IT trends with impact on privacy and security

Petra Hoepner, Maximilian Schmidt, Christian Welzel
Kompetenzzentrum Öffentliche IT
Fraunhofer FOKUS
Kaisierin-Augusta-Allee 31
10589 Berlin
petra.hoepner@fokus.fraunhofer.de
maximilian.schmidt@fokus.fraunhofer.de
christian.welzel@fokus.fraunhofer.de

Abstract: Based on the revelation of broad surveillance programs and fundamental security risks, social discussions arise on security and privacy issues. This paper suggests a fundamental change in such discussions. Outlining current IT trends it recommends to focus on innovative perspectives rather than acquired behaviour.

1. Introduction

Privacy can be seen as the right of a person to act, feel and think decoupled from the community, unobserved and (at least actively) uninfluenced. In the digital world, privacy is primarily a matter of data protection and security. Identity management maps an analog identity to one or several digital identities and results in a filtered essence of privacy related information. Data integrity is essential to retain the value of such personal and identity-related data. Security is required to maintain that integrity and authenticity and is as such an important part for data protection and thus also for privacy. From a 2014 perspective, digital security mechanisms have been breached in many cases and therefore digital privacy as well. Stolen user data is no longer a rarity, even for large internet providers. Identity theft is one of the fastest growing forms of cybercrime (cf. [BSW+11]), and thus a key challenge for the digital society in general. Additionally the apparent extent of monitoring by intelligence agencies combined with the helplessness of individuals and entire countries makes visible, that by simple means there is no absolute security. At least by means of usability, security seems to be always a compromise. Today the digital society is at a breaking point that can be seen as a chance to review and revise the understanding of privacy, data protection and data analysis.
To address the issue as a whole, this paper will not suffice. However, by outlining current IT trends it may stimulate the discussion and raise questions to fundamental issues that need to be worked on.

2. Future IT-Trends

This chapter briefly describes the latest trends ([WGA+14]) of the digital discourse and connects them to the terms of privacy and identity management.

Ambient World
Ambient Assisted Living (AAL) describes technical systems that disburden everyday life. For this purpose, networked and partially autonomous installations of sensors, actuators and computers regulate, control and automate situational aspects of domestic life. However, providing automation and simplicity in everyday tasks and satisfying individual needs at the same time is a balancing act. It may result in an atmosphere of social isolation or helplessness, instead of improving comfort and safety and therefore strengthen freedom and independence. Crucial for trust in such systems is to safeguard against active or passive influences. This also includes an integrated identity management, which authenticates and distinguishes users. Additionally. when external systems are connected, issues about privacy and ownership of collected data become relevant.

Data- Philanthropy
Data Philanthropy means, that data is voluntarily provided in order to serve the common good. Based on such data, new knowledge can be found and new trends or changes discovered. Data donors can be individuals, businesses or public administrations.
For digital data resources to be used for the public good, trust and confidence in the data analysts are required. One way to gain confidence would be a free license model for data. Similar to the licensing model Creative Commons, it would offer the donor to determine the possibility for what purposes he wants to make its data available. Regarding anonymization of such data, it has to be taken care that individual data is proper handled and does not allow inferences about identities on its own.

Digital Integrity
The right to physical integrity is one of the main rights in many constitutions and one of the most fundamental human rights. With the increasing digitalization of society, the question arises, whether and how the fundamental right to physical integrity can be transferred to the digital world. Digital identities can be "stolen" and used to cause financial or personal damage. However, there are also substantial differences between physical and digital identity. In the digital world injuries might be undetected by the victim for years. Nevertheless these injuries coincide with significant consequences. Despite the virtual nature of digital humiliation and threats, the impact on the life of the victims can be serious and real.
Necessary but not necessarily sufficient conditions for ensuring digital integrity are the technical requirements for data protection and IT security: availability, integrity, confidentiality and authenticity. But digital integrity goes far beyond, in such as the goal of the users should be to handle their own data in a self-determined way. This includes deletion of published data, which is still an unsolved technical and social challenge.

Smart Data
The Internet has enabled entirely new forms of communication between human beings. New communication possibilities between objects, called "*Internet of Things*" open up technical requirements and social effects. These can by far surpass the first information technology revolution of the Internet with respect to observation, data production control, and self-coordination. This includes current trends like *wearables* and *drones*.

Wearables are one of many variations of inter-object communication and are best described as portable miniature electronics with sensors that occur as a standalone product, integrated into materials or even as an implant in organs. As such, they can be understood as the most personal form of IT utilization. They are becoming increasingly important in areas such as health, self-management, or for day to day assistance in various tasks. The price of such functional support is the disclosure of personal and sensitive data - especially if the *wearables* communicate with services on the Internet.

