SCRAMBLE!
A PET FOR YOUR FACEBOOK?

An assessment of the legal status of a Privacy Enhancing Technology in social network sites: a European and United States perspective.

SANDRA OLISLAEGERS
TILBURG UNIVERSITY

Student number: 174347
***Thesis supervisors**:* *Prof. dr. R.E. Leenes and ir. M.E. Pekárek*
Date: June 2010
Master: Law and Technology

1: INTRODUCTION

1.1 Privacy risks and lack of control in social network sites

The rise of web 2.0 and, along with that, popular social network sites (hereafter: 'SNSs') such as Facebook[1], MySpace[2] and Hyves[3] (a Dutch SNS) has led to new issues regarding privacy.[4] Internet users provide personal content on a massive scale via such web 2.0 platforms and by doing so they are likely to be confronted with a wide variety of privacy risks. These risks include, *inter alia*, cyberbullying, harassment, identity theft, loss of reputation, libel and slander. The severity of these risks is increased by the fact that SNS users often post *truthful* personal data on their profiles, ranging from pictures or personal stories to full name, address, email and phone number.

SNSs, where much personal information is stored and exposed, are a particular source of privacy risks mainly due to its *architecture*[5] (and the architecture of the internet in general). This architecture facilitates certain privacy risks. For example, online data often cannot easily be erased, or sometimes even not at all. When a user erases his own profile,

---

[1] Facebook (2010a)
[2] Myspace.com (2003-2010)
[3] Hyves (2004-2010)
[4] There is no general universal definition of privacy. However, the notion of privacy can generally be divided into four separate, yet related concepts: relational or communications privacy; territorial or spatial privacy; bodily privacy and informational privacy. See Electronic Privacy Information Center (EPIC) and Privacy International (PI) (2007). Relational and communications privacy concerns the 'security and privacy of mail, telephones, e-mail and other forms of communication' (think of anonymity, secrecy and solitude, cf. Gavinson (1980)), and also, in my view, to the ability of establishing and maintaining relationships and of developing oneself (autonomy, identity, free will and authenticity, cf. John Stewart Mill). Privacy does not only refer to solitude, it is also a freedom: this is illustrated by the fact that the fundamental rights to privacy and data protection as incorporated in the Charter of Fundamental Rights of the European Union are placed in chapter II: Freedoms. Territorial privacy regards the inviolability of the home and other private places such as the workplace and, in some cases, extends to public places. Bodily privacy concerns bodily integrity and the protection from 'invasive procedures such as genetic tests, drug testing and cavity searches'. See Privacy Information Center (EPIC) and Privacy International (PI) (2007). Finally, informational privacy refers to data protection. In Europe informational privacy is called data protection, whereas in the US it is mainly called information privacy. In this thesis, data protection or information privacy refers to protection against unlawful and/or disproportionate processing of personal data. This thesis will revolve only around information privacy, or data protection. Hence, when the word 'privacy' is used, I refer to information privacy, and data protection is used as a synonym for information privacy.
[5] See Lessig (1999) and Lessig (2006). Architecture, or 'code' when relating to software and the internet', is one of the four modalities of regulations as described by Lessig. The best way to explain what the modality of architecture entails is by the following example: why can people not steal a skyscraper? Because its architecture (i.e. that is impossible to move a skyscraper) does not allow one to. A car, however, is more easy to steal because, if someone has the skills to do so, it can easily be moved. Another example is speed bumps: this design of the road disables drivers, to some extent, to speed. The same counts for the internet: if the computer code (someone who develops computer programs or a website on the internet, designs that program or webpage by, simply put, creating a "manuscript" for that program that entails rules which enable and disable certain functions of the program or webpage. Thus, the developer designs the architecture of the program or webpage by means of computer code) does not allow, or only allows a certain action, than it is impossible for the program or webpage user to act otherwise. Think for example of passwords that prohibit unauthorized access, or the architecture of Facebook where it is possible to add people to a friend list only if they too are a Facebook member, or that private messages are not visible to others whereas wall posts are.

cached versions of the profile can still be found by search engines such as Google because these versions stay intact on the Google servers.[6] Furthermore, a user can never be sure whether others have saved profile information by, for example, making a print screen or saving pictures. Related this problem is the fact, at least this is the case with most SNSs, that where certain information was shared with "friends"[7] that information remains intact on the profile of that friend, even after deletion of the user's profile. Another issue related to the architecture of most SNSs, and in particular to that of Facebook, is that users not only create privacy risks for themselves but also for those that are added as their friends. In Facebook, this occurs in two ways: by sharing content with friends and by using Facebook applications such as games, quizzes, jokes, etcetera. An example of the first case is the situation where a Facebook user uploads a group picture and tags[8] him or herself and his or her online friends. The picture will then not only appear on the profile of the user who has uploaded the picture, but also on the profiles of the tagged friends. Say, for example, that one of them has a 'private' profile (meaning that only the user's own friends can view the profile) while another tagged friend has set his profile to 'friends of friends' (meaning that the user's friends and the friends of all those friends can view the profile). In this case, the tagged picture can be viewed by the friends of the user with the private profile *and* the friends and friends of friends of the other tagged Facebook user. When, for example, five friends are tagged in one picture, and one of these Facebook users has set his profile to 'public' (meaning the profile can be viewed by anyone, including non-Facebook members) the picture can be viewed by anyone, including people off of Facebook. In the second case, personal data of a user's friends are shared with third parties trough the use of Facebook applications: by using an application, a Facebook user gives, often unconsciously, permission to the application to pull profile information from not only his own profile[9] but also from those of his friends.[10]

---

[6] Facebook states in its Terms that cached versions of the profile remain intact on their servers too: 'When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).' See Facebook (2010d), section 2 (2).

[7] The quotation marks are used because the perception of "friends" in the online SNS world is different from its perception in the offline world. In the online world friends are the people, or profiles, someone adds to his profile friend list in order for them to be able to view each others profile information and interact with each other. These people can be anyone, and often not only include real-life friends.

[8] "Tagging" in Facebook means linking a person on a photo to a particular Facebook user account. The person that is tagged is informed of this and has to accept the tag. After acceptance, the user's name will appear below the particular photograph. When you hold the cursor of the mouse over a particular person in the picture you can see what name is tagged to that particular person.

[9] Facebook (2010d), see section 2(3): 'When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information.'

[10] See Facebook Developers Wiki (2010). To illustrate, I give the example of the agreement Facebook users make with the highly popular Facebook application 'FarmVille': 'Allowing FarmVille access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.' See http://www.facebook.com/FarmVille and click on 'Go to Application'.

It is not only the architecture of SNSs that facilitates online privacy risks. A lack of true informed *consent*[11] of SNS users about what happens with their[12] personal data, and a lack of *control* of SNS users over their online privacy, also attribute to the possibility of being confronted with these risks. This lack of consent and control is partly caused by the assumption of SNS users, especially the young ones amongst them[13], that their profiles are their own private space. This assumption, however, is unfortunately wrong. I will illustrate how this is so, by referring to the observation of Erving Goffman (1959)[14] in relation to social interactions; that people, in everyday lives, present themselves differently in a number of distinct contexts, by Goffman referred to as "audience segregation". According to this idea, people adapt their behaviour when they enter into a different environment with a different audience; they switch roles when the audience changes. Think of a work or school environment, or the roles people have as a mother or child, pupil or teacher, etcetera, and the switch people make when they are, for example, with their friends or go out. Another distinction Goffman makes is between "front-stage" and "back-stage" regions.[15] The back-stage is where people retreat from their role(s) or audience(s). When applying these ideas to Facebook, it becomes clear that here, the audiences are no longer separated. Anyone who is able to view the profile is now the audience, and these people can come from all sorts of "offline" audiences and contexts – ranging from friends and family to colleagues and current or future employers. In this regard, Boyd (2006) refers to 'invisible audiences'. When these audiences from different contexts mix, which particularly can happen on SNSs, this can cause problems for the SNS users involved. For example, where one audience, e.g. an employer, gets mixed with the audience 'friends' (meaning that the person involved acts as if he or she were amongst friends, yet this person would behave differently when being with his or her employer), the employer can, perhaps without the employee knowing, make decisions about that person because the employer sees this person in a different role with different behaviour on Facebook; behaviour he or she would normally "turn off" when being at work. The employer can, e.g, dislike certain hobbies or interests of the employee, and decide, consciously or unconsciously, to treat the person differently. Another example is when colleagues, that are added to a person's friend list on Facebook, tattle about this employee

[11] I will discuss the issue of consent in more detail in par. 2.1.3.
[12] I will not enter into a discussion on whether personal data relating to a certain persons are owned by these persons and therefore have property rights to "their" personal data. When I use the wordings 'their personal data' I mean personal data that refers to, concerns or is related to a particular identified or identifiable person.
[13] Grimmelmann (2009), p. 1179 under note 261: 'See AMANDA LENHART ET AL., PEW INTERNET & AM. LIFE PROJECT, TEENS AND SOCIAL MEDIA 13 (2007), http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf (finding that fifty-five percent of online teens had a social network profile compared with twenty percent of older users).'
[14] Goffman (1959), p. 48-49.
[15] *Ibid.*, p. 106-140.

to the employer, e.g. when noticing that this person, while he or she called him or herself sick at work, in fact when out to the beach to enjoy the nice weather. There are many more examples that can be thought of where a mix of (invisible) audiences causes problems to the person involved. It is noteworthy in this regard is that, according to some authors, the ability of being immune from judgements of others is seen as the core of privacy.[16]

It appears that users are either not aware how, or not able to efficiently control their privacy.[17] This unawareness is attributed, *inter alia*, to the invisible audiences SNS users have, as I explained above. The ability for SNS to *control* their online privacy is, however, completely determined by (the architecture of) the particular SNS. Facebook allows their users to use and adapt the privacy settings, thus making it possible to, for example, shield off profile information from those that they do not accept as a friend. Nowadays Facebook also allows users to select which individually selected friends, i.e. Facebook users they have accepted as a friend, can view a status update.[18] However, the privacy measures Facebook offers users to use do not work very effectively, for three reasons. First of all, SNS users do not seem to use many of these options.[19] Many Facebook users do not even keep their profile private but set the privacy settings for their wall[20] and or photos on 'public'. The second reason why the Facebook privacy settings are not effective in managing privacy is that users often accept friend-requests from people they hardly know or perhaps not know at all. Especially young SNS users tend to add as much people to their friend-list as possible as this is seen as some kind of social achievement. While they think that having a large number of online "friends" is equal to being popular, they bring along the risk of giving profile access to people with bad intentions. The third reason why SNS users are generally not capable of managing their privacy on SNSs is that it is impossible to hide profile content from the SNS *provider*. The fact that this is impossible is not some coincidental design of the platform. The content provided by users tells a lot about the users' personal interests, which in turn creates a valuable market for advertising. By recording and classifying profile content and internet behaviour, SNS providers make their own profiles of specific users or groups of users, making it easy to identify what interests whom.[21] These profiles, which are often

[16] Johnson (1989) on the conception of privacy as 'immunity from the judgments of others' and also Vedder (2000), p. 7-8.
[17] Westin (1967) defines privacy as 'the ability to determine for ourselves when, how, and to what extent information about us is communicated to others'.
[18] A status update is a short text message that Facebook users can put on your profile for others to see. This message will also appear on the news feed of the user's friends so that they automatically see that you have updated your status.
[19] Debatin et al. (2009), p. 83-108 and Tuunainen et al. 2009).
[20] The Facebook "wall" is a part of the user's Facebook profile where status updates appear, other users can write on and content, such as videos, are shared.
[21] See extensively the Electronic Information Privacy Center, *Privacy and Consumer Profiling*. [Online] Available from: http://epic.org/privacy/profiling [Accessed 1st June 2010] and Edwards & Hatcher (2009).

generated without the user(s) knowing or being able to opt out, are, at least in the case of Facebook, used for marketing purposes.[22]

1.2 The solution: an encryption tool

Keeping in mind the aforementioned privacy risks, and their causes and sources, it is worthwhile to consider implementing a privacy enhancing mechanism, or privacy enhancing technology (hereafter: PET), that allows SNS users *themselves* to control what information can be seen by others. A possible solution is this respect is an encryption tool that allows users to individually determine which information can be accessed by whom.

Such a tool has been developed within the PrimeLife project.[23] The tool, called 'Scramble!', is a Firefox extension that enables users to establish rules for audience segregation, i.e. to disclose information to specifically chosen individuals or distinct groups within a user's list of "friends", such as 'family', 'hobby', 'school', 'colleagues', etc. Another prominent feature of Scramble! is that it enables its users to hide profile content from, and disable access to profile content by the SNS *provider*. Scramble! enforces these access rules by means of encryption.[24] I will explain how this works in par. 1.2.2, through some screenshots, after having explained generally what encryption is in the next paragraph.

1.2.1 Cryptography

In today's modern information society, the art or science of keeping information secret, also referred to as 'cryptography', has become increasingly important. Nowadays, cryptography mostly refers to the process of digital modification of regular information into cipher text, i.e., text that is encoded by going through an encryption algorithm. In principle, cipher text can only be decoded by those who have the matching key.

With regard to the latter feature of encryption two distinctions can be made: *symmetric*-key cryptography and *a-symmetric* or *public-key* cryptography. In symmetric-key cryptography the sender and receiver of the information share the same key, whereas in a-symmetric or public-key cryptography they use different keys; one *private* key and one *public* key. The public key is used to encrypt the message while the receiver can decrypt the cipher

[22] See Facebook (2010c), Section 5: 'We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are.'

[23] PrimeLife (2010a).

[24] For an elaborate (technical) description of Scramble! see the article from the developers of this tool: Beato et al (2009). For more (general) information on Scramble! see PrimeLife (2010b), where the tool can also be downloaded.

text with his private (secret) key.[25] The public-key encryption method was introduced in 1976 by Whitfield Diffie and Martin Hellman and since then cryptography has become more widely used in the private sphere, mainly for reasons of confidentiality. Nowadays, cryptography is available or used on almost every personal computer in the world through a crypto mechanism called 'Transport Layer Security', provided by popular web browsers such as Firefox and Internet Explorer and almost every, if not all, email servers.

1.2.2 How Scramble! works

Scramble! is a Firefox extension, which means that the tool can only be used in the web browser Firefox. The tool can be used on any SNS, e.g. Facebook, MySpace, Hyves, Twitter, etcetera, provided that a Firefox web browser is used. Scramble! is able to encrypt any kind of text, including wall-posts, notes or blogs and profile information such as name, age, interests, and so on. Scramble! uses hybrid encryption, which entails that a combination of symmetric and asymmetric algorithms is used in one single crypto-mechanism.

Figure 1 shows information about who has developed Scramble! and that the tool based on Open Source encryption, namely PGP.[26]

Figure 1.

Figure 2 shows how Scramble! allows the user to segregate audiences. The user can create different groups and add contacts (i.e. contacts from the SNS in which the user is using Scramble!, e.g. Facebook, MySpace, etcetera) to each group (figure 3). One contact can be in more than one group.

[25] Cf. Koops (1999), p. 35-39.
[26] PGP stands for Pretty Good Privacy.

Figure 2.

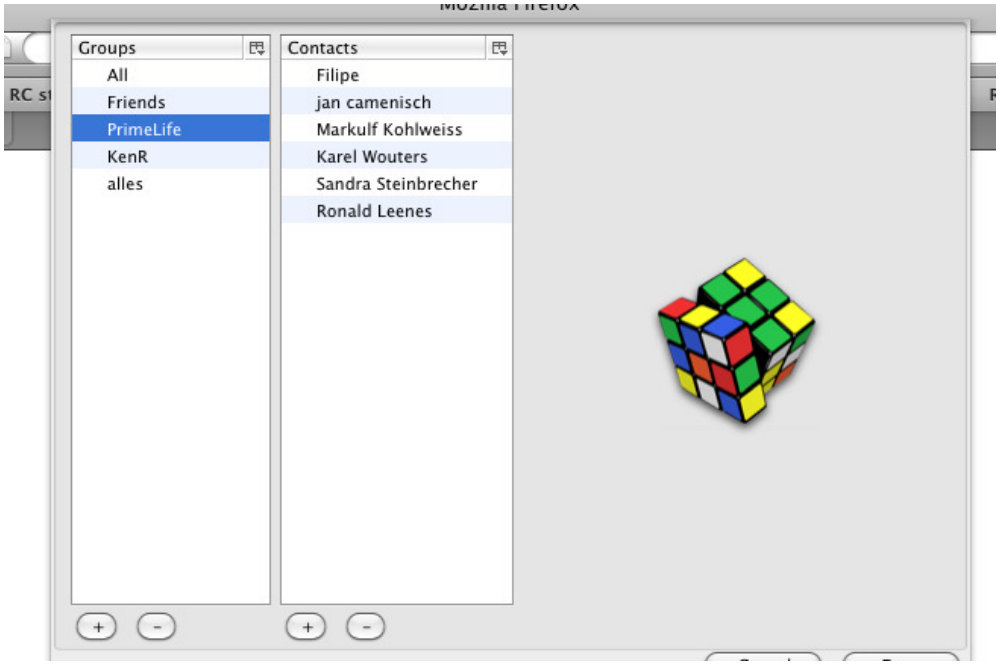
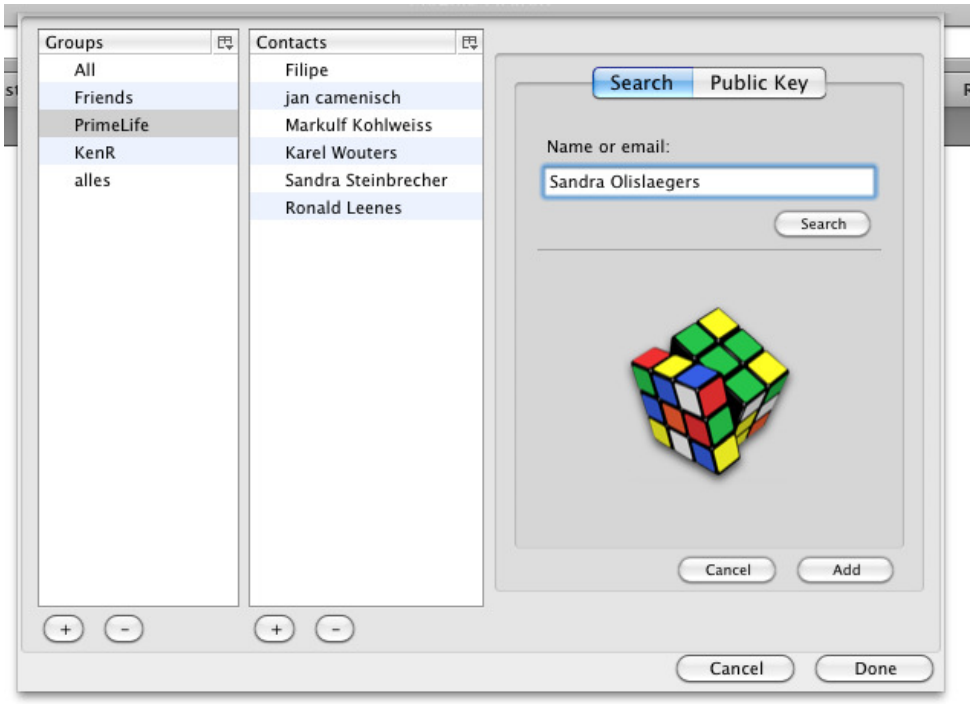


Figure 3.



Besides the possibility of audience segregation, Scramble! allows users to encrypt text in SNSs (figure 4). The user can select which individuals or groups in the user's contact list can

see the human readable text. The other contacts, that are not authorized to see the plain text, see lines of unintelligible gibberish; cyphertext. Figure 5 shows what this looks like in Facebook. The Facebook user Calvin has encrypted his comment and did not authorize the Facebook user Danny Buck to see it, therefore Danny cannot see the human readable text. He can merely read “non authorized encrypted content”. This works the same in Facebook with status updates (figure 6).

Figure 4.

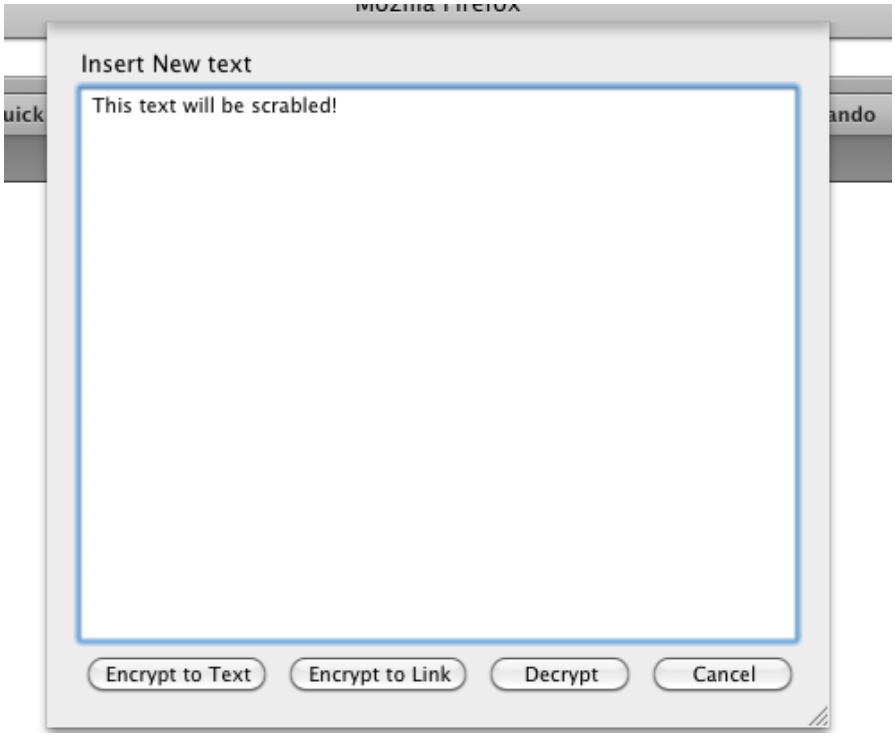


Figure 5.

Figure 6.

The final screenshot (figure 7) shows what the encrypted content looks like to the SNS provider. On their servers they will not see the plain, human readable text, but these lines of characters.

Figure 7.

