Engaging Privacy

Round table discussion, 26/2 2016.

Introduction

The following document provides a summary of the February 26 Engaging Privacy roundtable event at SICS Swedish ICT. Participants were invited to discuss how privacy issues can be used as an opportunity and competitive advantage for the Swedish ICT industry.

In summary, the participants agreed that there is a trust gap between customers and companies when it comes to the collection and processing of personal information, and that the gap limits innovation in the ICT sector. Not addressing that gap might drive people away from products and services, or push governments to regulate industry in such a way that innovation and growth becomes more difficult.

The representatives also agreed that the competence for dealing with privacy related questions, in development as well as in customer relations, might not be at a sufficient level in all organizations. There is a lot of room for improvement in making more conscious design choices, and to raise the attention to privacy among engineers and developers in their everyday work activities.

Finally, the participants took inspiration from how Volvo managed to brand themselves as one of the safest car brands, and how the Euro NCAP rating system became one of the most important branding tools for car manufacturers in the safety segment. Being able to prove a high standard of privacy management might sway the entire industry to follow if that proves valuable for consumers as well. As another example, a parallel was made to banks and how they enjoy an extremely high trust rating in Sweden when it comes to privacy - an example that led to a discussion about how regulated markets and trust affect each other, and how that affects innovations.

Setting

Commonly expressed phrases like “data is the new oil” and “the home is the new Texas” clearly illustrates the interest and market value of collection and processing of personal information. But while the practice of ubiquitous data collection and use in web and mobile settings surge, end users’ attitudes to data collection remains negative, although also fragmented and contradictory. In a recent study (in press), 58 % of the Swedish population express a negative attitude towards the increase of data collection online, and only 19% express a positive attitude. Banks are the only institution that more than half of Swedes have confidence in when it comes to management of collected data, and 45 % of the Swedes claim to have become more restrictive with sharing personal information online during 2014.

While the latter claim most likely correlates poorly with real sharing practices, it is a good indication of how Swedes feel about data collection in general.

In media and the public debate, privacy is almost exclusively described in limiting terms. Data sharing practices are described in terms of violations and infringements of individuals' privacy, sometimes even as offences and insults. When describing means for upholding privacy, it is often done in terms of hiding and concealing personal information as well as protecting, limiting, and stopping access to the same. It is either data, and thereby violations of privacy, or no data, therefore privacy.

This is unfortunate for two main reasons. First, it diminish and blur the many merits and opportunities with large scale data collection and processing for a great number of reasons and purposes, not least with regard to societal challenges with sustainability in various forms. Second, it portrays a situation in which sharing of personal information equals loss of privacy. This is simply a false assumption. There are many examples of situations where people share personal information in various forms while not impeding on their privacy the slightest bit. Privacy is not violated unless the agency of an individual with regard to collection, processing, or use of personal information, as well as the setting in which this takes place, is limited.

However, promoting agency is not straightforward and it requires attention to many different mechanisms for its fulfilment, like: engineering practices of different kinds, including data security and interaction design; purposive data collection, processing, and dissemination; a clear value proposition as a foundation for accountability; informed consent in its both interpretations; and continuous communication promoting transparency and traceability of data collection and use practices.

Challenges for the industry

Many of the participants shared the view that there is a gap of faith and trust between the general public and products and services from the ICT-sector. In many aspects, that trust gap is the main limitation for data driven innovation in the sector. If there is a lack of trust in how technology and service providers manage individuals' personal information, people will eventually either abandon the technology and services or call for legislation in order to get a level of protection or ethical treatment that they are comfortable with. With that in mind, the industry must find voluntary way to bridge the trust gap, or risk losing their independence and autonomy.

While not all regulation is harmful, there is the risk that legislation championed by fear and mistrust might put a wet blanket over future innovation capabilities. The German push on data protection issues within the European Union is one such example where mistrust has led to political requests for a more rigid legislative structure. On the other hand, one possible reason why banks are the most trusted institution regarding the management of personal data might be that it already is a highly regulated industry, with relatively little room to innovate new products and services.

One reason why the trust gap has been growing might be that the industry is moving at a quicker pace, innovation-wise, than it is actually capable of managing properly in an ethical sense. Most actors are extremely good at getting their products online, to start collecting and process data. The downside is that they do not have time to properly discuss how and why to collect and process data and how to build trust with the consumers of the products and services. It's a question of maturity within industry as a whole as well as in individual corporations. Another possible reason is that smaller startups are pushing work with trust and privacy issues into the future because they have little to lose and much to gain by just focusing on the core technology at hand—a strategy that may be successful for individual companies in the short term but clearly problematic ICT sector as a whole in the long run.

