Cross-border use of WhatsApp, Pandora, and Grindr: on global norms and how to enforce these when "there" can be everywhere

Arno R. Lodder
VU University Amsterdam
Department Transnational Legal Studies
CLI[3] – Center for Law & Internet, Intellectual Property, ICT

ABSTRACT

Smart phones and tablets are becoming the main devices for accessing internet, and will outnumber the world population in 2016. Mobile Devices contain photos, contacts, unique identifiers, payment data, logs, etc., and are used everywhere, including abroad. apps process user information, including the user's locality to offer dedicated services and advertisements, and may turn on cameras and microphones. Most users lack awareness of what apps do, what data are used, and what norms apply. Mobility complicates norm application. Global use, on a global infrastructure does not match well with local, national law. The quadruplet contracting, security, privacy and advertisements are interconnected, form the future landscape of internet services, and asks for a coherent analysis.

This paper briefly discusses the norms concerning contracting, privacy, advertisements, and security applicable to smart devices. The core of the paper is the discussion of three cases to illustrate the complexity of the mobility of the smart devices, in particular when used abroad. First the communication program WhatsApp, followed by the music app Pandora, and finally the dating app Grindr. The difficulties of application and enforcement of norms on the internet severely increases now the devices providing internet connections are seamlessly taken from one country to another, and are always in the proximity of their users: always connected, always available. This paper does not offer answers, but asks questions that need attention and hopefully can be answered sometime in the future.

Introduction

Only seven years ago apple introduced the iPhone; the expectancy is that, by 2016, there will be over 5 billion smart phones users. If we add tablets to those figures, mobile internet devices outnumber the world population. While the digital divide applies to PC and wired internet, inhabitants of Africa and South America are used to cell phones and are now switching to smart phones. Additionally, August 20 2013 Facebook and others introduced Internet.org: "Technology Leaders Launch Partnership to Make Internet Access Available to All". Finally, the world wide web is

going to do justice to its name: the internet is becoming truly global. What about the law? (Mac Sithigh 2013, Tu 2013)

Law is still primarily local and struggling with 'traditional' internet. Jurisdiction is based on territory, but whose territory is the internet? This question has been addressed in a wide body of literature, but without a final answer yet (e.g., Goldsmith & Wu 2008, Post 2009). The next five years with increased mobile access to internet will further challenge the legal system. Due to the use of mobile devices the internet user can access the internet with the same device at any place, including cross-border. People already use many apps and the number of location based services is increasing: local weather and travel information, the nearest Starbucks, tourist highlights in the immediate vicinity, near field communication payments, Groupon offers for nearby restaurants, amber alerts, locations of friends (of friends), social media updates, etc. These services are delivered on the basis of a contract, and make use of a variety of personal information.

How are contracts concluded, under what conditions? And what exactly is the service the app delivers, what data are processed, and by whom, what features are used? Is security guaranteed? What is the role of third party advertisers? In the light of the current developments these questions demand an integrated approach. Questions about contracting, security, privacy and advertisements cannot be treated in isolation, but this quadruplet that forms the future landscape of mobile internet services is interconnected and needs a coherent analysis. So far the world-wide use of Internet hardly led to global norms, but this may change due to widespread mobile access to internet in combination with the mobility of smart device users. My claim is that global norms are needed to protect and facilitate 'smart users', with all their personal and valuable information continuously at the same time physically near them and globally connected, in their own country and when traveling abroad.

The paper is structured as follows. First I briefly introduce the legal smart landscape, viz. norms on contracting, privacy, security and advertisements applicable to apps. Subsequently the topic of crossing borders with smart devices is introduced, and further elaborated upon in the discussion of three apps: WhatsApp, the music app Pandora, and the dating app Grindr.

