Rebuilding Trust Through Privacy by Design

by
Alexander Hanff
alexander.hanff@startmail.com
The Principles of Privacy by Design
(You all know this stuff right?)

- Proactive not Reactive; Preventative 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
Proactive not Reactive; Preventative not Remedial

Both Ixquick and Startpage are built on the same privacy focused principles.

- No IP addresses recorded.
- No record is made of your searches.
- No identifying or tracking cookies used.
- All communications with both sites are encrypted by default over a Secure Socket Layer (SSL/HTTPS) with highest-level encryption including Perfect Forward Secrecy and supporting TLS1.1 and 1.2.
- No logs are retained of any personal information.
- No personal information is being send to third parties. (no search leakage)
Proactive not Reactive; Preventative not Remedial

- Users can customise their experience and make those customisations persistent without the use of cookies by using a “url generator”
- Users can view search results anonymously via a proxy server which automatically parses the incoming data for malicious technologies to further protect users
- Users can choose whether to use European servers or servers in the United States
- Search requests are sent using the POST method instead of GET
Proactive not Reactive; Preventative not Remedial
StartMail

- Minimal logging
- All internal emails encrypted
- User Vault (encrypted Inbox)
- Question/Answer
- HTTPS/PFS
- PGP Public Key Server
- Works seamlessly with desktop client PGP plugins
Privacy as the Default Setting

- As with StartPage & Ixquick, StartMail has Privacy by Default
- HTTPS/PFS
- Encrypted Inbox (they cannot read your email)
- All internal mail encrypted (no-one else can read your email when you are logged in)
- Revocable Addresses
- IMAP Support
Privacy Embedded into Design

- StartMail developed over 3 years with Privacy embedded at the core from the beginning
- Surfboard Holding BV consulted with respected privacy advocates, regulators & lawyers from the start
- Before the first piece of code was written, the foundations were built around privacy with a clear strategy and focus in place
- In order to fulfil PbD principles, entire system written from the ground up
Full Functionality -- Positive-Sum, not Zero-Sum

- StartMail has been developed to provide a feature-rich solution to users rather than a half measure
- Through innovation and collaboration StartMail provides users with a Positive-Sum service
- Even most geeks do not use encrypted email because PGP plugins are non-trivial – StartMail makes PGP trivial
- Don’t just sign your email – encrypt it
End-to-End Security – Full Lifecycle Protection

- As already mentioned – encryption, encryption, encryption
- Encrypted inbox (user vault), encrypted emails
- HTTPS + PFS is essential in light of Snowden revelations
- Don’t forget your PGP passphrase (but if you do you can revoke & set a new one)
- Recipient has client without PGP support? No problem with Question/Answer challenge for decryption
Visibility and Transparency – Keep it Open

- As with StartPage & Ixquick – StartMail is completely transparent to users
- Clear and Plain Language Privacy Policy
- Knowledge Resources
- Honesty is key to building trust
Respect for User Privacy – Keep it User Centric

- Surfboard Holding BV places user privacy as their top priority across their entire product range
- With constant innovation and re-investment coupled with ongoing and open dialog with regulators, legislators and privacy advocates, Surfboard Holding BV keeps on pushing the bar higher, enhancing privacy well beyond mere compliance
- Users maintain a very strong and interactive relationship via email, forums and Twitter
- All tickets answered & all bugs escalated – users are the customer not the product
Respect for User Privacy – Keep it User Centric

- Surfboard Holding BV also act as the citizens’ champion, pushing for stronger privacy regulations and deconstructing the moral panic built by “big data” corporations who seek to weaken citizens’ fundamental rights through aggressive lobbying against existing and emerging privacy and data protection legislation and regulations.

- StartPage & Ixquick prove that Privacy can be a viable competitive differentiator with staggering year on year growth.

- Over 40,000 accounts reserved on StartMail before the service has even launched illustrates growing trust in the brand.
Privacy by Design Ambassadors

- It is because of these strong principles and policies that they are Ambassadors of Privacy by Design.
- For more information on StartPage and Ixquick’s Privacy by Design template:
  

- Or by following the Ambassadors link on the Privacy by Design main page.
Startmail – a new era for email

- After nearly 4 years of development, StartMail.com just entered Public Beta.
- 50,000 people enrolled for the Public beta programme.
- Built on the same principles of Privacy by Design.
- Extensive collaboration with privacy advocates.
- Feature rich – **positive sum**
The Snowden Apocalypse

- Snowden has opened Pandora’s Box
- Can the public trust giant US companies with their data?
- Users looking for privacy focused alternatives
- Now is the time to rebuild trust through Privacy by Design
- Now is the time to use Privacy as a competitive differentiator
Lessons Learned

- Even with a history of providing privacy enhancing services it took nearly 4 years to develop StartMail
- Privacy is never a cookie cutter solution – every service & product has unique obstacles to overcome
- Collaboration with experts, looking outside the organisation, listening to advice and acting on it is key
- Speak to the public, privacy advocates and regulators – look for solutions based on their feedback
- Don’t assume people will not pay for your product/service – data is not the ONLY currency – FREEMIUM is not the only model
Focus

- The most important principle of Privacy by Design is Focus
- Focus on Privacy above all else – as soon as you lose that focus your design will fail
- Developers are bad at privacy, listen to the experts, let those experts talk to your developers
- Make sure your developers listen and act on their advice
- Control the development cycle, don’t let it control you
- A strong finished product is always better than a rushed beta