

THE SWISS STYLE

RESONDING TO THE NEW REALITY – by Anne Réthoret and Ita McCobb



THE RIGHT TO DISAPPEAR:

regaining control of your ID and personal data

Data protection agencies are demanding proof that measures to protect online consumer data have been put in place. Meanwhile, sharply different attitudes towards privacy are tearing the map apart. “Suddenly social networks and other businesses are compiling data on a daily basis (whether we want it or not) and they are totally unregulated,” points out Carlos Moreira, CEO and founder of WISeKey, a leading Swiss eSecurity company. “There are no international standards and no international organization is taking decisions to handle and regulate these issues, so we have an environment which is open to all kinds of abuse.”

In the past year, run-ins between regulators and the Big Four – Google, Microsoft, Yahoo and Facebook – on the use of private data have become increasingly frequent. Privacy has become an unequivocally controversial issue. More importantly, while data flows around the globe, privacy laws and rules have become a matter of geopolitics. Despite such differences, the current situation in Europe is that regulations are inspired by the conviction that data privacy is a fundamental human right and that individuals should be in control of how their personal data is used and by whom.

Antiquated or non-existent legislation

The flagship Data Protection Directive came into effect in 1995, before firms such as Google, Facebook and Twitter were even created. However, in America the US Federal Trade Commission has only recently published a “Do Not Track” proposal as part of a framework to protect against the commercial use of consumer data.

A privacy and security researcher cited in the *International Herald Tribune* in December, said that the majority of consumers do not have privacy software and that the use of privacy options in most Internet browsers does not make much of a difference. This is due to the fact that web browsers are partly supported by advertising networks.

When companies such as WISeKey started trying to sell the CertifyID Personal eID integrated within Microsoft Office, the market response at the time wasn't what one would expect. Aside from digitally permitting the user to sign and encrypt Word documents, Excel spreadsheets, PowerPoint presentations and Outlook e-mails, CertifyID also secures e-mails and documents using strong encryption. It aims to protect users from identity theft and data leaks and has WebTrust accreditation and uses a globally trusted personal X509 digital certificate.

The commercialization of this product coincided with a tougher Internet regulation on consumer data in the United States last May. However, at the time, the US media regulator agreed that the government would show restraint under a new plan to regulate providers of high-speed Internet. This happened in response to the panic that hit investors on Wall Street at the prospect of tougher regulation.

David and Goliath

“One of the topics of the WEF Meeting in Davos this year will be focused on rethinking the personal data initiative in a ‘think global, act local’ manner”, explains Carlos Moreira. Currently there are no international standards for personal data and consumer data protection and the Geneva-based founder of WISeKey does not believe there will be.

“Although the Internet is global, regulation is not applicable worldwide. It is now up to the various governments to protect their Internet users. Last month the European Union launched a new directive stating that there is a need for a delete button on the content we add to the Internet. Meaning that if you have been using social networks for months or years and your status changes, then maybe the data that you have compiled is no longer accurate and you may want to opt out of the social networking site. In this case you will need a delete button for your personal data. Currently, if you opt out of a social networking site the data on the site remains the property of the social networking organization.”

This protection is currently available in other industries but it is not yet available in social networking. The philosophy of rethinking personal data is not a technology issue because the technology already exists; the problem is that the data does not belong to the individual concerned. When you transfer data to Facebook or Twitter or indeed any other social network, you are giving your data away for free. But if you give something away for free, how can you recover it later? “There is no method of recovery,” says Moreira. “Once you give something away for free it is no longer yours – it belongs to the organization that you gave it to.”

The rethink of personal data has to move forward together, maintaining equilibrium between technology, legislation, standards and geopolitical focus, which means that each country will have a different way to organize their data. China’s approach is different to that of Europe’s which is again different to the American’s, which means that there is not one solution to suit everyone. “Actually, if we don’t find an international mediation for this then the Internet will be divided into different internets which will no longer be compatible. The Internet started as a network of computers, now it has become something totally different, a network of people. Facebook is now the 4th largest “virtual country on earth” and has more personal data on their “Friends” than any government on earth has on their citizens. If this is not regulated you will have Russia, China, Brazil, Europe and America each having their own Internet to protect their “citizen data”. This is already happening with Facebook being banned in China. We will find ourselves going back to the ’80s when we had an Intranet with big walls to block people’s access and we will destroy the original spirit of openness on the Net and WWW,” comments Carlos Moreira.

The right to disappear

While the Directive's core principles issued in 1995 remain valid, modern technology and globalization pose new challenges to data protection. These changes have led to questions on whether the existing EU data protection legislation can still fully and effectively be relied on or whether reform is needed. For instance, how do we know what happens to our personal data when we book and board a plane, open a bank account, make a payment, make an IP call or share photos online? How is this data used and by whom? How do we permanently delete the PII (Personal Identifiable Information) on social networking websites? Can we even transfer our contacts and photos to another service?

