The false prometheus: customer choice, smart devices, and trust

The False Prometheus

Customer Choice, Smart Devices and Trust

By Janne Lahtiranta, Sami Hyrynsalmi, and Jani Koskinen

In the information society of today, privacy is a premium service and user-related information a commodity. This development has gone unnoticed for many, but for some it contradicts with their common sense and perception of right and wrong. If we look into user agreements, and the effect Fair Information Practice Principles (FIPPs) seem to have, this development is particularly evident. One-on-one agreements such as End User License Agreements (EULAs) between the providers and users have become ubiquitous to most users who simply scroll through the agreement and click 'I agree' without actually understanding or caring what they have accepted.

There are various reasons for this kind of behavior ranging from complete indifference, to inadequate internet and technology literacy, and even to peer pressure as certain applications have become a 'must have' amongst a group of users. This problem is particularly current as personal mobile devices have become important, for some even inseparable, part of our daily lives. These devices, such as smart phones and tablets, have also become *user-centered aggregation points* of information that contain personal, even sensitive information about us, and those around us. At the same time, the number of different applications that have practically unrestrained access to the Internet, is on the rise.

When combined with ignorance and negligence, the risk of placing personal information into wrong hands is a very real one. In the following, we focus on this well-explored challenge from a novel perspective—informed consent—and argue that one way to address this problem is to develop solutions that not only promote personal choice and awareness, but are also context-dependent. In order to provide a practical insight into our primarily conceptual work, we use one of the most popular applications, the Pokémon GO by Niantic Inc., in highlighting some of the encountered privacy-related issues.

Keywords: Informed Consent, Smart Phones, Society
Categories: *Social aspects of security and privacy, Usability in security and privacy, Mobile platform security.*
Corresponding Author: *Sami Hyrynsalmi*
Email: *sami.hyrynsalmi@tut.fi*

Introduction

The legal and ethical challenges related to user agreements, and more specifically End User

License Agreements (EULAs) and Terms of Services (TOSs), are a well-explored topic in literature[1,2,3]. In the extant literature, the harmful nature of these equivocal 'contracts', and contradictions between them and the national legislation of the user, are well-known, and well reported by organizations that promote consumer awareness, such as the Electronic Frontier Foundation (EFF). Despite these problems, the legitimacy of these contracts is often upheld in courts[4]. In some cases, these agreements even limit the freedom of expression as they try to curtail users from publicly voicing their potentially negative sentiments about the product. One example of this is a condition, commonly used in EULAs[5]: "You may not disclose the results of any benchmark test of the Software to any third party without [provider's] prior written approval."

The challenges with the one-on-one agreements such as TOSs are also economic and social by nature as the users often face 'take it or leave it' type of a decision, as their peers and family members expect them to use a specific application (or service). A prime example of this kind of a 'de facto' service is Facebook, which has become a primary communication channel for many, and a prerequisite for taking part in social activities, such as volunteering, sports or other (recreational) activities. The social nature of the problem is further emphasized, if we look further into user behavior. The lack of skills in terms of internet and technology literacy, indifference, and pure ignorance are also factors that lead to the final click of 'I agree'. Recently, this issue has been discussed in the context of smart devices–smart phones and tablets–where users have not been interested on the apps' access rights[6].

Even though the aforementioned challenges are well-known and commonly addressed in the literature, we argue that there is one socio-technological factor that has been left to a lesser attention; *aggregation*. Technology has a tendency of converging separate services and related information into a single one[7]. This is a clearly visible in the mobile device sector[8]. As the different services are becoming more and more electronic by nature, and the information is turning digital instead of analog, smart phones and tables (and associated cloud storage services) are becoming aggregation points and predominant repositories for user information. As this kind of a digitalization gains foothold, it can be accurately said

---

[1] Learning to detect spyware using end user license agreements. Niklas Lavesson, Martin Boldt, Paul Davidsson and Andreas Jacobsson. Knowledge and Information Systems, 2, 285-301, 2011.