Background of the legal smart landscape

Internet and how we use it is in a transition phase. Access is increasingly mobile and on small devices. Services are delivered via apps instead of via websites. The application of existing norms to these services is complicated. In particular location based services may access and use (sensitive) personal information. Mobility of users complicates the application of norms, viz. what norms do apply to global apps (Facebook, Hotel.com, Groupon, etc.) and what norms to local apps? In particular in case of the former, someone travelling abroad would not expect a different service when using global apps. However, other information may being processed or different information being disclosed depending on where the user is physically located. I briefly introduce the relevant legal issues related to privacy, security, contracting, and advertisements.

Contracting

At its core, contract formation in an electronic environment is not different from other contract conclusions, viz. there will be an offer and acceptance, meeting of the minds, etc. In the early days of the internet people feared that mere clicking could lead too easily to contracts of which the terms and conditions were not known if at all communicated. The European Union Directive 2000/31/EC on e-commerce created, besides the principle that any placing of an online order should be confirmed by the provider as quickly as possible, a series of information requirements. These

requirements meant to guarantee that a recipient of an information society service was well informed about, e.g. the name and location of the service provider, price information, the necessary steps to conclude the contract, and how to change accidental errors in the ordering process. Subsequently, the Services Directive 2006/123 defined additional disclosure duties for service providers, such as about after-sales guarantee and insurance. Quite recently the Consumer Directive 2011/83 (amongst others replacing Directive 97/7 on distance selling) added over 20 information requirements on the main characteristics of what is ordered, payment schemes, vendor information, value added tax number, etc.

It is hard to communicate all this information via an ordinary website, let alone if an app is ordered via a smart phone. On the contrary, services via smart phones are often offered without hardly any information about the service being communicated. Information is central in our information society and it is important to find the right balance between information overload and too little information to make an informed decision (Lodder 2014). Obviously, if someone sees a nice app he just want to have, he is not really interested in the terms and conditions. This lack of interest can hardly be remedied, but important is that the recipient of the service had the opportunity to become informed. What information should be communicated and how the information should be communicated is difficult to determine since the existing EU norms were not drafted with app stores in mind. An exception Is on Article 8(4) Consumer Directive: "a means of distance communication which allows limited space (…) to display the information", that restricts the information that has to be communicated.

Privacy

Control has diminished since Westin in 1968 indicated about 'data subjects' that he "balances the desire for privacy with the desire for disclosure and communication of himself to others". Already in the early days of internet it was claimed that privacy is an illusion. Privacy decreased ever since, partly due to actions by users themselves via social networks. However, also online privacy is still a fundamental right. Privacy rights cannot be waived by contractual agreement. There is a lot of data on smart devices of which the processing may significantly impact privacy of users as well as others (Arabo, Brown & El-Mousa (2012)), e.g.:

- Location information;
- Address books;
- Unique device and customer identifiers;
- Credit card and payment data;
- History of phone calls, SMS or instant messaging;
- Music;
- Photos;
- Browsing history.

Through the application Programming Interface (API) apps can collect above data continuously, and even can send emails or social network updates, messages, read/modify/delete SD card contents, record audio or use the camera.

Security

Security is closely linked to privacy. Information and network security norms and principles justify specific attention in relation to the relevant actors involved, as these principles surpass just privacy interests. For the majority of apps security is highly relevant (Ghogare *et al.* 2012), with special attention to NFC payments. The NIS[1] recognizes:

[1] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, 7.2.2013, COM(2013) 48 final.

"network and information systems play an essential role in facilitating the cross-border movement of goods, services and people. They are often interconnected, and the internet is global in nature.",

but does not focus on smart devices as the main points of internet access. Smart devices and apps should form an integral part of cyber security actions.

Advertisements

Advertisements used to be general communications, and personalized advertisements scarce and costly. Internet added the personal dimension at a low price, with spam as the notorious and widespread example. Even more targeted to a person are behavioral advertisements or interest based advertising. Even if no personal data is processed, or at least that is the position by some, the nature of such advertisements can be infringing and even compromising. After sending an e-mail about a train trip to Rome, you get advertisements for hotels in Rome. Or, the urban legend about the son who's parents found out he was gay due to targeted advertisements.

