Chapter 7
Digital Sovereignty and IT-Security for a Prosperous Society

Reinhard Posch

Abstract With the Digital Single Market and the supporting programs H2020, CEF, ISA2 and other instruments Europe is making a big effort to shape up its ICT. This is also supported by legislation where IT-security plays an excelling role. Not only is the eIDaS regulation as an example offering a seamless legal framework for all 28 member states also it is a unique chance for Europe to show its ICT-strength with its open and innovative approach to attract European industry as a provider and businesses as major enablers. IT-security and data protection need to enable digital sovereignty and at the same time are fields where Europe has developed renowned expertise in the past and could develop further strength in the future.

7.1 Introduction

As the incompatibility of US and European legislation (US Government 2001) as well as the impact of US legislation on data stored in Europe came under discussion, digital sovereignty has gained an increasingly attention also in the open public (Nojeim 2014).

In general, digital sovereignty can be defined as the ability to have full knowledge and control by the individual or by the society about who can access ones data and where ones data are transferred. The latter is of high importance as different jurisdictions have quite different regulations about data protection and data security. While in general, the perception is that cyber space has its own rules it is clear that the same laws apply as in the physical world unless explicitly regulated otherwise. The only remaining problem is that the enforcement of legal regulation differs in practice. This fact makes it even more important that appropriate precautions are in place.

Looking into daily practice and incidents, we observe that digital sovereignty is endangered not only theoretically, but also in practice. Many of these situations are only marginally observed by the public or even by professionals (Fig. 7.1).
The above notice that “test certificates for Google” have been issued by employees of a major security company like Symantec (Budington 2015) was rarely echoed in the press. There have been similar attempts by third parties as also shown above, however, this new one shows that such activity is capable of impersonating any company, administration or private person—no matter whether this entity ever had a relation to the rogue certificate issuer.

Only this very recent issue which made it to the public shows that the infrastructure and the capabilities have to be revisited in the light of digital sovereignty, trust and security.

We have opened up our communications perimeter in a generous way but have not understood the impact and are using communications infrastructures as if they were under control. Measures that would make these assumptions valid even if available are not widely used by the majority or by companies at least up to a certain size.

The following chapters flash out some areas where digital sovereignty has quite some room for improvement and at the same time shows potential avenues to approach the goal.
7.2 Jurisdiction Aware IT and Communications

There is a need to make it easier for the everyday user private or professional to allow for a higher level of prevention from being subject of malicious attempts. The focus in practice is too much oriented towards observing what has happened and not on how to enable tools and infrastructures to prevent in a better way. The press also fosters this attitude, as it is easier to report on incidents than to contribute to general education and awareness.

Security-wise and trust-wise the internet is still single level unstructured. While there is broad discussion about bandwidth dedication as there is a commercial interest, the consumers and general public interest in trust is not well enough reflected (Fig. 7.2).

It is about protecting interests. In this context the above figure shows a realistic scenario of interest clustering: The actual clustering in the E-Commerce scenario “C” is arbitrary. This basically illustrates that there is a very small amount of information that allows identifying the relevant context in terms of applicable jurisdictions. For a general government data scenario “B” that may include personal data, data protection regulation asks for adequate protection that is to be assumed in the EU/EEA. And there is a sensitive government data scenario “A” where organisational or national borders are the perimeter.

As with many other trust issues we have pieces that could help to improve situations, but we lack a framework transparent to the user and to the service so that it can be efficiently applied. Concerning the applicable jurisdictions we could use DNSSEC (IETF 1999) and client certificates to ensure end to end trust. There are however some stumbling stones with this:

(a) DNS and DNSSEC address the domain but not the jurisdiction the domain is in
(b) DNS only addresses the endpoint not the route the communication flows
(c) Client certificates are rarely used and impose quite some complication in terms of organization

This points only to technical issues. Moreover some countries and organizations would not even favour such situation as communication relaying including scanning for malicious elements is in place and would contradict the above. This already makes clear that we need to concentrate on a framework.

Having in mind that the information to identify the jurisdictional context is very small, it could be handled even with two or three bits in the packets of existing communications which—if properly applied—could be asserted in a responsible manner by the communications provider.

The following is to give an example for feasibility:

11 communications within own legislation
10 communications within area (e.g. Europe)
01 communications among “cooperating countries”
00 unknown source

Optionally the travelling of the packets could be flagged
xx1 xx applies to source and transit of communications
xx0 xx applies to source of communications

If such scheme would be agreed by cooperating providers in a transitive way the user and the services would receive trusted information, if their own provider was offering this service. As any cooperating service provider would only inherit or generate such information, if the communication came from a provider cooperating in the scheme, the service provider is also subscribing to responsibility.