[2] Re-Mediating Research Ethics: End-User License Agreements in Online Games. Florence Chee, Taylor T. Nicholas and Suzanne de Castell. Bulletin of Science Technology & Society, 32 (6), 497-506, 2012.

[3] What We've Learned From Software License Agreements: A Response to Comments. Florencia MarottaWurgler. Jerusalem Review of Legal Studies, 12, 171-182.

[4] cf. ProCD v. Zeidenberg – http://cyber.law.harvard.edu/metaschool/fisher/contract/cases/procd.htm - Accessed 02/08/2016.

[5] cf. EULA: Knox Express – https://www.samsungknox.com/en/eula-knox-express - Accessed 22/11/2016.

[6] Do Android users write about electric sheep? Examining consumer reviews in Google Play. Elizabeth Ha and David Wagner. Consumer Communications and Networking Conference (CCNC), 2013 IEEE, 2013.

[7] Convergence between telecommunications and other media. Colin R. Blackman. Telecommunications Policy, 22 (3), 163-170, 1998.

[8] Visualization of Interfirm Relations in a Converging Mobile Ecosystem, Rahul C. Basole. Journal of Information Technology, 24 (2), 144–159, 2009.

that there is only one 'binder' the users carry with them to banks, travel offices, doctor's appointments, etc. and that is their phone.

When coupled with the challenges above, a disturbing eventuality arises. The users, completely unaware, some even unconcerned, about the functionality of their applications and services, grant a provider an unrestricted access to their 'digital life' (and often by association, that of one's family). Furthermore, depending on the effective legislation and enforceability of the agreement, the provider may even be free from any responsibility in case something happens to the information as the one-on-one agreement with the user is effectively a liability waiver in front of the law. We argue that instead of complex and ambiguous agreements, a user-centric and marketplace-level solution should be defined and put into effect. In this, the basic concept of informed consent commonly employed in the field of health care can be of the essence.

Different fair information practice principles (FIPPs), such as the HEW Code of Fair Information Practices, FTC Fair Information Practice Principles, OECD Privacy Guidelines, and the Common Framework of the Markle Foundation have been devised to protect the users but they have been reduced to narrow, legalistic principles[9]. As such, they have largely failed as safeguards for personal safety. One reason for this is the one-on-one agreements, where the users have dissuaded to give up their rights, often without a real consent.

In this paper, we focus primarily on mobile phone applications and related user agreements, due to their popularity and widespread use throughout different areas of life (i.e. health, sports, work…). We argue that permissions given in the context, do not meet the criteria of an informed consent, and they are more a result of a force of habit. We argue that the consent given by the customers to mobile applications in their smart phones and tablets is not *informed* one. This situation may lead to dangerous misuses of sensitive information that is increasingly health-related as different health and fitness related applications are becoming more commonplace. Provocatively, it can be argued that instead of liberating information from the hands of the Gods as in the story of the Titan Prometheus, the endusers place the information into the hands of one; some willingly, others unaware.

Background

Informed consent has been a basic concept and a matter of law in the field of health care for a long time. In the United States, informed consent was articulated in the law already in 1957[10], and the doctrine has survived ever since. In the basest form, the concept has two corner stones that effectively define it. One, the patient has bodily integration; autonomy and self-determination over one's body. Two, the patient must be sufficiently informed

[9] The Failure of Fair Information Practice Principles. Fred H. Cate. Consumer Protection in the Age of the Information Economy, 2006

[10] Informed Consent Law, Ethics and Practice: From Infancy of Reflective Adolescence. Roberta M. Berry. HEC Forum. Marc 2005, 17 (1), 64–81.

prior to asked to make health-related decisions (for example, a decision whether to undergo a certain surgery or not).

In the core of the concept is the patient-physician relationship that has changed in the past and still is. Originally, physician dominated and paternalistic, nowadays the relationship is changing into a more balanced and even consumer oriented one[11]. This change in balance between the primary actors is also a shift in responsibilities; as the patients are becoming more involved with the care, they are also expected to carry more of its weight; duties, consequences, and costs[12].