Smart devices add a new dimension to targeted, personal advertisements: location. Push advertisements can be very personal: you pass a store and get an offer that is only for you. Law does not explicitly regulate this type of advertising (Leontiadis 2012). Existing norms cover the content of advertisements (e.g., tobacco, alcohol), the medium used (e.g., TV or radio commercials) or the means employed (e.g., comparative and misleading advertisements). From a more recent date is the regulation of cookies, in particular related to tracking cookies, used for advertising purposes. Indirectly concerning advertisements is the definition of internet services used in EU Directive 2000/31 on e-commerce which includes "normally remunerated for". This is a general EU law term, and means that a service should relate to an economic activity. Payment is not necessary. For instance, you do not pay money for using a search engine, but advertisements compensate for the service you receive. Many free apps as well as paid apps generate income from advertisements.

The information apps have access to, including the user's location, can be used by third party advertisers. An app developer can generate revenues by using code supplied by advertisers he can build into the app he develops. Even getting revenues from (physical) product selling is possible, as Mike Hines from Amazon announced on August 27, 2013:[2]

> "the Amazon Mobile Associates API, currently available for Android (including Kindle Fire). The Mobile Associates API allows developers to sell real products from the millions of items at Amazon, whether physical (i.e. toys, clothing) or digital (i.e. eBooks), from inside their apps or games while earning up to 6% in advertising fees from those purchases."

The built in code may also show advertisements when using the app, but can also collect data and send them to the advertiser. This type of communication is not always transparent to users, and the Smart Experiment likely will show traces of data being communicated unknown to users. Norms are needed for in particular app stores and app developers.

Combination

All norms interlock. Terms of contract should include information on privacy, advertisement, and security. Privacy on a smart device without adequate security is without meaning. Consent needed to conclude contracts is also needed for the processing of personal data. Advertisements are based on processing of personal data. What is more, the relevant norms can be subject to various jurisdictions, and a wide range of actors is involved: developers, governments, advertisers, apps

[2] Mike Hines, Announcing the Amazon Mobile Associates API—Earn Advertising Fees by Selling Products from Amazon in Android Apps and Games, Amazon Blog 27/08/2013

stores, etc. This complexity is used as the background in this paper, and in the remainder the focus is on characteristics of cross-border use and three specific apps.

Apps crossing borders, changing rules?

Apps are not ordinary services delivered by a provider to a recipient. Rather a wide variety of actors is involved, with different roles and responsibilities. The parties do include but are not limited to the app developer, the buyer of the app, manufacturer of devices (the phone or tablet), the telecommunication provider, operating system developer, and stores plays an important role as intermediary between the vendor of the app and the buyer app. Obviously, the app ecosystem knows many actors. In particular in cross-border situations the question what legal norms do apply, to what actors is very complicated (Kohl 2010). What legal norms apply to the Dutch smart phone user, ordering a ticket while in Cape Town, for a concert in Shanghai, from a New York concert promoter? What roles and responsibilities do the various actors have against the background of worldwide and cross-border use of apps?

Law can only be applied after jurisdiction is established. Typically, jurisdiction deals with territory, so what happens on the internet should be linked to a particular country, or to be more precise: to an actor (person, company, government) and/or a computer. On the internet information is communicated from one point to the other, from end-to-end. The moment what happens on the internet (communication, dissemination of information) is linked to the physical world, *internet law* originates. Correctly creating this link is a crucial but difficult step (Lodder 2013).

Grotius (1583-1645) introduced the concept Law of the Sea that is now regulated in the 1982 UN Convention. The basic idea is that a country has power over the sea for a specified number of miles from the coast. Most sea (about 40% of the world surface), called the high seas, does not fall under the jurisdiction of any country. Some people claim that the internet should be treated as the high seas. Most people consider decisive the fact that any internet communication in the end is taking place from a physical location, and defend that jurisdiction can always be established.

