Service Providers Accountability

Sergi Torralba
Albert Meroño
Antoni Roig
Institute of Law and Technology, Autonomous University of Barcelona
(IDT – UAB)

Abstract. The goal of this paper is to guide through some obscure parts of the regulation and legislation related to technology. Even if we are not experts on security Internet, we will try to explain the difficulties that lawyers should be aware of when regulating rights and limits in the net. Some real cases related to service providers (ISP and others) are described and complemented with the technological context of each case.

Keywords: Regulation, Technology, Internet, Legislation, ISP.

1. Introduction (end-wire users are transparent to ISP)

Recently there is a trend to make Internet Service Providers (ISP) responsible for any infraction committed by their users. There are technological arguments to hold that may be this is not the correct way.

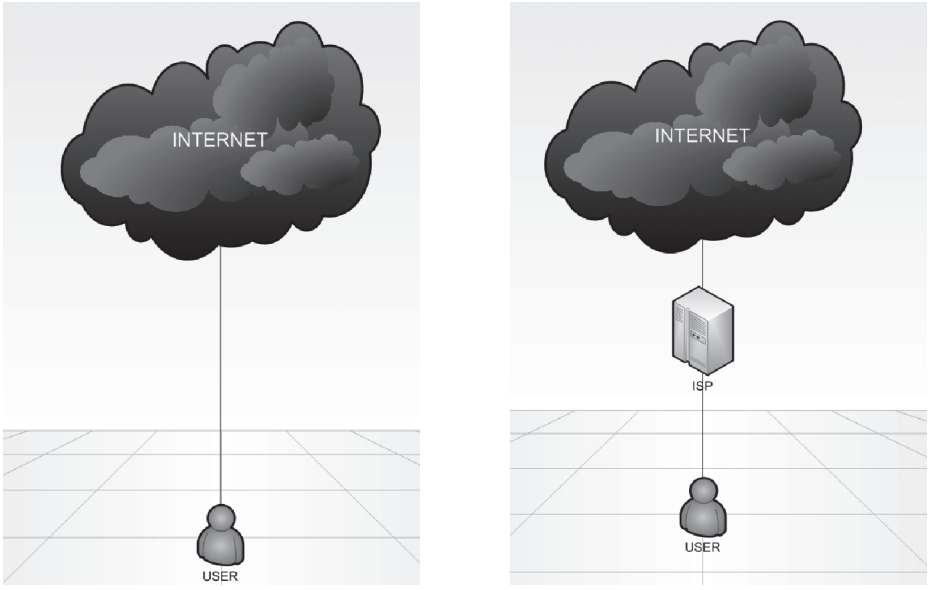
In this introduction, we are going to explain a general framework on how technology and Internet connections have evolved in the last 15 years. In Spain all began with InfoVia[1] in 1995 and its speed was 28.800 bps. Meanwhile, Intel presented the Pentium 133 which has a speed of 133 MHz. Nowadays we have multiple of options to connect to Internet from de evolution of InfoVia, which are the ADSL connections at a speed around the 20 Mbps more than 700 times faster. And the technology has also improved. Some processors like Core 2 Quad Q9650 of Intel have a speed of 3 GHz, and even if it is only 30 times faster, we have to consider that 15 years ago there was only 1core. Now we can have 4, which is similar to having 4 processors working together. Furthermore, in the 90s very few could imagine how many devices would be able to connect to Internet. Not only are computers connected to the Internet, but even some fridges are able to be connected. So, technology went fast, and laws could not follow.

Maybe because at the beginning there was a lack of control and Internet was something only for few people, there has been a misconception with the users. At the beginning of the use of Internet in Spain, users were quite ex-

1. Article about the creation of the creation of InfoVia: http://www.elprofesionaldelainformacion.com/contenidos/1995/noviembre/impacto_de_infova_de_telefnica.html

perts, and Internet was lawless. Perhaps people thought they were connected to Internet directly, and did not realize that there was something between them and the net, may be something like Figure 1.

