A Privacy-Enhancing Eco-System (or a Privacy Risk Reduction Framework & how to make organisations care)

Robert Navarro, Managing Director, Sapior Ltd.

Valuing Personally Identifiable Information

There is a risk of a major breakdown in consumer trust of new electronic ways of interacting and the resulting proliferation of databases. Addressing this risk will require an adjustment in the way organisations and individuals treat Personally Identifiable Information (PII). Just as a bank protects the financial assets of its customers, so it must shield customer data against breaches of privacy. Incentives, market discipline and supervisory review are all components of a Privacy-Enhancing Eco-System with the best chance of aligning society's actions with what is ethically acceptable.

Privacy Breach Basics – what makes data identifiable

Identifiable data lies at the heart of all privacy breaches. If the data can be connected with individual people it is identifiable. If it cannot, no privacy breach can occur. What makes data identifiable can be described by two factors: data ambiguity and volume.

The more ambiguous the data is, the more private it is. Does a data item apply to one or more people? Billing records are rarely ambiguous whereas loyalty cards are often only unique at the household level.

The greater the volume of data connected to an individual, the easier it is to identify from background information. Pay-as-you-go calling cards are not identifiable by the times or duration of a call until they've been used for some weeks or months.

Hence storing ever more information linked to a given individual enhances the identifiability of that data and therefore increases the core vulnerability to privacy breaches.

A Self-Sustaining Privacy Eco-System

The benefits of using PII should be matched with a cost to the same stakeholder in a self-correcting system that adapts to societal changes.

Measuring the problem – A risk assessment framework

Centralised, commercial and/or academic breach tabulation and classification are required to assess scale and nature of the problem and to determine the efficacy of any privacy system.

How a data holder functions and in what context it operates affects its risk of a breach. Policies, staff training and deployment of Privacy Enhancing Technologies (PETs) are clearly part of the solution. The key is to know how much of these are needed to reduce the illicit identification risk below an agreed acceptable level. This raises the question of what is acceptable and how the risk can be measured in the first place.

Under the Basel II international banking initiative, if banks measure and model their "operational risk" they are rewarded by being allowed to set aside smaller amounts of cash for bad loans. Similarly, data holders that measure their illicit identification risk and actively reduce it should get an advantage over their competitors that do not.

Privacy Breach Pain

Nothing focuses the mind more than cash. Breach notification has its place, but will not suffice on its own. As notification volumes increase, only the worst offenders will be visible. Fines are needed for egregious or negligent failure.

Additionally, mandatory financial "provision" proportionate to an organisation's illicit identification risk is proposed. This could be a capital set-aside or an insurance premium purchase. This pool would then pay for breach rectification (fines or restitution).

Good Privacy Management Dividend

As with a market-based system, there must be some financial benefit for acting ethically. Where data holders reduce the risk of identification (via data deletion, PETs, staff training, Kitemarks, etc.) they will qualify for a smaller mandatory "provision". Kitemarks or ISO standards also serve as vendor trustworthiness indicators. These enable consumers to make rational choices thus rewarding vendors that take privacy seriously.

For more information, contact:

Sapior Ltd.
t: +44 (0)20 7060 2965
f: +44 (0)20 7748 0970
www.sapior.com