However, while a boat cannot be at the high seas and in the harbor at the same time, this is what characterizes internet communication: internet traffic is in fact in the harbor and at the high seas simultaneously. Both visions (harbor, high seas) as well as the combination (at the same moment high seas and harbor) can be defended, it depends on what perspective is taken (Kerr 2003), on where the emphasis is put. In the end, however, law can only be applied if you decide on jurisdiction.

Jurisdiction can be established at both ends, depending on the place (1) where the communication originates and by whom; (2) where the communication is received and by whom. Some developments complicate this establishment, e.g. the prominent cyber element of virtual worlds and social media, and varying cloud computing locations. One could say that due to cloud computing one of the harbors is on the move. Cloud computing turns the harbor into a flexible spot in terms of jurisdiction: it is not always clear where information is coming from, or at least the physical location varies. There is a lot of literature on law and cloud computing (Millard 2013). This paper focuses on the other end of the internet communication, flexibility due to the mobility of people.

Mobile devices add a new dimension: they are moved from one place to another, from one country to another. The nation state, both for national and international law the main actor as it comes to drafting and enforcing norms, does not match well with the cross-border nature of the internet. Sticking to the physical location would lead to application of different legal regimes during a car or

train trip, and in the not so near future the same will apply to plane trips. The fact that people travel and pass various jurisdictions is not new, but what is new here is that the same app, is used on the same device, by the same user, but with different law being applied? International Private Law does no longer work satisfactorily in this kind of situations.

Privacy: WhatsApp and Dutch DPA

WhatsApp is one of the most popular apps. Internet services are commonly free, or at least no direct costs are involved, and in this vein WhatsApp offers an unlimited number of text messages to be sent to your contacts. The telecom providers were not happy with this new service, for they charged for text messages. Interestingly enough, in the beginning telecom operators did not charge for text messages, as a colleague and seasoned observer of the telecommunication market often refers to during lectures. First, they did not expect many people would be interested to send such short, 140 character messages. Second, it did not cost additional bandwidth for it could easily be merged next to the relative voluminous voice communication. In 1992 cell phone users sent on average less than a single message per month.[3] The immense popularity of text messaging later turned this feature into a golden cow. Therefore, the growing popularity of the free WhatsApp caused concern for the telecom providers. In reaction, the Dutch provider KPN proudly presented to their stakeholders that by using deep packet inspection they could identify what services their customers were using:

> "We can measure the penetration of WhatsApp making us to my knowledge the first operator in the world that implemented the functionality to identify streams."[4]

This announcement was not received as enthusiastically as it was brought and actually caused major criticism. In fact, this action by KPN was one of the catalysts for Dutch Net neutrality regulation. Long before the European Parliament passed in April 2014 Net neutrality Articles as part of the Regulation Connected Continent, the Dutch government enacted in 2012 Article 7.4a on Net Neutrality in the Telecommunication Act.[5] Early 2014 KPN announced a rivaling service offering text messages to be sent over IP.[6] Their service would be based on RCS (Rich Communication Service/Suite).

A year before, in January 2013 the Dutch Data Protection Authority published a report on WhatsApp. They communicated in January 2013 "WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities". In their press release from 28 January 2013:[7]

> Privacy Commissioner of Canada (OPC) and the Dutch Data Protection Authority (*College bescherming persoonsgegevens,* (CBP)) today released their findings from a collaborative investigation into the handling of personal information by WhatsApp Inc., a California-based mobile app developer. (…)
> This marks a milestone in global privacy protection. (…)
> especially in light of today's increasingly online, mobile and borderless world (…)
> users (…) do not have a choice to use the app without granting access to their entire address book. The address book contains phone numbers of both users and non-users.