Government authorities and the public sector also need to assist in ensuring that the trust for data collection and processing can increase over time. Unfortunately, many authorities are locked in rigid structures that make it hard to comply with or help more flexible models that exists in enterprises. One of the leading authorities in the area in Sweden, Datainspektionen (The Swedish Data Protection Authority) is already understaffed and will become increasingly so when the new data retention regulation comes into play in 2018.

Knowledge about privacy enhancing measures have to be shared through the companies, so that developers and marketers alike know how and why information is collected and processed. While the public tend to worry mostly about malicious breaches of collected data, the most common risk is generally either malpractice or bad choices by employees or managers when it comes to treatment of persona data. How does a company make sure that all employees are aware of risks and vulnerabilities related to privacy and trust issues? How do companies make sure that product development engineers as well as customer relations specialists have a good grasp of privacy and the implications of personal data usage? While some representatives of the industry have started dealing with this challenge by giving in-house lectures and seminars, others feel that this may be one of the biggest obstacles.

Connected to this lack of privacy and trust awareness is another risk, namely that knowledge about what kind of data and whether that relates to individuals is lacking, even on an oversight level. This may be due to lack of routines and processes for how to extract data upon customers' requests, or there might not be a plan for how to deal with new data sources. Without having a long term strategy for data, being proactive within the field of trust and privacy might be difficult, even if there is a well-developed understanding of the challenges involved.

Finally, another multi-faceted challenge is how to a good practice for gaining informed consent. Informed consent can't be about simply agreeing to a vast document of terms and conditions, instead it contains two profound ideas that must be accommodated. Informed consent means that not only should information about what a contract or agreement contains be available to the customer, but it should also be presented in such a manner that the customer can fully understand what it entails and thereafter be allowed to either agree to the terms, or choose to not use the service or product.

Strengths in the industry

There are, however, strengths that are inherent both in Swedish industry and in Sweden as a marketplace. Sweden has, in general, a population that has a large degree of technological competence and Swedes are often early adopters of new technologies. At the same time, Swedes have a high level of trust, especially in public institutions, that can be translated into digital markets as well. These strengths provide a solid base to move the market to a more privacy enhancing position for the entire market and dealing with the problems of establishing adequate privacy and trust practices head on.

Despite widespread concerns regarding privacy issues, people still share personal information to a fairly large extent. Most seem to feel that in the current tradeoff between surveillance and the ability to use certain services and products, the value of use currently outweighs the lack of trust. That's not to say that the relation can't change in the future. However, it does mean that there is room for testing and experimenting with new solutions to bridge this trust gap. There is also a possibility to further highlight the benefits of sharing data, and how to use those benefits to create trust. After all, people want to use the internet, and the ICT sector wants to use data and deliver better services online.

Trials with customization of and transparency in data collection settings have also begun appearing in different services and products and we are getting early insights into how they are received. Examples that were mentioned include the ability to customize feeds and rights on Facebook, and the increased customization that Windows 10 implemented, although there was a backlash in that implementation that is interesting in itself to study. Having a continuous dialogue with customers might also improve an understanding of which privacy issues that needs to be addressed, and how to better deliver services such as portability of data, which might become enshrined in law in the near future.

Large companies have the possibility to set a precedent for smaller actors by providing either guiding examples, or advice on how to manage privacy concerns and create better policies. Smaller actors can acquire a huge amount of information very rapidly today, but have less scruples about security and proper policies than the bigger actors do. It is therefore vital that the larger actors take the initiative in moving the issues forward so that smaller actors may follow.

Ways forward

An important step forward is to find the balance between giving people power over their individual data, while not seriously crippling businesses that use the data. That the individual owns her data is a fundamental principle that many user interest groups uphold, and that will be encoded into law with the new General Data Protection Regulation from the European Union that will most likely come into effect in Sweden in 2018. Making it possible for all personal data to be ported out of a system makes it necessary to tag such data to each individual as well. If metadata is supposed to be included, since it can sometimes be used to identify persons and thereby fulfills the requirements for being personal data (according to Datainspektionen), many it-systems will have to be reconfigured down to their cores.

Moving forward with the initiative, one problem that was mentioned consistently throughout the discussion is how to measure success, and what we want to achieve. Measuring is beneficial in that it provides a way to view your progress, but measuring also makes you adapt to the thing you are measuring so that you become great at that one thing. We want to decrease the trust gap between customers and the industry in regards to privacy. Measuring small parts of that relationship might hamper the overarching goal, while measuring only the overarching goal might not show any form of result even over a three year period. Since the initiative has an initial runtime over three years, seeing if overall trust in digital services increases can work as a measurement.

The participants discussed what the main competences of the initiative ought to be. Providing a platform for a discussion, disseminating research, providing input into government investigations and providing support for startups were the roles that were highlighted.

Jacob Dexe
Administrator, Engaging Privacy initiative.