When 'there' can be everywhere: On the cross-border use of WhatsApp, Pandora, and Grindr

Arno R Lodder[1]

Cite as Lodder A.R., "When 'there' can be everywhere: On the cross-border use of WhatsApp, Pandora, and Grindr", in European Journal of Law and Technology, Vol 5, No 2, 2014.

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 of users complicates norm application. Global use, on a global infrastructure does not match well with local, national law.

This paper briefly discusses the quadruplet contracting, security, privacy and advertisements. The main question addressed is how the use of apps, in particular when crossing borders, has impact on the traditional jurisdiction model. Three cases are used to illustrate how apps and smart devices complicate norm application. The issue of privacy is exemplified by discussing the program WhatsApp, the music app Pandora is used to address copyright, and finally the dating app Grindr focuses on criminal law. The already difficult application and enforcement of norms on the Internet increases now devices providing Internet connections are seamlessly taken from one country to another, and are always in the proximity of their users: they are always connected, always available.

1. 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, soon 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. It seems the World Wide Web is going to do justice to its name: the Internet is becoming truly global. What about the law?

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 without a final answer yet, in a wide body of literature that is covered in section 3 of this paper.

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

[1] CLI - Center for Law and Internet, Department Transnational Legal Studies, Vrije Universiteit Amsterdam & SOLV attorneys-at-law Amsterdam. I want to thank the referees and the audience at the Bileta conference in April 2014 where a draft version of this paper has been presented.

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, and under what conditions? What service does an app exactly deliver, 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.

Some authors did cover the topic of mobile devices and apps yet. Mac Sithigh (2013) analyses the role the app stores play in regulation of apps and smart devices. Kemp (2013) discusses contractual and regulatory issues related to mobile payments. Tu (2013) also addresses the growing use of smart devices for payment, and suggests changes in the regulation of money transactions that do take consumers interests into account. Various publications cover the issue of privacy in the context of smart devices (e.g., Enck *et al.* (2010), Beresford *et al.* (2011), and Arabo *et al.* (2012)). Leontiadis (2012) discusses the use of advertisements and the impact on privacy. All these papers add to the analysis of the legal landscape that is briefly discussed in section 2, viz. norms on contracting, privacy, security and advertisements applicable to apps.

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. In section 3 the topic of crossing borders with smart devices is introduced.

The approach in this paper is different from what has been written until now, because it focuses on the complexity of cross-border law in relation to apps and smart devices. The paper adds a new chapter to the older jurisdiction on the Internet discussion, and offers an analysis of the need for a globally oriented normative framework. The paper discusses three apps: the communication app WhatsApp, the music app Pandora, and the dating app Grindr. The reason to select these apps is first that these cases cover important Internet law areas: WhatsApp focuses on privacy, Pandora on copyright, and Grindr on criminal law. Second, the cases describe three different situations regarding location: The WhatsApp-case is about legal implications of local use in the Netherlands, the Pandora case is about the legal differences between local use in the USA and use elsewhere, and the Grindr case is about the use of the app abroad.

2. 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 often delivered via apps instead of via websites. 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.

Norms on contracting, privacy, security and advertisement can be considered the four pillars concerning the regulation of apps. All these norms interlock. Terms of contract should include information on privacy, advertisements, 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 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. But first I briefly introduce the relevant legal issues related to contracting, privacy, security, and advertisements.

2.1 CONTRACTING

Contracts are the fundament of law surrounding smart devices and apps. If users buy apps they conclude a contract, and before doing so they should be informed about privacy, security and if and how advertisements are used. The actual conclusion of the contract is not really posing challenges, because 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. This latter aspect, information requirements related to electronic contracting, is covered in various European Union directives.

Regarding information to be communicated the question is first what information should be communicated to the buyer of the app, and second how this information should be 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. Article 5(1) requires information society service providers to present their name (sub a), geographical address (sub b), e-mail address (sub c), etc. Article 6 addresses commercial communications, e.g., these should be clearly identifiable as such (sub a), and discounts, premiums and gifts shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously (sub c). Finally, Article 10 addresses information particularly related to electronic contracting, such as about the different technical steps to follow to conclude the contract (sub a), and the technical means for identifying and correcting input errors prior to the placing of the order (sub c). Compliance with this series of information requirements already poses challenges for ordinary websites, let alone on the small screen of a smart phone. But there are even more information duties. Article 22 of the Services Directive 2006/123 defined additional disclosure duties for service providers, such as about the existence of contractual clauses concerning the law applicable to the contract and/or the competent courts (sub g), and after-sales guarantee (sub h). Most recent is the Consumer Directive 2011/83 (amongst others replacing Directive 97/7 on distance selling) adding in Article 6(1) over 20 information requirements on the main characteristics of what is ordered (sub a), payment schemes (sub g), a reminder of the existence of a legal guarantee of conformity for goods (sub l), 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 an informed decision requires the right balance between information overload and too little information (Lodder 2014).