Figure 1. User vision of the Internet connection



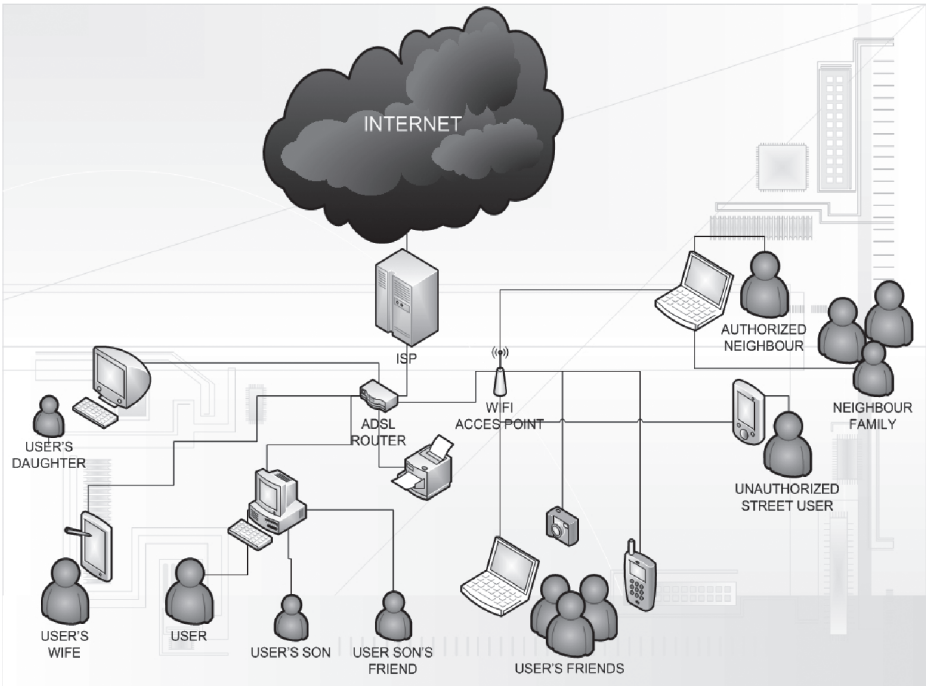
When the user, mainly the classic user, considers that everything can be done, then the reaction of regulators is to limit some possibilities. But here comes a new misconception, from the legislators' point of view (Figure 2). Regulators consider that the ISP is responsible because it knows exactly who the user is and what the user does. And this is not true. The ISP only knows who pays the service, but it can't say if there is only one person using that user account. There might be many different persons with the same line (Figure 3):

Let's imagine a house, Alice lives there and she is a mother who pays the Internet account. Alice has a computer and she does not worry about security. They have only one account and all the family uses it. The son does his homework and sometimes some friends come to work together. Furthermore, the father of that family uses his PDA to connect to Internet. Their daughter also has another computer in her room, and sporadically some friends come to the house with their own laptop. One of them is a geek and has a SD (Eye-Fi[2]) that connects automatically with the WIFI access point and sends the photos to Internet. Alice is a good neighbour. She shares her connection with a neighbour that has promised her to use it for email, but the neighbour's children have not

2. SD with WIFI connection: http://www.eye.fi/overview/index.html

promise anything. And finally, there's a bar with a terrace in front of Juan's home and where some people try to and get access to his connection.

Figure 2. An example of a possible Internet account use



In short, at least 7 different persons can connect to Internet with Alice's account. And we have not taken in account the printer that automatically connects with the technical service if it detects any problem. We can also add a fridge with Internet connection. This is not science fiction: someone has even excused crimes alleging that it was due to his pet[3]. It is easy to see that end-wire users (final users who use Alice's router to reach the Internet through Alice's ISP) are transparent to the ISP itself. Due to technical limitations or features of the IP protocol (IPv4 has an insufficient number of IP addresses to reference all current Internet users; Network Address Translation (NAT) solves it assigning one –and only one– IP address to all users using Alice's subnet), the number of users or their identity far away from Alice's router is totally unknown for the ISP. So, the ISP could avoid some responsibilities and make Alice responsible of any user (known or unknown to her) using her account.

3. Some people do not bother to accuse their own pet: http://www.nbcmiami.com/news/local-beat/Man-Naughty-Kitty-Downloaded-Kiddie-Porn-52640667.html

Imagine that in Spain we want to make Telefonica, and the others ADSL providers in charge of all the people connecting with their services. More than five million lines have ADSL contracted[4]. If we include business, then there are more than nine million lines.

2. Industry wants to ban a woman from downloading ("access" and "download" are technically synonyms)

After a federal judge ruled that a woman accused of sharing over 1700 song had to pay $1.92 million, the Music Industry wants now to ban that woman from downloading[5]. This is not easy to implement. For example, you can ban her user, her name or ID and make impossible to her to contract any service, but she can steal the Internet of a neighbour, or she can contract Internet with a name of a relative. Then we can use something like MAC (Media Access Control) address, and block that address from the Internet, but she can change the MAC address, or buy another network adapter. So, then, we will have to prohibit her to buy any adapter or device that can be connected to Internet, but then someone can give her a Smartphone or any similar device as a present and she will have access to Internet again. So we will have to contract an inspector to watch her house and monitor that no one lets her to connect to Internet and download anything. But she can go to an Internet coffee and download something to a pen drive, so we will have to have a fulltime employee keeping an eye on her. The easiest would be to keep her in a dungeon. Why not? She would not be left there to stop her from seeing the light of the sun, but because the castle's walls impede good coverage. However, that solution would imply cutting her freedom for more than "don't let her download again".

In IT, and more precisely in computer network language, the words "access", "upload" and "download" are technically synonyms. Accessing a website, for example, consists of uploading a request to a web server and receive a download (possible a HTML document), which is the web document that we finally see in a web browser. With this in mind, it is easy to see that banning someone from downloading Internet content is banning him or her from accessing any Internet content. To sum up, this means banning him or her from using almost any electronic device, which is not feasible nowadays.

3. FACUA accuses Microsoft, Yahoo and Google for low security in the access to email accounts

FACUA has informed the Spanish data protection Commissioner (AEPD) that Microsoft, Yahoo and Google do not respect the Spanish Data Protection Act[6].