WhatsApp made some approvements, according to the same press release:

---

[3] http://nieuws-uitgelicht.infonu.nl/electronica/107507-we-smsen-al-sinds-1992.html
[4] Webwereld 12 May 2011
[5] Stb. 2012, 235; Stb. 2012, 231.
[6] http://tweakers.net/nieuws/93413/kpn-wil-whatsApp-beconcurreren-met-gratis-chatdienst.html
[7] http://www.cbpweb.nl/downloads_pb/pb_20130128-whatsApp-opc-cbp-newsrelease-en.pdf

> In September 2012, in partial response to our investigation, WhatsApp introduced encryption to its mobile messaging service.

Before that, the messages were not encrypted, so when intercepted could be easily read. Another point WhatsApp improved was the authentication of the service:

> WhatsApp has since strengthened its authentication process in the latest version of its app, using a more secure randomly generated key instead of generating passwords from MAC (Media Acess Control) or IMEI (International Mobile Station Equipment Identity) numbers (which uniquely identify each device on a network) to generate passwords for device to application message exchanges.

However, the policy WhatsApp still applies and is considered by the Dutch DPA a violation of privacy is the use of phone numbers of people not subscribed to WhatsApp. In their terms of services formulated under their Privacy notice as:

> "In order to provide the WhatsApp Service, WhatsApp will periodically access your address book or contact list on your mobile phone to locate the mobile phone numbers of other WhatsApp users ("in-network" numbers), or otherwise categorize other mobile phone numbers as "out-network" numbers, which are stored as one-way irreversibly hashed values."

The Dutch Privacy authority indicated that by doing this WhatsApp violates internationally accepted privacy principles:

> Rather than deleting the mobile numbers of non-users, WhatsApp retains those numbers (in a hash form). This practice contravenes Canadian and Dutch privacy law which holds that information may only be retained for so long as it is required for the fulfilment of an identified purpose.

In February 2014 the Dutch DPA announced they may fine WhatsApp for they had not reacted yet to the above 2013 observations.[8] It is questionable whether the Dutch DPA has authority to do so, because WhatsApp is American. Also, in their terms they explicitly state they offer their service for the US market and that people from EU of Japan should be aware of the fact their service may not comply with local rules. Terms of Service under 8 states it as:

> The Service is controlled and offered by WhatsApp from its facilities in the United States of America. WhatsApp makes no representations that the WhatsApp Service is appropriate or available for use in other locations. Those who access or use the WhatsApp Service from other jurisdictions do so at their own volition and are responsible for compliance with local law.

They do have part of their website in Dutch[9] which is an indication to under International Private Law to become subject to Dutch Law. The announced take-over by Facebook in February 2014 could be of influence too. Facebook has an office in Ireland and as a consequence is subject to EU law.

The case of WhatsApp clearly shows the complexity of enforcing norms. As the DPA stated, the norms they applied are internationally accepted principle privacy principles. However, if the US law

[8] http://www.nrc.nl/nieuws/2014/02/25/cbp-dreigt-met-dwangsom-tegen-whatsApp-vanwege-privacyschending/

[9] http://www.whatsApp.com/?l=nl

does not explicitly recognize these principles it is difficult to enforce these norms by the DPA. One could question what legitimization WhatsApp hat to impose norms on EU users that conflict with democratic enacted norms. WhatsApp can claim it is the responsibility of the users, but this is a bit naïve. If you offer services on a global scale, you should accept global norms. At least, in theory this makes sense. It could be only a matter of time before it works in practice as well.