Obviously, if someone wants to have this particular nice app, he is not really interested in the terms and conditions. This lack of interest can hardly be remedied, but the recipient of the service should at least have 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 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.

What is needed is a reconsideration of the current information requirements landscape. My suggestion is to develop a reduced set of necessary information, and guidelines on how this information should be communicated on small screens. In addition to what has been addressed above, also information should be communicated about privacy, security and advertisements.

National laws will not always be effective, since app developers can be located anywhere. State regulation on a global scale will prove difficult, but maybe the European Union could play a leading role, and by creating a good solution for all parties involved realize global effect. The App stores of Apple and Google seem, due to their market share and global presence, the best actors to address norm enforcement. It is questionable whether they are willing and able to act as such.

2.2 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 Ethan Katsh 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.

App developers should define the purpose (cf. Article 6(1)(b) Directive 95/46/EC) for the processing of personal data, and maybe even more important restrict the collection and processing of personal data to what is necessary, so-called data minimisation cf. Article 6(1)(c). Then, in line with the above discussion under contracting, users should be adequately informed about the processing.

2.3 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 European Union proposed early 2013 a Directive on network and information security in which it is recognized under 3.1 legal basis:[2]

> 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.

Although no particular attention is paid in this Directive to smart devices as the main points of Internet access, they naturally add to the transnational nature of security issues. Apps that are not developed meeting state of the art security requirements are a threat, not only to the device of the user but may also impact the national infrastructure. Another point related to security is necessary awareness of users, e.g. risks related to using unsecured WIFI or being connected to a WIFI spot without even knowing.

Security of apps and smart devices only become more important, now smart phones can be used for payments and all kind of other sensitive services (put your light on at home, open your house and start your car).

2.4 ADVERTISEMENTS

Advertisements used to be general communications, and personalized advertisements were 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, according to the urban legend parents found out that their son 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. There is a wide body of literature on cookies related to websites (e.g., Hoofnagle *et al.* 2012, Helberger 2013). Interestingly enough, the neutral definition of cookie in Article 5(3) Directive 2002/58 as "store information or to gain access to information stored in the terminal equipment of a subscriber" means it also applies to whatever information apps put on the smart device.

The definition of information society services used in EU Directive 2000/31 on e-commerce 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 (Lodder 2002).[3] Many free apps as well as paid apps generate income from advertisements. In

[2] 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.

[3] Confirmed by the European Court of Justice on 11 September 2014, case C-291/13: "must be interpreted as meaning that the concept of 'information society services', within the meaning of that provision, covers the

case of free apps the use of in app purchases raises legal concerns that need to be addressed. Both the FTC[4] and the EU[5] urged apps stores and developers to be cautious with in app purchases, also because of children using smart devices.

Third party advertisers may have access to user information, including the user's location. 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:[6]

> 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 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. Practical experiments, amongst others carried out by some of my students in 2013,[7] show that the information communicated surpasses what users would expect. For instance, while not respecting their own terms the app Tinder shared information of its users with the data mining company Kontagent.com. So even if contractual terms are communicated, users can be unaware of what really is happening. This demonstrates once more the need for normative boundaries, the question of course is who is going to create the norms and who is going to enforce them. This leads us to the cross-border aspect of using apps.

3. 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 app stores. Obviously, the app ecosystem knows many actors. The question then becomes, in particular in cross-border situations, what legal norms do apply and to what actors. 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).

---

provision of online information services for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website."

[4] *FTC Sues Amazon Over In-App Purchases by Children*, Wall Street Journal 10 July 2014.

[5] *In-app purchases: Joint action by the European Commission and Member States is leading to better protection for consumers in online games*, http://europa.eu/rapid/press-release_IP-14-847_en.htm, 18 July 2014.

[6] 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

[7] Experiment carried out November 2013 by Sandy Pronk, Samuel Wiegerinck and Gregory Van Zetten.

Grotius (1583-1645) introduced the concept Law of the Sea that is now regulated in the 1982 UN Convention.[8] 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, as a place (e.g., Johnson & Post 1996):

> Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character, which differs markedly from anything found in the physical world.

