Microsoft

Evolving Privacy Models

There is a growing focus among privacy experts on the need for new data protection models, as the generation and use of data continues to grow.

Today, under our current model, much of the responsibility for privacy protection rests with individuals, who are expected to read and make informed decisions based on the numerous detailed privacy statements and disclosures of online service providers. It is absolutely essential that organizations be transparent about their data collection and use practices. However, if we are to achieve meaningful protection of personal privacy, while benefiting as a society and as individuals, from the ever growing uses of data, new models should be explored; ones that retain the value of notice and consent in appropriate ways while shifting the focus of data protection to the use of information by accountable organizations.

Today's privacy statements often contain too much or too little information for individuals to absorb if they are to make meaningful privacy choices. For example, research conducted in 2012 revealed that many privacy policies total more words than Shakespeare's Hamlet or Macbeth.[1] Other research suggests that people don't typically read these statements. Many people simply click through to "agree" with the terms of privacy notices without reading and understanding the terms. If people's privacy expectations are not based on the notices, then our overreliance on notice and consent may in fact be creating situations where their privacy expectations do not match the reality of modern data collection and use.

Even if we were to assume people typically read all privacy statements presented to them, there are many scenarios in which there is no practical place to offer notice. For example, in the world of the Internet of Things, data about an individual may be collected automatically from sensors typically present in an individual's environment. These sensor experiences generally do not have a screen or interface to enable a notice and consent experience, and in many scenarios there will be no realistic opportunity to provide notice.

There is another challenge in our current data protection model relating to the specification of data use at time of collection. Today's technology-enabled data analysis and use are providing rich value-added scenarios and services to consumers, businesses and society in general, but there may be the potential to unlock additional value in data that was not contemplated at the time of collection. As Scott Chaney wrote in the TwC Next Paper[2], "the true value of data may not be understood at the time of collection and future uses that have significant individual and societal benefit may be lost." Examples of this concept were highlighted in Viktor Mayer-Schönberger and Kenneth Cukier's book[3] on Big Data. Tremendous societal benefits can come from new uses of existing data. One such example was recently demonstrated through search query research that identified adverse drug interactions. In research published in 2013[4], Microsoft combed through 100 million de-identified search queries from 2010, and was able to confirm a previously unpublished drug interaction (hyperglycemia) resulting from individuals taking two commonly prescribed drugs: paroxetine (an antidepressant) and pravastatin (a cholesterol-lowering drug). Hyperglycemia is high blood glucose and occurs when the body has too little, or can't properly use, insulin. Temporary hyperglycemia is often nonthreatening. However, chronic hyperglycemia can result in serious complications, including damage to kidneys, retinas, feet and legs, as well as neurological and cardiovascular damage. Most severely, failure to treat high hyperglycemia can result in a diabetic coma, which can be life threatening.[5] A Stanford study

1 Reference, 2012 data: http://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/

2 Trustworthy Computing Next

3 http://www.amazon.com/Big-Data-Revolution-Transform-Think/dp/0544002695

4 http://research.microsoft.com/en-us/um/people/horvitz/Pharmocovigilance-signals from the crowd.pdf

5 Source: American Diabetes Association

formally reported the adverse drug event in 2011, but this research demonstrates that by using and analyzing individuals' search data in real time or close thereto, dangerous drug interactions might be detected in advance of the FDA Adverse Event Reporting System, ultimately saving lives and improving drug safety. Now, hypothetically if this same research used identified data and specific individuals could be notified of the potential for hyperglycemia based on their search terms, would that notification be appropriate? Would society be more concerned? Would the benefit to the affected individuals outweigh the heightened privacy risk?

A growing number of privacy leaders recognize that we must evolve our current protections and address the shortcomings of the current model by focusing less on the collection of data and more on the use of data. This does not mean collection limitation is unimportant; rather it's not something we can depend on as heavily in today's data-driven society.

It is also essential to underscore that shifting the focus from a "consent" model to a "data use" model does not mean eliminating the concepts of notice and consent. Individual participation and consent remain critical parts of the privacy model. Indeed as the models evolve, these should rise in prominence in cases when individuals are confronted with data use or collection requests that are outside of the norms set by societies. Similarly, increasing data protection's reliance on use and accountability programs does not mean eliminating all other information principles outlined in the Organization for Economic Cooperation and Development Guidelines. Rather, this model adds tools to the data protection arsenal that can help cover gaps which are currently difficult to govern.

To balance a lessened focus on collection and consent, we believe that privacy frameworks need to evolve with a greater focus on organizations being held accountable for responsible use of information, through formal assessments of the risks to individuals of particular information uses. This will shift much of the burden from the individual to the organization and provide more assurance that individuals' privacy rights and expectations will be upheld in the next phase of the information age.

Late last year two papers were released with an intent to advance the dialogue and outline important new thinking on this topic: "Data Protection Principles for the 21st Century" and "Data Use and Global Impact." The visions outlined in these papers start with the premise that we need to build on existing models and shape them to fit our ever-advancing and complex digital ecosystem.

As we think through this evolution, there are significant unknowns as well as exciting opportunities for us to come together as a community and design a future of more meaningful data protection. Collectively we should focus on how to enable accountable organizations to leverage the economic and social value of data use in a world of big data, with privacy models in place that protect the individual's privacy needs. As we collectively work to evolve today's privacy models we will need:

1. **Public-private partnerships** that envision and identify the future of privacy models;
2. **Evolved legislation** that supports new frameworks for data use;
3. **Evolved business processes** that incorporate risk-based assessment and accountability for data protection and use;
4. **New technologies** that assist in data management and consumer engagement; and
5. **New enforcement models** that are resourced to tackle the challenges of overseeing greater organizational accountability in a data rich world.

There is not yet a clear solution, but as we collectively advance the dialogue across private and public sectors around the world, we continue to generate innovative thinking about a sustainable data protection model; one that provides utility for organizations focused on innovative data use, value to society and consumers and effective data protection.