# The Future Identity Card: privacy and security for authentic personal data

Gergely Alpár

October 26, 2015

## 1 Privacy in action

Whenever you buy things online, post something on Facebook or Twitter, wander around with your mobile phone in your pocket, you create data. You do this because you need to buy things, you want to communicate with your friends, and you want to be available anytime, anywhere. So, functionality is important.

The data that you create, wittingly or otherwise, is valuable. Your purchase history, your social profile and your location patterns can be precious information from another perspective. The profiles built upon this information that can be extracted are important business resources. So, data is important.

The interesting interplay between functionality and data can perhaps be most clearly demonstrated by considering Google. On the one hand, from a web user's perspective it is an excellent search tool. On the other hand, from the perspective of the advertising companies, Google is an outstanding ad targeting instrument. The former is functionality for users, the latter is data for companies. In fact, we – human beings, aka customers – are the products to be sold in this business model.

Targeting can be privacy invasive. This is well demonstrated by a story about the retailer store chain Target. "[A] man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry, [...] 'My daughter got this in the mail!' he said. 'She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?' " It turned out she had already been pregnant, but her father wasn't aware of that yet.[1]

Privacy has many aspects (including information privacy, bodily privacy, privacy of communications, territorial privacy). Privacy is very hard to define well in our digital world. But, for sure, privacy is a fundamental human right.

There are initiatives for protecting privacy. To implement privacy-friendly services, however, is not easy. A tangible example is the so-called ID cover[2], a new technology to hide certain data items from your passport or driving license when it is placed on the copier. I have a personal experience how difficult it is. Last time I rented a car, I noticed that the assistant at the counter had to use this plastic ID cover before scanning the card. It acted as a mask to conceal

[1] http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[2] https://nvvb.nl/nl/producten/id-covers/

personal information on the card, including my photo. Although the idea is nice, the usage was really cumbersome, making the whole procedure long. This example clearly indicates that in practice it is not enough if there are privacy-enhancing technologies, we also have to make them easy and efficient.

## 2 Identity card

Identity cards are being introduced all over Europe. Some examples include Estonia, Belgium and Germany. The systems are surprisingly diverse in terms of functionality, trust model and privacy features. What is common is that all of these identity cards include a chip, and most of them also have a unique identifier (a public key).

Two popular functions that many identity cards provide for citizens are digital signature and decryption. Using digital signatures, people can sign electronic documents, in much the same way as handwritten signatures. Citizens can write and store contracts entirely digitally. Using decryption, a user is also able to read confidential documents or e-mails sent to this particular person, the owner of the identity card.

Since these purposes are inherently identifying, the use of a unique identifier makes sense. However, a third very important function, to enable citizens to communication and access control easier with the government, may exclude necessary identification. A modern identity card is often marketed as a device that makes all kinds of arrangements more convenient for the citizens. Meanwhile, a side effect appears – seemingly unavoidably. Various kinds of currently separate national databases (tax-related, social security, pension, *etc.*) can get linked to each other. Besides that, all transactions carried out by a citizen become usually linked to each other because of the unique identifiers, and such identifiers, in turn, lead to specific people.

## 3 Authentic personal data

In order to appreciate the problem better, we need to elaborate more on three topics: data, personal data, and finally, authentic personal data.

I. First let us consider *data*. It's fair to say that information is essential in the digital world. Some claim that it is the currency of our age. Moreover, data storage is increasingly easier, faster and cheaper. Not only do we have lots of data, but also search engines make the required piece of information effortlessly accessible.

Data mining and big data are buzz words heard everywhere, but they provide truly powerful tools. They constantly improve search results, predict spread of epidemics, forecast weather, climate change and market trends. Companies decide where to build their next store based on aggregated and analysed data from various sources. Just to mention a few examples.