Others (e.g., Goldsmith & Wu 2008) defend the position that on the Internet national law remains most relevant. In that perspective decisive is the fact that any Internet communication in the end is taking place from a physical location, and 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 (Kohl 2010).

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 (Reed 2010, 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.

4. 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. Telecom providers charge for text messages, so they were not happy with this new, free Internet-based service. Interestingly enough, at first telecom operators did not charge for text messages, as a colleague and seasoned observer of the telecommunication market often refers to during lectures. In the first place because telecom providers did not expect people would be interested in sending such short, 140 character messages. Second, the sending of text messages did not cost additional bandwidth for it could

[8] United Nations Convention on the Law of the Sea of 10 December 1982.

easily be merged with the relative voluminous voice communication. In 1992 cell phone users sent on average less than a single message per month.[9] The immense popularity of text messaging later turned this feature into a cash cow. The growing popularity of WhatsApp led the Dutch provider KPN to proudly presenting to their stakeholders that by 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.[10]

This announcement was not received as enthusiastically as it was brought. Instead major criticism was raised, and the incident became one of the catalysts for Dutch Net neutrality regulation. Long before the European Parliament passed in April 2014 Net neutrality Articles[11] as part of the Connected Continent Regulation,[12] the Dutch government enacted in 2012 Article 7.4a on Net Neutrality in the Telecommunication Act.[13] Early 2014 KPN announced a rivaling service offering text messages to be sent over IP.[14] 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:[15]

> 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 improvements, according to the same press release:

> 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.

---

[9] http://nieuws-uitgelicht.infonu.nl/electronica/107507-we-smsen-al-sinds-1992.html
[10] Webwereld 12 May 2011
[11] Colin Mann, European Parliament passes telecoms reform package, http://advanced-television.com/2014/04/03
[12] http://ec.europa.eu/digital-agenda/en/connected-continent-single-telecom-market-growth-jobs
[13] Stb. 2012, 235; Stb. 2012, 231.
[14] http://tweakers.net/nieuws/93413/kpn-wil-whatsApp-beconcurreren-met-gratis-chatdienst.html
[15] http://www.cbpweb.nl/downloads_pb/pb_20130128-whatsApp-opc-cbp-newsrelease-en.pdf

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.[16] An interesting question is whether the Dutch DPA has authority to do so, because WhatsApp is an American company. One could argue WhatsApp links the domain name Whatsapp.nl to a Dutch language version of Whatsapp.com. According to the EU Court of Justice:[17]

> In order to determine whether a trader whose activity is presented on its website (…) can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001, it should be ascertained (…) that the trader was envisaging doing business with consumers domiciled in the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them.

Use of the language, Dutch in this case, is considered a strong indication for a service being directed to a particular country. It seems reasonable that service providers targeting customers in the Dutch language have to comply with Dutch (in this case EU) law, but this is not globally accepted. An American country can offer services, and as long as they are not established within the European Union they cannot be legally forced to comply with EU law, yet.

Also, in their terms WhatsApp explicitly states 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:

> 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.

The take-over by Facebook in February 2014 could be of influence, because Facebook has an office in Ireland and as a consequence is subject to EU law.

---

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

[17] On 7 December 2010, joined Cases C-585/08 and C-144/09 (Pammer & Alpenhof).

The case of WhatsApp clearly shows the unsatisfactory consequences of applying traditional rules of jurisdiction. As the DPA stated, the norms they applied are internationally accepted privacy principles. However, if the US law does not explicitly recognize these principles it is difficult to enforce these norms by the DPA. One could question what legitimization WhatsApp has to apply to EU users terms that conflict with democratic enacted EU 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 be willing to accept global, and sometimes even local, norms. I expect over time law adapts to what I would say is a justifiable approach, viz. respecting fundamental as well as other legal norms applicable to user's locality.

5. COPYRIGHT: PANDORA APP CROSSING BORDERS

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 application was made popular or – depending on your perspective – infamous by 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 successful remuneration model of online distribution of music. Presently music streaming services such as Spotify, and Netflix for videos, 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. The parallel can be drawn with 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 you listened to as well as user profiles. 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. The reason they could no longer offer their service was that they needed licenses from right management organisations. These organisations are nationally organized,[18] and are not always very cooperative. Even if they were, this would mean that to offer Pandora within the EU, contracts with 28 collective right management organisations had to be concluded. Or as Manziotti (2011) puts it:

> The unbearable complexity of online rights clearance processes is a major problem for commercial users wishing to develop and launch pan-European online content services and to take advantage of the E.U. cultural sector as a whole.

