

- the more we get used to it
- the more we assume it is normal
- the less sensitive we become to further information revelation

So, in the long term, our sensitivity toward privacy could become even more reduced.

A few years ago, at privacy conferences, people used to talk about expecting a "Privacy Chernobyl" that would make people understand how important their personal information is.

But that may never happen. We may instead see a slow, continuous erosion of the balance of power between consumers and entities that have information about them.

**Resources**

Acquisti, Alessandro; Friedman, Allan; and Rahul Telang. "Is There a Cost to Privacy Breaches? An Event Study." Twenty Seventh International Conference on Information Systems, Milwaukee 2006, and Workshop on the Economics of Information Security 2006. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf

Acquisti, Alessandro, and Ralph Gross. "Information Revelation and Privacy in Online Social Networks." Forthcoming in Proceedings of the 2005 Workshop on Privacy in the Electronic Society (WPES 05). ACM Press, 2005. http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

"The Economics of Privacy" website, maintained by Alessandro Acquisti. http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

---