And data is available for nearly all of us now. Making a small detour to put the Internet and data access into perspective, we clearly see that this was not always like this. While in the first phase of the Internet, from the 60s to the early 90s, Internet wasn't really public. The World Wide Web made it appealing for a broad audience, and from the mid 90s to about 2010 people were willing

to pay a lot, albeit relatively less and less, to connect to the Internet. Their incentive was to have access to the information and the communication enabled by the Internet. Since 2010 we have seen a new trend. The Internet assists so many aspects in our lives that governments and businesses want the Internet to be freely available. The Internet is even becoming a fundamental right[3] in some countries. Google and Facebook are running projects to embrace the entire humanity and to provide access to the Internet free of charge. In my view, in a few years a next phase will come. The Internet will become mandatory. One won't have a choice to access the Internet and to use certain services. It may seem grotesque that in the end the Internet won't be a *possibility* but it'll rather be an *obligation*. Perhaps then many will fight for the *right not to access* the Internet.

II. Second, let us focus on *personal data*. The Circle, a recent fiction book by Dave Eggers, describes an extreme example where data sharing can lead. This book is about a company, The Circle, resembling a combined version of today's Apple, Google, Facebook, Twitter and PayPal. It is worth quoting from the book: "Secrets are lies; Sharing is caring; *Privacy is theft.*" These catchphrases can be understood fully by recognising that information and access to information are crucial in an open society according to this fictitious company. Whatever is happening to you is information belonging to the world. And as such, other people have the right to know about it. Thus, hiding is a sin, privacy is theft.

Although this book may appear to have gone too far, if we look around, we can see that these things are already partly happening. We are, to a large extent, an open book. Business models are designed on profiling people and intelligent services build similarly detailed profiles about all citizens. We know that from Snowden's revelations.

Privacy is endangered. First, personal data is not always kept securely enough. There are hundreds of failures every year affecting millions of people. And not only small companies, but significant ones such as Sony, LinkedIn or Target. Organisations are losing credit card information, passwords, or even medical information. Second, privacy is often viewed as a trade-off with security, resulting in weakening the privacy concern. This view is reinforced by news about privacy-appreciating technologies applied for surreptitious purposes, such as the Tor anonymous communication channel used by Silk Road, and the Bitcoin cryptocurrency used to pay for child pornography and terrorism. Third, privacy is hard to achieve in a digital context. Sophisticated privacy-enhancing technologies tend to be badly designed and hard to use. Finally, privacy means different things in different cultures. Most importantly, Europe's notion of privacy is far from that of the US. Silicon Valley companies consider Europe's fragmented and privacy-protecting legal system outdated.

What exactly privacy or privacy protection is, is under constant debate. Businesses are lost in the legal forest, and they try to follow a sort-of checklist approach to comply with the current legislation. Meanwhile, the EU is busy with creating an extensive law, the General Data Protection Regulation (GDPR) which is hoped to be finalised soon and adopted in 2017.

[3]See, for instance, `https://en.wikipedia.org/w/index.php?title=Right_to_Internet_access&oldid=687076845`.

Additionally, a very interesting community of white-hat hackers, engineers and researchers tries to find ways to rethink the Internet and the whole digital world as we know today. They try to build privacy-enhancing technologies (PETS), including digital money, electronic communication, information storage and credentials. These technologies are supposed to be secure and they provide privacy for the users.

III. Finally, let's turn our attention to *authentic personal data* (which can loosely be defined as certified pieces of information about an individual). In the sea of information it's becoming increasingly hard to trust data. While in certain contexts this is not crucial, it is essential in others. For instance, it is important for businesses to comply with the law, and avoid selling alcoholic drinks for minors. They have to check that the customer is over 18. Also, a government wants to make sure that the one who declares the annual self-assessment tax return, is eligible to do so. Furthermore, travelling is another relevant example for the need for non-transferable validity information. Lastly, without a passport (or an identity card within the Schengen Area) you can't board an international flight.