This change in relationship in conjunction to digitalization of the field, has also opened up a discussion on patient information ownership. As the information is becoming increasingly and even solely electronic by nature, its ownership has become contested between different actors (software vendors, health service providers, patients, etc.). Koskinen[13] has approached this dilemma from an ethical perspective, introducing the concept of *Datenherrschaft*, mastery over information and 'digital self' that provides a richer perspective than ownership[13]. Unlike ownership, Datenherrschaft[13], takes into consideration use and existence of patient information, regardless of the service, media, or operator. In this, information is seen as a digital representation of the patient and an expansion of bodily integration into virtual one.

If we apply these concepts into the field of technology, certain analogies can be made even though the change from the field of health care alters the point of focus slightly from a subject to an object (technology), and the primary actor changes from a patient to a customer[13]. In this, the concept of Datenherrschaft[14] depicts our view as it makes a strong case on who should control personal information. We argue that personal information, the digital self of the customer, should not be a commodity but similarly inviolate part of autonomy and self-determination; a property of virtual integration. In our view, and in the spirit of bodily integration[15], virtual integration as a concept is a more profound one than ownership or control over matter; the concept can be seen as constitutive to individual's autonomy and a constructive part of person's identity and selfhood in this day and age.

---

[11] Konsumerismi, potilaiden ja kuluttajien aktiivinen toiminta sekä erityisesti lääkärien kokemukset ja näkemykset potilaista kuluttajina. Hanna Toiviainen. Helsingin Yliopisto, Lääketieteellinen Tiedekunta, 2007.

[12] New and Emerging Challenges of the ICT-mediated Health and Well-Being Services. Janne Lahtiranta. Turku Centre for Computer Science, 2014. [13]

[13] Emerging Roles in eHealth". Janne Lahtiranta. Promoting Health in Urban Living, 2nd International Conference on Well-being in the Information Society, Turku, Finland. TUCS General Publication No. 49, 141-152, 2008.

[14] Datenherrschaft – An Ethically Justified Solution to the Problem of Ownership of Patient Information. University of Turku, School of Economics, 2016.

[15] Persons with Severe Dementia and the Notion of Bodily Autonomy. Wim Dekkers. In Hughes, J.C., Lloyd-Williams, M. & Sachs, G.A., (Eds.), Supportive Care for the Person with Dementia, 253-261, Oxford University Press, Oxford, 2010.

In other words, we consider person and personal information as inseparable, and call this principle *information inseparability axiom*. The axiom can be seen as an aspect of the Datenherrschaft concept. As the information is in the spirit of *herrschaft*[16] – mastery – of the person, the rights for it are *permanent and non-transferable*. In this, the axiom carries a notion of individual freedom in the spirit of classical liberalism [17] ; freedom from government control (or more specifically, oppression in general), and absence of restraint on thinking and acting for ourselves.

The respect for persons, individuals, as presented above, is a central concept in many ethical theories, such as in the works of Kant. These works, and those according to 'Kantian tradition', can be used for highlighting the problems that occur when personal information is used as a commodity[18]. The Datenherrschaft concept carries with itself the highly individualistic values, and it follows from this that the inseparability of the information and the individual is permanent in similar fashion to the human rights – people cannot give it up even if they want to.

This kind of a tight coupling that binds information and individual, separates the concept from many others, such as the MyData[19] approach. The approach underlines the rights of an individual to access and use their personal data, at the same time balancing the individual's needs with those of the industry. In this, technology comes into play in the form of an operator account that is used for managing different data streams. As a result, the approach can be regarded as a view on permission management, trying to find the 'common ground' between the service provider and the user. In contrast, the Datenherrschaft concept calls for control and uncontestable mastery.

As discussed, a certain analogy remains when the focus changes from health care to technology and to electronic services in general. We regard consent as a mechanism for customers to grant a temporary and limited access to their personal information. However, the consent should be informed. In the field of health care, there has been some skepticism towards consent in relation to the (primary and secondary) use of data. The patients do not necessarily understand for what purposes they are giving their consent (or they cannot deny it for practical purposes), and the service providers cannot ensure that the consent is valid[20, 21]. One reason for this is that there is a mismatch between the practical realities and legal (ethical) theories.