7.3 Switching Mobile Connections: Floating Cross-Jurisdiction to Reduce Cost

It should be considered to introduce identity management for carriers with roaming and reconfiguration and to add this to device management to enable efficient control by the user. Also the present practice leaves quite some questions open in the context of data protection and person related data.

The availability of mobile switching capacities exceeds by far the need and this results in a situation where switching of mobile communications might be done in a far away country with very different legal provisions. This may well also apply to communications where source and destination are in the same country irrespective of the provider.

The crypto protection over the air does not help in this case and interception—even if not legal in the country or countries of the source and destination of the communications—can never be fully excluded. Neither as concerns the metadata nor the content. Since communications can cross the mobile/landline border the provider and the switching provider must be able to handle the encryption and,
therefore, the over the air encryption cannot be seen as a hindering aspect for legal interception.

The situation becomes even more complicated in case of roaming or pretended roaming. The whole system builds upon fully trusted carriers. That might have been the case when there had been only a few and within landlines, but is no longer a realistic assumption at this point in time. Moreover the technically and cryptographically supported identification of a provider towards other providers and especially towards the user is certainly insufficiently in place to support the need of sovereignty in a transparent way.

This is essential since roaming means reconfiguring the device on the communications level. This is triggered with “huge SMSes” that are interpreted by mobile device as commands. This makes evident that the identification and security measures with this reconfiguration process has a significant importance. As an example for this important “feature” it has to be mentioned that at this level the encryption of the traffic over the air can also be configured.

### 7.4 Push Notification: Always on a Short Leash

Like many of the technologies that are widely used push notification came out of consumer devices and have not been adjusted after being scrutinized in the context of sovereignty and use cross jurisdictions.

The convenience of being reached basically at zero cost at the level of applications results in the situation where all mobile devices that are online have an open connection to the communications hub of the manufacturer (Google, Apple, Microsoft, Blackberry) depending on the operating system of the smartphone (Hafizji 2013).

Depending on the system settings and the operating system, this mechanism can be used to assist updates of APPs and operating systems. The average user is unable to control these capabilities.

As we have already a hand full of manufactures and this mechanism works cross such manufacturers (e.g. WHATSAPP to give an example that is widely used) there is no barrier to change this to be compatible with legal requirements. E.g., installing such hub by a European trust provider rather than with the manufacturer would not need conceptual changes. In many ways these push notifications carry personal data subject to data protection regulation putting in scene an additional need beyond sovereignty. The general question in this context is the societal approach returning more powers to international companies than to national governments where the latter in many cases are at least democratically elected.
Like with data protection that has popped up recently, in many ways it is about incompatibility of legal systems. This aspect has already been addressed with the jurisdiction aware communications. However, this turns out to get even more complex in case legislations ask for applicability outside national borders. That this is the case not only in the cyber sphere but also with physical storage has been brought to visibility by the “Ireland Case” where Microsoft (Nojeim 2014) is asked to hand over data from Ireland to the US according to US legislation (Fig. 7.3).

The big conflict remains with the companies. If such company is US based the decision has to be made not to offer services outside US or to remain silent about the truth and the legal obligations towards its customers as set out in US law.

While US law at least does not allow to use intercepted data for competitive advantage of private sector players, this is not even generally the case in all countries. When it comes to Cloud and sensitive data—be it governments or industry—we need improvement on this situation before we can fully profit from Cloud.

If it is about storage, only encryption might be a tool from the practical demands giving a high level of assurance. Still there is quite some clarifications open in the context of data protection:

- Encrypted data is data that can relate indirectly to a person. In such case trans-border communications would require specific precautions not possible in most cloud settings.
- If encrypted data separated from keys is not yet person related, what about deleting data? Unless we come to a legal opinion that deleting keys is equivalent to deleting data, in the data protection context this leaves open questions.
- Still encryption only solves storage demands for time being and only if encryption happens external to the service in a “trusted” environment. After all we need
also to process—search, sort, etc.—data and there is very limited remedy in sight for these aspects.

With this regard Europe is in a dilemma. Not making full usage and taking advantage of the Cloud will be a competitive disadvantage. Like with environmental issues and a labour-related legislation this might be a further asset Europe would not like to give in and then will notice that some of the business is not realistic. With the “safe harbor case” this has clearly demonstrated its international and global dimension.