Passports are interesting for another reason as well. A modern passport is supplied with a chip which digitally stores most of the printed information, including the passport number, the name and the photo. By means of a mobile phone, one can read this data.[4] All of these data items can be called attributes. Note that not only your name and the date of birth, but also your photo is an example of an attribute.

Using the chip and the passport photo, the current passport technology enables offline verification. Users can show their document a let a machine read out the information stored on the chip. Although this process is easy and convenient, it has an important downside. It applies an all-or-nothing approach. Either all your information can be read out, or none. This can be an overkill in situations which should otherwise make use of authentic personal data. For instance, proving that one is over 18, neither a passport number nor a photo is required to be processed.

Studying the attributes further, we can also notice that some of them are identifying, while others are non-identifying. Your passport number is definitely identifying, whereas your date of birth – at a national level – is not identifying. Accordingly, authorisation, the process to gain access based on some attributes, can be identifying and non-identifying. When you prove your name or you log in to a website, you definitely identify yourself, while showing that you're over 18 should not be identifying (unfortunately, this is often not the case currently).

What is the link between a passport and its owner? Clearly, the photo is a link, and possibly other biometric data, such as a fingerprint. Without this, passports could be used by others. However, it is interesting to realise that a photo provides this connection only offline, that is, in scenarios when the owner is physically present at the verification. In an online contexts, there would be no way for the verifier (for instance, a service provider) to check that the passport is actually used by its owner.

[4]Trying it (with *e.g.* the NFC Passport Reader app), you will see that the data items, such as your name and passport number, are quickly conveyed, while the colour passport photo of quite a good quality takes some seconds to read out.

# 4 IRMA

Now, we are ready to talk about the fundamental technology of the future identity card. It is called IRMA, "I reveal my attributes".[5] It enables someone to request and get a card to which they can collect independent virtual credentials; so-called, attribute-based credentials, cryptographic containers of attributes. An IRMA card serves as a digital wallet of credentials, such as a digital identity card, a driving license, a social security card, a mini personal medical file, a student card, a passport or a loyalty card. These credentials are possibly issued by different parties. Attributes can only be extracted by verifiers that are eligible to do so. So, a border-control system can access very different attributes from the ones that a supermarket can see. This mechanism is called *selective disclosure*, and to realise it in practice requires quite intricate cryptographic techniques. The reason for the difficulty can be described as *"authentic randomisation"*. Any other similar systems are based on a unique identifier or at least some constant information. Every time when you use your bank card or your passport, there are numbers which never change. Therefore, all the activities that one performs with these devices are linkable. An IRMA card, on the other hand, reveals no other information than the authentic attributes; everything else looks completely random. And still, attributes are very secure, they cannot be forged or transferred, and each attribute (more precisely, each attribute-based credential) can only be issued by a particular, authoritative party. This is quite natural: Your birth certificate for instance should only be issued by some designated government agency.

The IRMA technology enables three important functions: i) dynamic and transparent issuing of various credentials, ii) selective disclosure of attributes, and iii) the possibility of online and offline attribute verification. In sum, IRMA is a privacy-enhancing technology that enables *data minimisation*, that is, to disclose a minimal amount of personal information whenever one interacts with the digital world. Therefore, it is also in line with the GDPR, without any loss of functionality or security.

# 5 Discussion

There are plenty of PETS and plenty of identity card projects. On the one hand, PETS are often hard to use or not realistic in their model. On the other hand, identity cards are often based on old technologies with a low level of security, privacy or flexibility. The future identity card is a personal storage of authentic personal data. This data can be used for multiple purposes; the card is user friendly, user controlled and privacy friendly.

By means of the IRMA technology, in the future I can easily rent a car unlike my recent personal experience. The entire verification can be performed by the IRMA card; I can even collect loyalty and bonus points. And although the same card would be used for credentials from various contexts (driving license, credit card, loyalty card), the government administration or any other authorities would not need to know about it. The card will do every interaction without the participation of any central systems.

[5] `https://www.irmacard.org`