Bayview Insight Management Inc.

[redacted]

Letter to Article 29 Working Party Guidelines on the Right to Data Portability – *How Certain GDPR Requirements Reduce Cybersecurity*

First of all I would like to thank the working Party for its encouragement for comments from all interested parties, not just from EU residents.

I will start with a review to the Right to Be Forgotten and then proceed with analogous remarks about the Right for Data Portability.

Finally, I will ask WP 29 to consider the following:

1. Extending the trial Period and additional 3 years to properly define and test exactly how to safely implement the new requirements.

2. Adding Cybersecurity experts to WP 29 and its successors to work alongside the current membership and intertwined with the decision-making process.

The Right to Be Forgotten

I will start here because the concept seems so simple. After a natural person agrees to the uses of his/her personal data for the purposes disclosed to him/her, the data is then saved in the controllers system as well as to processor systems or third party systems. After that the natural person has a right to withdraw permissions for the use of any and all data and permanently erase it for a variety of reasons.

The assumption made by the formulators of the above process is that once it has been designed and implemented, the Cybersecurity community can do its magic and Bolt On whatever may be needed to keep the data safe and secure.

Nothing can be further from the truth. Bolt On is not good enough. Cybersecurity must be either Built in to this process's design, or woven right into the fabric of the underlying communications infrastructure, for example in the Estonian X-Road.

Let's start with a request for erasure of certain data by a data subject. Article 12 provides leeway for a controller deciding to refuse to act if it can "demonstrate that it is not in a position to identify the data subject". Hackers are extreme experts in using false identities or creating real identities and inserting any identity they like into the database. The right of the controller to decide to process the request if the authentication is incomplete must be removed. He/she must be forbidden to act unless full authentication is accomplished.

Once a request has been made by an unauthenticated person, experienced hackers can tag on bots to ascertain how the system processes data all the way through to the database. It can then inject malware that can do a number of things:

1. Erase, publish, sell or alter all the data of every in the database

2. Cyber lock the database and demand ransom

3. A mix of the above and more

If the data is transmitted to third party databases, the cybercriminal can set up the attack at the time the original record is created in all downstream databases. The attack can then be executed on any and all affected databases on the back of a real or fake request to erase something -- at any time.

The organization cannot block attacks by injecting "manual" steps instead of automated ones. In today's world, manual means an email with an attachment – and that's the playing ground hackers cut their teeth on.

My opinion, and I'm not a cybersecurity expert by any means, is that if RTBF is to be implemented securely, Cybersecurity by Design must go hand-in-hand with Privacy Design. Bolt-On Solutions won't work. Even Built-In solutions are problematic because of links to 3rd party databases. I think one needs to start with a secure multi-database infrastructure, hardened database storage methodologies and a 2-factor hardened Identification Gateway to validate all data subjects from the outset -- and subsequently to validate the authenticity of any requests to correct the data or change consent.

The Right to Data Portability

All of the above arguments extend to designing the means to implement this right as well. Movement to automating data portability via interoperable means just makes it even easier for hackers to quickly infect the target systems.

The target system can be infected even if the original host system is secure. Hackers work best at the point of transfer of data too. They learn exactly how the transfer process works and can inject malware at the time of the transfer, however secure the host system that originally held the data might be.

Recommendations

1. Extend the Trial Period for an additional 3 years to properly define and test exactly how to safely implement the new requirements. It is not realistic to expect that all new protocols and systems can be designed, tested and implemented by the entire user base in time for March 25, 2018.

2. Add Cybersecurity experts to WP 29 and its successors to work alongside the current membership and become intertwined with the decision-making process.

Any decision or implementation process should not just be left to be implemented ad hoc by interested parties differently, and should be accompanied by tested guidelines and precise technical designs to affect the change safely. Relying on unspecified industry standards and bodies in the target area of knowledge is just not enough.

It is one thing to keep the legislation technology-free. If implementation is not specified precisely at some other level than the legislation, we will be faced with an ad hoc collection of implementations and a hackers dream.

In summary, Cybersecurity by Design needs to be built into Privacy by Design from the outset.

Very truly yours,

[redacted], Founding Director January 31, 2017