FLORENCE, NOVEMBER 1st, 2014

PRIVACY BY DESIGN
AND BY DEFAULT

Sébastien FANTI

Attorney at law and public Notary
Elected as Cantonal Data Privacy Officer (Valais)

www.sebastienfanti.ch
sebastien.fanti@sebastienfanti.ch
Overview

• Preliminary remarks and definitions
• The example of the Blackphone
• The Swiss Privacy by Design and by Default approach
• Impact analysis about privacy - modelization of risks – a practical approach
• Future evolutions
• Conclusions
Preliminary remarks and definitions

Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. Ann Cavoukian

Privacy by Default has another dimension than Privacy by Design. Privacy by Default covers applying default settings in such a way that the best possible privacy is guaranteed. Privacy by Default reacts to the enormous growth of internet facilities and apps and must ensure that the low-threshold use leads too quickly to the unwanted showing and/or sharing of (too much) of personal data or compromising of security. Viviane Reding
Preliminary remarks and definitions

The 7 Foundational Principles of Privacy by Design:

- **Proactive** not Reactive; **Preventive** not Remedial
- Privacy as the **Default Setting**
- Privacy **Embedded** into Design
- Full Functionality – **Positive-Sum**, not Zero-Sum
- End-to-End Security – **Full Lifecycle Protection**
- **Visibility and Transparency** – Keep it Open
- **Respect** for User Privacy – Keep it **User-Centric**

The example of the Blackphone

Secure by Design

A 21st-century smartphone

Blackphone combines a custom operating system with leading applications optimized for security. The result: an unparalleled product ideal for people who recognize a need for privacy and want a simple, secure place to start.
The example of the Blackphone

Spider Oak: Online File Sharing & Secure Cloud Backup – strongly recommended by Edward Snowden

“Our smartphone won’t make you NSA-proof, but it’s a good start”

Phil Zimmerman
# Privacy by Design and by Default

The example of the Blackphone

<table>
<thead>
<tr>
<th>Feature</th>
<th>Android Default</th>
<th>PrivateOS Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Trackable</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Bundled Apps</td>
<td>Many, with privacy disabled by default</td>
<td>Few, and all privacy-enabled</td>
</tr>
<tr>
<td>Wi-Fi usage</td>
<td>Always on for geolocalisation and user tracking</td>
<td>Smart disabling of all Wi-Fi except trusted hotspots</td>
</tr>
<tr>
<td>App permissions</td>
<td>All-or-nothing</td>
<td>Fine-grained control in a single interface</td>
</tr>
<tr>
<td>Communications tools</td>
<td>Traceable dialer, SMS, MMS, browser. Vulnerable to spoofed cell networks and wi-fi</td>
<td>Private calls, texting, video chat, file exchange up to 100 MB, browsing, and conference calls</td>
</tr>
<tr>
<td>Updates</td>
<td>Supplied infrequently after carrier blessing</td>
<td>Frequent secure updates from Blackphone directly</td>
</tr>
<tr>
<td>Remote Wipe &amp; Anti Theft</td>
<td>Requires use of centralized cloud account</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Business Model</td>
<td>Personal data mining for tracking and marketing</td>
<td>Delivering privacy as a premium, valued feature</td>
</tr>
</tbody>
</table>
I have read this article and I’m very surprised. I have bought this phone because it was a secured phone. If not, I think you should give the money back! I would be happy to have a feed-back quickly.

August 12, 2014 / 08:00 PM
The example of the Blackphone:

Nothing is perfect!

Thanks for contacting us and I understand your concern. I think the links in https://support.blackphone.ch/customer/portal/questions/8315538-blackphone-rooted-in-5mn will address your concerns.

Please let me know if you have any more questions.

August 13, 2014 / 01:44 AM
The Swiss Privacy by Design and by Default approach

No legal rule refers explicitly to these principles at the moment in the Federal Act on Data Protection of 19 June 1992.

Federal Data Protection and Information Commissioner has taken part to the 32th international Conference of Data Protection and Privacy Commissioners in Jerusalem, where one resolution was adopted about the need to include the principle of Privacy by Design in the legislation.

The need to revise our Federal Act on Data Protection is evaluated by a Commission of experts.
The Swiss Privacy by Design and by Default approach

Each Swiss Company who handles the data of European citizens or receives such data from one member of the UE should respect the legal rules of the UE and of all the Member States.

Art. 23 of the future European regulation:

Data protection by design and by default
Privacy and data protection impact assessment: a practical approach!
The Swiss Privacy by Design and by Default approach

• Switzerland can’t afford to stay out of significant legislative changes which will undoubtedly impact a lot of companies in our country

• Ordinarily, we adopt new UE legal rules with a slight delay

• Even if the rules aren’t changed immediately in our country, most international companies will have to adapt their legal approach and become early adopters

• The global market with a fierce competition is the best way to uphold these principles
Future evolutions

Two postulates are now pending before our Parliament to introduce in our Federal Act on Data Protection of 19 June 1992 the principles of Privacy by Design and Privacy by Default (postulates Schwaab).

The Government agrees with both postulates.

Our law should normally change in some ... years!
Swiss citizens really love Privacy!

Our companies and schools are for some of them between the best in the world in their scale of competences (Logitech, Swisscom, EPFL, etc.).

The only solution is to apply immediately both principles and go further than what the law currently requires.
Thank you for your attention

Follow me on:

Twitter: @sebastienfanti
Facebook: https://www.facebook.com/sebastien.fanti
Linkedin: http://ch.linkedin.com/in/sebastienfanti/