---

[16] The term *herrschaft* is used to make a distinction to the concepts of property and ownership, that 'disconnect' the information and the rights from its source, the individual.

[17] Cf. Two Treatises of Government. John Locke. Awnsham Churchill, U.K. 1689.

[18] An Unclear Question: Who Owns Patient Information? Jani Koskinen and Kai Kimppa. In D. Kreps, G. Fletcher, & M. Griffiths (Eds.), Technology and Intimacy: Choice or Coercion: 12th IFIP TC 9 International Conference on Human Choice and Computers, Salford, UK. Cham: Springer International Publishing, 2016.

[19] MyData - http://www.lvm.fi/julkaisu/4440204/mydata-anordic-model-for-human-centered-personaldatamanagement-and-processing - Accessed: 25/01/2017.

[20] Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. Anja Bechmann. Journal of Media Business Studies, 11 (1), 21-38, 2014.

[21] The Crisis of Consent: How Stronger Legal Protection may Lead to Weaker Consent in Data

This mismatch is particularly evident if we look into the European Union Directive 95/46/EC that defines the European view on protecting personal data. The directive in itself is defined in such a fashion that the consent should be "freely given" (Article 2, item h), and "explicit consent" is needed especially cases where the data has a potential for "infringing fundamental freedoms or privacy" (item 33 of the Directive). Furthermore, the data collection should be "fair" and "the data subject must be in a position to learn of the existence of a processing operation" (item 38).

In the light of the current one-on-one agreements such as End User License Agreements (EULAs) and even individual application permissions, it is difficult to see how the requirements of the Directive are fulfilled. For example, is the consent "fair" and "freely given" if the underlying rationale of the agreement, and the actual choice left for the customer to be made is 'take it or leave it'? Understandably, the issue is not unidimensional or simple as the business-side must be taken into account as well. In the field of health care particulars of a consent have been examined for a long time. In the following, we will look into the field and discuss what kind of practices can be transferred to field of technology and electronic services.

The Case

Nowadays applications stores follow rather similar logic in their user agreements and application level permissions. Majority of the agreements are non-consenting clickwrap (clickthrough) agreements that require the user to scroll through a set of terms and conditions, and to give their permission by clicking "I Agree" at the end if they want to use the application. The actual content of these agreements is heterogeneous, varying from vendor to vendor, and even from country to country.

In comparison, application level permissions are more homogenous by nature. The applications require access to a range of functions, such as to read contact information or to use the location of the device. The user grants access to these functions upon installing the application, or upon first use (of application, or a certain function of it).

For example, Google's Android operating system for smart devices offers a system for managing the permissions of applications. Permissions describe which information and capabilities the application needs for working as intended (Figure 1). In older versions of the operating system, the user accepts all requested permissions upon installing the application. In these versions, it is 'take it or leave it' type of a decision where the user either accepts all permissions, or does not install the application at all.

In the Android operating system's latest versions (Codename Marshmallow and up) user is able to manage application's permissions on a more fine-grained level. Instead of granting

---

Protection. Bart W. Schermer, Bart Custers and Simone van der Hof. Ethics and Information Technology, 16 (2), 171-182, 2014.

all requested permissions to an application, the user can select which permissions are granted, and which are not, for an application. Furthermore, the user can change these settings after installation of the application (in similar fashion to the Apple's iOS operating system).