Copyright: Pandora app in EU

Music and the internet are intrinsically connected. Since the days of Napster the music industry has changed dramatically. The initial central server based applications in 1999 were followed by Peer-to-Peer services such as KaZaa and Gnutella in 2000, and the bit-torrent protocol in 2001. The latter became in particular popular or – depending on your perspective - infamous through the Pirate Bay. All the mentioned providers were based on file sharing, whether or not via hyperlinks. Whereas the music industry concentrated primarily on fighting illegal trade, the technology company Apple launched in 2001 iTunes and this became the first model of online distribution of music for remuneration. Presently streaming services such as Spotify are gaining popularity. The concept no longer is based on sharing or downloading files, but bears more resemblance with radio. The main difference with radio is that the recipient can select the songs or albums she wants to listen to, so it is more like an infinite juke box. The streaming services are offered via internet connections, including apps on smart phones. One such app is Pandora. Pandora uses recommender systems to suggest music to listen to based on music she listens to and profiles of the user. On their website the following notice can be read:

> Dear Pandora Visitor
> We are deeply, deeply sorry to say that due to licensing constraints, we can no longer allow access to Pandora for listeners located outside of the U.S., Australia and New Zealand.

This notice is about the web service. I cannot find the terms of the app, and I am not sure whether the Pandora app can be used within the European Union. To make my point it actually does not matter, so I discuss both scenarios: that you can use the Pandora app everywhere, and that you can use the Pandora app only in US, Australia and New Zealand.

First, assume you cannot use the app outside US/AU. This means at least two things. The US/AU user is no longer able to use its app once abroad. Even when hiking or on a bike trip near the Canadian or Mexican border, the app may suddenly stop functioning. The mobility of devices puts the geographic enforcement of copyrights under severe pressure. Pandora has settled the copyright issue for US/AU but what does US/AU mean? Pure physical territory, not people? Is not it strange that someone visiting the US can use the Pandora app, but a US citizen cannot outside the US. Is this because GEO-blocking works on devices and not on people? Does technology determine how legal rights are managed? Whatever the reason is, if the enforcement would be linked to persons strange situations would occur too. The US student visiting Amsterdam could listen to Pandora while sitting next to his Dutch friend who would not be able to. The mobility of devices seems to beg for global oriented copyright norm enforcement. This brings us to the other scenario.

Second, assume anyone, anywhere could use the Pandora app. This would lead to a strange situation too. For users of smartphones it would make sense that they could use their Pandora app indifferent of their exact location. But if the IP-ban would still be enforced, it would be impossible to listen to Pandora via the regular website. Probably even Pandora would not work on the smart phone in case the web browser app is used, because then the regular website is visited. This would mean that enforcement would be localized depending on what application is used. So on smart phones and

tablets one could listen to Pandora as long as apps are used, as long as this app is not a web browsing app. On a laptop or desktop geography would still determine enforcement. So someone from the US/AU could not listen to Pandora on his laptop while in Amsterdam.

The internet already puts the geographic enforcement of norms under pressure, but mobile devices increases the pressure on global norms, or at least global enforcement of norms. Global norms or global enforcement may open another Pandora, in the sense of the well-known box from Greek mythology. If we would stick to national schemes and global enforcement, other countries may object to enforcement of these norms on their territory. What's more, it could lead to a situation in say Amsterdam or New York where over 100 different legal regimes would be applied to the same app, on the same location. If we would develop global norms this would lead to difficult questions as who should enforce these norms. Moreover, the past showed that the development of global norms is not an easy endeavor. But who knows, copyright has quite a good tradition with TRIPS and WIPO. Still, the question remains who is going to enforce these global norms.

Criminal law: Grindr in Russia

The last example is about using apps when travelling abroad and being criminalized for doing so. Given the wide variety of apps, one could easily be using an app in a country and doing something that is not allowed, or rather, that is criminalized. Probably users will not be aware of this. I am not sure whether foreign countries would prosecute tourists or business men because of the apps they use, but it might occur. So as long as countries being visited do not enforce their norms on strangers, there is not much of a problem. But what if they do? One of the central principles in criminal law is lex certa, and the question is how someone can know about the criminal nature of activities carried out by apps on a smart phone. People travelling abroad always should inform themselves about local norms. One could argue that apps are used on devices temporarily physically present on a foreign territory, but from a jurisdiction perspective one might as well consider the smart device, either a communication tool used anywhere irrespective of location or a private instrument governments should not interfere with anyway.