This may become easier in the future, since there are initiatives to develop pan-European clearing (Hilty and Nérisson 2013). The consequences of Pandora not being able to clear the copyrights was a nuisance to users who liked Pandora outside the US, Australia, New Zealand.

[18] See a column pleading for Pandora services in the Netherlands by Menno Heerma van Voss, http://www.solv.nl/weblog/red-pandora/4571

The mobility of devices in combination with the blocking of services by geo ID software leads to users not being able to use a service they have paid for while travelling. Or, as more and more users do abroad, they can use Virtual Private Network (VPN) software in order to circumvent the technical measures (Trimble 2012).

I cannot find the terms of the Pandora app, and I am not sure whether the Pandora app can be used within the European Union. I presume you cannot use Pandora abroad, but 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 the US. This means at least two things. The US user is no longer able to use his 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 rationale of geographic enforcement of copyrights under pressure. Pandora has cleared copyrights for the US but what does the US mean? Pure physical territory, not people? Is seems strange that someone visiting the US can use the Pandora app as long as he is in the country, and a US citizen cannot use it outside the US. Is this because GEO-blocking works on devices and not on people? Does technology determines here 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 was used, because then the regular website is visited. This would mean that enforcement would be localized depending on what device is used, and what program on that device. 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 could not listen to Pandora on his laptop while in Amsterdam.

The option to have national schemes and global enforcement would not work, because then 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. In case of copyright enforcement, mobile devices increase the need for global norms. The past showed that the development of global norms is not an easy endeavor. However, copyright has a good tradition with initiatives like TRIPS and WIPO. If we succeed in developing global norms, the question regarding who should enforce these norms remains. The country of origin principle could be the solution. Enforcement would then take place where the provider is established, so the location where the provider of the service, notably the app, is initiated.

6. CRIMINAL LAW: GRINDR IN RUSSIA

The last example is about using apps when travelling abroad and being criminalized for a particular use of an app. Given the wide variety of apps, one might use an app in a country that forbids this use. Users will not necessarily be aware of this. It depends on the country whether tourists or business men would be prosecuted because of the apps they use, but it is not unthinkable. As long as countries being visited do not enforce their norms on strangers, there is not really 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 the devices are 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 have the power to prosecute 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? As a sample app I use the special dating app for the Gay community called Grindr.

In 2013 Russia passed the anti-gay propaganda law, or as it is officially called "propaganda of nontraditional sexual relations to minors". Assume a 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 the use of electronic media, e.g. apps on a smart phone, multiplies a possible 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.[19]

Of the discussed cases this 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 that the user is on Russian territory. It is questionable whether such a built in feature can be demanded from the provider of the app.

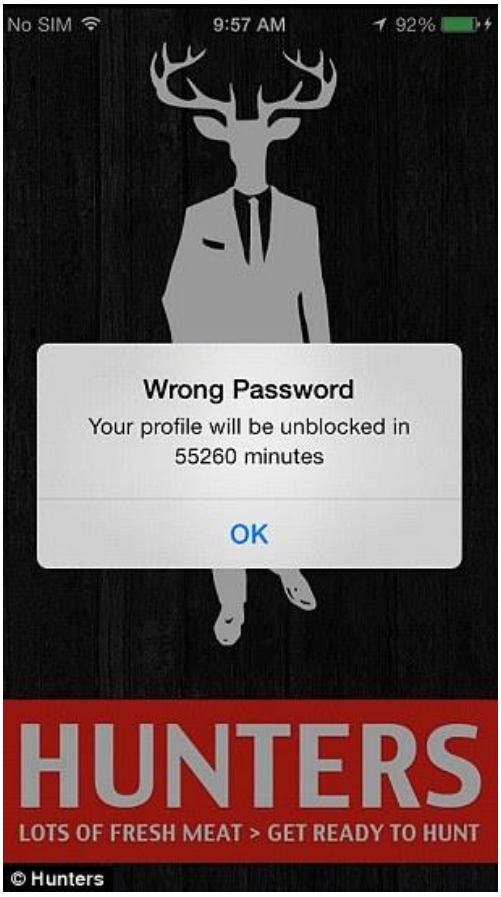
At the time of the Olympic Games in Sochi users of the app Hunters, a Russian gay hook-up app pretty similar to the American app Grindr, received on 1 February 2014 the following message: [20]