To address these issues, the EU Commission held public consultations in 2009 and stakeholder consultations throughout 2010. In 2011, the Commission will propose a new general legal framework for the protection of personal data in the EU, covering data processing operations in all sectors and policies of the EU. The European Parliament and the Council of Ministers will then negotiate and is expected to adopt the Commission's proposal.

“We believe that PII needs to be strongly protected as this is the most sensitive information and allows the person to be tracked. The only way to do this is by encrypting your PII and defining standards that clearly give the ownership of the PII to the user and not to the service provider. If this is done, then the PII is associated with your Digital Identity which can then protect the personal data, as it belongs to you,” says Moreira. “If your data is associated with your PII, and if your identity is encrypted, the data can be activated or deactivated the moment your identity wishes and without any need for a decision from anybody else.” So if you put your pictures on Facebook and those pictures are linked to your digital identity, which is outside Facebook, the moment you change the privileges associated with your digital identity, those pictures will be deleted. WISeKey has also developed a technology called WISeID, which has the ability to **protect and control users’ documents or media** that are posted on the web. These objects are associated with a remote server validation system so that whenever an object is accessed from the web, validations are carried out (revocation, status, validity check...) and a key accessed to decrypt and view the object (via a plug-in). The WISeID user has total control over the lifecycle of the objects and can at anytime revoke access to them through WISeID. By doing so, these objects posted on the web will no longer be readable by anyone. WISeID runs on mobile phones, iPads and many other devices and allows you to put all your confidential data into an app format. You can put your Facebook/social network description, your credit card accounts, and your bank account details into this format – all in an encrypted environment – and the application allows you to keep control of your data yourself, and is encrypted with your own identification. You can then put content wherever you want – the application will allow you to go to Facebook or anywhere else and activate your profile there – but the day that you want to deactivate that profile you can deactivate it. This is referred to in the new EU Directive as “the right to disappear”.

Embedded in legislation

WISeID means that you don’t need a deactivate button because you never give your identity and personal data to anyone, you just allow the use of it while you are in agreement. “This creates an environment that allows a person to regain control over their personal data,” says Moreira. WISeKey technology is based on International Standards such as those applied by all UN member countries and regulated by International Organizations based in Geneva – it offers, in essence, a de facto legislation which is endorsed by all the countries of the world and can be used as the means of regulating and mediating personal data standards and changes.

We already have International Organizations and treaties on how we can exchange goods. We have organizations, such as the World Trade Organization, which put into place controls over physical goods. But today we have goods (data) which are non-physical goods. We live in an environment where non physical goods, especially data, are becoming as important as physical goods, even more so, and we don’t have any international treaties to protect people from abuse of these non physical goods. We have reached a point where one can imagine a situation in which someone will be storing all the data of the world in one warehouse in one specific country – an obviously unacceptable scenario which is happening now.

“I think there is something which needs to be embedded into legislation,” says Moreira, “something which means that companies of the future do not compromise their customers’ personal data and if they do they are punished by the customers. In the same way as in the car industry, where security has to be there to guarantee the value of the vehicle and the protection of its driver. The equivalent of security in cars has to be standard when dealing with security and protection of data.”

Moreira believes that the drivers of change will be both technology and next-generation companies such as WISeKey. Companies who not only care about the technology business but are more responsible in providing technology and services to customers by showing them how to access the Internet, share their media and have exchanges with friends without compromising their personal data, so that people can use social networking sites in the confidence that their data is secure and will not be abused.

Acting with a little more foresight

Technology is about being increasingly responsible in the way we access data. Companies such as Google or Facebook do not have this concern in their DNA as they were not thinking about it when they were created, but sooner or later they are all going to have to comply with international standards. Approaches like “Let’s solve that problem later. Let’s first create a critical mass and worry about personal data issues later” won’t work anymore. The danger of doing that (after collecting such a huge amount of data) is that by the time you try to solve the problem, you have a structure that makes it impossible, as other forces get involved. You need to embed personal data protection into the DNA of your company from inception.

“Today we are officially in the Web 3.0 era and everyone is trying to act with a little more foresight”, Moreira adds, “and I expect that this next generation of companies will be companies which will, from day one, start thinking of how to protect confidentiality issues.”

In fact what is being planned is a situation where we handle our personal data on the Internet in the same way as we do in private life or we do with our financials– showing our personal data only to the people that we trust. Imagine, for instance, that you meet some people at a cocktail party, you may exchange cards with everyone but you give your mobile phone number to only a few and your home address to even fewer. That is the basis of WISeID: you can disclose whatever you want to the people you trust and you disclose less to others depending on the level of trust – creating the same interaction as we have in everyday life.

As Carlos Moreira emphatically puts it, “The concept of WISeID is that a person has the human right to be anonymous, and technology designers must take this right into consideration.”