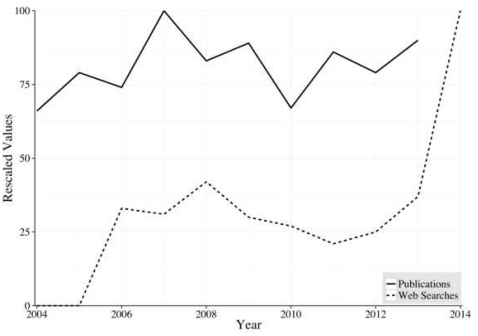

Figure 1: Relevance of "Wearables" in publications ([WGA+14])

Drones generally refer to unmanned aircraft, which are remotely controlled from drone pilots or operate autonomously. UAVs are mostly equipped with one or more sensors to detect the characteristics of the environment. Drones are another variation of object communication but are usually ignored in the broader discourse, since they directly attract attention in public and trigger an entirely different debate.
The trend word "*Internet of things*", as well as the latest developments of *wearables* and *drones* open up completely new social debates that can be bundled in the core theme of "Smart Data". And it is "Smart Data" that describes the actual problem: the accumulation, processing and analysis of personal data leads from a technical and legal point of view to questions about privacy, data integrity, data ownership and security regarding the underlying infrastructure.

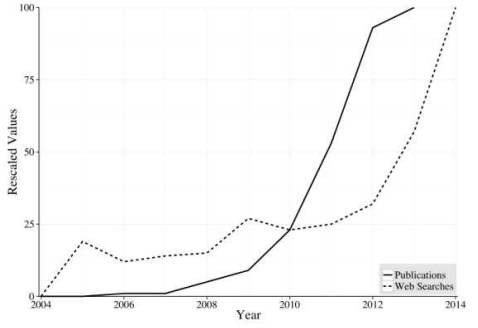

Figure 2: Relevance of "Internet of things" in publications ([WGA+14])

Prosument
With industrialization, there came a separation of production, reproduction and consumption. With today's *prosumer*, these separate spheres are reconnected by IT and evolve previously passive consumers to active producers. Information and electricity as well as music and media were the initial priority product groups, but a dramatic decline in prices by means of production (such as 3D printers) provides a potential of significant expansion of the phenomenon.
Where there are decentralized generated goods, there must be distribution platforms and a higher-level operational management. These instances have access to the give and take of *prosumers* and thus hold important and critical data. Depending on the application, such data partially allows for concrete conclusions to private data and thus requires specific technical policies for safeguarding and access.

Emerging authentication methods
Instead of using username/password or other single-factor authentication methods, future authentication methods must meet higher standards and incorporate several independent factors. In addition to the knowledge factor (secret, such as a password or PIN), factors of physical property (e.g. possession of a card) or biometrics (immutable physical characteristic) are of interest. Comprehensive solutions for 2-factor-authentication are researched and developed in various associations such as the FIDO alliance [SBT14], the initiative Liberty Alliance Project, or the Kantara initiative [SB10]. Lately, biometric characteristics and approaches with smartphones hit the market for innovative 2-factor authentication methods. Examples of biometric variants are smart phones with fingerprint scan, face recognition using cameras, iris scan, vein scan, bracelets for heart rate or other bio-profiles and head attachments for the evaluation of certain brain areas. Many, if not most, of these biometric technologies can be fooled by simple means and are not suitable for security-critical applications. Smartphones as a second authentication factor are a more realistic option, however great emphasis should be placed on data integrity, prevention of profile tracking and the security of communication channels.

3. The digital society

The term "*Digital Natives*" describes people who have grown up with the current up-to-date digital infrastructure. They possess and expect other approaches to knowledge supply, selection and processing, and implicate a new behavior and understanding of their environment (cf. [SDG+14]). They are "embedded" in a technical infrastructure that has always been there, and they are confronted with "Digital Outsiders" - people with traditional ways of thinking, etiquette and behavior. "Digital Immigrants" on the other hand describes a group between "Digital Natives" and "Digital Outsiders", that has followed the digital revolution and adopted its tools and techniques. The terms are controversial and there is at least another group that might be called "Digital Mediators". "Digital Mediators" partly originate at "*Digital Natives*", partly at "*Digital Immigrants*" but have a broader understanding of the technical and organizational background. The question is, what the main differences in understanding and approaching the Internet are and how these groups can learn from each other.