[19] http://www.policymic.com/articles/58649/russia-s-anti-gay-law-spelled-out-in-plain-english
[20] http://www.policymic.com/articles/81359/this-is-the-message-people-on-russia-s-version-of-grindr-just-received

> You will be arrested and jailed for gay propaganda in Sochi according to Russian Federal Law 135 Section 6

It is not known who the sender of this message was, but it could have been hackers and even the Russian government. It has been reported that accounts were blocked for a period to end after the Olympics:[21]

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



A message similar to the above, more friendly phrased of course, could be sent be either the provider of the app or, e.g., the ministry of foreign affairs of the home country of the user. In the latter case the message should be of a more general nature. Currently ministries do warn people for particular countries, and they may adapt their activities to the use of apps. In the Netherlands the ministry of foreign affairs is working on apps to inform their citizens abroad, as well as helping them to get in contact with each other in a case of catastrophes. Based on voluntary subscription an app could be offered that warns for use of certain apps depending on the country where you are travelling. The sending of information about what is and is not allowed could be coordinated on a global scale, e.g. by a UN agency.

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

7. 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 towards the development of global norms, 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.

In the case of WhatsApp the Dutch Data Protection Authority claimed to apply a global norm, viz. internationally accepted privacy principles. The Pandora app, and services as Spotify and Netflix, clearly is a case in point of global oriented copyright norms. The criminal law case on Grindr is of a different nature, in that local norms are applied. The harmonization of substantial criminal law is not very realistic, probably harmonization of the not discussed procedural criminal law is sooner to be expected but still difficult.

It may be a matter of time before providers of apps comply with local norms, just as we have seen happening on the Internet, where providers such as Google, eBay and Yahoo do comply. I expect over time law adapts to what I would say is a justifiable approach, viz. respecting fundamental as well as other legal norms applicable to user's locality. It would be better though, in particular in the light of users that travel, if global norms are developed.

In the discussion of WhatsApp it was argued that it does make sense for a provider to comply with democratically drafted norms that are applicable to the users of their app. In the area of privacy and copyright, as well as for the not discussed contracting, advertisements and security, the cross-border use of apps could stimulate the development of global norms. One way this may be realized is that EU norms are accepted by countries outside the EU.

If we do succeed in developing global norms, the question regarding who should enforce these norms remains. The country of origin principle could be applied. Enforcement would then take place where the provider is established, so the location where the provider of the service, notably the app, is initiated. App stores could play a crucial role in enforcing these norms. It may even turn out that the normative standards App stores set become a global standard. Whatever happens in the future regarding norms for smart devices and apps, I expect globalization to strengthen due to the mobility of users, and global norms to increase.

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 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

Hilty, R. and S. Nérisson (2013), Collective Copyright Management and Digitization: The European Experience, in: R. Towse and C. Handke (eds.), *Handbook of the Digital Creative Economy*, Cheltenham: Edward Elgar, 2013

Johnson, D.R. and D.G. Post (1996), Law and Borders - The Rise of Law in Cyberspace, *Stanford Law Review*, Vol. 48, p. 1367.

Kemp, R. (2013), Mobile payments: Current and emerging regulatory and contracting issues, *Computer Law & Security Review*, Volume 29, Issue 2, April 2013, Pages 175–179

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. (2002), Chapter 4 - Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. In A.R. Lodder & H.W.K. Kaspersen (Eds.), *eDirectives: Guide to European Union Law on E-Commerce. Commentary on the directives on distance selling, electronic signatures, electronic commerce, copyright in the information society and data protection*. Den Haag: Kluwer Law International, http://ssrn.com/abstract=1009945

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

Manziotti, G. (2011), *New Licensing Models for Online Music Services in the European Union: From Collective to Customized Management*. Columbia Public Law Research Paper No. 11-269, http://ssrn.com/abstract=1814264

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

Reed, C. (2010), *Information 'Ownership' in the Cloud*. Queen Mary School of Law Legal Studies Research Paper No. 45/2010. Available at SSRN: http://ssrn.com/abstract=1562461

Trimble, M. (2012) The Future of Cybertravel: Legal Implications of the Evasion of Geolocation, *Fordham Intellectual Property, Media & Entertainment Law Journal*, Vol. 22.

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

Walden, I. (2011), *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, Queen Mary School of Law Legal Studies Research Paper No. 74/2011. Available at SSRN: http://ssrn.com/abstract=1781067