

In this site we are promoting innovation with passion in the context of the participatory web, but at the same time we would like to call the attention of web 2.0 enthusiasts on a number of challenges. To name a few, the social web may influence promote or harm your reputation; when acting online your privacy should be dealt with the utmost attention, In an era of the real-time web, one could easily face greater information overload, and the social web could turn, in some cases, into a hatred web. Therefore, we have decided to publish a series of short articles dealing with the 'dark side' of Web 2.0. This first post deals with the issue of "privacy".

History

Looking back 10 years before the Internet became mainstream, only a tiny fraction of personal information was digitally stored. It was either protected by higher authorities or stored on your unconnected personal computer. Nowadays, the situation looks a substantially different. The connection of computers to the Internet has led to an unprecedented disclosure and exchange of personal information. Within seconds large amounts of data can be shared throughout the world. The recent debate about the [SWIFT agreement](#) between USA and Europe, which allows governments' insight into bank transfers, is evidence on the fact that it does not really matter if you are using the Internet or not. Nowadays a lot of personal is digitized such as consumer habits, health data or bank transfers.

A global database of information

But .. back to the Internet. If you are a person spending a considerable amount of time online, then nowadays, part of your personal data is likely to be widely available throughout the Internet. Online sites requiring registration store not only your physical address and payment information, but are in the position to easily track your visiting path on their website, the time you spent and the pages you visit. As an example the outcome of such tracking and profiling are the recommendations you receive for books and videos, which best fit your interests. Search engines index sometimes in a matter of seconds your published content and then archive it, making it hard to delete. The [Wayback Machine](#) saves a large part of the web for eternity. That's why there are discussions to give data a date of expiry. One might have discovered that typing the name of a person into a search engine can lead to finding mailing list comments dating back ten years, or a frustrated remark in a forum. One should be aware that it is almost impossible to erase completely content published online. But more on this topic will be published on a forthcoming post on "online reputation".

Tracking personal information

For hard-boiled privacy activists, the latest trend in web development looks like a nightmare – the web becomes a surveillance tool. But others might argue that it is only data mining on millions of users, harmless to the individual; and on the contrary, it brings benefits in terms of offering more accurate and targeted information matching the user's needs. A case on point is that your internet service provider (ISP) logs in your browsing history (i.e. the websites you have visited, at what time, and what you did there). To mention one example, here is Google with its slogan " [Don't be evil](#) ".

Google gathers, thanks to its widely used free [Google Analytics](#) tool, very detailed browsing statistics for millions of web users visiting sites embedding the Google Analytic tracking code.

[GMail](#)

analyses your content for advertisement and has years of personal (anonymized) histories saved on its servers even though Google

[changed its policy](#)

one year ago: "Google used to store such data for 18 months, but has now trimmed that duration down to

[nine months](#)

." But this is no guarantee for protection of your personal data as Google's latest Voice service offered voice messages appearing in

[public search results](#)

.

Data in the cloud

There is a huge trend to put a massive amount of data in "the cloud" – on central servers, easily accessible from everywhere. This may be practical for users but it makes their personal data somehow vulnerable to misuse. The developments are so fast and new that it is very difficult to assess the consequences and unfortunately many people, thoughtlessly, give out too much of their personal information.

The problem is that if personal data are placed online, it is difficult to delete them for ever and even claim their ownership. The heated debate around [Facebook new terms of services](#) evidenced the fact that in publishing content such as photos, these become a property of Facebook and could be used, for example, for producing advertisements. Facebook has changed this policy, but it still does not erase your account when you cancel it. The same applies to Google Picasa, where you do not necessarily have full control of your photos once uploaded. Here is an abstract of the Terms of service (TOS) which we light-heartedly accept when subscribing to the service: "By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services." More information on the [TOS of Google](#)

But one has to say, in defence of Google, that they are under public scrutiny. There are countless social network websites with missing disclaimers, no privacy regulation and no information on how they may use your personal data. There is a clear shift to monitor users activities as the Iphone shows too, where [spyware can be implemented](#) by any Iphone-application-developer and can send your location and much more to the developer.

How to browse securely?

There are many ways and tools you can use to browse more securely. For example, customize Firefox to [surf more protected](#) . Firefox 3.5 and Internet Explorer 8 offers the option for “private browsing”. There are many different tools to surf more anonymous or protect your information. One good tool is [TOR](#) . You have to be aware that websites and provider track all actions you do on throughout your web journey. Particular in countries with an authoritarian regime this can become critical. Patrick Meier has an excellent guide: [How To Communicate Securely in Repressive Environments](#)

But in any case the golden rule is to think twice when you publish content online, particularly when it comes to sensitive information.

Author: Christian Kreutz