-----BEGIN PrimeLife ENCRYPTION----- Version: GnuPG v1.4.8 (Darwin) hQEOAwAAAAAAAAAEAP8CBSx/lwuPfUUWLHARPz2F4Q1uFWIU8j5j2OEbXrrLnnp
7+K06QB0Hcbs5kzVuTFV5F6I9wewgcHYpAepJJAV01Xw77jPSJlpBDi3aYrOj33J RBdAF8iqt0w5/rf2aggJq0MF4e1tJPV+1Vk1nLp4NjfqeDxvjj8qGcWpX00X8CcD
/RbcqMU5El+qmqAu6433MI3sS0jFn8pNm52sZv73GxxMu3ExXa6rS7bZmdGC2wvq Lzb0Z+8XlyRxV+ZPhwyvAOjyAc5XLrt5hiRZ65960SogNIROcArbmzkPtXu9Ixtb
+a3Cds609dyq4WPKj+K6GRXjsGTTjuiP5HsJV9J7CscGhQMOAwAAAAAAAAAEAv/ eOLVg05mYN14mHy3fUODrtMYq+cPE2x+yrkd81nOjUl3rYm/2i1BzLHMwUmlnxpu
y2fbgZJT88fdPvqVhZT8mO/VGDHnu7JWPh5e56D2BwZa4FeROGaqI/uSIBrjd36c qSrO7a2JBJe58pAOuicKITV5etOahj8k5ElTj1MJ9Cs9m8oREvean l/z9/zTB8R27
yYg+4kJsRaz7dTm2tnB3ZpJYDiOjf2jODVawdw59vx+vU/Kh67IFPWfaz1why4KO 16TKVbSdbbr0yhFub4ccrGVhkJpCLWGkbgKkeCZulfKfBqqN5kDIDkdfSrArphb8
lRtcb+pjF+FNOVQM6DORjQldXrAk+4c3JU4s4Yi9ZwaIGBAUgzAQjfGNjQR3aJLt mMZUijUgPzCIdxmtVtXkhcQLjt995fevgMB5THZWDqD4d+2pyPQLEwev+q2Nhcyu
BN64ozpDzRnCB5EMAZf7VeOayUWotfNqtoYtbNxa7/bgqb9OfdyuDk0PZ4v6rcwN C/4jAemy0XKq7Qa7qU1rAY/4Z6uplqxdGXg7jBmc+66d8dL8oTNG0I+r6OTNVGAW
wlkOkb8HncRfiqkb5TLr1KK11OOXDmr+tjRO+e6u6KwF5eXyM4/429llzpE49i+E uC6luYi16X+yhVr/uLdT9BR3xyV+GAt1iFeF8ITJjfZ1+LGQisSosUQ+jTmzeWuX
N9X2mNmGrX7MznqONmVDvYelcffk3ht2nHbvm2T3cQl7fcNG4Xclv0AkCcqwQWD9 q35fxuhTkRSs43XwnhIM/hv1dvCfAaIf5Z6TQWsu9ZPY5WiiMAvmA/IpkPSMnRqm
aEaaeieWWsmYp0lavbr3zQ1BYON/2scrEfThm3cVffJpfc/AlGOA64c9TazL/tMD ClBXUkGYjGgNcEQxTDnNa/zZUr1OKzUv2GZ408nuUnfXVesRnyGqGc1D2QKoS9mZ
P9Y21rwonSktAoSERDiivMyNXN1z9mjWSHYbUof0AusPXPCMdpC3knEV3Y4ajV64 mhCFAg4DAAAAAAAAAAAQB/9y3yvQetQ2ON6rquuX8414dG4S+ijb+FpEJr5nbVWQ
6FTUOSf98aBSG2/3SGpRTONSffb/xHxn8v5FJcFywS9r9GslAJwfmsKh+eg/gKFF VPHG1ip/JZSb9EO5OyDwIFHafl/RNg51vwkHlQLeW24nLgQTv+x5xeOeWlk1lNzm
w4HWoKRV9KrEm/jlhGKbO3qgXBBbMzx2YHRxsx7uXBcNXiyPIxCMVkWE7D/w6g7N 6e3Q6PhpHIsFQ8zHTGzqqk5XpWR5iuAAPX6RyVnExeKiOL3xAxEXNNHaNud4xHIc
CM9HWdmtJnrtKmtHNIe9ZFclhF9frQusGsNrAyJ4XHsUCAC+RjN5UNdV5JPJSDAw 7y7jYAx/3oiB01AwK0uiFH5ih6jS5ThLzEiwRUomz9LSlNAaw8aQ934oz//8EE/N
FEhSKjtFATHA0jYS+Z5aoi1o3jkAUWYVmP0aIir2aZFTOEWfzaWm7fXq2L435hdi 9Q3SpQ65ujCBYr+AQ4T4r19+rfRnFhKOaNT+/X1UKPKdNlXmBRggBOptKtDiXVSO
SnK93X82SfmXDGg7jqz2PAdX4zPT8q+1Xdb6+BhEW38WCjbJ989BBH36M/3YMKeX iVN4KiYok25aOukG3ABL8dHBauBNQgZgPgwqxs1trwuBokZUNZ5HP33Lpefq7PVP
6qW2hQEOAwAAAAAAAAAEAP7BfUMd08G58OWt0/wRQ8uVp20xjPKMHQEkUsGygFw 9/M5jjUaJYvy+VGdpkX24zKEqjhggQKsx0Jf3M8vJ2Hu3C/lIy3cF718pEKvZKq5
2X5R+EumlUsIR4sODLYz1d9mM0fRcw0q79rf5uHvyoqRAvT61QP5jI5EEcdwpsRQ AuQD/jnf8CBIx9OnuhuTWpzj+ZM0M1HkUUHO5EFjiqotGIFIVxN78WaSmYBI+r5a
wSJleb/X0kssGWV4+PJt2dDHV76IK7x7BUklD5IbaiacFrpL4JNJvP8in6nw0dXO P6ghAG1vo+ZoqbaLvaSTJAhfsDPIXpz1uoEEkxIzTtW0LMFXhQEMAwAAAAAAAAA
AQf+M2We0cvGsV8Ng9M+XiUOxz61K4Bon9u1TU5mZNbwO0uInWDn2Pcf0AgOMHwx /35JbPIzGebqYvUy3FPNKrSxeQ4OExL4LApfgT9sPCIt8IGPswD9NFNBSgYp5CJL
1xh9fB5tFlz05m0nl2levPoVQ+iCajG2PwahuXzQR7R/5wd/9SsNAyO+IzkpK8VL ksFL0IOLLhvIJGCn3Gr4SxkVFrCh/zAcE+oLejuOnWUGIXi4BdObBeEHlgl5h99+
154QV6BY4mjFEAlKsJCPgbyrKOGwPt4jFtlaZt+wsNdjWlIEVyQNT74Z8jW2NQeX uY4NZDtqkl/tMXO3nJ34GsALdoUCDgMAAAAAAAAAABAH/27dMqAyjEpWaBHNUOuX
UEkuyH9UMcGyQsaV2Vd1bpvI5C6pkAcuO7CuWcbgHQkXR8FbpEYHW6YCjzZU+g6d S5kGPsCaWG/Dc/52VF8VjiQgUB4ZsWhFM1sz5Ts4SaA2bcFdgerH5JoR5Rqnpel7
YbS57ZWePtYUuES3QzchJcn462wBK8rETEIXNIkg/tYAc5PWJLv+XS4U1i6bKvk+ h1glDe4tSow3DiiNeQgV81oeywx99modXw3I0egKuW88lTILZdyAY5ndNTq0xdCy
UhO4aWH+YDZCGuIZcys4QLHa5t/cGmx47PPdVv0VceuBc64P6kIRBODcNrXc3k5W NwMH/A2kxp+FWffpS9CQg34jnxv/uXCnLL8JGWFhhg7Xj633B/juFGdavhCze5iV
A4KIueicoz9dGKYwQv8v5f+2/MLKpITuT+DA9fvj5rQ5CiFg2+YYtsCTXDbiIBsf FFQGPs+19PQEElZrt4AWkZ+DXyQ2aLRp8UgbZOtymozCZ3bX5399lfKUu72Cz/CF
rHofIRGwIJrjRr7Sdxe3Ow0mL+E98isqNy52MPxLvEVVmHtcyVTyqjO+choee3as EqJScUunKFl/WQEuUC/NK8D45L6qJ99Clyci569r6pWjsHvmmBJYoEUpIvr9Vq1A SV/BvBu
/ua5epOchM+hz+qUdCYuFAQ4DAAAAAAAAAAQA/0QYAnOqU4WLvPJToSH E5bLhGTJmFuu95MbqFGb4O80Mg0MYufYJ8dYrILNYAhmnZTLw6qo9EfVwEZRZ7Nz
ZKtuiKsrlUNIFgo3gPc19UFrQiHeqMJflbwsZtC0cBQ598lw9paWcpTQmA0DO1hU cgWItZfLNnosEouCIhCQtH7KJAQArfo0NcVVwvLNaKsnNAD/26jp8MvVeUKv7rpG
DAZWFUbXGcyqWdD7Et1uWhNDIaO6uz6Y+5d+SBIWAek9g6fajZO5oZxj8IzjoYAe P+9WGUNRvIfPlH+0AV6i5P92+3IJmxd4uVzjAgWgrX5jeRp3aM7r0QvG8rlvOeL7
HMEDvvnJMeQQA3wT7BRkevTmCj0AlIiHZrmeeHNuUSe6nnURTsU4oRmWPxhjxnRh sNEtdB0t2VE= =LSlR -----END PrimeLife ENCRYPTION-----

1.3 Aim, context, research question and structure

This paper aims to asses the use of Scramble! from a legal perspective. The purpose is, *inter alia*, to assess such use in respect of current privacy- and encryption laws and -regulations in Europe (hereafter: 'EU') and the United States (hereafter: 'US') and determine whether the use of Scramble! in SNSs brings along any (general) legal objections. Furthermore, to limit the scope of this research, I consider the use of the encryption tool to be private and personal, meaning that I will not assess what the legal status of Scramble! is in case the tool is commercially exploited and exported.

The SNS that will be used as an example throughout the assessment is Facebook; a US-based SNS and the largest SNS in the world, with some 450 million members from all over the world.[27] However, when assessing relevant EU regulations, I will focus on EU-based SNSs in general as well, which also include highly popular ones that have millions of users. The reason for this is that, in case of US-based SNSs, it is questionable whether EU regulation would apply. It should be kept in mind that where an EU user makes use of a US-based SNS, this SNS provider will always argue that EU law does not apply as the choice of law in their general terms and conditions will be US law. Even if EU law applies, it is highly likely that it would not be enforceable in US courts – not to mention the effort that would come along with such enforcement.

Additionally, a specific analysis will be conducted regarding the contractual relation between Facebook and its users; I will assess the use of Scramble! in Facebook from the

[27] Facebook (2010b). Aapproximately 70% of all Facebook users are outside the US.

perspective of Facebook's Terms (on the Facebook website referred to as: 'Statement of Rights and Responsibilities'[28], hereafter: the 'Terms' or 'Terms') and Privacy Policy.

The research question and related sub-questions I wish to answer are the following:

- *Which legal obstacles occur if Scramble! would be downloaded from the EU to other EU countries or to the US, and used by EU and US citizens for purposes of privacy protection or privacy control on their Facebook profile?*
  - How is this question answered in light of EU and US privacy laws and regulations?
  - How is this question answered in light of EU and US encryption laws and regulations?
  - How is this question answered in light of the specific contractual relation between Facebook and its users?

As appears from the research question, I will focus only on the situation where Scramble! would be downloaded from an EU member state to either another EU member state or to the US. To note, throughout the paper arguments pro and contra the use of Scramble! in Facebook (or, in case of EU law, SNSs in general) will be given, as if the user and the SNS provider were in a discussion on this use. As laws and regulations can be interpreted[29] in multiple ways, the arguments of both sides are important in examining the legal status of the crypto-tool.

This paper is structured as follows: paragraph 2.1 examines the legal status of (the use of) Scramble! in respect of EU privacy law, followed by an assessment of US privacy regulations in paragraph 2.2. Paragraph 3.2 and 3.3 discuss the relevant EU and US encryption regulations, respectively, whereby the discussion on EU encryption regulation covers both domestic and export crypto laws, whereas the discussion on US crypto-regulation is limited to domestic regulation.[30] Next, chapter 4 assesses whether a Facebook user would, when using Scramble! in Facebook, violate the Facebook Terms or Privacy Policy. Finally, chapter 5 answers the research question and provides some concluding remarks.

[28] Facebook (2010d).
[29] This is, in the end, generally the task of courts: by interpreting the law they shape that law or create new rules.
[30] The reason why the scope is limited to US domestic crypto regulation is explained in the relevant paragraph 3.3.1.

2: PRIVACY REGULATION

2.1 EU privacy regulation

2.1.1 Introduction

In this section, I will examine what the legal position of (the use of) Scramble! in SNSs is from the perspective of EU privacy regulation. I will first discuss the fundamental right to data protection as embodied in the *Charter of Fundamental Rights of the European Union*[31] (hereafter: 'the Charter') and show how the enforcement of this fundamental right can be facilitated Scramble! Next, I will analyze the use of Scramble! in light of the *Data Protection Directive* 95/46/EC (hereafter: 'DPD').[32] In doing so, I will first address the question whether the DPD is applicable to US-based SNS. Next, I will give a general overview of the systematics of the DPD and elaborate its requirements. Finally, I will assess the legal status of Scramble! in light of the DPD and specifically look at its requirements for SNSs as data controllers, and for SNS *users* as data controllers.

2.1.2 Article 8 of the EU Charter of Fundamental Rights: the fundamental right to data protection

The EU Charter of Fundamental Rights was signed on 7 December 2000 and, as it is incorporated in the Lisbon Treaty[33], entered into force on 1 December 2009. Before I discuss its provisions it must be noted that the Charter is not legally binding in the sense that it requires Member States to amend their constitution, or that it gives the EU new powers or tasks, see Article 51(2) of the Charter. Rather, the rules set out in the Charter must be taken into account by the Member States when they implement EU law, or by their national courts when interpreting EU law. Thus, the Charter is in the first case a political achievement.

The Charter establishes two rights that relate to privacy, Article 7[34] and Article 8. I will only discuss Article 8 as this article specifically concerns information privacy, whereas Article 7 relates to communications and territorial privacy. Article 8 states the following:

> 'Everyone has the right to the protection of their personal data. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other

[31] Charter of Fundamental Rights of the European Union of the European Parliament, December 7, 2000, *O.J.*, No. C 364, 2000.
[32] To prevent confusion: the E-Privacy Directive 2002/58/EC will not be discussed as it is not applicable to SNS: it applies only to publicly available electronic communications services, which definition excludes information society services. Cf. Council Directive 1998/34/EC.
[33] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *O.J.,* No. C 306, 17 December 2007, pp. 1-271.
[34] Article 7 of the EU Charter of Fundamental Rights reads: 'Everyone has the right to respect for his or her private and family life, home and communications.'

> legitimate basis laid down by law. Everyone has the right of access to their data, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority'

This article is new. As De Hert & Gutwirth (2009) state in this regard:

> 'In the ECHR there is no article that comes close this provision. Apparently, something new is happening at constitutional level.(…) Here the constitutional lawmaker goes one step further and provides for an independent fundamental right.' (p. 6)

No similar right can be found in the ECHR and the DPD certainly does not create a human right to data protection, but should rather be seen as the elaboration of a specific element of the broad notion of privacy, which is information privacy.[35]

As said, in the Charter, the right to data protection has become a stand alone right. Clearly, this given is important in the context of online social networking. With Article 8 of the EU Charter, the argument that SNS users, by creating a SNS profile and posting personal information on the web give up (a piece of) their right to privacy, is no longer relevant. Even if people decide to post personal information about themselves on a SNS, they are protected by the fundamental right to data protection. Article 8 of the Charter needs no in depth discussion here as this right, and all its elements, are elaborated in the Data Protection Directive, which will be discussed in par. 2.1.4.

2.1.3 Enforcement of Article 8 of the EU Charter of Fundamental Rights by PETs

As the fundamental right to privacy of the Charter is clearly no obstacle to the use of Scramble! in SNSs, it is worthwhile to discuss how Scramble!, as a PET, could facilitate the enforcement of these rights. However, in the introduction I mentioned that the Charter is not legally binding and the question arises whether EU citizens have a right to enforce these fundamental rights. In my opinion the answer should be affirmative, because the non-binding status refers to the sovereignty of states rather than to the individuals. The rights are reiterated (because that is what the Charter in fact does) for the protection of its individual citizens, which allows them to, at least in proportionality, enforce these rights for themselves.

To some (though minor) degree the possibility for self-enforcement of information privacy exists within the architecture SNSs, as users have the opportunity to shield whole or

[35] See De Hert & Gutwirth (2009): 'The Council of Europe's Convention on Data Protection (ETS No. 108) and the European Community's Data Protection Directive 95/46 only regard data protection as a facet of the existing fundamental rights such as the right to privacy.' (p. 6) We will discuss the DPD in more detail in par. 2.1.4.

part of their profile content from those that are not in the user's friend-list. However, it is impossible to make profile content inaccessible to the SNS *provider*. In this regard, Article 8 of the Charter can easily be violated as the user has no concrete efficient *control* over how his profile content is used after it is submitted to the profile and SNS servers. Add a lack of informed consent amongst users[36], and you have a perfect climate for Article 8 violations. To quote Grimmelmann (2009) in this respect:

> 'The problem is that there's a consistent difference between how much privacy users expect when they sign up for a social network site and how much they get. That's a market failure; if users overestimate how much privacy they'll get, they won't negotiate for enough, and companies will rationally respond by undersupplying it.' (p. 1178-1179)

The general terms of a SNS provider generally state that information is collected only after consent of the individual.[37] But consent is, in such cases, already given by clicking an 'agree' button[38] – a SNS user is never able to create a profile without doing so first. It is questionable whether this 'one-click action' constitutes actual informed and considered consent. Of course, a user can choose not to fill in certain fields in the profile. However, some fields, such as name and email address in case of Facebook, always have to be filled in for the user to be able to create a profile (i.e. a lack of control). A user can also choose to delete his profile or not make one at all. Deleting a profile is however inefficient for the protection of ones privacy as the content that was already posted online may remain on the servers of the SNS provider. Moreover, when data is shared with online friends that data remains, even after the deletion of the profile, on the profiles of these friends. [39]

One way to enforce the human right to data protection of the EU Charter and henceforth diminish the aforementioned privacy risks and increase the level of control and information transparency, is by means of encryption. On the one hand, privacy risks are mitigated as encryption makes it possible to shield of content from both internet users (individually defined) and SNS providers, while on the other hand the user does not have to

[36] This lies in the fact that many (especially young) users regard their profile, their personal page, as a private space. Additionally, but very important, most users do not read, or are unaware of the meaning of the Terms of Use, where it is often stated (though vaguely) that their data is used in one way or another for commercial purposes.

[37] Cf. the Facebook Terms section 16.1: 'You consent to having your personal data transferred to and processed in the United States.' Facebook (2010d).

[38] Facebook places the following statement on its website where someone wants to create a Facebook account: 'By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.' See Facebook (2010a).

[39] See the Facebook Terms section 2.2: 'When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).' Facebook (2010d).

depend on the information and promises given by the SNS provider. Especially when a user makes use of a non EU-based SNS situated in a country where a right to privacy and/or data protection is not (equally) acknowledged, encryption is a useful tool for enforcing such a right. In this way an individual can impose the rule (do not invade my right to privacy) and enforce that rule at the same time (it is impossible for those who are excluded by the user, except in the case of intentional hacking, to read the encrypted data).

Privacy enhancing technologies (hereafter: 'PETs') are also very useful considering the problems of jurisdiction and enforcement inherent to this digital age. In the 'Communication from the Commission to the European Parliament and the Council: on Promoting Data Protection by Privacy Enhancing Technologies' (2007) it is stated that:

> 'this system [i.e. the legislative system the Data Protection Directive, ePrivacy Directive and Data Protection Regulation provide] may prove insufficient when personal data is disseminated worldwide though ICT networks and the processing of data crosses several jurisdictions, often outside the EU. (…) [C]onsiderable practical obstacles may exist as a result of difficulties with the technology used involving data processing by different actors in different locations and there may be hurdles intrinsic to the enforcement of national administrative and court rulings in another jurisdiction, especially in non-EU countries.' (p. 2)

In this regard, the European Commission endorses the use of PETs, such as encryption, complementary to legislation as this can, to a large extent, solve these jurisdiction and enforcement problems:

> 'The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfill data protection rules.'[40]

Additionally, in their Opinion to the European Parliament the Commission has established three objectives:

(1) To support the development of PETs;
(2) To support the use of available PETs by data controllers;
(3) To encourage consumers to use PETs.[41]

[40] Commission of the European Communities (2007), p. 4.
[41] *Ibid.,* p. 8.

With regard to the third objective, the Commission has noted that it is not only important to develop PETs such as encryption tools, but also to make consumers aware of the risks of data processing and the possibilities that PETs offer to mitigate those risks.[42] Additionally, in my view, consumers should also have more general awareness on the rights they have in the context of social networking, in particular the right established in Article 8 of the EU Charter of Fundamental Rights. The Commission has implicitly mentioned this aspect of raising awareness amongst consumers by stating that:

> 'consumer associations and other players such as the Consumer Centres Network (ECC- net), in its role as an EU-wide network to advise citizens on their rights as consumers, could become partners in the quest to educate consumers.'[43]

2.1.4 The Data Protection Directive

In this paragraph I will look at the legal status of the use of Scramble! by SNS users in the context of the DPD[44], and particularly in the context of the processing of personal data for commercial purposes. I will again focus both on the example of Facebook and EU-based SNSs in general. In par. 2.1.4.1 I will question if, and to what extent, the DPD is applicable to US-based SNSS. In par. 2.1.4.2 I will show how the DPD should be read and applied and elaborate its requirements. Finally, I will discuss the legal status of Scramble! in light of the DPD. In this regard, I will specifically examine the DPD in relation to the processing of personal data for commercial purposes by SNS *providers* and in relation to the processing of personal data by SNS *users*, in par. 2.1.4.3 and 2.1.4.4 respectively. I will not examine whether SNSs, and Facebook particularly, comply with all the rules regarding data processing. The purpose of analysing the DPD is to show how the use of Scramble! fits into the framework of data protection law in Europe.

2.1.4.1 Applicability of the DPD to US-based SNSs

According to Article 3 (1) DPD, the Directive applies

[42] *Ibid.*, p. 9.
[43] *Ibid.*
[44] A Directive is a piece of European Community legislation that is established within the first pillar, which means that Directives can only cover subjects that regard the establishment of an internal market within the EU. However, note that, with the entry into force of the Lisbon Treaty in December 2009, this pillar structure has been abolished. Directives are addressed to the Member States, not to their citizens. Member States are obliged to implement the rules set out in the Directive into national law within the time period set out in the particular Directive. All Member States have now transposed the Directive to their national law. See COM(2007) 87.