However, all countries do have power, including prosecuting authority, over the people physically present on their territory. Therefore it is possible that they decide to prosecute foreigners not even being aware of doing something wrong with their smart device. Who should warn them? Should the country at the border provide an overview of the basic rules? This is not common practice, and I would not expect countries would be willing to do that regarding apps. Maybe it should be the task of the home country, or even on a higher level like the European Union, to warn for use of certain apps or particular conduct in specified countries. For the Arab peninsula it may be wise to inform people about in particular speech and religion related issues. The example I want to use here is about the currently popular dating app Tinder. Assume someone is travelling to Russia, would he run a risk if his settings are on either male looking for male or female looking for female? In the example I will use the special Gay community app called Grindr.

In 2013 Russia passed the anti-gay propanda law, or as it is officially called "propaganda of nontraditional sexual relations to minors". So this 19 year old gay student visits Moscow, starts his Grindr app, likes a particular boy that appears to be 17, and starts chatting with this boy. Note that using electronic media, e.g. apps on a smart phone, multiplies the fine by 10-20:

> **If you're an alien.** Foreign citizens or stateless persons engaging in propaganda are subject to a fine of 4,000 to 5,000 rubles, or they can be deported from the Russian Federation and/or serve 15 days in jail. If a foreigner uses the media or the internet to engage in propaganda, the fines

> increase to 50,000-100,000 rubles or a 15-day detention with subsequent deportation from Russia.[10]

Of the discussed cases this one may be the least problematic. Obviously not in terms of possible consequences, but in terms of remedies. Ministries of foreign affairs could inform people when travelling to Russia. Maybe incidents in other countries with people being criminalized when using apps could be collected and communicated to travelers via, e.g. ministries of foreign affairs. It is always better not to wait for incidents to happen, so if people know about possible dangers of using, in particular popular, apps this information should be widely communicated, with an active role for governments.

As for the Grindr app, a possibility could be that the provider of the service sends an in app-message the moment he finds out through GPS that the user is on Russian territory. This in fact happened at the time of the Olympic Games in Sochi:

"You will be arrested and jailed for gay propaganda in Sochi according to Russian Federal Law 135 Sektion 6,"

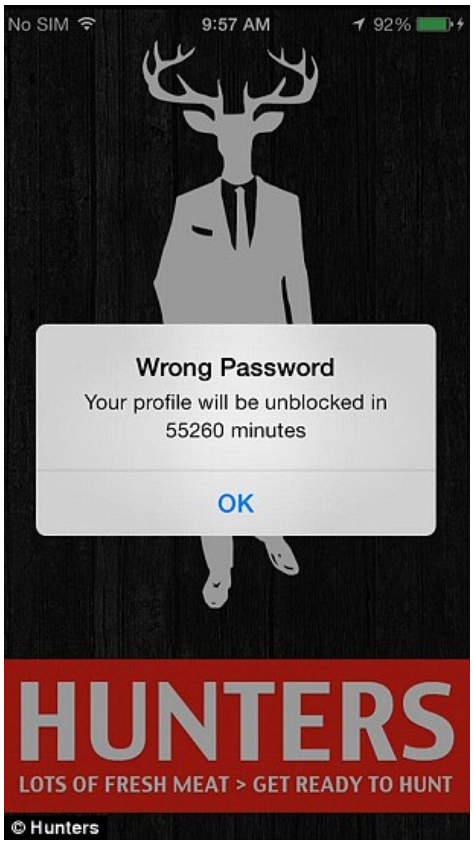
It could be phrased more friendly, of course. The sender of this message is unknown, but could have been hackers and possibly the Russian government. The message was sent on 1 February 2014 to users in Russia of the app Hunters, a Russian gay hook-up app pretty similar to the American app Grindr.[11] Another source mentioned hackers, and also that accounts were blocked for a period to end after the Olympics:[12]

“Anti-gay hackers have reportedly shut down more than 70,000 accounts on a Russian gay dating app and threatened its users with arrest.”