4. More exactly 5.598.691: http://www.cmt.es/es/publicaciones/anexos/I_Trimestral_09_OK_.pdf
5. http://arstechnica.com/tech-policy/news/2009/06/jammie-thomas-retrial-verdict.ars.
6. https://www.facua.org/es/noticia.php?Id=3774.

FACUA does not blame those companies for having a bad encryption mechanism, or a bug that makes easy the access to other people's account. What they say is that the mechanism of the "security question", used to in case of having forgotten the password, is not trustful. That mechanism is provided to help the user and relies on the user. The "security question" asks the user to select a question from some predefined (as "What's your favourite pet's name?", "What's your primary teacher's name?" and similar) and provide the answer to them. But if the service provider asks the user to choose one question the user is not forced to answer sincerely that question. This gives the service provider a way to help the user if he forgets the password. The user may write what he wants in the answer: a more complicated password, a fake answer, the real one but writing numbers between the letters and many other options. The solution that FACUA propose is to give another email address to have the password sent in case the user asks for it. This requires that the user has a second email address and a different password from the one that is forgotten. Indeed, if the two email accounts have the same password and both email addresses are used as a backup address, you have lost the two accounts. Common sense is also useful in Internet. If you are a famous actress and you have a dog and everybody knows how much you love your dog, please do not use as security-question "What's your favourite pet's name?", as Paris Hilton did[7].

4. Germany will block by law online children pornography

Germany is going to install some kind of software that will block the access to child pornography web sites[8]. This would be very beautiful if it was possible, but this would be like blocking all the content of one kind. All the authoritarian countries would pay a lot for this software, because they would be able to block what they do not want to be accessed by their people. For the moment, it is not possible. Furthermore, paedophiles usually share their data using private channels like forums, or they send via classical mail DVDs. There is no intelligent software that can discover if the images of a website or the videos are classified as child pornography. We can imagine that paedophiles will neither buy the domain www.childporn.com or www.paedophilesclickhere.com, nor will name the files childporn.jpg childporn2.jpg. So what can be done is to block known websites, as the Spanish Science and Technology Ministry did with the Euskal Herritarrok sites. For the moment, we cannot automatically detect new sites. Someone has to monitor the whole web if we want to avoid people to connect to any worldwide site, not only the German ones. If Germany is the only country to block, then we could avoid the effects of the measure with a

7. How Paris Hilton account was hacked: http://www.oreillynet.com/pub/a/mac/2005/01/01/paris.html
8. http://noticias.terra.es/Economia/2009/0325/Actualidad/Alemania-bloqueara-por-ley-la-pornografia-infantil-online.aspx

web proxy server. A proxy is a machine that provides you with the content you are trying to get. Nevertheless, your ISP detects that you are only connecting to the proxy. The same can be done with the prohibition to visit the Euskal Herritarrok sites in Spain. The only condition is that the proxy server has to be outside Spain.

5. Social Networks, YouTube and similar

Judges, prosecutors and politicians have realized that social networks can be used to help extremists or to practice bulling and many other misuses[9]. Yes, it's true, but why do we only blame the service providers? We can also blame the mobile phone makers because with a mobile phone and a camera, recording a video of a violent aggression to a school mate is much easier than recording it with a steady-cam. And with the extremists using social networks, it is obvious that they will used every method that helps them to communicate. We are not saying that the user of social networks has to be free of control. However, is too easy to say "we are going to control all the traffic of the social networks to avoid future terrorist incidents". The problem is how are we going to monitor more than 250 million users of Facebook[10]? How privacy is going to be respected? Furthermore, would it be useful if they use an invented language or communicate with themselves with codes like "changing the state of Facebook means that I'm ready to operate"?

6. Conclusions

It is not easy to match our desires with reality. The majority of people would be happy with an Internet without child pornography or without terrorists, a world without children bulling their classmates and recording it with the phone and posting it to YouTube. But is it a problem about Internet Service Providers, or is it about child pornography, terrorism or bullying? So the best solution is education, not only education of the children about violence and sex, but education for everybody. Lawmakers who have to rule laws about technology must know a bit of it to avoid the goal of monitoring "all the traffic of internet". We should be concerned, while writing this paper we used the Internet to find information about child pornography, terrorism and so on. We could be classified as dangerous people. As stated before, finding exactly who is at the end of the connection is difficult. So, ISP responsibility is the easiest and the wrong option.

9. http://iblnews.com/story.php?id=46447.

10. http://www.facebook.com/press/info.php?statistics.

Many people in our days prefer having free things than privacy: many applications in Facebook ask to provide access to your data to get the results, and many people do it. So, people firstly have to be aware of this fact and protect their privacy.

In a world that changes so fast, where everyday borders are more diffused, it is going to be difficult for the lawmakers and politicians to do their job. They have to change their minds and try to be near to technology and all the new discoveries: regulation includes technological issues. Unless everybody has a chip installed in their bodies and we can only connect to internet with this chip, it is going to be difficult to know who exactly is doing illegal actions. But if that moment arrives, be sure that there will be a black market to change or to have more chips o to get access to the Internet.