'to the processing of personal data wholly or party by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'

In case of EU-based SNSs the applicability of the DPD is quite evident, but where it concerns *US-based* SNSs, such as Facebook, this is not so obvious. The applicability of the DPD to US-based SNSs has been elaborately discussed by Kuczerawy (2009). It appears that where Facebook[45] makes use of cookies[46], the provisions of the DPD, as implemented by the national laws of the Member States, apply. Cookies are placed on the hard disk of the SNS user's PC and these PC's, with a (Facebook) cookie on its hard disk, have been acknowledged as equipment[47] in the sense of Article 4.1 (c) DPD. This article stipulates that national data protection laws, adopted pursuant to the DPD, apply where a data controller 'is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State'. In this regard the Article 29 Working Party[48] notes that, as cookies are placed on SNS users' personal computers, the laws of the Member State where the PC is located apply.[49] Hence, Facebook would be subjected to the laws of each EU Member State.

[45] Facebook states that it uses cookies in its Privacy Policy, see Facebook (2010c): 'We use "cookies" (small pieces of data we store for an extended period of time on your computer, mobile phone, or other device) to make Facebook easier to use, to make our advertising better, and to protect both you and Facebook. For example, we use them to store your login ID (but never your password) to make it easier for you to login whenever you come back to Facebook. We also use them to confirm that you are logged into Facebook, and to know when you are interacting with Facebook Platform applications and websites, our widgets and Share buttons, and our advertisements. You can remove or block cookies using the settings in your browser, but in some cases that may impact your ability to use Facebook.'

[46] What cookies are is explained by the Article 29 Data Protection Working Party (2002): '*Cookies* are pieces of data created by a webserver that can be stored in text files that may be put on the Internet user's hard disk, while a copy may be kept by the website. They are a standard part of HTTP traffic, and can as such be transported unobstructed with the IP-traffic. A *cookie* can contain a unique number (GUI, Global Unique Identifier) which allows better personalisation than dynamic IP-adresses. It provides a way for the website to keep track of a user's patterns and preferences. The *cookies* contain a range of URLs addresses), for which they are valid. When the browser encounters those URLs again, it sends those specific *cookies* to the Web server. *Cookies* can differ in nature: they can be persistent, but can also have a limited duration, the so-called session *cookies*.' (p. 10 under note 23)

[47] Article 29 Data Protection Working Party (2002), p. 10-11 and Article 29 Data Protection Working Party (2009), p. 5.

[48] The Article 29 Data Protection Working Party was established by Article 29 (1) of the Data Protection Directive. The Working Party is composed of one representative of the national data protection authorities of each member state (cf. Article 28 DPD), of the data protection authority of the community (cf. Article 41 – 48 of Regulation (EC) No 45/2001) and of one member of the Commission (Article 29 (2)). Its tasks are mainly of an advisory nature and the Working Party and acts independently. For a more elaborate description of its tasks see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf.

[49] Cf. Article 29 Data Protection Working Party (2002): '(…) the user's PC can be viewed as equipment in the sense of Article 4 (1) c of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and, as it has been explained in the previous paragraphs, several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory. The Working Party is therefore of the opinion that the national law of

This presumption is however not as black and white as it is stated here, for three reasons. First, Article 5.3 of the E-Privacy Directive allows the use of cookies only when the user 'is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.' Moreover, the user must be notified of the use of cookies and consent prior to such use. This as a consequence means, as Kuczerawy (2009) states, that:

> 'where the user, wishing to protect his privacy by refusing the cookies would in fact deprive himself of the protection by his national data protection law. This would happen because art. 4.1 (c) DPD applies only if the data controller uses equipment (the cookie) on the territory of the Member State (user's computer).' (p. 5)

Hence, when users would not accept cookies from a US bases SNSs like Facebook, they would not be protected by their own national data protection laws because there is no longer any equipment located in his country. This conclusion is ironical because if a user declines cookies this is usually motivated by privacy concerns, while not accepting cookies in fact deprives the user from this privacy protection. However, using Facebook without accepting cookies is impossible.[50]

A second case where the presumption that Facebook is subjected to the laws of all EU countries is invalid is where profile content of SNSs is collected and sold 'to advertisers and third parties marketers, in anonymised or aggregate form', which often occurs.[51] As anonymous data receives no protection under the DPD, the user has no protection in this respect. This is of course valid in case of EU-based SNSs as well, as they too can create anonymized data profiles for commercial purposes. The question that arises here is what anonymous processing is, because only hiding someone's name does not mean the data is anonymous. According to Article 2 (a) of the DPD, personal data means 'any information relating to an identified or identifiable natural person' and an 'identifiable person' is defined in that same article as

> 'one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

---

the Member State where this user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk.' (p. 11)

[50] See Facebook (2010c).

[51] Edwards & Hatcher (2009), p. 21. See also Facebook (2010c), Section 5 and 6.

The Article 29 Data Protection Working Party (2007) has, *inter alia*, analyzed in its opinion 4/2007 the definition of "personal data" according to the DPD (section III). The Working Party states that the words 'any information' (Article 2 (a) DPD) call for 'a wide interpretation'.[52] With regard to the terms 'identified or identifiable' the Working Party notes the following:

> 'in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (…).Identification is normally achieved through particular pieces of information which we may call "identifiers" and which hold a particularly privileged and close relationship with the particular individual.' (p. 12)

An example of direct identification is identification by name; examples of indirect identification are identification numbers or a combination of criteria such as age, place of residence, etcetera.[53] What is of crucial importance in determining whether someone is identified or identifiable, is that the person can be distinguished from others; that the person can be 'singled out' from a group. The Working Party notes that this ability to distinguish a person from a group depends on context. For example, a common family name makes direct identification more difficult, hence additional criteria are needed to single out a specific person. When applying this to data in Facebook profiles, it becomes clear that the combination of both direct (name, perhaps profile picture[54], date of birth and email address) and indirect identification factors (preferences, interests, hobbies, political and/or religious views, etcetera) will identify a user in almost all cases. In these cases, i.e. where data relating to an identified or identifiable natural person is processed, the DPD applies. Additionally, to my view, it is not relevant whether a user has set his profile to private or public for determining whether a person is identified or identifiable. In this regard, Recital 26 of the DPD states the following:

> '(…) to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used *either* by the controller *or* by any other person to identify the said person (…)'. (emphasis added)

---

[52] Cf rr. 26 of the DPD: '(…) the principles of protection must apply to *any information* concerning an identified or identifiable person (…)'. (emphasis added)

[53] The DPD refers in Article 2 (a) to 'one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

[54] A profile picture can be any picture, i.e. from a user him or herself but also from a group of friends, their favorite animal or soccer player, etc. Hence, a profile picture will not always play a roll in identification of a person.

In any case, with SNSs both the SNS provider (i.e. the data controller, see par. 2.1.4.2) and other people (how large an audience SNS users have depends on their privacy settings) are able to see the data on the SNS users' profiles and thereby can determine whether that person is identifiable.[55] In these cases, the personal data is not anonymous and the DPD applies.

The third and most important reason why it is not likely that Facebook will be bound by the laws of all EU countries, or the DPD in general, is, simply, that it is practically impossible to enforce the DPD or national laws of the EU Member States in the US. Theoretically, it is possible for EU citizens to go to court in the US and try to enforce their EU rights there. However, it is not likely that the US court will accept these rights as legally binding, because according to international law principles all states are equal and cannot impose rules or laws on each other.[56] A US court therefore does not have to, and probably will not, accept that their citizens or companies are bound by EU law.[57] However, I conclude that where Scramble! is used, EU Facebook users do not have to legally enforce their rights under the DPD in the US, as they can enforce their information privacy rights simply by using Scramble!, while sitting at home behind their PC.

2.1.4.2 Requirements for the lawful processing of personal data: a layered system

Generally, according to the DPD, not the processors[58], but the controllers[59] of personal data are accountable for the processing of personal data.[60] SNS providers fall under the definition of 'data controller' in the DPD.[61] In that capacity, these providers have a

[55] Cf. rr. 26 of the DPD: '(…) to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person(…)'.
[56] I refer to the sovereign equality principle. This principle entails that, in accordance with international law, no country is higher in rank than other countries, and therefore a country cannot make laws that bind another country.
[57] Not to mention the costs, time and effort it would take for an EU citizen to go to court in the US.
[58] 'Processor' is defined by the DPD in Article 2 (e) as: '(…) a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (…)'.s
[59] 'Controller' is defined by the DPD in Article 2 (d) as: '(…) the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law (…)'.
[60] Cf. Article 6 (2), Articles 10 and 11 (information obligations), 17 (security), 18 (obligation to notify the supervisory authority), 23 (liability), which articles all mention the data controller as the one who has to assure particular rights or obligations in that article. Article 23 (1) even states that 'any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to [the Data Protection Directive] is entitled to receive compensation from the controller for the damage suffered.'
[61] See Article 29 Data Protection Working Party (2009): 'SNS providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties.' (p. 5) Cf. also rr. 47 of the DPD.

number of obligations and responsibilities that follow from the DPD, and they can only process personal data in a legitimate and proportionate way when they meet the DPD requirements.[62] What requirements, obligations and responsibilities that are depends on the type of data that are processed and how that data are processed. In this regard, the DPD distinguishes between personal data, sensitive personal data and personal data transferred to third countries, and has a layered system.

The first layer, or level, provides 'general rules on the lawfulness of the processing of personal data' (see Chapter II of the DPD). This level includes the rules stated in Articles 6, 7 and 17 DPD relating to data quality and the legitimate and secure processing of personal data, and Articles 10-15, 18 and 22-24 relating to rights of data subjects and obligations and responsibilities of data controllers. These rules of level one apply to all processing of personal data.

The second level concerns the processing of sensitive personal data and is elaborated in Article 8 (1) DPD, whereas Article 8 (2) and 9 DPD formulate the exceptions to Article 8 (1).[63] When a data controller processes sensitive personal data, they have to comply with the rules of both the first *and* second level.

The third and final level in the DPD is elaborated in Articles 25 and 26 and regards the transfer of personal data to third countries. Such transfer is according to Article 25 (1) allowed where 'the third country in question ensures an adequate level of protection.' Article 26 provides for derogations to Article 25. Where personal data is transferred to a third country, the data processor must also comply with the rules set out in the first level and, in case sensitive personal data is transferred to a third country, the rules of level two.

Additionally, a fourth level and fifth level exist that are not included in the DPD. The fourth level entails sector specific law provisions, such as those provided in the e-Privacy Directive 2002/58/EC and the related Data Retention Directive 2006/24/EC.[64] These specific law provisions are used to 'complement comprehensive legislation [in this case the DPD] by providing more detailed protections for certain categories of information'[65], or for certain specific technologies. The fifth level of data protection rules regard those rules that follow from a contractual relationship between the data controller and the data subject.

[62] It must be noted that these requirements and obligations, and rights on the side of the data subject, are not meant to prevent the processing of personal data. Rather, they are meant to prevent unlawful and/or disproportionate processing of personal data. Furthermore, the DPD principles and requirements build, to a large extent, on the 1981 Council of Europe 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', ETS no. 108.

[63] Sensitive data is defined by the DPD in Article 8 (1) as 'the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.'

[64] Other examples of sector specific laws that build on the DPD are the Consumer Credit Directive 2008/48/EC and the Telecommunications Privacy Directive 97/66/EC.

[65] Electronic Privacy Information Center (EPIC) and Privacy International (PI) (2007)

2.1.4.2.1 Requirements of level one: general rules on lawfulness of data processing

The first set of requirements within level one are listed in Article 6 (1) (a) – (e)[66] and Article 7 DPD and include the following rules and principles:

(1) Personal data must be processed fairly and lawfully, Article 6 (1) (a);
(2) It must be collected for specified, explicit and **legitimate purposes**, and may not be processed in a way incompatible with those purposes, Article 6 (1) (b); what falls under 'legitimate purposes' is stated in Article 7 DPD:
    (a) unambiguous consent;
    (b) performance of a contract;
    (c) legal obligation;
    (d) vital interest of the data subject;
    (e) public law duty;
    (f) legitimate interest controller or third party to whom the data are supplied.
(3) The requirement of data minimization: the processing of data must remain within the specified purpose and be relevant to that purpose, hence the processing of personal data 'shall be limited to the minimum necessary for achieving the specific purpose'[67], Article 6 (1) (c) and (1) (e) (data preservation);
(4) Requirements regarding data quality: the data must be adequate, relevant, accurate, complete and kept up to date in relation to the purpose for which it is collected and processed, Article 6 (1) (c) and (d).

Additional general requirements are set out in:

(5) Articles 10 and 11[68]: the data controller is obliged to inform the data subject about the data controller's identity, the purposes for processing and other information;
(6) Article 12[69]: data subjects have, *inter alia*, the right to obtain from the data controller information about whether information about them is processed and, if so, access to

[66] Note that Article 6 (1) can be restricted under national law of the Member States according to Article 13 (1) DPD when such a restriction is necessary to safeguard, *inter alia*, public or national security, criminal prosecution, an important economic or financial interest of the Member state, etcetera.
[67] Guarda & Zannone (2009), p. 339.
[68] Note that these two articles can be restricted under national law of the Member States according to Article 13 (1) DPD when such a restriction is necessary to safeguard, *inter alia*, public or national security, criminal prosecution, an important economic or financial interest of the Member state, etcetera.
[69] *Ibid.*

that data that is related to them, and additionally, the right to have that data rectified or erased;

(7) Article 14: data subjects have the right to object, in the specified conditions, the processing of their personal data

(8) Article 15: data subjects have the right

> 'not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him (…)'.

(9) Article 16 and 17: confidentiality and data security: the data controller is obliged to 'implement appropriate technical and organizational measures' to assure the security[70] of data processing;

(10) Article 18 and 19: notification and registration: the controller is required to notify the national supervisory data protection authority before processing personal data;

(11) Article 22 – 24: these articles provide rules on judicial remedies, liability (of the data controller) and sanctions.

2.1.4.2.2 Requirements of level two: the processing of sensitive personal data

As said, the requirements, obligations (of the data controller) and rights (of the data subject) of level one apply to all processing of personal data, including the processing of sensitive data. Additionally, when processing sensitive personal data, the rules of level two apply which are set out in Article 8 of the DPD. In principle, the processing of sensitive data is prohibited. However, in Article 8 (2) - (5), (7) and Article 9 DPD, a number of exemptions to this prohibition are formulated. These exemptions include, *inter alia,* the explicit consent of the data subject to the processing of the sensitive data[71]; when the processing is in the vital interest of the data subject[72]; when the data 'are manifestly made public by the data subject'[73]; when the processing of data is necessary according to employment law[74]; necessary in the public interest of the Member State[75]; when it concerns medical data[76] or

[70] Under security falls: 'accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and (…) all other unlawful forms of processing.' See Article 17 DPD.
[71] Article 8 (2) (a) DPD.
[72] Article 8 (2) (c) DPD.
[73] Article 8 (2) (e) DPD.
[74] Article 8 (2) (b) DPD.
[75] Article 8 (4) DPD.
[76] Article 8 (3) DPD.

data processed for criminal investigation or enforcement purposes[77]; when it is processed solely for journalistic purposes or literary or artistic expression[78]; etcetera.

2.1.4.2.3 Requirements of level three: transfer of data to third countries

For data that are transferred to third countries outside the EU or European Economic Area, a three step approach is provided for by the DPD. The first step, is set out in Article 25 (1) and imposes that personal data may only be transferred to a third country if that country 'ensures an adequate level of protection.'[79] Whether a third country meets this requirement is decided by the Commission, see Article 25 (6) DPD.[80] The second step is to look at the derogations from Article 25, provided in Article 26 (1) DPD. In the following cases, a transfer of personal data to a third country that is *not* found to have an adequate level of protection, may take place: in case of unambiguous consent of the data subject[81]; where the transfer is necessary for the performance of a contract[82]; where it is legally required on important grounds public interest[83]; when the transfer is necessary 'in order to protect the vital interests of the data subject'[84] and finally when the personal data was listed in a public register[85]. The third step is formulated in Article 26 (2) DPD, which states that a transfer of personal data, to a third country that does *not* provide an adequate level of protection, is allowed where a Member State has authorized that transfer.[86]

An interesting question here, as this thesis is mostly about Facebook, is whether the EU Commission has decided that the US provides an adequate level of protection, as data of EU citizens is transferred massively to Facebook (US) servers.[87] Formally, the Commission has never provided a decision stating that the US meets the requirement of an adequate level of protection.[88] However, in 2000, after a strong lobby from the US, the Commission accepted the 'Safe Harbor Agreement'. This Agreement includes a number of privacy and

[77] Article 8 (5) DPD.
[78] Article 9 DPD.
[79] An 'adequate level of protection' does not mean the third country has to provide a similar protection as the DPD. Cf. Article 25 (2) DPD.
[80] All the 'Commission decisions on the adequacy of the protection of personal data in third countries' are available at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.
[81] Article 26 (1) (a) DPD.
[82] Article 26 (1) (b) and (c) DPD.
[83] Article 26 (1) (d) DPD.
[84] Article 26 (1) (e) DPD.
[85] Article 26 (1) (f) DPD.
[86] Here, the data controller has to adduce adequate safeguards, see Article 26 (2).
[87] When EU Facebook users put personal data on their Facebook profile, they, by doing so, store this data on the Facebook servers, which are located in the US. See Facebook (2010d), Section 16:
'Special Provisions Applicable to Users Outside the United States
We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users outside the United States:
1. You consent to having your personal data transferred to and processed in the United States.'
[88] Electronic Privacy Information Center (EPIC) and Privacy International (PI) (2007).

data protection principles[89] and US companies can voluntarily join the Safe Harbor project, thereby signifying that they provide an adequate level of data protection. However, these Safe Harbor principles are in no way binding or enforceable; the associated companies merely promise to act in accordance with their privacy principles (in which the Safe Harbor principles have to be incorporated). Facebook has joined Safe Harbor in 2007[90], yet again, this does not effectively assure that EU Facebook users are guaranteed an adequate level of data protection.[91]

2.1.4.3 SNS providers as data controllers

I argued earlier that the DPD applies to EU based SNSs, but that, in case of US based SNS, this is not evident. Although the fact that US based SNSs, and Facebook in particular, make use of equipment in the EU (see Article 4 (1) (c) DPD) by means of cookies brings along that the DPD applies, in practice, this will not have much effect.[92] I will nevertheless asses the use of Scramble! in relation to the DPD as this is relevant for EU based SNSs as well, and also interesting to consider for (EU) SNS users which, although using a US based SNS, wish to enforce their EU data protection rights.

We saw that, in the DPD, there are three levels of requirements. Scramble! generally gives SNSs control over their related personal data that is processed by a SNS. The tool can facilitate the enforcement of several DPD principles of the first level, such as those provided in Articles 12 – 17 DPD. A specific requirement that comes to mind is the requirement of data minimization. According to Article 6 (1) c, the DPD requires that the data is 'not excessive in relation to the purposes for which they are collected and/or further processed'. In the case of Facebook, this has implications for the following requirement set by their general terms: that

[89] See Commission Decision 2000/520/EC of 26 July 2000. The Electronic Privacy Information Center (EPIC) and Privacy International (PI) (2007) summarizes the principles as follows: 'The principles require all signatory organizations to provide individuals with "clear and conspicuous" notice of the kind of information they collect, the purposes for which it may be used, and any third parties to whom it may be disclosed. This notice must be given at the time of the collection of any personal information or "as soon thereafter as is practicable." Individuals must be given the ability to choose (opt-out of) the collection of data where the information is either going to be disclosed to a third party or used for an incompatible purpose. In the case of sensitive information, individuals must expressly consent (opt-in) to the collection. Organizations wishing to transfer data to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the data. Organizations must take reasonable precautions to protect the security of information against loss, misuse and unauthorized access, disclosure, alteration and destruction. Organizations must provide individuals with access to any personal information held about them, and with the opportunity to correct, amend, or delete that information where it is inaccurate. This right is to be granted only if the burden or expense of providing access would not be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would not be violated. In terms of enforcement, organizations must provide access to readily available and affordable independent recourse mechanisms that may investigate complaints and award damages. They must issue follow up compliance procedures and must adhere to sanctions for failing to comply with the principles.'

[90] See http://www.export.gov/safehrbr/companyinfo.aspx?id=9633 and Facebook (2010c).

[91] Electronic Privacy Information Center (EPIC) and Privacy International (PI) (2007).

[92] See par. 2.1.4.1.

users should subscribe with their real name.[93] Keeping in mind that Facebook generally uses the profile information for commercial purposes in *anonymised* form[94], it is questionable whether the publishing of the real name of members might not be excessive according to this article. As is stated in the Opinion 5/2009 of the Article 29 Working Party on online social networking: 'SNS should consider carefully if they can justify forcing their users to act under their real identity rather than under a pseudonym.' (p. 11) Thus, according to EU law an SNS user would have a good argument in saying he wants to use an encryption tool for the purpose of staying anonymous.

Another requirement that is relevant when using Scramble! in SNSs is the requirement of purpose specification and legitimate purpose, see Article 6 (1) (b) and 7 DPD. Article 7 (a) and (b) are of specific relevance for SNS that require their users to accept general terms and conditions before creating a profile, such as Facebook. The article states that data processing is based on a legitimate ground[95], *inter alia,* if the user has given his unambiguous consent, Article 7 (a) DPD, or when the processing is necessary for the performance of a contract between the data subject and the data controller Article 7 (b) DPD. With regard to 'unambigious consent' and creating a Facebook profile (and thereby forming a contract with Facebook) I wish to make some critical remarks. As said earlier, SNS users give their consent by clicking an 'Agree' button[96], thereby agreeing to the SNS's terms, and, in some cases, privacy policies.[97] Consent must be given before one can actually proceed in making an online profile. In this regard, the SNS provider will always argue that clickwrap agreements[98] are binding agreements[99] as the provider then processes personal on the basis of a legitimate ground. It nevertheless remains questionable whether, when a consumer merely clicks an agree button for the sole purpose of being able to continue in making a profile, unambiguous informed consent, as stipulated in the DPD, is given. The DPD defines 'consent' in Article 2 (h) as: 'any freely given specific and informed indication of

[93] Cf. the Facebook Terms section 4: 'Facebook users provide their real names and information ...'. Facebook (2010d).
[94] Facebook (2010c), Section 5.
[95] Keep in mind that this legitimate ground is only one element of the many requirements that have to be fulfilled by data processors in order to comply with EU data protection law.
[96] Facebook places the following statement on its website where someone wants to create a Facebook account: 'By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy.' See Facebook (2010a).
[97] This is the case with Facebook, see Facebook (2010c) and Facebook (2010d).
[98] Clickwrap agreements are agreements where 'the transaction will not go forward unless and until the consumer clicks a button indicating "I agree" (or similar terms of express assent) after the statement of terms and conditions.', see Winn & Bix (2006), p. 177.
[99] A contract comes to exist by offer (Facebook offer the Terms on its website) and acceptance (the Facebook users clicks an 'Agree' button). After acceptance, a contract is formed. However, there are circumstances, e.g. in case of unfair contract terms, where one (or both) of the parties, in that case the consumer, can terminate the contract. Until one of the parties has terminated the contract in court, the contract generally is legally binding. This is, for example, not the case where the contract is not in accordance with law.

his wishes by which the data subject signifies his agreement to personal data relating to him being processed.' With this definition in mind, I must conclude that clickwrap agreements' at least when concluded by consumers, are controversial. By that I mean that it is not likely that many consumers, and especially young or inexperienced internet users, fully read the general terms before clicking and therefore there cannot be informed consent.[100] In the EU, consumers might get protection from, e.g., the Unfair Commercial Practices Directive 2005/29/EC. As the scope of this thesis is limited, I will not assess when and how consumers can rely on this Directive in case of clickwrap agreements concluded with (US-based) SNS. In general it can be noted that according to this Directive, contractual terms that are not individually negotiated 'will be deemed unfair if they crate a significant imbalance, to the consumer's detriment, between the rights and obligations of the contracting parties.'[101] However, in case of US-based SNS, the contract is generally governed by US law as the terms will include a clause saying that US law applies, which is the case with Facebook.[102] It might however be that, according to principles of international private law, binding national rules can not be contracted away by forum selection clauses, but I will not discuss this here. It suffices to say that where US law governs the contract, the SNS users that feel they have not consented to the agreement or that the terms are unfair, can (possible successfully) try to challenge the clickwrap agreement in court.[103] Additionally, with regard to the validity of clickwrap agreements in the US Pacini et al (2002) state that it is:

> 'not require[d] that the recipient of the electronic message know of, open or read the message. All it requires is that the electronic message be available for processing by the recipient's information system.' (p. 47)

I conclude, with regard to the discussion on consent, that the clickwrap agreement Facebook users conclude with this SNS is legally binding both in the EU and in the US, but that, where there are unfair contract terms, consumers can generally rely on consumer protection.