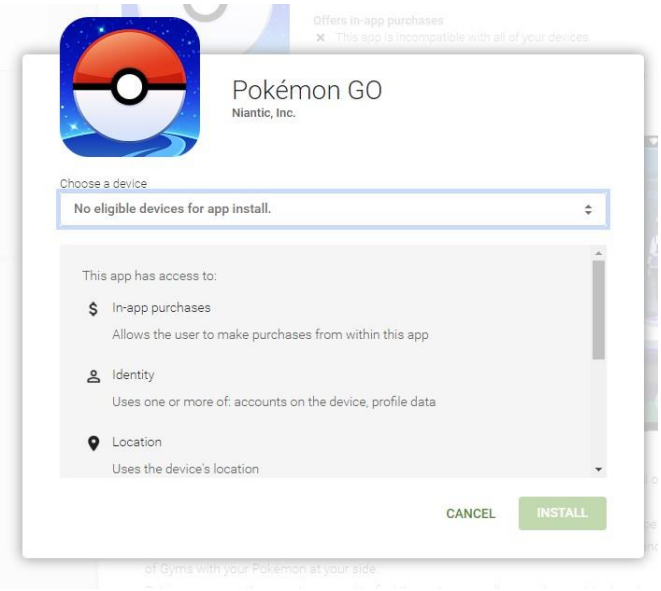

Figure 1. Pokémon GO (Niantic Inc.) installation screen in Google Play marketplace.

This approach used to request permissions that are grouped together with similar ones into groups, is nowadays the most common way that all major mobile application marketplaces have implemented. For example, the permissions of the Pokémon GO, a location-based augmented reality mobile game published by Niantic, Inc. that become a global phenomenon during the summer of 2016, for Android devices (version 0.51.0) are:

i) 'In-app purchases',
ii) 'Identity',
iii) 'Contacts',
iv) 'Location',
v) 'Photos/Media/files',
vi) 'Storage',
vii) 'Camera', and
viii) 'Other' (e.g., Internet and Bluetooth connections).

From these categories, e.g., 'Photos/Media/Files' stand for the permissions of reading, writing and deleting media content from the storage, and 'Storage' present the permissions of reading, modifying or deleting content from the devices USB storage.

Some of the permissions required by Pokémon GO are easy for a technology savvy person to deduce. For example, it is reasonable that a location-based (e.g. 'Location' permissions)

augmented reality (e.g. 'Camera' and 'Photos/Media/Files' permissions) ask certain permission categories. In addition, it is likely that the phone and registered user information (e.g. 'Identity' permissions) are needed to verify the player automatically. However, regardless of the recent developments[22], the company does not offer any information before, during or after installation why the game should be granted access to, e.g., device's contacts and storage.

In a small field test, done as the part of this study, a researcher restricted the permissions of Pokémon GO application (version 0.51.0) for an Android device (Samsung Galaxy A5 2016, operating system version 6.0.1). The behavior of the game was compared against unrestricted version of iOS version run in Apple iPhone 6S Plus (iOS version 10.2) in January 2017. Restricting permission of using camera and location worked as one would expect: the augmented reality part of the game did not work and the game could not locate the player, respectively. However, the researchers did not found any difference in the game play whether the game has rights to access storage and contacts, or not.

Nowadays, smart devices contain personal information ranging from temporarily stored attachments to specified applications of medical clinics. That is, these devices are the aggregation points of our daily lives and personal information. However, at the same time literally millions of users have installed and granted permissions to applications without either understanding or caring about the possible privacy risks[23]. As a case in point, the case application Pokémon GO has been installed more than 100,000,000 times from Google Play app store (January 18, 2017).

The approach described above that has become the de facto practice of managing and granting application permissions in modern mobile operating system of smart devices – as well as with similar technologies in other domain – has certain problems. First of all, on the level of user agreements, there is no way to ensure that the user has read, or understood, the content of the agreement. The user is provided, what is regarded as "reasonable notice and opportunity to review"[24] the agreement. In other words, the users are shown the agreement, and they sign it by action (by clicking the "I Agree", "OK" or "Install" button).