7.6 Document Collaboration: In the Cloud as You Type

Cloud, mobile devices and many others—we observe an increasing level of complexity reducing the number of players to multinational companies or even to a monopoly. With operating systems and large multipurpose packages companies offering both conventional and as a service approaches have a clear handle to set the directions by their pricing policies.

In a few years it is most likely that the majority of document editing also will be done online offering the option of collaboration. In fact this is starting already now despite of all problems that would have needed to be considered from the data protection perspective. Decreasing budgets for government IT will at least partly force them also to join this trend (Fig. 7.4).

The evolution is introduced silently, but has a huge impact.

• Any change of a document is immediately available over the internet
• Users have no knowledge of the “software” that is used for generating/editing documents
• The “software” can even without the user noticing change even temporarily at any point in time as it comes online in a browser-like way or even through the browser

Fig. 7.4 Documents in the cloud
As for the time being user driven encryption is not possible. Identification methods are according to the provider not according to the demands of the users.

In the public sector this might even be seen as incompliant with the eIDaS regulation—or the levels substantial and high of eID, with the web server authentication etc. At least there is a substantial gap before we get there.

From a sovereignty viewpoint the basic needs would be:

- **eID as a basis**: Access to remote data (Cloud.Mail.Calendar) shall be configurable in a way that the user can determine availability of services only through eID (according to the eIDaS requirements). It should be possible that the owner of data can set the level of requirement (eID only). Consequently all internal mechanisms should make sure that there is no possible circumvention by even very long secret authentication strings that are prone to be replayed.

- **Static data encrypted**: Data that are not necessarily processed shall at the choice of users be attributed to be encrypted and decrypted only at the client (e.g. in the browser or at a user chosen trusted third party) where the user can also choose the key management. An appropriate interface accepts such data for the repository or for sending. Evading or violating the policy should require explicit user intervention (e.g. in case of sending an email or calendar entry to a partner not being part of the crypto management). Any operation that need server-side processing (e.g. search) might become unavailable or substantially increase consumption of computing power (e.g. due to homomorphic encryption). This should be left solely at the choice of the user.

- **Validation of active elements**: It shall be possible to restrict the origin of active elements (e.g. HTML5 javascript) to origin from a server trusted by the user to disallow circumvention of the criteria above. One possible way to accomplish this would be to cache active elements after a certification process in the user-environment or at a party explicitly trusted by the user.

- **Encrypted collaboration**: When documents originate from a collaboration process it shall be possible to encrypt every piece of the document that leaves the user’s device/browser using user chosen key management for encryption and decryption.

- **Availability**: The security features shall be equally available for all platforms (PCs, laptops, tablets and mobiles) for the main operating systems. Unless this is reached, laziness of users will jeopardize security and data protection.

### 7.7 Conclusions

Due to economies of scale IT has developed a process that increasingly focuses on very limited set of providers. Hardware and manufacturing as a business with labour and environmental demands has concentrated in far east where these aspects can be handled in a less expensive manner.
Operating and systems and integrated packages of software are increasingly coming from US where the development towards cloud and provision as service is both adding momentum and possibly reducing user’s choice.

In this context European IT industries needs to rethink its focus. While many innovations are coming out of Europe and is structured around SMEs such innovations i.e. such innovative companies are often acquired by large software companies in the US. This happens for the sheer reason that Europe is not offering enough potential to buy innovations and innovative companies at competitive prices. The cluster security, identity and data protection at least has the potential to become an exception, if it is handled appropriately (Fig. 7.5).

At the end it should probably not only be a decision that is driven by commercial and financial aspect, but also should respect societal and sovereignty aspects. IT and the technology coming with it is ubiquitous—from housing to traffic, office to healthcare IT is a major and sometimes the driving factor. This is getting an even further dimension with the internet of things.

Leaving the key decisions about technology to big market player only might be step back at least in societies that strongly believe in democratic values.

References

Budington B (2015) Symantec issues rogue EV certificate for Google.com. https://www.eff.org/deeplinks/2015/09/symantec-issues-rogue-ev-certificate-googlecom

Hafizji A (2013) Apple push notification services in iOS 6. http://www.raywenderlich.com/32960/apple-push-notification-services-in-ios-6-tutorial-part-1
IETF (1999) RFC 2535 domain name system security extensions. https://tools.ietf.org/html/rfc2535

Nojeim G (2014) Can a U.S. warrant compel a U.S. provider to disclose data it stores abroad. https://cdt.org/files/2014/07/Microsoft-Ireland-Memo-formatted.pdf

US Government (2001) Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) Act of 2001. http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.