Finally, level 3 is not of relevance for Facebook as Facebook does not transfer personal data from the EU to the US, but the users do.[104] I will discuss this issue in par. 2.1.4.4.

---

[100] Cf. Hillman (2006).
[101] Winn & Bix (2006), p. 186. See Article 3 (1) of the Unfair Commercial Practices Directive 2005/29/EC.
[102] See Facebook (2010d) Section 15: 'The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims.'
[103] See e.g. Willians v America Online, Inc., No. 00-0962, 2001 WL 135825, where the court did not accept the full enforcement of a click-wrap agreement. The unfairness lied in both the formation of the contract and its substantial content.
[104] Facebook itself does not transfer data from the EU to the US. See Kuzcerawy (2009), p. 3 and De Terwange & Louveaux (1997).

Furthermore, it can be noted that in the case of SNS, generally no sector specific law provisions apply.[105]

Overall, it can be said that the DPD's requirements, either separate or together, are no hindrance for the use of an encryption tool by SNS users. Rather, the data protection principles, and especially the principle of data minimalization, and additionally of data control and security of data processing, are each reasons to encourage the use of encryption by SNS users. However, it must be kept in mind that when Facebook users use Scamble! in Facebook they might possibly violate Facebook's Terms, which in this thesis I deem to be legally binding.[106] I will deal with the contractual relation (level 5, see par. 2.1.4.2) between the SNS provider Facebook and its users in chapter 4.

2.1.4.4 SNS users as data controllers

Not only SNSs are data controllers, also SNS users can, in certain circumstances, be considered as data controllers. It has been argued that in some cases, e.g. when the user's activities or the access to their profile goes 'beyond a purely personal or household activity'[107] or when sensitive data of others are processed, SNS users are data controllers.[108] This is the case where SNS users have a large amount of people added to their friends list or where their profile is public, thus having a large audience. If these users then post personal data about others one their profile, such as pictures or stories about their friend which friends are identified or identifiable, they process personal (perhaps even sensitive) data have to comply with EU data protection rules.

A case of the European Court of Justice (hereafter: ECJ) that illustrates this is the *Lindqvist* case.[109] Ms. Lindqvist had made a personal website about her work at a local parish church and she had put personal information of her colleagues, including full name and telephone numbers, hobbies and interest, on that website. She also wrote down stories about her colleagues and mentioned that one of them had injured her foot.[110] Both Ms. Lindqvist's colleagues and the Swedish data protection authority were not happy about this

[105] One might think an SNS is an electronic communications service and that the e-Privacy Directive and Data Retention Directive apply. However, SNS do not fall within the scope of the definition of 'electronic communications service', which definition is provided in Article 2 (c) of the Framework Directive (2002/21/EC). In this regard the Article 29 Data Protection Working Party (2009) notes that 'SNS providers may offer additional services that fall under the scope of an electronic communications service such as a publicly accessible email service. Such a service will be subject to the provisions of the e-Privacy Directive and the Data Retention Directive.' (p. 10)
[106] See note 89.
[107] Article 29 Data Protection Working Party (2009), p. 6.
[108] Cf. Wong (2008) and Wong (2009), p. 144.
[109] Lindqvist C-101/01, ECJ judgment of 6 November 2003.
[110] Information about an injury of an identified or identifiable person is sensitive (medical) personal data, see Article 8 (3) DPD.

and went to court. The Swedish court had asked the ECJ, in a preliminary procedure[111], two question: the first was whether putting personal data on a website falls under the definition of 'processing of personal data'[112] of Article 2 (b) DPD (cf. Article 3 (1) DPD) and the second was whether putting personal data on a website constitutes a transfer of personal (sensitive) data to a third country.[113] The first question was answered affirmatively: putting information on a website constitutes the 'processing of personal data wholly or partly by automatic means'.[114] The second question was answered in the negative: the ECJ ruled that there is

> 'no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.'

What implications does this case have for EU SNS-users using Facebook, a US-based SNS? With regard to the first question posed in the Lindqvist case, it can be said that where SNS users put personal data of others who are identifiable on a website (Facebook), this falls under the definition of 'processing of personal data'. Consequentially, this processing falls within the scope of the DPD, see Article 3 (1). SNS users might be able to invoke Article 3 (2) DPD: 'this Directive shall not apply to the processing of personal data (…) by a natural person in the course of a purely personal or household activity.' The ECJ has noted the following about this in the *Lindqvist* case:

> 'As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses. That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.'

[111] Article 267 (ex Article 234 TEU) of the Treaty on the Functioning of the European Union.
[112] Under the definition of 'processing of personal data' falls 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'
[113] The reasoning behind this is that when someone puts personal data on an internet website anyone in the world who has access to the internet can view and access that personal information.
[114] Lindqvist C-101/01, ECJ judgment of 6 November 2003, par. 27.

Not much SNS users will limit themselves purely to 'activities which are carried out in the course of private or family life of individuals'. In these cases SNS users cannot invoke the Article 3 (2) exception and, when they are data controllers, hence they are obliged to meet all the DPD requirements for data processing, depending on what kind of data they are processing. With regard to the second question posed in the Lindqvist case I conclude that EU citizens using Facebook *do* transfer personal data (when they post personal data of another person that is identifiable on their profile and are data controllers) to third counties. In this regard the following sentence in the reasons of the ECJ is important: there is 'no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is *stored with his hosting provider which is established in that State or in another Member State*.' (emphasis added) When using Facebook, EU users do not load the personal data on an internet page that is stored with a hosting provider in the EU, but they load this data to servers located in the US. Facebook users specifically consent to do so by accepting the Facebook terms:

> '**Special Provisions Applicable to Users Outside the United States**
> We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users outside the United States: 1. You consent to having your personal data transferred to and processed in the United States. (…)'[115]

As a consequence, EU SNS users that post personal data of another person that is identifiable on their profile and are considered data controllers, do not only have to comply with level one DPD requirements[116], and possible level two[117] in case of sensitive data, but also have to comply with level three[118] of the DPD. We saw that where personal data are transferred to a third country this is only allowed if that country 'ensures an adequate level of protection. We also saw that the Commission has not yet officially declared the US to have such an adequate level of protection.[119] The Safe Harbor agreement only applies where US companies have joined this project, which obviously does not apply to individual EU SNS users. This implies that EU Facebook (or other US-based SNS) users are not allowed to transfer personal data, via the Facebook website, to the US. These users will usually not be able to invoke of the derogations provided in Article 26 DPD, except for the derogation under

[115] Facebook (2010d), par. 16.
[116] See par. 2.1.4.2.1.
[117] See par. 2.1.4.2.2.
[118] See par. 2.1.4.2.3.
[119] Article 25 (6) DPD.

Article 26 (a) DPD: namely the unambiguous consent of the data subject. This consent is given, e.g., when the data controller SNS user puts a picture, that includes another person, on his Facebook profile, and this other person accepts the 'tag' by which his name appears under the picture.[120]

With this in mind, the use of an encryption tool by SNS users should be encouraged as it helps them to effectively fulfil the obligations they have under level one and two of the DPD, which obligations I have elaborated in par. 2.1.4.2. Additionally, level three would no longer apply if a EU Facebook users puts encrypted personal information on his profile, as no personal data would be sent to the Facebook servers located in the US. Facebook would only be able to see scrambled gibberish, see par. 1.2.2, figure 7.

2.1.5 Conclusion EU privacy regulation

In par. 2.1, I discussed the legal position of (the use of) Scramble! in SNSs is from the perspective of EU privacy regulation. The EU Charter of Fundamental Rights provides a fundamental right to data protection, and in this regard I concluded that this right, obviously, does not form an obstacle for the use of Scramble!. Rather, this fundamental right should be seen a reason to encourage its use, since SNSs currently do not provide sufficient (technological) means for its users to control their online information privacy. Additionally, I explained how Scramble! can enforce the right to data protection, and which benefits such independent technological enforcement has regarding SNS user privacy control and enforcement of the right to data protection outside the EU. Moreover, the European Commission supports the use of PETs such as Scramble!

In assessing the DPD, I argued that while EU law theoretically applies to US based SNSs, - on the condition that cookies are accepted by the SNS users and that the data processed are related to an identified or identifiable person - in practice EU law cannot be enforced in the US. However, I concluded that although EU Facebook users cannot get legal protection from the DPD in the US, they can enforce their information privacy rights under the DPD by using Scramble! I continued to examine the DPD and explained that data controllers are, according to the DPD, obliged to meet a number of requirements for the processing of personal data. In this regard, the Directive is built up of three different layers, or levels. The first level provides general requirements that apply to all data processing under the DPD. The second level provides additional requirements for the processing of sensitive data, and the third level contains rules on the transfer of personal data to countries

[120] In this regard, the Facebook Terms (Facebook (2010d)) state the following in Section 3 (9): 'You will not tag users or send email invitations to non-users without their consent.' This is because non-users cannot accept a tag and therefore have to give their consent for the publication of their picture in another way. For an explanation about tagging, see par. 1.1. and note 8.

outside the EU. Next, I assessed the use of Scramble! in light of the DPD and looked at the situations where either the SNS provider, or SNS users are data controllers. In relation to the first situation, I argued that Scramble! facilitates the requirement of certain DPD requirements, such as data minimization. I also discussed whether the consent - as being one of the legitimate grounds for data processing - of Facebook users to the processing and collection of data as stated in Facebook's Terms and Policies, constitutes consent as stipulated by the DPD. My conclusion was that clickwrap agreements are controversial, but that consumers can generally rely on consumer protection in case of unfair contract terms. In relation to the second situation, i.e. where SNS users are data controllers, I noted that EU SNS users using a US based SNS such as Facebook are obliged to meet the DPD requirements of the third level where they transfer personal data of others to the US. Next to that, they, as data controllers, have to meet the requirements of the first, and possibly second level. After having established this, I concluded that where SNS users are data controllers, the use o Scramble! is useful for them to be able to fulfil the obligations of the DPD.

In general, I conclude that EU privacy law does not provide for any obstacle for the use of Scramble! in (US based) SNS, but that these laws rather, either implicitly or explicitly, encourage the use of this crypto tool.

2.2 US privacy regulation

In this section I will evaluate the extent to which US law allows for the use of Scramble! for purposes of privacy protection. More specifically, I will examine whether SNS users can claim a right to online information privacy on the basis of US privacy law, and what the outcome of this examination means for the use of Scramble! in Facebook. In doing so, I will only asses US information privacy law (i.e. data protection law) in a horizontal relationship, i.e. a relationship between citizens and/or companies.[121] Hence, the US constitutional right to privacy, that touches upon the status of bodily, communications and territorial privacy of US citizens in relation to the government (a vertical right to privacy) and is based on the Fourth Amendment, will not be discussed.[122] The assessment will also not include the US privacy Act of 1974, which regulates 'the government's use collection and disclosure of all types of personal information.'[123]

[121] In the US the wording 'information privacy' are used more commonly than 'data protection'.
[122] The US Constitution only contains negative rights, and does not create a positive right to data protection either. See Solove (2001), p. 1435.
[123] Bignami (2007), p. 1. Cf. Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

2.2.1 A short introduction to US information privacy law

In the US there are no general public - i.e. federal - laws that regulate the horizontal privacy of their citizens; neither in terms of a general horizontal right to privacy nor in terms of (a right to) data protection.[124] The US information privacy law system makes use of a multitude of different norms from different sources, which Purtova (2009) explains as follows:

> 'US information privacy law (…) comprises norms of tort, constitutional, and statutory law – a patchwork of the rules different in sources, subjects of regulation, and applicability.' (p. 509)

To enable some insight in the US information privacy law system, I will now briefly explain what the sources of laws and norms in the US are. In the US, the people and the states have, by setting up the US Constitution, conferred a limited number of powers to the federal government. In this regard, the Tenth Amendment to the US Constitution (which Amendment is part of the Bill of Rights) states the following: 'The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.' This implies that the powers of the federal government are limited by the US constitution and that 'state autonomy is both limited and protected by the terms of the Constitution itself'.[125] With regard to the powers of the States Killian et al. (2004) remark that '[s]tates retain a significant amount of sovereign authority "only to the extent that the Constitution has not divested them of their original powers and transferred those powers to the Federal Government." (469 U.S. 528 (1985), at 549).'[126] To clarify, no laws, regulations or other federal or state acts may violate the US constitution. Another source of law is statute law, which laws can be created by both the federal government and the distinct states. State statute laws can, with regard to one subject, vary from state to state, as each state is autonomous in that regard. States also each have their own State Constitution. What also can vary from state to state are court rulings; another source of law in the US. Courts have the power to create laws within the gaps of the US Constitution and (state or federal) statutory law.[127] Moreover, anything not pre-empted by these aforementioned sources of law can be covered by court rulings. State courts have to take into account the rulings of the US federal courts (which includes the US Supreme Court) as well, as the latter are higher in rank than state courts.

[124] There are vertical rights to (information) privacy in the US, cf. the US Privacy Act of 1974 and the Fourth Amendment to the US Constitution.
[125] Killian et al. (2004), p. 969.
[126] *Ibid.*
[127] The US Supreme Court has the power to declare federal or state laws unconstitutional. However, where there are differences in interpretation across different states the US Supreme Court will not consider this to be unconstitutional per se.

An additional source of rules that I have not mentioned earlier is self-regulation, which plays a prominent role in the US. US lawmaking is based on the idea of *laissez faire,* and encourages self-regulation rather than federal or state regulations. As Blok (2002) states:

> 'In general, the government relies on the self-regulating capacities of the private sector. Regulation is considered justified only when data processing in the private sector appears to get out of hand.' (p. 268)

Self-regulation has taken over in the field of information privacy law as there is a lack of general federal or state regulations in this regard. The main reason why there is a lack of information privacy law that covers the private sector, is that at the time such regulation was created for the *public* sector[128] there was no *need* for regulating the private sector. At that time, the private sector, to the government's knowledge, hardly violated any principles of data processing. This is no longer the reality of today. In the introduction of the international the 'Principles for providing and using personal information'[129], which principles are expressly directed to both the public and private sector, it is stated that: 'The private sector now rivals the government in acquiring and using personal information.'[130] Besides these international principles there are other non-binding principles such as the 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'[131]; the 'Code of fair information practices'[132] and the Safe Harbor Agreement[133]. Neither of these principles is codified; they merely serve as non-binding guidelines for the private sector.[134]

After briefly having explored the sources of US information privacy law, it appears that it is not easy to comprehend these rules and regulations, especially since there are many levels of sources and the rules (i.e. state statute laws, State Constitutions and state court rulings) and interpretations (of the US Constitution and US statute law) can differ from state to state. Within the US information privacy law system, Solove (2001) states, information privacy issues are dealt with by using 'whatever is at hand (…) to deal with the

[128] That is the US privacy Act of 1974.
[129] NII Privacy Principles 1995.
[130] NII Privacy Principles 1995, Introduction.
[131] Available from: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [Accessed 22nd June 2010].
[132] See the Electronic Privacy Information Center (EPIC) [Online] http://epic.org/privacy/consumer/code_fair_info.html [Accessed 22nd June 2010].
[133] See par. 2.1.4.2.3.
[134] Because principles deriving from self-regulatory mechanisms cannot be enforced in court, I will not involve these principles in the assessment of the legal status of the use of Scramble! in SNSs. In the case of Facebook, the Safe Harbor principles are incorporated into the Facebook Privacy Policy (this Policy is part of the contract between Facebook and its users and is therefore enforceable in court), which Policy will be examined in par. 4.3.

emerging problems created by the information revolution.'[135] I will nevertheless attempt to illustrate what the legal status of Scramble! is in relation to US information privacy law, but this assessment will be limited to tort law.[136] There are a number of sector specific statutory laws relating to information privacy, such as the Video Privacy Protection Act (1988), the Right to Financial Privacy Act (1978) and the Child Online Protection Act (1998), on the basis of which a SNS might be able to invoke a specific right to information privacy. However, due to the word limit and limited scope for this thesis, I will not take into account the specific situations in which these Acts can apply.

2.2.2 Privacy tort law and Scramble!

2.2.2.1 Introduction to privacy tort law

Tort law is defined by White (2003) as: 'a field that (…) [is] reflected in individual actions seeking civil redress for injuries not arising out of contractual relations (…)'.[137] This means that it enables those, that have suffered an injury which was caused by a civil wrong acknowledged as a tort, can go to court to claim damage for that injury. It is important to note that tort law does not create rules which impose that x, or y is, or is not allowed. Tort law creates rules saying that if someone does x, which causes damages to y, that someone has to pay damages to y for doing x. Tort law is mainly state law based on and developed by courts, hence tort law varies from state to state.[138] The American Law Institute has catalogued the law of torts in the non-binding *Restatement of the Law of Torts* (hereafter: the Restatement), to 'address uncertainty in the law through a restatement of basic legal subjects that would tell judges and lawyers what the law was.'[139] As the Restatement is received very well in the legal (scientific) field[140] and is used frequently to refer to the law of torts[141], I will base my assessment regarding the legal status of Scramble! on the law of torts as formulated in this Restatement.

Within the Restatement four types of tort that relate to privacy are distinguished:

(1) Intrusion into seclusion or solitude[142];
(2) Appropriation of name or likeness[143];

[135] Solove (2001), p. 1430.
[136] See note 136.
[137] White (2003), p. xxiii.
[138] Purtova (2009), p. 509.
[139] American Law Institute [Online] http://www.ali.org/ali_old/thisali.htm [Accessed 22nd June 2010].
[140] Prosser & Keeton (1984);
[141] Purtova (2009), p. 509.
[142] Restatement (Second) §652B: 'One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.'

(3) Public disclosure of embarrassing private facts[144];

(4) False light publicity (defamation)[145].

Privacy invasions relating to SNSs profile content can potentially be caused by SNS providers, e.g. where these (mis)use personal data of SNS users in a way that is not in accordance with the SNSs' general terms or privacy policies (being the contract between the SNS provider and its users).[146] Also others that can access the profile content can possibly misuse that content.[147] The question in both cases is whether SNS users can successfully invoke, where personal information was voluntarily disclosed by them on their SNSs, a right to informational privacy. Whether this is the case, and what the outcome of this question means for the use of Scramble! in Facebook, will be discussed in this paragraph. I will focus only on the tort of intrusion (1), as the other three torts are much less relevant in assessing the use of Scramble! in Facebook.[148] What I mean by 'less relevant' is that the tort is not likely to be successfully invoked by SNS users that claim online information privacy[149] and/or are not relevant in the sense that what the tort protects, does not cover information privacy as such.[150]

---

[143] Restatement (Second) §652C: 'One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.'

[144] Restatement (Second) §652D: 'One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.'

[145] Restatement (Second) §652E: 'One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.'

[146] Keep in mind that in the US, invoking a right to informational privacy for situations that occurred online is not evident. As Abril (2007) states: '(…) privacy is usually a function of the physical space in which the purportedly private activity occurred (…)'. (p. 2) See also Abril (2007), p. 17-20. In the next paragraphs I will explain in which "online situations" a, in this case, SNS user can invoke a right to information privacy.

[147] Think of the case where a 15 year old girl from the US claimed that a picture of her, she placed on a social networking site, was taken and used without her permission by Virgin Mobile for a billboard campaign in Australia. See The New York Times (2007).

[148] Due to the focus on the tort of intrusion only, I will not include into the assessment a discussion on the relation between privacy and the First Amendment to the US Constitution. This particular relation only plays a role in the tort of public disclosure of embarrassing private facts, see Solove (2006b), p. 131-136. See also Abril (2007), p. 9, citing Prosser & Keeton (1984), p. 173.

[149] With regard to the tort of public disclosure of embarrassing private facts both Purtova (2009), p. 510 (in relation to information privacy issues in general), and Abril (2007) (in relation to online social networks specifically) claim that it is extremely difficult to claim a right to information privacy for online situations (i.e. information privacy invasions that occurred in "cyberspace") by invoking this tort. Each requirement that needs to be met for this tort would face difficult obstacles inherent to online situations / the architecture of the internet, making it difficult to satisfy these requirements in case one wants to claim privacy in online situations. See Purtova (2009), p. 510-511 and Abril (2007), p. 17-27.

[150] With regard to the tort of false light publicity, Purtova (2009), p. 511, states the following: The tort of false light publicity 'has limited or no applicability to the data protection problem.' She continues by saying that this tort 'protects one's reputation, whereas data processing is rarely harmful to this interest.' See also Solove (2001), p. 1433 and Bergelson (2003), p. 405. With regard to the tort of appropriation of name, Purtova (2009), p. 511 states that this tort can be invoked where personal information is users for targeted marketing

2.2.2.2 The use of Scramble! in SNSs and the tort of intrusion into seclusion or solitude

The tort of intrusion is formulated in the Restatement (Second) §652B as follows:

> 'One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.'

