From: Jerry Kickenson
To: privacyeng
Subject: Privacy Engineering Objectives and Risk Model -Discussion Deck
Date: Sunday, September 14, 2014 4:55:32 PM

I won't be able to attend the workshop. Comments on your questions follow.

I think this is a great exercise that can help systematize specification and design thinking around privacy!

- Privacy Engineering (slide 4): Is this definition helpful?

It is helpful. Rather than a list of harms to be avoided (the list would have get even longer) you might state "violations of privacy, including intrusion of solitude, appropriation of name or likeness, disclosure of private information, and putting one in a false light" (these are legal views of privacy violations).

• Privacy Engineering Objectives (slides 8-10): Are these objectives actionable for organizations? Are there any gaps?

> Yes, they are actionable.
>
> Predictability - "reliable assumptions about the rationale" seems a bit weak. Why only rationale, and not assumptions about the actual use to which private data is put?
>
> Manageability - there is nothing about who is authorized to modify personal information. Shouldn't this be the person to which the information applies?
>
> Confidentiality - by reusing the security engineering view of confidentiality, the definition allows divulgence of personal data as long as an "authorized" entity does so. For privacy engineering, confidentiality should be associated more closely with the individual. For instance, legal view would prohibit any action that "publicly reveals truthful information that is not of public concern and which a reasonable person would find offensive if made public". Whether that action was "authorized" is not relevant.
>
> What I find missing is an objective that addresses intrusion, like surveillance, or misusing name or likeness or putting someone in a false light - would all this be part of predictability objective?

• System Privacy Risk Model (slide 13): Is it constructive to focus on mitigating problematic data actions?

> Yes, it is constructive.

• System Privacy Risk Equation (slide 14): Does this equation seem likely to be effective in identifying system privacy risks? If not, how should system privacy risk be identified?

> "System privacy risk is the risk of problematic data actions occurring" ==>
> "System privacy risk is the likelihood of problematic actions occurring with data

considered private in context"

I don't think system privacy risk is a simple sum, but rather more of a risk product (likelihood x impact/harm), where impact/harm is a function of the sensitivity of the personal data within the context. So:

System Privacy Risk = f(Personal Information Collected or Generated, Data Actions Performed on that Information, Context) where

f = Sum over all problematic data actions [(Sensitivity of Personal Information within the Context) x Likelihood of Data Actions Performed]

- Context (slide 16): Are these the right factors? Are there others?

I'd see context as the reasonable expectation of the individual with respect to the service or system. So, "the extent to which personal information under the control of the system is exposed to public view" is certainly a factor (as is "how public", that is within a community of registered users, an organization of employees, the entire Internet), "the relationship between individuals and the organization that controls the system", and "the types of personal information that is foreseeably necessary for the system to process or generate in order to provide the goods or services". I'm not sure about the others. Additional factors of the context might be:

- how the personal information relates to the system's purpose or service
- how the individual is identified - user name, verified identity, pseudonymously, anonymously?
- existence of explicit agreements or contracts, and are those agreements or contracts reasonable and usable given the type of individual

- Problematic Data Actions (slides 18-24): Are these actions functional? Are there additional ones that should be included?

Looks good to me.

- Harms (slides 26-29): Are these harms relevant? Are there additional ones that should be included?

Listing harms is not so relevant, if the risk approach is to reduce likelihood of problematic data actions, not directly of harms. It is not necessary to try to list all the possible harmful consequences of violations of privacy - I think that's been done to the point where it is accepted that violations of privacy should be avoided.

--

Jerry Kickenson

SWIFT   The global provider of secure financial messaging services

c: 240-839-1075

Facebook LinkedIn Twitter

e: jerry@kickenson.info

w: www.kickenson.info

Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety. (Benjamin Franklin)