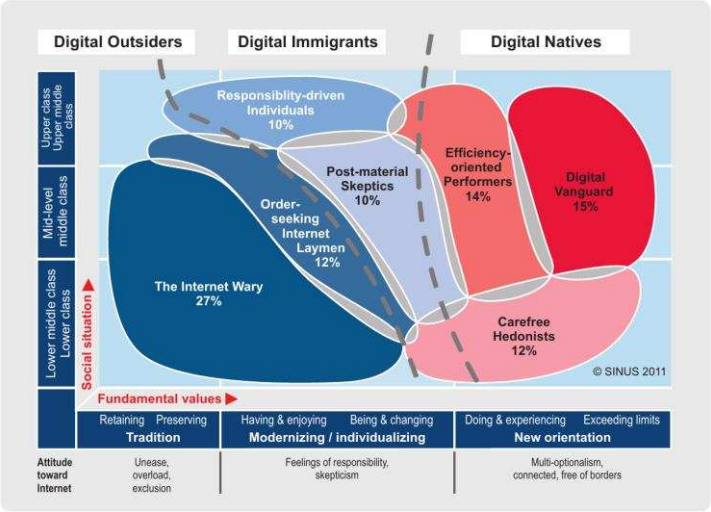

Figure 3: Social environments to trust and security in the net ([SBR+13])

The key to an answer is the actual object and media of observation: the Internet and its different perception and use. While some are philosophizing about Industry 4.0, Internet of Things, Digital Estate, Copyright and privacy protection, others are busy playing with new gadgets, uploading their fitness rank to improve and compare their performance, or are collecting achievements using augmented reality tools.
Each of these actions and buzzwords operates a different viewing angle on a few basic requirements: It's about usability at maximum user experience, ease of data use and innovative data linkage. At the same time it questions data protection and privacy, high security and established moral principles. The question actually is, which of those requirements are in their definition still up-to-date and whether the different viewing angles from the aforementioned groups can be narrowed somehow to provide solutions or at least a common understanding that we can agree upon.

4. Conclusion

Summing up future IT trends
As seen in the "Future Trends of IT," many current topics cover the collection and linkage of data and identities. For this, systems are being used that can be questioned in terms of security and data protection. Currently, new and partly innovative variations of identity management and 2-factor-authentication are being designed and offered. However, all of them are based on the same old fragile infrastructure. With new authentication methods, security concepts are created, that may be invalidated by simple approaches on a more fundamental layer and are as such only partially convincing. Trends like the aforementioned add new aspects and requirements to digital identity management that need may not be covered by current technologies.

Questions on the future of identity management and privacy

With a view on the groupings of persons in the digital landscape, it might be a good idea to ask questions on the needs of "*Digital Natives*", because here lays the innovation. A mere glance at the current trend of crowd funding shows, that new ideas and methods are en vogue and yet find support - against the clichés of the convenience and laziness of the "average" user. Perhaps it is precisely the task of established companies to promote such innovations and to define privacy in a less constricting perspective? Do seemingly thoughtless posts in social networks really blur the boundaries between private and public or is it just a boundary shift? Facebook and Google have already set new standards of identity management and authentication with the adaptation of OpenID and OAuth, but we should not assume that they are able to redefine society. This task is a generational issue and is contrary to various dystopian fictions still decided by the masses of users themselves. With respect to that, "Digital Mediators" are in demand to take up the ideas of "*Digital Natives*" and bring them closer to the less tech-savvy users. The Internet was, is and will be always subject to attempts of control by governments or companies. However it will remain open and accessible since the fundamental idea and need for it is already there. Herein lays also an opportunity for change and renewal.

References

[BSW+11] Borges, G.; Schwenk, J.; Stuckenberg, C.-F.; Wegener, C.: Identitätsdiebstahl und Identitätsmissbrauch im Internet. Springer, 2011

[SB10] Soutar, C.; Brennan, J.: Identity Assurance Framework: Overview. Kantara Initiative, 2010. Available at https://kantarainitiative.org/confluence/download/attachments/38371432/Kantara+IAF-1000-Overview.pdf (Last access: August 2014)

[SBR+13] Schmölz, J.; Borgstedt, S.; Roden, I., Schäuble, N.; Tautschner, M.: DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet. DIVSI, 2013, Available at https://www.divsi.de/wp-content/uploads/2013/12/DIVSI_Milieu-Studie_Aktualisierung_2013.pdf (Last access: August 2014)

[SBT14] Srinivas, S.; Balfanz, D.; Tiffany, E.: Universal 2nd Factor (U2F) Overview. Fido Alliance, 2014, Available at http://fidoalliance.org/specs/fido-u2f-overview-v1.0-rd-20140209.pdf (Last access: August 2014)

[SDG+14] Schmölz, J.; Demattio, M.; Graudenz, D.; Borgstedt, S.; Roden, I.; Borchard, I.; Rätz, B.; Ernst, S.: DIVSI U25-Studie. DIVSI, 2014, Available at https://www.divsi.de/wp-content/uploads/2014/02/DIVSI-U25-Studie.pdf (Last access: August 2014)

[WGA+14] Weber, M.; Gauch, S.; Amini, F.; Kaiser, T.; Tiemann, J.; Schmoll, C.; Henckel, L.; Goldacker, G.; Hoepner, P.; Menz, N.; Schmidt, M.; Stemmer, M.; Weigand, F; Welzel, C: ÖFIT Trendschau – Mantelblätter. ÖFIT, 2014, Available at http://www.oeffentliche-it.de/documents/18/0/OeFIT-Trendschau-Vollversion (Last access: August 2014)