This tort can potentially be invoked in case of 'an unauthorized acquisition or transfer of personal information'[151] but is limited to cases relating to data *collection*.[152] Hence, I will only discuss the tort of intrusion in relation to this particular information privacy intrusion. An example related to SNSs in this regard, is the situation where a SNS provider (mis)uses personal data of SNS users in a way that is not in accordance with the SNSs' general terms or privacy policies (being the contract between the SNS provider and its users). However, not only the SNS provider can possibly misuse profile content; also others can.[153]

I will now assess whether SNS users can successfully invoke this tort in case of an unauthorized collection or transfer of personal information. The requirements that need to be met in order for the claim to succeed are specifically stated in the Restatement (Second), §652B: there must be an intrusion, physically or otherwise, of another his private affairs or concerns; the plaintiff must have been in solitude or seclusion (meaning the intrusion occurred while the plaintiff was in a private place) and the plaintiff must have a reasonable expectation of privacy ('if the intrusion would be highly offensive to a reasonable person'). Where SNS users claim information privacy on the basis of the tort of intrusion, they are confronted with a number of obstacles that are related to the fulfillment of the requirements[154] of this tort:

---

only where the name of the person is used to profit. See also Solove (2001), p. 1433-1434 and Bergelson (2003), p. 411.

[151] Bergelson (2003), p. 405. Cf. also Solove (2001), p. 1432.

[152] Bergelson (2003), p. 406 and Purtova (2009), p. 510.

[153] Think of the case where a 15 year old girl from the US claimed that a picture of her, she placed on a social networking site, was taken and used without her permission by Virgin Mobile for a billboard campaign in Australia. See The New York Times (2007).

[154] The requirements are specifically stated in Restatement (Second) §652B: there must be an intrusion, physically or otherwise, of another his private affairs or concerns; the plaintiff must have been in solitude or seclusion (meaning the intrusion occurred while the plaintiff was in a private place); the plaintiff must have a reasonable expectation of privacy.

(1) Courts are not likely to accept that the requirement of 'seclusion or solitude' is fulfilled where the plaintiff was in a public place while the intrusion occurred[155], and in relation to this Solove (2001) argues that 'many parts of cyberspace may well be considered public places.'[156] Solove does not, however, explain which particular parts of cyberspace fall under public places. In my view, a distinction must be made between data collection by Facebook and data collection by others to determining whether a SNS profile is public or private. Where SNS users have set their privacy settings to 'private'[157] (either for their entire profile or for particular content, e.g. a photo album or wall[158]) these users seclude themselves from the rest of cyberspace (i.e. from others but not from the SNS provider) and are therefore no longer in a public place. However, where an information privacy issue arises between an SNS user and SNS provider, in my view, the SNS users are never in a private situation. The SNS provider can always view their users' profile content.[159] And this is where Scramble! comes to play an important role in determining whether a possible information privacy invasive action occurred in a public or private place: if Scramble! would be used by a SNS users, the encrypted content would by definition be private. Scramble! users can change (the notion of) a public place in SNSs into a private place, even with regard to SNS providers. Moreover, even *if* an information privacy invasive action could occur (if one would want to do so he or she would have to be able to either hack Scramble! or decrypt the cyphertext/), this action clearly occurred in a private place as the information was encrypted; thus secret.

(2) Only unauthorized intrusions are covered by the tort of intrusion.[160] The question that arises here is what 'unauthorized' means. In my view, an intrusion is unauthorized where the person involved has not given its (prior) consent[161] to the specific intrusion, but also

---

[155] Purtova (2009), p. 510: cf. note 33 where Purtova mentions the case *Muratore v. M/S Scotia Prince*, 656 F. Supp. 471, 482-83 (1987). See also Abril (2007), p. 18: 'Under the Restatement, an individual cannot have a reasonable expectation of privacy in any public place.'

[156] Solove (2001), p. 1433.

[157] With 'private' I mean that only those added to users' friends lists can view the content, provided that these users have no excessive amount of friends and/or have added many people they do not, or barely know.

[158] Where only part of the SNS user's profile is set to private that user have secluded themselves only for that particular part of content.

[159] The question might arise whether SNSs should be assessed separately for determining whether these, or a particular profile, are public or private, or whether these should be assessed in the context of cyberspace in general. As appears from my conclusion here, I view Cyberspace not as one single "territory". Rather, Cyberspace is chopped up into different areas (websites) that each can have a different sphere, i.e. either public or private or a combination of the two. I refer to Abril (2007), p. 20: 'By its own architecture, however, cyberspace lacks a public sphere, as it is composed of "a mosaic of private allotments," or websites. (Abril cites: Benoliel, D. (2005) Law, Geography, and Cyberspace: The Case of On-line Territorial. *Arts and Entertainment Law Journal*, 23, p. 125-126.) Hence, whether an information privacy issue occurred in a public or private place should be assessed in the context of the particular website.

[160] Purtova (2009), p. 510.

[161] The prevailing opinion amongst US judges is that there is no breach of a right to privacy when the person concerned has given implicit or explicit consent for that particular "breach". See Blok (2002), p. 216.

where the intrusion is unauthorized according to law. Regarding the latter I refer to, e.g., anti-circumvention law provided in the Digital Millennium Copyright Act, which prohibits the circumvention of copyright protection mechanisms such as Scramble!.[162] If someone, e.g. a SNS provider (or anyone else), would circumvent Scramble! (as a copyright protection mechanism) without prior consent of the person using that tool, the requirement of 'unauthorized' for the tort of intrusion would be fulfilled. While I think that, in the case of Facebook, SNS users do not give permission for the circumvention of Scramble! by Facebook[163], I do believe that Facebook users generally consent to an intrusion by Facebook (but not to people who don't have "normal" access to the user's Facebook profile) by accepting the Facebook Terms and Privacy Policy.[164] What this "intrusion" may include is determined by the scope of the Facebook Terms and Privacy Policy. Anything that falls outside that specific scope is *not* authorized. An intrusion may be not unauthorized not only on the basis of *consent,* but also on the basis of the fact that the private information was *disclosed voluntarily*[165]*.* In this regard, Purtova (2009) mentions the case *Dwyer v. American Express Co.*[166], where the profiling practices of the creditcard company on the basis of spending habits[167] were challenged before the Illinois Appellate Court.[168] The Court ruled that these practices were not unauthorized because '[b]y using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences.'[169] Thus, it seems that profiling practices for marketing and sale purposes based on personal information voluntarily given to the company making these profiles, e.g. SNSs, does not constitute an *unauthorized* intrusion into seclusion or solitude.[170] Whether that company can *transfer* personal data to other companies is determined by the contract between the company and the data subject.[171]

---

[162] Indeed, Scramble! is also a copyright protection mechanism. I will discuss this and the related anti-circumvention law in par. 3.2.1. (EU anti-circumvention law) and par. 3.3.2 (US anti-circumvention law).
[163] I explain this in par. par. 3.2.1. (EU anti-circumvention law) and par. 3.3.2 (US anti-circumvention law).
[164] Generally, the Facebook Terms and Privacy Policy are legally binding. See par. 4.1.
[165] To note, the use of information that is in public databases is also not unauthorized. See Purtova (2009), p. 510 and Solove (2001), p. 1432.
[166] *Dwyer v. Am. Express Co*., 652 N.E. 2d1351, 1352-53 (Ill. App. Cr. 1995).
[167] These profiling practices were 'part of a targeted joint-marketing and sales program' whereby American Express categorizes and ranks their cardholders 'into six tiers based on spending habits'. See the opinion of justice Buckley in *Dwyer v. Am. Express Co*.
[168] Purtova (2009), p. 510.
[169] *Dwyer v. Am. Express Co.,* at 1354.
[170] Cf. Purtova (2009), p. 510 and *Dwyer v. Am. Express Co.,* at 1354. See also note 160.
[171] For Facebook, see Facebook (2010c), section 5 and 6. In addition, Facebook states the following on it's Facebook Site Government page: 'Facebook will not sell your information to anyone. We may provide information to other companies to help us bring you the services we offer. However, these companies can only use this information for reasons that we specify.' See http://www.facebook.com/note.php?note_id=183539710300 under 'Other Comments'.

(3) The tort of intrusion (and any tort for that matter[172]) can only successfully be invoked where the person concerned has a 'reasonable expectation of privacy in the space in question.'[173] This requirement of a reasonable expectation of privacy follows from the following sentence of the Restatement §652B: 'the intrusion would be highly offensive to a reasonable person'. In assessing whether a plaintiff can claim to have such reasonable expectation of privacy, the court 'considers the physical location of the disclosure of information'[174] and will furthermore take into account 'the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.'[175]

Now I have indicated what courts considers in determining a reasonable expectation of privacy, I will discuss these factors in relation to information privacy and the collection of personal information[176] by SNSs in general, and the use of Scramble! in Facebook specifically. By Solove (2001), it is argued that an 'intrusion would be highly offensive to a reasonable person'[177] only in case of the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time.'[178] When following this argument, that would mean that SNS users can only claim to be highly offended when a multitude of information privacy invasions have occurred.[179] Considering this argument specifically in relation to Facebook and its Terms an Privacy Policy, I argue that its users can only claim to have a reasonable expectation of privacy when the data collection practices of Facebook significantly exceeds the scope of the contract (i.e. the Terms and Privacy Policy). An example where Facebook's data collection practices would exceed this scope is where Facebook, while it has stated in its Terms or Policy that personal data is collected or transferred only in 'non-personally identifiable' from, collects or transfers that data in a way that the data can be linked to identifiable persons. However, I reiterate that such an information privacy intrusion should be '*highly offensive* to a reasonable person'[180] in order to successfully be considered a tort of intrusion. A single intrusion is, in my view, not likely to be considered

[172] See Abril (2007), p. 18: 'In deciding privacy tort claims, courts are charged with determining whether there was a reasonable expectation of privacy in the space in question.'
[173] *Ibid.*
[174] Abril (2007), p. 18.
[175] *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003), p. 1008-09. See also Purtova (2009), p. 510.
[176] Privacy claims based on the tort of intrusion can only cover cases of data *collection*. See Purtova (2009), p. 510 and Bergelson (2003), p. 406.
[177] Restatement (second) §652B.
[178] Solove (2001), p. 1432.
[179] *Ibid.* See also Purtova (2009), p. 510.
[180] Restatement (second) §652B. (emphasis added)

highly offensive by US courts.[181] Where the collection of personal data of Facebook users by Facebook remains *within* the scope of the Terms and Privacy Policy, it is highly unlikely that there can be claimed a reasonable expectation of privacy. Although Facebook's Privacy Policy acknowledges and emphasizes the importance of privacy[182], it is also stated clearly in that same Policy that Facebook collects their users' personal data in multiple ways.[183]

To what extent do SNS users have a reasonable expectation of privacy when their profile content is collected by people or companies other than the SNS provider? Where the particular content was visible or normally accessible[184] to that person or company the SNS user has no reasonable expectation of privacy. Abril (2007) states in this regard:

'Courts routinely reason that once a person communicates a fact or story about herself to anyone — including a friend, intimate circle, or other intended audience — that information is no longer protectable as a matter of law.'[185]

Does the use of Scramble! affect the evaluation of the criterium of a reasonable expectation of privacy? First of all, for content that can be encrypted by Scramble!, (information) privacy issues are not likely to occur as the encrypted cannot be accessed by those who are not authorized to see it. Where a person or company would, hypothetically, be able to circumvent Scramble! and would acquire or transfer the (at first) encrypted information, the plaintiff would, in my opinion, have a reasonable expectation of privacy with regard to the encrypted information. In relation to this, Solove (2006a) states the following:

> 'privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information.' (p. 497)

[181] See note 177 and 178.
[182] Facebook claims to adhere the US TRUSTe Program and Safe Harbor, see par. 4.3.
[183] See par. 4.3 where I discuss Section 2 of Facebook's Privacy Policy, which section explains what information Facebook collects.
[184] By 'normally accessible' I mean without much effort. This excludes situations where data is accessed by e.g. hacking Scramble!.
[185] Abril (2007), p. 23-24. In this regard Abril cites the cases *Wilson v. Harvey* 842 N.E.2d 83 (Ohio Ct. App. 2005) and *Nader v. General Motors Corp* 255 N.E.2d 765 (N.Y. 1970) , in which cases it was ruled that 'information must be completely secret to sustain a claim.' Abril (2007), p. 24.

Thus, where information was completely secret, the SNS user has a reasonable expectation of privacy. I interpret '*completely* secret' as information that is disclosed only to family and friends.[186] Scramble! facilitates this secrecy and, hence, a reasonable expectation of privacy. Even where SNS users have a huge friend list with many people added that the users do not know, these users are able to facilitate secrecy and a reasonable expectation of privacy by using Scramble!. SNS users can do so by making the information they wish to be secret inaccessible for people that are not their close friends and family. Hence, the notion that secrecy is not possible in cyberspace is no longer valid.[187]

In general I conclude that, after having viewed the aforementioned obstacles in relation to the fulfillment of the requirements for a successful claim based on the tort of intrusion, Scramble! makes the entire discussion about these criteria, and about privacy tort law, irrelevant. As it is practically impossible to decrypt content encrypted by Scramble!, and as SNS users using Scramble! have full control over which individual can see the content they post online, how can information privacy intrusions occur?

2.2.3 Conclusion US privacy regulation

In par. 2.2 I posed the question whether SNS users can claim a right to online information privacy on the basis of US privacy law, and what the outcome of this examination means for the use of Scramble! in Facebook. After having given a short introduction to US information privacy law in general and privacy tort law specifically, I assessed whether a SNS user can claim a right to information privacy, based the tort of intrusion into seclusion, in case of an unauthorized acquisition or transfer of personal information., and what the outcome to this assessment means for the use of Scramble! in Facebook. We saw that, in this regard, there are a number of obstacles that are related to the fulfillment of the requirements of the tort of intrusion. The first obstacle is related to the requirement of seclusion or solitude, where this requirement is established only if the intrusion occurred in a private place. Whether this is the case in SNSs depends, in my opinion, on whether the data collection was conducted by Facebook or by others. In any case, where SNS users would

[186] Cf. Purtova (2009), p. 511.
[187] See Abril (2007), p. 25: 'In cyberspace, the complete secrecy requirement of privacy torts is difficult, if not impossible, to satisfy. Total secrecy is difficult offline; this difficulty is magnified online. No information placed on OSNs [Online Social Networking sites] is completely secret, even if a profile is set to private. For example, consider the situation where a person reveals a fact on her profile, which is accessible to her entire network of friends. If courts apply the secrecy rationale used in physical space, this information would not be protected. Secrecy is destroyed even if a person reveals the fact via an OSN's private messaging function because it is not the medium of the revelation, but the revelation itself that is dispositive. Any information posted on OSNs — even if never actually transmitted to another — is not completely secret. This is because anything posted on OSNs is accessible to a third party — the OSNs themselves.'

use Scramble! to encrypt profile content, that user would create, at least in relation to that particular content, create a private place. The second obstacle concerned the requirement of 'unauthorized intrusion'. To the extent that an intrusion is possible after the information was encrypted, such intrusion is not authorized where Scramble! was used as a copyright protection mechanism, based on anti-circumvention law. However, in case of consent by the data subject, or in case the information concerned was provided voluntarily to the SNS provider, intrusions into information privacy are permissible, yet it is questionable whether the SNS provider is able to do so with encrypted content. Where intrusions by the SNS provider fall outside the contractual scope, these are not authorized. However, in both situations, i.e. where an intrusion would be authorized or where the intrusion unauthorized, Scramble! can be used to enforce information privacy, which makes this distinction (or discussion?) irrelevant. With regard to the assessment of the final obstacle, which obstacle related to the requirement of a reasonable expectation of privacy, I come to the same conclusion as with the second obstacle: the use of Scramble! makes a discussion on whether a SNS users has a reasonable expectation of privacy irrelevant because the encrypted content cannot be accessed by anyone the SNS users did not authorize to see that content. If any privacy intrusions would follow after Scramble! was be circumvented, clearly the plaintiff would have a reasonable expectation of privacy the plaintiff had made the information (technologically) secret. The general conclusion with regard to US privacy tort law is that the use of Scramble! would make the discussion on whether a right to information privacy can be invoked on the basis of these laws, irrelevant, as accessing content encrypted by Scramble! is practically, impossible. Hence, most risks to information privacy intrusions are vanquished by Scramble!, i.e. for content that can be encrypted by Scramble! The question that remains is: does US information privacy (tort) law provide an obstacle for the use of Scramble! in SNSs? The answer is no: the use of Scramble! is allowed, at least not prohibited by privacy tort law. What the use of Scramble! in SNSs establishes, is that it makes information privacy issues and the discussion on whether privacy tort law is applicable irrelevant, i.e. in situations where information is encrypted by Scramble!.

3: ENCRYPTION REGULATION

3.1 Introduction

3.1.1 Crypto regulation

At first, cryptography was used only by governments to keep confidential information secret. With respect to national security, governments wish to preserve information security on the one hand, while on the other hand they wish to be able to intercept such information of others. This tradeoff is clearly reflected in the legislation of most countries: legislators focused mainly on regulating the export of crypto systems – as they want to 'avoid strong cryptography from falling into the hands of foreign powers'[188] – while at the same time they are reluctant to enact import regulation on crypto mechanisms as these allow governments to, by cryptanalysis, reveal the state of art in foreign encryption technology.

Note that this tradeoff only related to the public sphere, while the use of cryptography in the private domain was (and in most countries still is) almost entirely disregarded in legislation. Nevertheless, with the excessive growth of the worldwide use of the internet an additional tradeoff, between national security and the private enforcement of the (fundamental) right to privacy and data protection, has come to the fore. In this regard one might expect an increasing need for domestic crypto regulation, more specifically, legislation regulating the private use of encryption mechanisms. But as said, such civil use of encryption is already widely accessible via web browsers and email servers and this ubiquity makes it impossible to enforce any national regulation, hence the lack of domestic crypto regulation still seems reasonably understandable.

One issue that is often regulated domestically is the use of encryption for criminal purposes. The most recent debate on encryption policy concerns the relation between such policy and the enforcement of criminal law, more specifically the extent to which citizens should be confronted with a decryption order in case of criminal suspicion. Note that in certain countries not complying with a decryption order is considered a criminal offence.[189] Another important issue in this debate is the relation between a decryption order and the privilege against self-incrimination. While in some countries – e.g. the UK, the Netherlands in case of terrorist activities, France and Belgium – such order is considered to be compatible with the privilege against self-incrimination, in others – e.g. the US, at least in certain circumstances – this compatibility is debatable. I will further address this specific topic in paragraph 3.2.3 for the EU, and 3.3.3 for the US.

[188] *Ibid*., p. 97.
[189] E.g. the UK and France, see par. 3.2.3.

3.1.2 Context and approach

In the next paragraphs, I will discuss the legal status of the private use of Scramble! in SNSs. I will presume the hypothetical situation where the encryption tool is downloadable from a EU-based website and discuss the legal context of this hypothesis from the position of EU and US encryption regulations. I will specifically look at EU domestic regulation in par. 3.2.1 and 3.2.3, thus assuming the crypto-tool will be downloaded and used by citizens in the EU Member States, and at US domestic regulation in par. 3.3, presuming the tool will be downloaded and used by US citizens. When the latter would occur, the encryption software could – although this is not as evident as it seems - be exported from the EU to the US, hence the relevant EU export regulations will also be examined (par. 3.2.2).

I will not assess relevant non-binding international regulations on encryption or the export thereof, such as the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* or the *OECD Crypto Guidelines*, as these regulations (or guidelines) are not directly applicable. As it is up to each member state to implement these into national legislation their effects depend on national implementation and the actual effect can differ from country to country.

With regard to the Wassenaar Arrangement - successor to the COCOM[190], signed in 1996 and now counting forty members[191] - it suffices to say that this is the most important piece of crypto-export regulation in the international field. It specifically controls the export of arms and 'dual-use goods'. Dual-use goods are goods, technologies or software that can be used for both military and civil purposes[192] and cryptographic systems fall under this category. The Wassenaar Arrangement has been implemented in the European Union's Commission Regulation (EC) 1334/2000, on which Regulation I will further elaborate in more detail in par 3.2.2.

With respect to the OECD Crypto Guidelines it suffices to say that these do not provide any effective direction for (international) crypto regulation and therefore its importance in the regulatory field is minor. As Koops (1999) states:

> 'The OECD 'guidelines' (…) do not guide. They leave it to every single state to strike a balance somewhere; virtually any balance, packed in proper rhetorics, will satisfy the OECD principles.' (p. 5)

[190] COCOM stands for Coordinating Committee for Multilateral Export Controls.
[191] The participating Member States are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and the United States. See www.wassenaar.org.
[192] Council Regulation (EC) No. 1334/2000, Article 2.

3.2 EU encryption regulation

In this paragraph I will look into the relevant encryption legislation of the European Union and the Council of Europe.

3.2.1 Domestic encryption regulation by the European Union: the Copyright Directive

Until now, I have looked at Scramble! as a means to protect privacy in SNS. However, the content that SNS users post on their profile is, at least in many cases, covered by intellectual property (hereafter: IP) rights; more specifically by copyright. Think, for example, of blog posts or self-made pictures or videos. With this in mind, encryption could function not only as a privacy enhancement mechanism, but also as a copyright protection mechanism. Following this line of reasoning, the *Copyright Directive 2001/29/EC* (hereafter: 'Copyright Directive') – implementing the *WIPO Performances and Phonograms Treaty* – would apply to encrypted IP-content in SNS since it regulates, *inter alia*, technological copyright-protection measures such as encryption. With this in mind, I will now assess what the legal status of Scramble! is in relation to the Copyright Directive, and we will see that this anti-circumvention law protects Scramble! as a copyright protection mechanism.

First of all, Article 6 of the Copyright Directive, placed in Chapter 3 which is entitled *'Protection of technological measures and rights-management information',* applies.

According to Article 6(1), Member States have to provide[193]:

> 'adequate legal protection against the circumvention of any *effective technological measures*, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.'[194] (emphasis added)

Article 6(3) defines 'technological measures' as:

> 'any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are *not authorised* by the rightholder of any copyright (…)' (emphasis added)

and continues by defining technological measures as 'effective' where:

[193] To note: although the implementation of this article can differ from country to county, it is required by this Directive that the Member States implement the rule in this article as a minimum. Cf. Recital 47 of the Copyright Directive.

[194] The ratio is behind this is 'to avoid fragmented legal approaches that could potentially hinder the functioning of the internal market, [creating] a need to provide for harmonised legal protection against circumvention of effective technological measures and against provision of devices and products or services to this effect.' Recital 47 of the Copyright Directive.

> 'the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.'

Strangely enough, it is not defined what 'circumvention' means.[195] This makes it harder to determine what a SNS provider can do with encrypted content. In my opinion, 'circumvention' includes at least that decryption or descrambling is not allowed (as encryption is specifically mentioned), but it does *not* include blocking the working of the technological measure. After all, blocking a technological IP protection mechanism does not mean that the IP content becomes accessible. Clearly, where the IP content, by means of the circumvention, *does* become accessible, the anti-circumvention regulation applies. In this regard it can be argued that, when a user would make use of Scramble! in a SNS, the SNS provider does not have a right to decrypt the encrypted content (by, for example, cryptanalysis) but blocking the crypto tool is by this regulation not prohibited, provided that this does not make the protected IP content accessible.