Secondly, the application level permissions that base on technological properties, such as access to camera or contacts, is hardly informative to a typical user. The decision to restrict the permissions on the basis of generic technical functions is understandable due to the simplicity in implementation, and clarity for developers. However, only a small minority of the end-users understand what Android operating system's permission "make/receive SIP calls" actually stands for. The application developers, or application market

[22] Update Your Pokémon Go App Now to Fix That Privacy Mess. Brian Barret. – https://www.wired.com/2016/07/update-pokemon-go-app-now-fix-privacy-mess/ - Accessed 23/01/2017.
[23] 40% of Top-selling Smartphone Apps Have No Privacy Policy. John Koetsier. – http://www.forbes.com/sites/johnkoetsier/2016/03/24/40-of-top-sellingsmartphone-apps-have-no-privacy-policy/#666899d15005 – Accessed 23/01/2017.
[24] The Clicks That Bind: Ways Users 'Agree' to Online Terms of Service. Electronic Frontier Foundation – https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service - Accessed 17/01/2017.

orchestrators, should not assume that a typical user would 'lift a finger' to get enough information about a particular technology in order to make an informed decision. Altogether, this is not a working strategy since technologies change in a rapid pace. The users do not necessarily have the time, interest, or competence to be up-to-date about the technologies that are part of their lives.

Thirdly, granting permissions is a case of 'flat broke or filthy rich'; a user is either granting all requested permissions in a certain category, or denying them. This is even more evident in the older versions of the Android operating system where the users accept *all* permissions or do not install the application at all. In the cases, where social pressures are present (e.g., Facebook or WhatsApp), the end-user only options are either to agree with what might feel unsecure, or become a 'social recluse' in terms of using the applications. In these kind of cases, there are no real options for a customer to choose. Regardless of the recent exemplary developments for example in Android operating system, there is still no 'middle way'; either the application has all rights in the permission category (such as 'Photos/Media/Files'), or not.

In addition, there is no quick and efficient way to control or modify applications permission during the use. For example, there is no straightforward way to prevent an application to take a picture or record audio during a workday or a meeting. For example, in Apple's iOS operating system, application permissions are managed in a separate privacy setting where the permissions are grouped on the basis of technological properties and generic functions (such as, Speech Recognition, Media Library and Motion & Fitness). Even though there is some merit in centralized permission management, accessing the function during the use of an application is cumbersome and requires some internet and technology literacy.

The Remedy?

Our principal argument, and the corner stone of our argumentation, is that if a customer gives up one's personal information, the handover should be an *informed* one. Something that the current way of using EULAs, TOSs and even application-level permissions clearly is not. As a prerequisite for this argument, the service providers should be able to make a clear case on a) what information is used, b) why it is used, c) how the information is collected, c) who has access to the information (incl. extent of confidentiality), and d) how long the information is accessible by the provider (and the named third-parties). In addition, should the premises change, the provider's rights should be invalidated by default, and new permissions requested from the user.

Some of the aforementioned principles are already employed by the more privacy-friendly companies, such as the Finnish F-Secure. The company addresses in their privacy related to the Freedome product[25] majority of the discussed principles. The company also goes the

[25] F-Secure Freedome Privacy Policy - https://www.f-secure.com/en/web/legal/privacy/freedome - Accessed 18/01/2017.

‘extra mile’ in terms understandability and readability as the policy is divided into two sections; a simple ‘In Brief’ section and a more thorough ‘In Full’ section. From the perspective of informed consent, use of simple, even colloquial language, is of the essence (on the other hand, so is avoiding oversimplification). The company also demonstrates their privacy-friendliness by making their terms of service available and accessible at all times; something that relatively few companies tend to be making.

Use of colloquial language and terms more familiar to the user is a major step in the right direction. More so, as this is something that is often missing from the health care sector where professional language often takes precedence in patient-physician communication. Another step that would take the user-perspective more into consideration, is addressing foreseeable discomforts the user might encounter, and describing the potential risks associated to the use of information as defined in the user agreement. While this kind of openness can be regarded as bad business, or even ‘opening a can of worms’ from the perspective of the service provider, it is more akin to looking into a mirror; discussing what the actual user experience is and what kind of privacy-related risks they face. In terms of trust-building, we regard this is kind of a dialogue of the essence, as it really puts the discussion on a new footing. Instead of discussing primarily legal particulars, emotional aspects are also taken into account.