[10] http://www.policymic.com/articles/58649/russia-s-anti-gay-law-spelled-out-in-plain-english

[11] http://www.policymic.com/articles/81359/this-is-the-message-people-on-russia-s-version-of-grindr-just-received

[12] http://www.dailymail.co.uk/news/article-2554971/You-jailed-gay-propaganda-Hackers-threaten-thousands-men-Russian-version-hook-app-Grindr.html



Concluding observations

The internet has challenged the legal system from the moment it became widely available in the 1990s. The European Union has been very active in drafting norms to harmonize law on electronic contracting, privacy and security. This is a good first step, though one should not expect that all countries in the world accept the legal framework developed by the European Union.

The mobility of people, and their smart devices they take everywhere, including abroad, begs the question whether the legal norms applicable to the apps being used should really vary depending on the physical location. The users of smart devices, e.g. tourists and business men, normally would not realize or expect that apps do things with the information on their phones not allowed in their home country, apply terms that are detrimental, and in the worst case may get them in jail.

Theoretically, global norms, and local enforcement may be the most optimal solution. In practice we maybe never accomplish this or another ideal situation. Nonetheless as scholars we should not stop addressing those challenging questions. I do not, however, have the definite answers, yet.

References

Arabo, A., Brown, I. & El-Mousa, F. (2012) Privacy in the Age of Mobility and Smart Devices in Smart Homes. ASE/IEEE International Conference on Privacy, Security, Risk and Trust, Amsterdam, Netherlands, September 2012.

Beresford, A.R. *et al.* (2011), MockDroid: trading privacy y for application functionality on smartphones, *Proceedings HOTMOBILE 2011 12th Workshop on Mobile Computing Systems and applications*

Enck, W. *et al.* (2010), TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, *Proceedings of the 9th OSDI'10 (USENIX Symposium on Operating Systems Design and Implementation),* http://static.usenix.org/events/osdi10/tech/full_papers/Enck.pdf

Ghogare, S.D. *et al.* (2012), Location Based Authentication: A New Approach towards Providing Security, *International Journal of Scientific and Research Publications*, Volume 2, Issue 4, April 2012

Goldsmith, J. & T. Wu (2008), Who Controls the Internet? Illusions of a Borderless World, Oxford university press

Kerr, O.S (2003), The Problem of Perspective in Internet Law. *Georgetown Law Journal*, Vol. 91, February 2003

Kohl, U. (2010), *Jurisdiction and the Internet: Regulatory Competence over Online Activity*, Cambridge University Press

Leontiadis, I. (2012) Don't kill my ads! Balancing Privacy in an Ad-Supported Mobile Application Market, *HotMobile '12 Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*

Lodder, A.R. (2013), Ten Commandments of Internet Law Revisited: Basic Principles for Internet Lawyers. *Information & Communications Technology Law*, Vol. 22, Issue 3

Lodder, A.R. (2014), Information Requirements Overload? Assessing Disclosure Duties Under the E-Commerce Directive, Services Directive and Consumer Directive, in: Savin, A., Trzaskowski, J., *Research Handbook on EU Internet Law* (Elgar, Cheltenham 2014), Forthcoming.

Mac Sithigh, D. (2013), App Law Within: Rights and Regulation in the Smartphone Age, *International Journal of Law and Information Technology*, 2013, 21(2), pp. 154-186

Millard, C. (ed.)(2013), *Cloud Computing Law*, Oxford University Press.

Post, D.G. (2009), In search of Jefferson's moose. Notes on the State of Cyberspace, Oxford university press

Tu, K.V. (2013), From Bike Messengers to App Stores: Regulating the New Cashless World, *Alabama Law Review,* Vol. 65, No. 77-138, 2013