An SNS provider can bring about two arguments in denying the applicability of this anti-circumvention regulation. First, the provider can argue that a copyright protection mechanism that can be circumvented does not fall within the scope of Article 6 of the Copyright Directive as it does not *effectively* controls access to the work. This argument does, in my opinion, not hold. In my view, the definition of 'effective' shows that the effectiveness refers to the making inaccessible of the copyright protected work by the rightholder and not to whether or not another person is capable or circumventing the measure. Also, Scramble! provides for quite strong hybrid encryption and it is therefore unlikely that it is considered an ineffective copyright protection mechanism. Above that, it would be extremely cumbersome to unscramble all IP content, which makes the circumvention option for SNS providers unrealistic. The second argument would be more interesting to SNS providers. The provider could potentially argue that prior permission for - possible - decryption was given by the copyright holder by granting an IP license to the SNS provider. To take the example of Facebook, which Terms of Use read as follows:

> 'For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free,

[195] The US Digital Millennium Copyright Act, which we will look into in par. 3.3.2, does define 'circumvention'.

worldwide license to use any IP content that you post on or in connection with Facebook ("IP License")'.[196]

First of all, when reading this section from the Facebook Terms, it becomes clear that the IP-license relates to the content that is put on Facebook profiles, not to a device that is independent from Facebook (i.e. the Firefox extension Scramble!). Facebook cannot touch Scramble! in any way (and by that I mean blocking or circumventing it) by relying on the IP-license. If Facebook users would use Scramble! in Facebook, the latter would merely receive a bunch of unintelligible lines of characters.[197] The question that Facebook then would like to pose is: to what profile content does the license agreement relate? Is it the source data as entered by the user in their web browser (human readable text), or is it the content as stored on SNS provider's servers (scrambled text)? In the case of the former, Facebook could require its users, based on the IP license and Terms, to provide them unencrypted content and not doing so would constitute a breach of contract. In the latter case, which to my opinion applies, Facebook would have a license to use the scrambled content stored on their servers. 'Use', as mentioned in the IP-license, is defined in Facebook's Terms as *"use, copy, publicly perform or display, distribute, modify, translate, and create derivative works of (...)"*. With this broad definition, Facebook could argue that 'use' includes decrypting encrypted work; think of the words 'display' and 'modify' mentioned in the definition. However, Article 6 (1) of the Copyright Directive requires the Member States to assure 'adequate legal protection against the circumvention of any effective technological measures'. To my view, this legal protection does not only cover the means (i.e. the technological protection measure) but also the end (i.e. inaccessible intellectual property content). Hence, it is not only prohibited for Facebook to circumvent Scramble!, (e.g. by hacking or cracking the tool) but also to, by means of e.g. decryption, (try to) get access to the encrypted content Scramble! has produced. On a side note, Facebook will prefer to block Scramble! in total as trying to decrypt content is almost practically impossible and highly expensive. Blocking Scramble! is, as I argued earlier, not covered by EU anti-circumvention regulation, thus an SNS provider can do so without being hindered by this specific regulation.

3.2.2 Export encryption regulation by the European Union

The most important piece in EU legislation regulating the export of encryption products, is the *Council Regulation (EC) No 1334/2000 on setting up a Community regime for the control of exports of dual-use items and technology* (hereafter: the 'Council

[196] Facebook (2010d), section 2.1.
[197] See par. 1.2.2, figure 7.

Regulation' or 'Regulation').[198] The Regulation includes, *inter alia,* the Wassenaar Arrangement and is directly applicable to all EU Member States. The next section will address the question whether the Council Regulation is applicable to the situation where Scramble! is downloaded from the EU to either another EU Member State or to the US.

3.2.2.1 The applicability of Council Regulation (EC) No 1334/2000

Article 3 par. 1 of the Regulation, determining the scope of the Council Regulation, stipulates that '[a]n authorization shall be required for the export of the dual-use items listed in Annex I.' For the Council Regulation to apply, Scramble!, or the downloading thereof, should fall under this article. Hence, it must be assessed whether Scramble! is a dual-use item as listed in Annex I and whether downloading - or possibly uploading – Scramble! constitutes 'export' as defined in Article 2b of the Council Regulation:

> '(i) an export procedure within Article 161 of the Community Customs Code;
> (ii) a reexport within Article 182 of that Code, and
> (iii) transmission of software or technology by electronic media, fax or telephone to a destination outside the Community; this applies to oral transmission of technology by telephone only where the technology is contained in a document the relevant part of which is read out over the telephone, or is described over the telephone in such a way as to achieve substantially the same result'.

First of all, the definition shows that any interchange of the crypto-tool within the territory of the EU is not considered export under the Council Regulation as this definition is limited by the phrase: 'to a destination outside the Community'. Hence, the only case in which export restrictions might occur under this Regulation is when the encryption tool would be downloaded from the EU to a non-EU country, in our assessment to the US particularly. In this regard, the relevant section of Article 2b is section (iii) as it specifically refers to he 'transmission of software (…) by electronic media (…)', which should be interpreted as to include the downloading of software.[199] Presumably it also includes the uploading of Scramble! as this too involves the transmission of software, but only when it would be uploaded to a non-European website, as the definition of export is limited to 'a destination outside the Community'.

[198] When referring to this EC regulation the author refers to the consolidated version of 2nd February 2009.
[199] Cf. Lindqvist C-101/01, ECJ judgment of 6 November 2003. Here it was ruled by the ECJ that merely putting personal data on a website does not constitute a transfer of data to third countries. Although this case relates to personal data, and the context of the export of dual-use goods is clearly different, it shows that the mere making available of data on a website does not necessarily mean this constitutes "export" of this data.

Not only a textual interpretation of Article 2b leads to the conclusion that downloading and uploading Scramble! constitutes export under the Council Regulation, also a teleological interpretation is in support of this conclusion. The latter interpretation method is, in case of EC Regulations, commonly deployed by examining the Recitals. Recitals 1 and 8 are most relevant:

> '1. Dual-use items (including software and technology) should be subject to effective control when they are exported from the Community.'
> (…)
> 8. Transmission of software and technology by means of electronic media, fax or telephone to destinations outside the Community should also be controlled.
> (…).'

Recital 1 states the main purpose of the Council Regulation, namely the effective control on the export of dual-use goods, and it specifically mentions that the export of software is to be included in this control. Recital 8 reiterates this more specifically for the transmission of software. Hence, the downloading – and uploading – of Scramble! to countries outside the EU must also be, according to the purpose of this Council Regulation, subjected to effective control.

To conclude, the downloading of Scramble! to the US constitutes 'export' as defined in Article 2b of the Council Regulation, both on the ground of a textual as well as a teleological interpretation.

Next, I will assess whether Scramble! is a dual-use item as listed in Annex I of the Regulation. Our crypto-tool does fall under this Annex, more specifically under part 5A002.a.1.a and 5A002.a.1.b (to be read in conjunction with 5D002.c.1), since it uses hybrid encryption. Hybrid encryption entails that a combination of symmetric and asymmetric algorithms is used in one single crypto-mechanism.

3.2.2.2 Do export restrictions apply to the export of Scramble! according to Council Regulation (EC) No 1334/2000?

In the previous paragraph I have concluded that Scramble! is a dual-use item that falls under the Council Regulation and that the downloading of Scramble! to the US constitutes export. The remaining question is whether, according to the Regulation, export restrictions apply. If so, this would mean that a prior export authorization is required.[200]

[200] Export authorizations are to be handled by the national authorities, see Article 6 of the Council Regulation (EC) No 1334/2000.

There are some exceptions to the rule that an export authorization is required for the export of dual-use items that fall under Annex I and these are likely to apply to (the export of) our crypto-tool. First, the Council Regulation provides that its export controls do not apply to products 'accompanying their user for the user's personal use'.[201] What this phrase exactly means remains unclear from reading the Regulation, but an example that occurs in literature is an installed crypto program on a person's laptop that he or she moves out of EU territory.[202] With this example in mind one can conclude that the use of Scramble!, and the wider dissemination of (the use of) this tool, does not fall under this 'personal use' exception as the crypto tool does not *accompany* the user when it crosses the border.

Second, another exception in the Council Regulation can be found under paragraph 2 of the General Software Note under Annex I. It states that the export controls do not apply to software '[i]n the public domain'. 'In the public domain' is defined in the Regulation as:

> ''technology' or 'software' which has been made available without restrictions upon its further dissemination [whereby] copyright restrictions do not remove 'technology' or 'software' from being 'in the public domain''.

Since Scramble! is available for public use[203] and is based on Open Source software the tool seems very likely to fall under the 'public domain' exception. Consequentially, its export would not be restricted by the conditions of the Council Regulation.

3.2.3 Encryption regulation by the Council of Europe

The Council of Europe has only one piece of *domestic* regulation - no relevant export regulation could be found - that is relevant in the case where Scramble! would be used for the protection of one's privacy, namely the *Convention on Cybercrime*[204] of 2001. Similar to the Wassenaar Arrangement mentioned earlier, the Cybercrime Convention is not directly legally binding on citizens, but has to be implemented by its Member States into their national laws. Thus, its application depends on the level of implementation in national law. Therefore, I will only discuss it briefly.

Law enforcement agencies wishing to gather digital evidence face serious problems when coming across computer data that is inaccessible due to encryption. As Aljifri and Sánchez (2003) state:

---

[201] See Council Regulation (EC) No. 1334/2000, Annex I, Note 2 in the Dual-Use List Category 5, Part 2, "Information Security".
[202] See Koops (2008) and Taylor (1999).
[203] Scramble! can be downloaded from: http://www.primelife.eu/results/opensource/39-scramble.
[204] The Convention on Cybercrime was signed by the United States, Canada, South Africa, Japan, and 26 of 43 Member States of the Council of Europe.

'It is evident that cryptography poses an important obstacle for their interests, as any kind of information encrypted using a powerful enough cryptosystem would turn out to be practically unbreakable without the decryption key, thus rendering the electronic wiretapping or computer search useless.' (p. 197)

In the Convention, the Council tries to strike a balance between 'the interests of law enforcement and respect for fundamental human rights', including 'rights concerning the respect for privacy' and the 'the right to the protection of personal data'.[205] Paragraph 62 of the Convention's explanatory report shows how this balance is struck in relation to the use of encryption for the protection of privacy. In this paragraph a distinction is made between punishable acts committed 'without right' and acts committed 'with right'. It then states the following:

> ´The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should *in principle* be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right.´ (emphasis added)

The words ´in principle´ show that Member States have some discretion in determining the legitimacy of the use of encryption for privacy purposes.

Nevertheless, in acknowledging the necessity of decryption for law enforcement agencies, Article 18 of Section 2 of the Cybercrime Convention stipulates *inter alia* the following:

> 'Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a.) a person in its territory to submit *specified* computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium'. (emphasis added)

In addition, Paragraph 176 of the Convention's Explanatory Reports mentions that:

[205] Convention on Cybercrime 2001, Preamble. With regard to the right to privacy the Convention refers in its Preamble to 'the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties' and with regard to the right to data protection the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'.

'[p]arties *could* establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order. This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text"'. (emphasis added)

These citations show that the Convention allows Member States to order decryption. However, this possibility should, at least in democratic societies, in principle be subjected to the privilege against self-incrimination as acknowledged in Article 6 of the European Convention on Human Rights (ECHR) as Article 15 of the Cybercrime Convention states that:

the establishment, implementation and application of the powers and procedures provided for in [Section 2] are subject to conditions and safeguard provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties'.

It must be kept in mind that the Cybercrime Convention is not directly binding in the Member States. Regarding the relation between a decryption order and the privilege against self-incrimination it must be said that some Member States do allow for such orders without deeming them to violate of Article 6 of the ECHR. As said, in the UK, the Netherlands in case of terrorist activity, France and Belgium a decryption order is compatible with the privilege against self-incrimination. Where it is not, this privilege can be "bypassed" by permitting law enforcement authorities to order decryption to anyone else who has the ability to decrypt the cyphertext - the suspect excluded. This means that, in the context of SNS, online friends who have access to the plain text can be ordered by an enforcement agency to provide the decrypted text. Even more disturbing is the fact that, in some countries – for instance in the UK[206] and France[207] - not adhering to such an order is penalized with two and three years respectively, or the suspect can get a higher sanction.

3.2.4 Conclusion EU encryption regulation

In par. 3.2 I discuss the legal status of Scramble! in relation to EU encryption regulation. In assessing EU domestic crypto regulation, I viewed Scramble! not longer as a privacy protection mechanism, but as a copyright protection mechanism instead. In this regard, the Copyright Directive applies, and as a consequence Scramble! is protected by this ant-circumvention law. This means that Facebook is not allowed to circumvent the tool in

[206] See Regulation of Investigatory Powers Act 2000 (2000 Section 23), Part III, Article 53 (1) and (5).
[207] See Law 2001-1062 of 15 November 2001 on daily security, Article 31(II).

order to be able to access the encrypted copyright protected materials. Does Facebook then have a right, based on the contract between Facebook and its users, to get access to the human readable text? My conclusion to this question is: no, in my view the Copyright Directive aims to protect the copyrighted material and prevent unauthorized access to it, in stead of the technological protection measure as such. Hence, Facebook, or anyone else, is neither allowed to circumvent Scramble!, nor to, by e.g. decrypting the encrypted content Scramble! has produced. Noteworthy, where Facebook, or another SNS, would block the crypto tool on its service the SNS would not violate the Copyright Directive, provided that blocking the technological protection measure does not make the protected IP content accessible.

In assessing EU export regulation, I looked into Council Regulation (EC) No 1334/2000 and concluded that, after confirming its applicability to Scramble!, the public domain exception applies. For that reason the export of Scramble! would not be subject to the export requirements stated in the Regulation. Additionally, the Regulation does not prohibit the use of Scramble! either.

Finally, I shortly discussed the Council of Europe's Cybercrime Convention. It appeared that, although encryption is not prohibited by the Convention, those using encryption (i.e. the suspect), or those that can access the plain text, can be confronted with a decryption order in Member States that have adopted laws allowing such orders, such as France and the UK..

3.3 US domestic encryption regulation

3.3.1 Introduction

In this paragraph I will examine the relevant domestic US encryption regulation, more specifically US statutory law, thus assuming that a US citizen has downloaded the Scramble! from a EU-based website. With regard to US crypto regulation is should be noted that the US have no import restrictions regarding encryption, thus the actual transmit into the US shall not involve any legal obstacle. There is however some, though very little, domestic crypto regulation. In the late 1990's a variety of Bills were introduced on (domestic) crypto-regulation; these Bills mainly sought to penalize the use of encryption to conceal information related to criminal offenses[208], yet at the same time aimed at relaxing the existing export controls for cryptosystems or software generally available in the international market.[209]

[208] E.g. the E-PRIVACY Act (1998); the Security And Freedom through Encryption Act (SAFE) (1996/1997/1999); the Encryption for the National Interest Act (1999).
[209] E.g. the E-PRIVACY Act (1998); the Security And Freedom through Encryption Act (SAFE) (1999); the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act (1999); the

Some proposals even specifically addressed the enhancement of, or even a right to the protection of privacy by means of encryption.[210] Eventually, none of these Bills were passed and as a result the current amount of domestic encryption regulation, to be viewed next, is limited.

3.3.2 Encryption and the Digital Millennium Copyright Act

In the US, the *WIPO Performances and Phonograms Treaty* is implemented in the *Digital Millennium Copyright Act* (hereafter: 'DMCA').[211] Similar as in the EU Copyright Directive, it prohibits, in § 1201 of the DMCA (17 U.S.C), the circumvention of copyright protection systems. The ratio behind this is to 'prevent unauthorized access to copyrighted works' and to prevent 'the theft of copyrighted works'.[212] Different from the EU Copyright Directive, the DMCA defines the 'circumvention of a technological measure' in § 1201(a)(3)(A) as a whole:

> 'to 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, *without the authority of the copyright owner* (…)'. (emphasis added)

Other than with regard to the EU Copyright Directive, the definition here does include blocking the technological protection measure, thereby making this a prohibited act too.

Facebook has two arguments in denying the applicability of § 1201 of the DMCA. The first argument has already been explained in relation to the EU Copyright Directive and although the DMCA does not provide for a separate definition of 'effective', it results in the same answer: Scramble! provides for strong protection and is difficult to circumvent, thereby likely to be considered effective. Hence, trying to circumvent Scramble! is prohibited under the DMCA. The second argument, whereby Facebook would argue that prior permission for decryption was given by the rightholder through the grant of an IP license to Facebook, should be explained somewhat differently from a DMCA perspective. § 1201(a)(3)(A) DMCA specifically mentions 'without the authority of the copyright owner' referring to the circumvention of the copyright protection measure itself. This means that Facebook should

---

Encrypted Communications Privacy Act (Leahy Bill) (1996/1997); the Encryption for the National Interest Act (1999).

[210] E.g. the E-PRIVACY Act (1998); the Security And Freedom through Encryption Act (SAFE) (1996/1997/1999); the Encrypted Communications Privacy Act (Leahy Bill) (1996/1997); the Electronic Rights for the 21st Century Act (1999); the Encryption for the National Interest Act (1999).

[211] Enacted by US Congress in 1998.

[212] U.S. Copyright Office (2000).

get *specific* authorization of the rightholder relating to the circumvention of the user's technological copyright protection measures. Such authorization does not lie within the agreement Facebook users conclude with Facebook, as this agreement covers the *content* users post on their profile, and the agreement is in no way related to the Firefox extension Scramble!.

3.3.3 Encryption and US criminal law: a decryption order?

3.3.3.1 US Code

In this paragraph I will address the question whether SNS users in the US can be confronted with a decryption order.[213] I will look at two specific Sections of the US Code (U.S.C.), which determine the extent to which law enforcement agencies can intercept and disclose electronic communications, or order such disclosure from individuals and social network sites, in our case, Facebook. First, I will discuss Title 18, Section 119 which is entitled: *'Wire and Electronic Communications Interception and Interception of Oral Communications'*. Next, we will address the Electronic Communications Privacy Act of 1986 as integrated in the U.S.C., Title 18, Section 121, which is entitled: '*Stored Wire and Electronic Communications and Transactional Records Access'*. The aim is to make clear the extent to which users and Facebook, as a 'remote computing service'[214], can be confronted with an order to deliver decrypted communications or other data in decrypted form for purposes of criminal investigation.

§§ 2516(2) and 2516(3) 18 U.S.C. state that the interception of electronic communications is allowed "by investigative or law enforcement officers" in case of certain criminal offences, for instance in case of a felony. Next, § 2517 clarifies to whom these intercepted communications can be disclosed, which implies that the communication should be disclosed in the form as it is intercepted. This means that encrypted communication should be disclosed in encrypted form and no decryption order can follow from this paragraph. Moreover, § 2517(4) explicitly states that: "No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this section shall lose its privileged character." From this article it appears that encrypted data will not lose their privilege when such data would be intercepted by a law enforcement agency.

The Electronic Communications Privacy Act states inter alia in § 2703 that under certain conditions *"a governmental entity may require the disclosure by a provider of*

[213] I have addressed this question in relation to EU law in par. 3.2.3.

[214] See US Code, Title 18, Section 121, § 2711. (2): 'the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system'.

electronic communication service" or *"a provider of remote computing service"* of the *"contents of a wire or electronic communication"*. 'Electronic communication' is defined in § 2501 of 18 U.S.C. – which definitions also apply to Section 121 – as: *"any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce (…)"*. Again, the article does not seem to imply an obligation on the part of Facebook to disclose the data it has stored in decrypted form as this would require an extra act from Facebook, namely to use cryptanalysis for cracking the key and decrypting the content. Above that, a decryption order for Facebook would lead to serious practical problems since Scramble! provides for quite strong protection, and the feasibility any decryption order, therefore, is questionable in this regard.

However, the Communications Assistance for Law Enforcement Act ("CALEA")[215] specifically mentions encryption in 47 U.S.C. § 1002(b)(3) as it states that:

> *'[a] telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.'*

Important to notice here is that "Information services" [216], such as Facebook, are excluded from this Act and this given, in combination with the fact that, as said earlier, (state) courts can create laws wherever statutory law leaves a gap , is very interesting. The CALEA neither specifically addresses information services, nor is it mentioned somewhere else in the U.S. Code that information services are not responsible for decrypting communication. Hence, this gap might be filled up by the rulings of state courts by which a rule could be created that does hold information services responsible for delivering decrypted content. Keep in mind that such a rule could only be made if this rule would not be unconstitutional; so the question that then arises is whether such rule would be. As our scope is limited, it goes too far to make this assessment, but in brief it can be noted that Facebook could possibly rely on the First Amendment (freedom of speech) to claim a decryption order unconstitutional as the US

[215] 47 U.S.C. §§ 1001-1010 (2006).
[216] "Information services" are defined in 47 U.S.C. § 1001(6) as "(A) (…) the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and (B) includes— (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services(…)".

have a wide definition of speech (this can be any expression); companies are allowed to have free speech claims regarding the use and transfer of personal data.[217]

3.3.3.2 *Caselaw: A decryption order and the privilege against self-incrimination*

Whereas Facebook would be the third party in getting information on criminal acts, Facebook-using suspects can be confronted with a decryption order – though we saw that 18 U.S.C. § 2517(4) provides that encrypted data does not lose its privilege – as appears from an interesting federal case regarding decryption and the privilege against self-incrimination (Fifth Amendment). Though there is no US statutory right for law enforcement agencies to compel decryption, the agencies can nevertheless be creative in trying to get decrypted testimonial information and court cases in this regard are dealt with in relation to the Fifth Amendment. In United States v. Boucher – 2007 WL 4246473, also referred to as Boucher I (D. Vermont, Nov. 29, 2009) the defendant, Boucher, was arrested for bringing child pornography from Canada into the United States by carrying a laptop that contained child pornography. At the time of the border search, the drive containing the child pornography files was accessible without the use of a password. Boucher had helped the border patrol officers in finding and accessing the relevant drives but the agents never saw him entering a password. Later, when the laptop – after shutting it down - was handed over to a law enforcement for further investigation, the same drive search appeared to be inaccessible due to the use of PGP – a form of encryption – and a password was required to access the drive.