Our secondary argument raises primarily from the user-experience point-of-view. The current design of the application permission management bases on technological foundations of the operating system. That is, if an Android operating system developer wishes to use SIP API classes and interfaces to implement a voice-over-internet service (or similar) in the application, the developer marks these permissions in the manifest of the application. Based on the manifest, the application store as well as the permission management system is able to tell the user what permissions the application needs. In this case, the application store show that the application ask permissions for “make/receive SIP calls”. This simple but yet illustrative example highlights how the current permissions management systems have been fully designed from the application developer (i.e., software engineer) point of view, and not from the end-user’s perspective.

Therefore, we call the engineers to reinvent the permission management system from the user’s point of view instead of a technological one. For example, a user might wish to restrict that an application (or applications) cannot use microphone during the working hours, or other ‘do not disturb’ period of time. In addition, a user might want to express that no other application can run at the same time when medical information or services are accessed with the device (privacy mode). The users should also be granted the right to decide whether the application has access to certain features and information every time the access is requested (in other words, allow or deny access, or allow once).

This kind of user-centric approach to application permission management would not only serve the purposes of informed consent, it would also give users more in the way of internet and technology literacy as the function and operating logic of individual applications would become more evident and tangible. In the longer run, this could also help the users become

more critical in terms of sharing their information, and therefore potentially even more savvy in terms of privacy and security.

One closely related aspect that needs addressing at some point in time are alternative ways of using the application. As services such as the Facebook have become monopolies in their own field of business, exerting near-exclusive control over (related) user information, there is no herrschaft or even real possibility for it. In this kind of situation, an alternative would be either to give users a limited basic functionality of the application with increased privacy, or premium privacy as a paid version. Paid herrschaft – a concept so profoundly in conflict with itself.

In the light of this argument, the analogy works across the domains, and certain principles that are commonly applied in the field of health care, can be applied to the field of technology, or more precisely to mobile commerce and 'app stores' that are in our focus.

Conclusion

In the ancient Greek legends, Titan Prometheus stole the fire from Mount Olympus and gave it to the mankind. For this, the Titan was punished and sent to eternal suffering by the judgment of Zeus. In this day and age, information is akin to fire in this legend; a power of so immense proportions that it can be wielded only by the Gods. However, unlike in the legend, information or even mastery over it, is never given to the humans but it is kept by the Gods – or even given to them willingly by the users. Who or what the actors in this play really are, is left for the readers to decide.

This study is motivated by the aggregation of information and services into a single device; to the smart device in our pocket. While the world of technology has massively changed over the last decade, and it will continue to do so for now, the privacy and security issues have not. A prime example of this are the end user agreements and application permission management functions that do not protect the user but the business. A hugely popular Pokémon GO application was studied and used as an example of a common application, which requested permissions and information use that has not been explained to the user on a sufficient level. While the application served as a prime example, another one (such as the popular selfie application Meitu[26]) could have been used as easily.

This study calls for bringing the concept and ideal of informed consent to the technological systems, and more specifically to the mobile applications. Thus, the users could become more informed and aware on the privacy and security related decisions they make almost on daily basis. Secondly, we call for redesigning the permissions management system from the end-user point-of-view instead that of technology. In other words, that the permissions

[26] Meitu, a Viral Anime Makeover App, Has Major Privacy Red Flags. Lily Hay Newman - https://www.wired.com/2017/01/meitu-viral-anime-makeover-app-majorprivacy-red-flags/ - Accessed 23/01/2017.

would not be requested on the basis of what property or function is used, but instead on the basis of very human notion of *curiosity*. In this answering to the questions like ‘why’, ‘how’, and ‘who’ is of the essence.

Finally, the Finnish security company F-Secure has demonstrated to a degree that taking privacy of the customer seriously, and laying ‘all cards on the table’ in order to build trust towards the products they are selling, can be a competitive advantage instead of a cost (or even a nuisance). In this post-Snowden, or even post-fact, era individuals have started valuing their security and privacy. Offering an easy-to-use and efficient permission management system, and coherent user agreements, that base on informed consent can be a fruitful new approach in the war of competing (mobile) ecosystems.