Again, regardless of the absence of a statutory right to compel decryption, the grand jury ordered Boucher to *"provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with"* the seized laptop, thereby trying to stretch police power.[218] Boucher labelled the subpoena as a violation of the privilege against self-incrimination as stated in the Fifth Amendment. Afterwards, the government agreed that providing the decrypted content – and thus not the password itself – was sufficient in adhering to the subpoena. The question that the Court then had to answer was *"whether compelling Boucher to enter the password into the laptop would violate his Fifth Amendment privilege against self-incrimination."*

The District Court of Vermont argued that *"[c]ompelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself"* and the Court decided to quash the subpoena, basically because *"the act of being compelled to turn*

[217] Solove (2006b), p. 673-680. Cf. Virginia State bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748 (1976); Central Hudson Gas & Electric Corp. v. Public Service Comm'n of New York, 447 U.S. 557 (1980); Rowan v. United States Post Office Department, 397 U.S. 728 (1970); Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F.3d 1228 (10th Cir. 2004).
[218] Cf. Ungberg (2009).

over an encryption password has testimonial aspects."[219] To clarify, for the Fifth amendment privilege to be invoked three requirements must be fulfilled, namely that the communication must be compelled, testimonial and incriminating in nature.[220]

The United States appealed and in Boucher II – re Boucher, 2009 WL 424718 (D. Vermont, Feb. 19, 2009) – the Court reversed the ruling in Boucher I, directing Boucher to *"provide an unencrypted version of the Z drive viewed by the ICE [Immigration and Customs Enforcement] agent"*. The Court quoted United States v. Fox – 721 F.2d 32, 36 (2d Cir.1983) and stated that: *"[t]he act of producing documents in response to a subpoena may communicate incriminating facts 'in two situations: (1) 'if the existence and location of the subpoenaed papers are unknown to the government'; or (2) where production would 'implicitly authenticate' the documents'."* The District Court noted further that the government must only show *"with reasonable particularity that it knows of the existence and location of subpoenaed documents."* Because border patrol agents had viewed at least one image of child pornography on the hard drive in question as Boucher had provided access to the laptop voluntarily, the court concluded that Boucher did not have Fifth Amendment protection.

The question that remains in the context of social network sites is whether law enforcement agencies can order decryption or the production of a crypto-key or password where the government does not know of - the existence of - the contents. According to caselaw, first, it would have to be tested whether the Fifth Amendment privilege could be invoked which *"applies only when the accused is compelled to make a* testimonial *communication that is incriminating"*.[221] This same test was applied in Boucher I where it was argued that the compelled production of the encryption password is testimonial. In doing so, the District Court referred to both United States v. Doe – 465 U.S. 605, 612 (1984) (Doe I)[222], where it was ruled that *"The act of producing even unprivileged evidence can have communicative aspects itself and may be "testimonial" and entitled to Fifth Amendment protection."* and to Doe v. United States – 487 U.S. 201, 209(1988) (Doe II) where the US Supreme Court ruled that "*An act is testimonial when the act entails implicit statements of fact, such as admitting that evidence exists, is authentic, or is within a suspect's control."* Additionally, also mentioned was United States v. Hubbell - 530 U.S. 27, 43 (2000), an important case for answering the aforementioned question. In this case, Hubbell, suspected of tax fraud, had been subpoenaed to provide *"any and all documents reflecting, referring, or*

[219] Palfreyman (2009).
[220] Fisher v. United States, 425 U.S. 391, 408 (1976).
[221] Fisher v. United States, 425 U.S. 391, 408 (1976).
[222] Cf. *United States v. Hubbell*, 530 U.S. 27, 36 (2000): *"'The act of production' itself may implicitly communicate 'statements of fact.' By 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.'"*

relating to any direct or indirect sources of money or other things of value received by or provided to" an individual or members of his family during a 3-year period (…)".[223] As appears from the text of the subpoena - like in the case of Boucher - the prosecutor *"needed respondent's assistance both to identify potential sources of information and to produce those sources."*[224] Hubbell did produce the requested documents after being granted immunity (18 U.S.C., § 6002), meaning that the evidence he produces cannot be used against him in criminal prosecution. However at trial, use, or derivative use, was made of the subpoenaed evidence against Hubbell and he invoked the Fifth Amendment privilege. It was ruled that, as the government 'has shown no prior knowledge of either the existence or the whereabouts of the documents ultimately produced here" i.e., it "(…) could not demonstrate *with reasonable particularity* a prior awareness that the documents sought existed and were in respondent's possession(…)', Hubbell is protected by the Fifth Amendment. (emphasis added).[225]

The conclusion is that, after having viewed the aforementioned cases, a social network site user confronted with an order to provide decrypted content or to provide access to that content can claim Fifth Amendment protection where the government cannot demonstrate with reasonable particularity to know the existence of the testimonial documents. If the government can demonstrate such awareness, the suspect is protected from compelled decryption under the Fifth Amendment only when he has not assisted the government in showing the testimonial content.

3.3.4 Conclusion US domestic encryption regulation

In par. 3.3, I examined only US domestic encryption regulation, as I have limited the scope of this thesis to the situation where Scramble! would be exported from a EU country to either another EU country or to the US. Similarly as with EU domestic encryption regulation, I considered Scramble! to be a copyright protection mechanism which makes the DMCA applicable. This anti-circumvention law also prohibits the circumvention of Scramble! Other than the Copyright Directive, the DMCA (and its definitions) are more directed towards the protection of the copyright protection mechanism as such. The definition of 'circumvention of a technological measure' within the DMCA includes only unauthorized circumventions as to constitute a circumvention of a technological measure. In this regard, I argued that the contract between Facebook and its users does not include an authorization for the circumvention of Scramble!, as this contract (i.e. the IP license in the contract) only covers

[223] United States v. Hubbell, 530 U.S. 27, 41 (2000).
[224] *Ibid., 28.*
[225] *Ibid.*

content posted by Facebook users on their Facebook profile and not the external Scramble! mechanism. Hence, Facebook is not allowed to impair the proper working of Scramble! where Scramble! protects copyright covered material.

Next, I assessed the legal status of the use of Scramble! in relation to US criminal law and posed the question whether SNS users using Scramble!, or Facebook as a 'remote computing service', can be confronted with an order to deliver decrypted communications or other data in decrypted form for purposes of criminal investigation. After examining the US Code, Title 18, Section 119 and Section 121, I concluded that both SNS users using Scramble!, as well as SNS providers, cannot be obliged to provide encrypted data in decrypted form. However, recent caselaw shows that where a criminal suspect (initially) cooperates in providing access to encrypted data, that suspect is obliged to adhere to a decryption order if the government can show '"with reasonable particularity that it knows of the existence and location of subpoenaed documents."[226] Hence, those using Scramble! should consider that, under these circumstances, they might be confronted with an order to decrypt in case of criminal suspicion. In addition, I asked the question whether a decryption order is possible where government agencies do *not* know of (the existence of) the contents, which I answered with no, as criminal suspects can claim protection under the Fifth Amendment in those cases.

[226] In re Boucher, 2009 WL 424718 (D. Vermont, Feb. 19, 2009).

4: THE CRYPTO TOOL: A VIOLATION OF THE FACEBOOK TERMS AND PRIVACY POLICY?

4.1 Introduction

Now I have assessed the use of Scramble! in either the EU or the US in respect of the relevant privacy- and crypto-regulations, I have come to assess the contractual relationship between Facebook and its user. In this regard, I will question whether any obstacles exist in light of this specific relationship when a Facebook user would use Scramble! in this SNS. The contract between Facebook and its users includes both the Facebook Terms and Privacy Policies. A contract generally comes to exist where an offer (in this case made by Facebook) is accepted (in this case by the users).[227] In this chapter, I will not question whether the acceptance of the offer by Facebook users is legally challengeable[228], but I will consider the Terms and Privacy Policy to be legally binding. What I mean by 'obstacles' is grounds on which Facebook, based on the contract with its users, is able to legally challenge the use of Scramble! in Facebook by its users. I will only distill these ground by looking at the specific clauses in the Terms and Privacy Policy; I will not assess whether a claim by Facebook would potentially be successful in a US court based on US contract or tort law. Beforehand, I want to note that Scramble! is, from a contractual point of view, legally allowed to be used by Facebook users when, by this use, they do not violate any of the legally binding Facebook Terms and Privacy Policy. Where these Terms and Policies do not explicitly (or implicitly) prohibit the use of an external PET, such use is allowed, meaning that Facebook cannot force Facebook users, by legal means, to stop the use of Scramble!.

The Facebook Terms will be discussed in par. 4.2 and Facebook's Privacy Policy in par. 4.3. Finally, in par. 4.4 I will provide a joint conclusion on these two analyses. Before I go into the analysis, I will first explain what the context of the relationship between Facebook and its users is and how profile content is of vital importance to SNSs.

As said earlier, SNS users nowadays provide content via their SNS profile on a massive scale. The scope of our paper is limited, so I will not go into the discussion on why these users act like they do in this Web 2.0 environment. What is important to know here is that the economic value of SNS depends for a large part on this profile content[229] as the SNS providers collect this data for marketing purposes. SNS users share all sorts of personal

[227] Facebook places the statement 'By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy' on its website (the offer), which Facebook users have to click (acceptance) to be able to create a Facebook account. See Facebook (2010a).
[228] Cf. par. 2.1.3 and 2.1.4.3.
[229] For the other part it depends on the amount of money they make with selling advertising space on their SNS, and the number of Facebook members is what determines the value of this advertising space here.

information on their profile such as their hometown, religion and political view, personal interests - e.g., favorite movies, music, activities, books, TV shows, etc. - and information related to work and education. Based on this information, individual and group profiles of users are made, which makes targeted advertising easy.[230] For example, knowing the location of the user makes it possible to recommend local restaurants. Another fact that shows the importance of content to Facebook in particular, is the previously mentioned IP license Facebook imposes in its Terms.[231]

On the one hand, disabling the possibility for Facebook to view and access profile content would dramatically decrease its economic value. In this regard, it seems likely that social network sites, such as Facebook, would strongly oppose the use of Scramble! within their domain since it shields the content that users place on their profile pages from the provider's and third parties' access. On the other hand, SNS users become more and more aware of the importance of privacy protection due to Facebook's notorious privacy failures in the past.[232] These aggravations could cause Facebook users to massively flee the system and join another SNS. Therefore, Facebook must show its users, to the greatest extent possible, that their personal data are protected. Furthermore, where SNS users are data controllers, they have to comply with EU data protection laws, and I argued earlier that Scramble! can facilitate SNS users' compliance with these rules.

4.2 An assessment of the Facebook terms

In Section 1 of its Terms, Facebook claims that their users' privacy is important to Facebook and continues in Section 2 stating: 'You own all of the content and information you post on Facebook, and you *can* control how it is shared through your privacy and application settings.' (emphasis added) It appears that Facebook wishes to offer their users means to protect their online privacy (i.e. the privacy and application settings) but the word 'can' leaves, to my view, the possibility of the use of other means of privacy protection open. As such, this clause does not form an obstacle to the use of Scramble! in Facebook. Section 2 additionally states that the user grants Facebook an IP-license on all content covered by intellectual property rights posted on the SNS. The license agreement reads as follows:

[230] paragraph 2.2.2.1.
[230] See extensively the Electronic Information Privacy Center, *Privacy and Consumer Profiling*. [Online] Available from: http://epic.org/privacy/profiling [Accessed 1st June 2010], and Edwards & Hatcher (2009).
[231] Facebook (2010d).
[232] Think of the Beacon issue and the recently changed Facebook privacy settings, causing over 60 % of all Facebook profiles to be visible without explicit consent of the users (the default setting was put on 'everyone' instead of 'friends'), to name just an example.

1. ‘For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.’

The use of an encryption tool, such as Scramble!, would seriously dilute the meaning and scope of the IP-license granted by the Facebook user over its profile content. When Facebook users would use Scramble! in Facebook, the latter would get an IP license to the scrambled content (to the extent that this content is covered by intellectual property rights), which obviously is of no use. Nonetheless, I conclude that the IP-license as such, does not prohibit the use of Scramble!.

The use of Scramble! violates in no way Section 3 of the Terms.[233] A Facebook user using Scramble! could, however, be alleged of violating Section 4(5) which required users to ‘keep (…) contact information accurate and up-to-date’. When Facebook users would encrypt such contact information it would render the information inaccessible and invisible to Facebook, thus inaccurate or not up-to-date as Facebook intends it to be. Additionally, Section 4(1) states that Facebook users must ‘provide their real names and information’ and, arguably, encrypting such data could be seen as a violation of this section.

An interesting issue with respect to using Scramble! in Facebook is related to Section 5(2) of the Facebook Terms: ‘We can remove any content or information you post on Facebook if we believe that it violates this Statement.’ Facebook cannot see the actual content of the data encrypted by Scramble! as what remains after the data has gone through the encryption algorithms is cipher text. Nevertheless, the scrambled data is stored on the Facebook servers and could easily be detected. If Facebook would feel, for any reason, that

[233] Facebook (2010d), Section 3: ‘**Safety:** We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that, which includes the following commitments: 1. You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook. 2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission. 3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook. 4. You will not upload viruses or other malicious code. 5. You will not solicit login information or access an account belonging to someone else. 6. You will not bully, intimidate, or harass any user. 7. You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence. 8. You will not develop or operate a third-party application containing alcohol-related or other mature content (including advertisements) without appropriate age-based restrictions. 9. You will not offer any contest, giveaway, or sweepstakes ("promotion") on Facebook without our prior written consent. If we consent, you take full responsibility for the promotion, and will follow our Promotions Guidelines and all applicable laws. 10. You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory. 11. You will not do anything that could disable, overburden, or impair the proper working of Facebook, such as a denial of service attack. 12. You will not facilitate or encourage any violations of this Statement.’

posting encrypted content is in violation of their Terms - e.g. because they have no ability to monitor such encrypted data - it could remove this content.

The argument that I posed earlier, saying that Scramble! does not only protect the users' privacy but at the same time can serve as an IPR protection mechanism, might, could Facebook argue, be countered by the Section 5(3) of Facebook's Terms: 'We will provide you with tools to help you protect your intellectual property rights.' However, the section does not express that the Facebook tools are exhaustive. Hence, in my view Facebook users can make use of other tools for protecting their intellectual property rights as well.

An interesting paragraph in the Facebook Terms is Section 14: 'If you violate the letter or spirit of this Statement, or otherwise create possible legal exposure for us, we can stop providing all or part of Facebook to you.(…)' Essentially, Facebook can deny its service to its users for any reason it deems necessary as the phrasing 'spirit of this Statement' can be interpreted in any way. Hence, when Facebook were to consider the use of Scramble! inappropriate for its own business model or service deployment, it would likely block those users using Scramble!.

I conclude that Facebook could potentially oppose the use of Scramble! by invoking its Terms only by relying on Section 4(1) and 4 (5). Such claims could, however, easily be avoided by Facebook users by not encrypting their name and contact information.

4.3 An assessment of Facebook's Privacy Policy

A number of sections in Facebook's Privacy Policy (hereafter: the Policy) are relevant for a discussion about the use of Scramble! in Facebook.[234] First of all, in the introduction Facebook claims[235] to adhere to both the US TRUSTe Program[236] and Safe

[234] The Privacy Policy states that it covers all of Facebook, but that it 'does not, however, apply to entities that Facebook does not own or control, such as applications and websites using Platform. ' Additionally, Facebook states that '[b]y using or accessing Facebook, you agree to our privacy practices outlined here [i.e. Facebook (2010c)]. See Facebook (2010c).

[235] I will not check whether every TRUSTe or Safe Harbor principle is incorporated in Facebook's Policy. This check is normally done by TRUSTe and the U.S. Department of Commerce (for the Safe Harbor program). However, it should be kept in mind that where Facebook does not live up to the principles of either one of these programs, these principles are nevertheless included in the contract between Facebook and its users, even where the principle(s) was or were not incorporated in Facebook's Policy.

[236] See http://www.truste.com/ [Accessed 28th June 2010]: 'TRUSTe helps thousands of businesses promote online safety and trust, and guides consumers to sites that protect their online privacy. TRUSTe helps both consumers click with confidence and online companies promote their Web site privacy policies online.' For Facebook's TRUSTe certificate see:
http://clicktoverify.truste.com/pvr.php?page=validate&url=www.facebook.com&sealid=102 [Accessed 28th June 2010]. For the TRUSTe Privacy Program requirements see
http://www.truste.com/privacy_seals_and_services/consumer_privacy/privacy-programs-requirements.html [Accessed 28th June 2010].

Harbor.[237] The Policy then continues by addressing the following subjects, each in a separate section:

'2. Information We Receive
3. Sharing information on Facebook[238]
4. Information You Share With Third Parties[239]
5. How We Use Your Information
6. How We Share Information
7. How You Can Change or Remove Information
8. How We Protect Information'[240] (footnotes added)

Section 2 clarifies that Facebook receives information about its users from a number or sources: from the users themselves[241]; from the interaction of the users with Facebook[242]; from third parties[243] and from other users[244]. Clearly, the use of Scramble! will not affect all these ways of data collection by Facebook, as the tool is only able to encrypt text which users enter into their (Facebook) profile, such as name, interests, political views, blogs, notes, status updates, wall posts and comments.[245] Where the tool can be used, Facebook is no longer able to collect that data. However, Section 2 does not contain any statement that prohibits the use of Scramble!, except where a user would encrypt his name or email

[237] See par. 2.1.4.2.3.
[238] Section 3, on explains 'how [the] privacy settings work, and how (…) information is shared on Facebook' and is not of relevance for the use of Scramble!. In any case, it can be said that this Section does not prohibit the use of Scramble!.
[239] This section explains how Facebook users share information with third parties and is not of relevance for the use of Scramble! in Facebook. Again, this Section does not prohibit the use of Scramble!.
[240] Facebook (2010c).
[241] This includes, inter alia, information users provide on their profile (e.g. name, gender, email address, interest) or other profile content (e.g. status updates, wallposts or pictures) and transactional information regarding transactions or payments made on Facebook. Facebook (2010c).
[242] This includes 'site activity information' (such as adding connections, creating a photo album, sending a gift, poking another user, where users indicate they "like" a post, are attending an event, or the fact that certain content is shared); 'Access Device and Browser Information' ('When you access Facebook from a computer, mobile phone, or other device, we may collect information from that device about your browser type, location, and IP address, as well as the pages you visit.') and cookie information. Facebook (2010c).
[243] Facebook receives information from Facebook Platform (Facebook (2009a)) and other websites. To clarify, with regard to 'information from other websites' the Policy states: 'We may institute programs with advertising partners and other websites in which they share information with us: [1] We may ask advertisers to tell us how our users responded to the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as "conversion tracking," helps us measure our advertising effectiveness and improve the quality of the advertisements you see. [2] We may receive information about whether or not you've seen or interacted with certain ads on other sites in order to measure the effectiveness of those ads.'
[244] 'We may collect information about you from other Facebook users, such as when a friend tags you in a photo, video, or place, provides friend details, or indicates a relationship with you.' Facebook (2010c).
[245] Additionally, information that has to be selected (not entered) by the users, e.g. gender and date of birth, cannot be encrypted.

address[246]: 'When you sign up for Facebook you provide us with your name, email, gender, and birth date.'[247] Thus, where Facebook users encrypt their name or email address, they violate both Facebook's Privacy Policy and Terms.[248]

Next, Section 5 contains some clauses that are interesting to discuss in relation to the use of Scramble! in Facebook. First of all, Facebook indicates that it uses the collected data to 'manage the service', which includes the monitoring of that data 'to prevent potentially illegal activities, and to enforce our Statement of Rights and Responsibilities.' The use of Scramble! would make such monitoring more difficult, but the clause as such does not prohibit the use of Scramble! Facebook also states that it uses user information for purposes of personalized advertising. Advertisers are able to choose 'the characteristics of users who will see their advertisements', such as a certain interest (e.g. soccer) or a specific age group, 'to select the appropriate audience for those advertisements'.[249] To the extent that such data would be encrypted, it would be more difficult for Facebook to provide this service to advertisers, but again the statement as such does not prohibit the use of Scramble! by Facebook users. Such use would be inconvenient, but, in my view, Facebook could not base a legal claim (i.e. on the basis of contract law for a breach of contract) on this specific Section. Possibly, if many Facebook users would start using Scramble! and encrypt much of their information about their interests (on which much personal advertising is based), Facebook would no longer be able to optimally provide such services to advertisers and for that reason block (users using) Scramble!.[250]

Section 6 includes the following clause that is interesting to mention for our assessment: 'We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law.'[251] Facebook can only provide this information when it is able to. In case the information is encrypted, Facebook is not able to adhere to the request, but this is not relevant with regard to the contractual relation between Facebook and its users. Users do not breach the contract with Facebook by not allowing Facebook to access profile

[246] See note 248.
[247] Facebook (2010c).
[248] See par. 4.2 and Sections 4(1) and (5) of the Terms, Facebook (2010d).
[249] See also Facebook (2010c) Section 6: 'Sometimes we share aggregated information with third parties to help improve or promote our service.'
[250] See Facebook (2010d) Section 14: 'If you violate the letter or spirit of this Statement, or otherwise create possible legal exposure for us, we can stop providing all or part of Facebook to you.(…)'.
[251] The clause continues: 'This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.' Facebook (2010c).

information for the purpose of adhering to such requests. I have already discussed whether a decryption order in the US, by law enforcement agencies for purposes of criminal investigations, is possible.[252]

A clause in Section 7 that might be of relevance for the use of Scramble! in Facebook, reads as follows: 'You may change or remove your profile information at any time by going to your profile page and clicking "Edit My Profile."' Facebook could ague that the way its users can edit their profile information is limited by the "Edit My Profile" options. However, in my opinion, the clause should not be interpreted as exhaustively, meaning that these options are the only option Facebook users can use to change their information.

The most interesting section in relation to the discussion about the use of Scramble! in Facebook is Section 8, which entails a number of clauses on security on Facebook. The introduction of this section reads as follows: 'We do our best to keep your information secure, but we need your help.' I argue that, indeed, Scramble! can help in keeping information secure. Next, regarding the steps taken by Facebook to keep information secure, Section 8 states that Facebook uses 'automated and social measures to enhance security, such as analyzing account behavior for fraudulent or otherwise anomalous behavior (…)'. Where content is encrypted by Scramble!, Facebook is no longer able to monitor that content for security purposes. As Facebook will wish to preserve the security of its service, and as disabling Facebook to monitor content provided via its service by means of encryption would likely violate Facebook's Terms[253], Facebook may, limit [the] use of site features in response to possible signs of abuse (…) and may suspend or disable accounts for violations of our Statement of Rights and Responsibilities.' Another interesting clause in Section 8 in relation to the use of Scramble! in Facebook is provided under the header 'Risks inherent in sharing information':

> 'Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices *such as* choosing a strong password, using different passwords for different services, and using up to date antivirus software.' (emphasis added)

[252] See par. 3.3.3.
[253] Think of Facebook (2010d), Section 3 (11): 'You will not do anything that could disable, overburden, or impair the proper working of Facebook' or Section 3: 'We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to do that (…).'

In my view this clause, in fact, states that Facebook users are *themselves*, for the large part, responsible for their own security on Facebook. Facebook alerts theirs users that it cannot guarantee absolute (information) security and that the users, therefore, must take their own steps to secure their (information) safety on Facebook. Using Scramble! would greatly contribute to such (information) security and such use is therefore, in my view, completely in line with this particular statement in the Privacy Policy. Additionally, Facebook mentions a few examples in Section 8 of how users can increase their security on Facebook, but it does not explicitly or implicitly exclude other possibilities of enhancing online security. Therefore, I argue that this particular section of Facebook's Privacy Policy encourages the use of (information) security enhancing mechanisms, such as Scramble!.

4.4 Conclusion on the assessment of the Facebook Terms and Privacy Policy

In chapter 4 I discussed the legal status of the use of Scramble! in Facebook according to the contractual relation between Facebook and its users. We saw that most of the Sections included in Facebook's Terms do not, as such prohibit the use of an external encryption tool such as Scramble!. Additionally, I argued that only where Facebook users encrypt their name and contact information, they might be alleged of violating the Facebook Terms.

With regard to the Privacy Policy I came to the same conclusion: where name and email address are encrypted users violate the Privacy Policy. Facebook could also potentially claim a violation of its Privacy Policy where it feels that the use of Scramble! in Facebook hampers their ability to monitor the website for security purposes. However, I argue that a legal claim for breach of contract by Facebook users for using Scramble! in Facebook cannot be based on the Policy's section on security. Additionally, sections 6 and 7 also do not constitute ground for claiming a breach of contract by Facebook. A most interesting section in the Privacy Policy in relation to the use of Scramble! in Facebook is Section 8: I conclude that this section requires Facebook users to be responsible for their own security on Facebook and that this Section encourages the use of (information) security enhancing mechanisms, such as Scramble!.

5: CONCLUSIONS AND RECOMMENDATIONS

In this section I answer the research question and subquestions as formulated in the introduction of this thesis:

- *Which legal obstacles occur if Scramble! would be downloaded from the EU to other EU countries or to the US, and used by EU and US citizens for purposes of privacy protection or privacy control on their Facebook profile?*
  - How is this question answered in light of EU and US privacy laws and regulations?
  - How is this question answered in light of EU and US encryption laws and regulations?
  - How is this question answered in light of the specific contractual relation between Facebook and its users?

I will start by answering the subquestions, then I will answer the main research question.

The first subquestion I answer with: no. EU data protection law does not provide any obstacles for the use of Scramble! Rather, the data protection rights and principles should be seen as reasons to encourage the use of Scramble! by (EU) citizens to enforce their data protection rights. The US information privacy (tort) law I assess also does not in itself provide any obstacles for the use of Scramble! in online SNSs. The use of Scramble! might even, when used by a large amount of people over a longer period of time, change the notion of information privacy in the US, as for content encrypted by Scramble! information privacy issues and discussions on whether privacy tort law is applicable, are no longer relevant.

In paragraph 3, I answered the second subquestion, which answer I conclude to be: no. Both EU and US anti-circumvention law protect Scramble! as a copyright protection mechanism, thus prohibiting others to circumvent it. These anti-circumvention laws do not prohibit the use of an encryption tool, but rather facilitate the ability to use it for purposes of protection copyright covered materials. Furthermore, EU crypto export regulation does not prohibit the use or export of Scramble! as the tool falls under the 'public domain' exception. With regard to the use of Scramble! and the possibility of a decryption order, I concluded both in the case of the US and the EU that in some cases, such an order might be possible; something that Scramble! users, and those having access to the readable text, should consider. However, the possibility of a decryption order does not prohibit the use of Scramble!. It only shows that, under some circumstances, one might be ordered to reveal the encrypted content.

With regard to the contractual relation between Facebook and its users, as discussed in Chapter 4, I argue, again that the question should be answered with: no. Provided that those using Scramble! in Facebook do not encrypt their name and email address. Moreover, I am of the opinion that the Facebook Privacy Policy, more specifically section 8, encourages the use of security enhancing mechanisms such as Scramble!, as the section requires Facebook users to be responsible for their own security on Facebook.

As appears, also the main research question can be answered with: no. Generally, within the scope of my research no legal obstacles - again, provided that in Facebook, name and email address is not encrypted - can be found that prevent anyone from using Scramble in SNSs, whether that SNS is EU, or US based.

REFERENCE LIST

Literature and websites

Abril, P.S. (2007) Recasting privacy torts in a spaceless world. *Harvard Journal of Law & Technology*, 21 (1), 1-47.

Aljifri, H. & Navarro, D.S. (2003) International legal aspects of cryptography. *Computers & Security*, 22 (3), 196-203.

Article 29 Data Protection Working Party (2002) Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites. Working Party on the Protection of Individuals with regard to the processing of Personal Data. Report number: 5035/01/EN. [Online] 1-16. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf [Accessed 23rd June 2010].

Article 29 Data Protection Working Party (2007) *Opinion 4/2007 on the concept of personal data.* Working Party on the Protection of Individuals with regard to the processing of Personal Data. Report number: 01248/07/EN. [Online] 1-26. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf [Accessed 18th June 2010].

Article 29 Data Protection Working Party (2009) *Opinion 5/2009 online social networking*. Working Party on the Protection of Individuals with regard to the processing of Personal Data. Report number: 01189/09/EN. [Online] 1-13. Available from: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf [Accessed 27th February 2010].

Beato, F., Kohlweiss, M. & Wouters, K. (2009) *Enforcing access control in social network sites*. [Online] 1-11. Available from: http://www.cosic.esat.kuleuven.be/publications/article-1240.pdf [Accessed 27th February 2010].

Bergelson, V. (2003) It's Personal, but Is It Mine? Towards Property Rights in Personal Information. *U.C. Davis Law Review*. [Online] 37 (379). Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=870070 [Accessed 22nd June 2010].

Bignami, F. (2007) *The US Privacy Act in Comparative Perspective*. Contribution to the European Parliament Public Seminar "PNR/SWIFT/Safe Harbour: Are Transatlantic data Protected?" [Online] Available from: http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf [Accessed 22nd June 2010].

Blok, P. H. (2002) *Het recht op privacy: een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*. [The right to privacy: a research on the scope of the concept 'privacy' in Dutch and American law] The Hague, Boom Juridische Uitgevers.

Boyd, D. (2006) Friends, Friendsters, and Myspace Top 8: Writing Community Into Being on Social Network Sites. *First Monday*. [Online] 11(12). Available from: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336 [Accessed 16th June 2010].

Commission of the European Communities (2007) *Communication from the Commission to the European Parliament and the Council: on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM (2007) 228 Final.

COM (2007) 87 Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, p. 5.

Debatin, B. et al. (2009) Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15 (1), 83 – 108.

De Hert, P. & Gutwirth, S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth, S. et al. *Reinventing data protection?* Springer Science, Dordrecht, 3-44.

De Terwange, C. & Louveaux, S. (1997) Data protection and online networks. *Computer Law and Security Report*, 13 (4), 234-246, p. 238.

Edwards, L. & Hatcher, J.S. (2009) Consumer Privacy Law 2: Data Collection, Profiling and Targeting. *Law and the Internet*. [Online] 1-25. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1435105 [Accessed 27th February 2010].

Electronic Privacy Information Center (EPIC) and Privacy International (PI) (2007) *Privacy & Human Rights 2006: Overview of Privacy*. [Online] Available from: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559474&als[theme]=Privacy%20and%20Human%20Rights [Accessed 20th June 2010].

Electronic Information Privacy Center (EPIC). *Privacy and Consumer Profiling*. [Online] Available from: http://epic.org/privacy/profiling [Accessed 1st June 2010].

European Union (1995-2010) *Europa.eu: Fundamental rights within the European union: Charter of Fundamental Rights* [Online] Available from: http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/l33501_en.htm [Accessed 27th February 2010].

Facebook Developers Wiki (2010) *Anatomy of a Facebook Application.* [Online] Available from: http://wiki.developers.facebook.com/index.php/Anatomy_of_a_Facebook_App

Facebook (2009a) *Facebook Platform*. [Online] Available from: http://developers.facebook.com/about_platform.php [Accessed 27th February 2010].

Facebook (2010a) *Facebook* [Online] Available from: http://www.facebook.com/ [Accessed 27th February 2010].

Facebook (2010b) *Facebook Press* [Online] Available from: http://www.facebook.com/press/info.php?statistics [Accessed 27th February 2010].

Facebook (2010c) *Facebook's Privacy Policy.* [Online] Available from: http://www.facebook.com/policy.php [Accessed 23rd June 2010].

Facebook (2010d) *Statement of Rights and Responsibilities*. [Online] Available from: http://www.facebook.com/terms.php [Accessed 27th February 2010].

Fox News (2009) Facebook CEO to scared users: Trust us [Online] Available from: http://www.foxnews.com/story/0,2933,494804,00.html [Accessed 22nd June 2010].

Gavinson, R. (1980) Privacy and the limits of the law. *The Yale Law Journal*, 89 (3), 421-471.

Goffman, E. (1959) *The Presentation of Self in Everyday Life*. Garden City New York, Doubleday.

Grimmelmann, J. (2009) Saving Facebook. *Legal Studies Research Paper,* No. 08/09-7, pp. 1137-1206. [Online] Available from: http://ssrn.com/abstract=1262822 [Accessed 27th February 2010].

Guarda, P. & Zannone, N. (2009) Towards the development of privacy-aware systems. *Information and Software Technology*. [Online] 51(2), 337-350. Available from: doi:10.1016/j.infsof.2008.04.004 [Accessed 27th February 2010].

Hendry, J. & Goodall, K. (2008) Facebook and the commercialisation of personal information: some questions of privacy. In: BILETA Annual Conference 2008. *Law Shaping Technology, Technology Shaping the Law, Glasgow Caledonian University, March 2008.* Glasgow, p. 1-30.

Hillman, R.A. (2006) On-line boilerplate: Would mandatory website disclosure of e-standard terms backfire? *Michigan Law Review*, 104, 837.
Hoadly, C.M. et al. (2009) Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, 9 (1), 50-60.

Hornby, A.S. (2005) *Oxford Advanced Learner's Dictionary of Current English*. 7th Edition, Oxford University Press.

Hyves (2004-2010) *Hyves* [Online] Available from: http://www.hyves.nl [Accessed 27th February 2010].

Hyves (2009) *Hyves Privacy Policy* [Online] Available from: http://www.hyves.nl/privacy/ [Accessed 27th February 2010].

Johnson, J.L. (1989) Privacy and the Judgement of Others. *Journal of Value Inquiry*, No. 23.

Killian, J.H. et al. (2004) *The Constitution of the United States of America: Analysis and Interpretation.* Washington, United States Government Printing Office.

Koops, E.J. (1999) *The Crypto Controversy.* The Hague, Kluwer Law International.

Koops, E.J. (2008) *Crypto Law Survey* [Online] Available from: http://rechten.uvt.nl/koops/cryptolaw/ [Accessed 27th February 2010].

Kuczerawy, A. (2009) Facebook and its EU users – Applicability of the EU data protection law to US bases SNS. In: PrimeLife EU project / IFIP. *Fifth IFIP TC9/TC11 Summer Schoo, 7-11 September 2009*, *Nice, France.*

Lessig, L. (1999) *Code: And Other Laws of Cyberspace.* New York, Basic Books.

Lessig, L. (2006) *Code: And Other Laws of Cyberspace, Version 2.0.* New York, Basic Books.

Lucas, M. M. & Borisov, N. (2008) FlyByNight: mitigating the privacy risks of social networking. In: *Conference on Computer and Communications Security: Proceedings of the 7th ACM workshop on Privacy in the electronic society, Alexandria, Virginia, USA.* New York, ACM. pp. 1-8.

Myspace.com (2003-2010) *Myspace* [Online] Available from: http://www.myspace.com/ [Accessed 27th February 2010].

Pacini, C., Andrews, C. & Hillison, W. (2002) To agree or not to agree: Legal issues in online contracting. *Business Horizons*. [Online] 45 (1), 43-52. Available from: doi:10.1016/S0007-6813(02)80009-X [Accessed 27th February 2010].

Palfreyman, B. M. (2009) Lessons from the British and American Approaches to Compelled Decryption. *Brooklyn Law Review*, 75 (1), p. 353.

PrimeLife (2010a) *PrimeLife - Bringing sustainable privacy and identity management to future networks and services: A research project funded by the European Commission's 7th Framework Programme.* [Online] Available from: http://www.primelife.eu/ [Accessed 1st June 2010].

PrimeLife (2010b) *Scramble* [Online] Available from: http://www.primelife.eu/results/opensource/39-scramble [Accessed 17the June 2010].

Prosser, W.L. & Keeton, W.P.P. (1984) *Prosser and Keeton on the law of torts.* West Group, 5th student edition, p. 17.

Purtova, N. (2009) Property rights in personal data: Learning from the American discourse. *Computer Law & Security Review*, 25 (6), 507-521.

Solove, D.J. (2001) Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review.* [Online] 53, 1393-1462. Available from: http://ssrn.com/abstract=248300 [Accessed 22nd June 2010].

Solove, D.J. (2006a) A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154 (3), 482.

Solove, D.J. (2006b) *Information privacy law.* New York, Aspen Publishers, pp. 673-680.

Schwartz, P.M. & Reidenberg, J.R. (1996) *Data privacy law: A study of United States data protection.* Charlottesville, Michie Law Publishers.

Taylor, G. (1999) Wassenaar - The Cryptic Enigma. *Internet Law Bulletin.* [Online] 2 (1). Available from: http://www.efa.org.au/Issues/Crypto/enigma.html [Accessed 27th February 2010].

Telegraph (2009) *Networking site cashes in on friends* [Online] Available from: http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/4413483/Networking-site-cashes-in-on-friends.html [Accessed 22nd June 2010].

The New York Times (2007) *Use My Photo? Not Without Permission.* By NOAM COHEN. [Online] Available from: http://euro.ecom.cmu.edu/program/law/08-732/Copyright/UseMyPhoto.pdf [Accessed 26th June 2010].

Tuunainen, V.K. et al. (2009) Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. *BLED 2009 proceedings* [Online] Available from: http://aisel.aisnet.org/bled2009/42/ [Accessed 22nd June 2010].

Ungberg, A.J. (2009) Protecting privacy through a responsible decryption policy. *Harvard Journal of Law & Technology*, 22(2), p. 538.

U.S. Copyright Office (2000) *Joint Study of Section 1201(g) of The Digital Millennium Copyright Act* [Online] Available from: http://www.copyright.gov/reports/studies/dmca_report.html#N_5_ [Accessed 27th February 2010].

Vedder, A. (2000) Medical data, new information technologies and the need for normative principles other than privacy rules. In: M. Freeman & A. Lewis (ed.), *Law and Medicine.* (Series Current Legal Issues). Oxford: Oxford University Press, 2000, 441-459.

Westin, A. (1967) *Privacy and Freedom*. New York, Atheneum.

White, G.E. (2003) *Tort law in America: an intellectual history.* New York, Oxford University Press.

Winn, J.K. & Bix, B.H. (2006) Diverging perspectives on electronic contracting in the U.S. and EU. *Cleveland State Law Review*, 54, 175-190.

Wong, R. (2008) *Social networking: anybody is a data controller!* [Online] Available at: http://ssrn.com/abstract=1271668 [Accessed 22nd June 2010].

Wong, R. (2009) Social networking: a conceptual analysis of a data controller. *Communications Law*, 14 (5), 142-149.

Laws, regulations and case law

American Law Institute (1965) Restatements of the Law 2nd, Torts.

Charter of Fundamental Rights of the European Union of the European Parliament, December 7, 2000, *O.J.*, No. C 364, 2000.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441)

Council Directive (EC) 1995/46 of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

Council Directive (EC) 1998/34 of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

Council Directive (EC) 2001/29 of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

Council Regulation (EC) No. 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology.

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (1950). ETS 5; 213 UNTS 221. [Hereafter: 'ECHR'].

Council of Europe, Convention on Cybercrime (2001). CETS No.: 185. [Hereafter: 'Convention on Cybercrime 2001' or 'Cybercrime Convention'].

Fisher v. United States, 425 U.S. 391, 408 (1976).
IITF Information Policy Committee: Privacy Working Group (1995) Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information. [Online] Available from:http://aspe.hhs.gov/datacncl/niiprivp.htm, [Accessed 27th February 2010]. [Hereafter: the 'NII Principles 1995'].

Lindqvist C-101/01, ECJ judgment of 6 November 2003.

Regulation of the European Parliament and of the Council (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, O.J., No. C 306, 17 December 2007, pp. 1-271.

United States Code, Title 18.

United States v. Boucher, 2007 WL 4246473 (D. Vermont, Nov. 29, 2009)

United States v. Hubbell, 530 U.S. 27, 36 (2000).

U.S. Digital Millennium Copyright Act, 1998. [Hereafter: 'DMCA'].

BIBLIOGRAPHY

Literature

Abril, P.S. (2007) A (My)space of one's own: On privacy and online social networks. *Northwestern Journal of Technology and Intellectual Property*. [Online] 6 (1), 73-88. Available from: http://ssrn.com/abstract=1392285 [Accessed 27th February 2010].

Barnes, S.B. (2006) A privacy paradox: Social networking in the United States. *First Monday*. [Online] 11 (9). Available from: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312 [Accessed 27th February 2010].

Baumer, D.L., Earp, J.B. Poindexter (2004) Internet privacy law: a comparison between the United States and the European Union. *Computers & Security*. [Online] 23 (5), 400-412. Available from: doi:10.1016/j.cose.2003.11.001 [Accessed 27th February 2010].

Fleischer, P. & Cooper, D. (2005) EU data privacy in practice – Microsoft's approach to compliance. *Computer Law & Security Report*. [Online] 22 (1), 57-67. Available from: doi:10.1016/j.clsr.2005.11.004 [Accessed 27th February 2010].

Fox News (2009) *Facebook CEO to Scared Users: Trust Us* [Online] Available from: http://www.foxnews.com/story/0,2933,494804,00.html [Accessed 27th February 2010].

George, C. & Scerri, J. (2007) Web 2.0 and User-Generated Content: Legal Challenges in the New Frontier. *Journal of Information, Law and Technology*. [Online] Vol. 2. Available from: http://ssrn.com/abstract=1290715 [Accessed 27th February 2010].

Gorham-Oscilowski, U. & Jaeger, P.T. (2008) National security letters, the USA Patriot Act, and the Constitution: The tensions between national security and civil rights. *Government Information Quarterly*. [Online] 25 (4), 625-644. Available from: doi:10.1016/j.giq.2008.02.001 [Accessed 27th February 2010].

Hoadley, C.M., Xu, H., Lee, J.L. & Rosson, M.B. (2009) Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*. [Online] Available from: doi:10.1016/j.elerap.2009.05.001 [Accessed 27th February 2010].

Hodge, M.J. (2006) The Fourth Amendment and privacy issues on the "new" internet: Facebook.com and Myspace.com. *Southern Illinois University Law Journal*.[Online] 31, 95-122. Available from: http://www.law.siu.edu/research/31fallpdf/fourthamendment.pdf [Accessed 27th February 2010].

Hogben, G. (2007*) Security issues and recommendations for online social networks*. ENISA. Position Paper No.1. [Online] Available from: http://www.enisa.europa.eu/publications/position-papers [Accessed 27th February 2010].

Iyengar, R., Han, S. & Gupta, S. (2009) Do friends influence purchases in a social network? *Harvard Business School Marketing Unit Working Paper,* No. 09-123, pp. 1-34.[Online] Available from: http://ssrn.com/abstract=1392172 [Accessed 27th February 2010].

Kunkel, R.G. (2002) Recent Developments in Shrinkwrap, Clickwrap and Browsewrap Licenses in the United States. *E-Law – Murdoch University Electronic Journal of Law.* [Online] 9 (3). Available from: http://www.murdoch.edu.au/elaw/issues/v9n3/kunkel93.html [Accessed 27th February 2010].

McGeveran, W. (2009) Disclosure, endorsement, and identity in social marketing. *Minnesota Legal Studies Research Paper*, No. 09-04, pp. 1104-1166. [Online] Available from: http://ssrn.com/abstract=1334406 [Accessed 27th February 2010].

Narayanan, A. & Shmatikov, V. (2009), De-anonymizing Social Networks. *30th IEEE Symposium on Security and Privacy 2009, Oackland, United States.* pp. 173 – 187. [Online] Available from: doi:10.1109/SP.2009.22 [Accessed 27th February 2010].

Nu.nl (2009) *Pas op met quizjes op Facebook.* [Watch out for quizzes on Facebook] [Online] Available from: http://www.nu.nl/internet/2070552/pas-op-met-quizjes-op-Facebook.html [Accessed 27th February 2010].

Ohm, P. (2009) Broken promises of privacy: Responding to the surprising failure of anonymization. *University of Colorado Law Legal Studies Research Paper,* No. 09-12, pp. 1-64. [Online] Available from: http://ssrn.com/abstract=1450006 [Accessed 27th February 2010].

Pooley, J. (2010) The Authenticity Bind: From Flappers to Facebook. In: Aronczyk, M. & Powers, D. (ed), *Blowing Up the Brand: Critical Perspectives on Promotional Culture*. New York, Peter Lang.

Prinz, K. (2009) *Silicon Valley IP Licensing Law Blog: Facebook Licensing Controversy Prompts Public to Take Closer Look at Social Networking Site Terms and Conditions.* [Online] Available via: http://www.siliconvalleyiplicensinglaw.com/ [Accessed 27th February 2010].

Steinke, G. (2002) Data privacy approaches from US and EU perspectives. *Telematics and Informatics*. [Online] 19 (2), 193-200. Available from: doi:10.1016/S0736-5853(01)00013-2 [Accessed 27th February 2010].

Stelter, B. (2009) *Facebook's Users Ask Who Owns Information* [Online] Available via: www.nytimes.com [Accessed 27th February 2010].

Svantesson, D.J.B. (2007) *Private International Law and the Internet*. Alphen a/d Rijn, Kluwer Law International, pp. 142-155.

Trusov, M., Bucklin, R.E. & Pauwels, K.H. (2008) Effects of word-of mouth versus traditional marketing: Findings from an internet soacial network site. *Robert H. Smith School Research Paper*, No. RHS 06-065, pp. 1-48. [Online] Available from: http://ssrn.com/abstract=1129351 [Accessed 27th February 2010].

Van den Berg, B. & Beato, F. (2009) Access control through audience segregation in social network sites. HARTBEAT 1.2.6 [SNS], 27 August 2009, Version 2.7.

Van der Hof, S. (2002) Internationale on-line overeenkomsten. [International online agreements] The Hague, SDU Publishers, pp. 102-107, 208-213, 266-267.

Zuckerberg, M. (2009) *On Facebook, People Own and Control Their Information* [Online] Available from: http://blog.facebook.com/blog.php?post=54434097130 [Accessed 27th February 2010].

Laws, regulations and case law

Council Directive (EC) 2000/31 of June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

Council Directive (EC) 2002/21 of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

Council Directive (EC) 2002/22 of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

Council Directive (EC) 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).