<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ero Balsa</td>
<td>ESAT/COSIC, KU Leuven</td>
</tr>
<tr>
<td>2</td>
<td>Laura Brandimarte</td>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>3</td>
<td>Alessandro Acquisti</td>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>4</td>
<td>Claudia Diaz</td>
<td>ESAT/COSIC, KU Leuven</td>
</tr>
<tr>
<td>5</td>
<td>Seda Gürses</td>
<td>ESAT/COSIC, KU Leuven - New York University</td>
</tr>
</tbody>
</table>
1 Introduction

In this document we report on the results of a usability study of a privacy enhancing tool, *Scramble!*, which was designed for Facebook users by researchers from the KU Leuven (see Beato et al., 2011). The usability study was run at Carnegie Mellon University in the summer of 2013 by a team combining researchers from different SPION-member institutions.

In the last 10 years, the success of online social networks (OSN) has raised significant privacy concerns. The wealth of data that can be collected by OSN providers has raised questions regarding the balance of power between data subjects and data holders, their respective trade-offs, and how to balance their respective interests.

Computer scientists and security engineers have developed cryptographic tools (e.g., Baden et al., 2009, Lucas and Borisov, 2008, Guha et al., 2008, Beato et al., 2011), aimed at providing users greater control over privacy in OSNs. Many of these tools are grounded on robust security foundations that try to provide the average Internet user with greater autonomy and freedom from online surveillance. These tools are arguably especially needed in the context of OSNs, given the sensitive nature of the information that users often share through those platforms. Information related to private realms of their lives is uploaded by the users, and stored and processed by the service providers of these platforms, often without users’ awareness or informed consent (Acquisti and Gross, 2006). For instance, users are often unaware of how their information is processed, which users and third parties are given access to it and, even most importantly, which decisions are made based on it and how these decisions affect us (Acquisti and Gross, 2006).

Privacy-preserving tools can be used to solve certain mundane privacy problems, such as preventing employers from finding out about blatant criticism from their employees or avoiding that parents intrude the social space of their children. However, existing tools - even those which are free and publicly available - have seen little adoption in practice (Acquisti, 2004). Security and privacy experts have put forward several possible explanations to the lack of interest of OSN users in privacy technologies. Some of them have pointed out to the poor understanding that many users have with respect to privacy problems online (Mazzia et al., 2012). Another plausible explanation relates to the main motivation of the SPION project: poor privacy and security design in social networks presents a risk to individual users and burdens them with the management of these risks. Therefore, users would renounce greater control when it comes at the expense of greater responsibility, greater burden. Yet little work has been done so far that studies the perceptions and attitudes of users towards privacy technologies specifically tailored for OSNs.

In this document, we report on the results of a usability study aimed at discovering the hitches and obstacles for the adoption by the general public of privacy technologies for OSNs. In this study we investigated participants’ attitudes towards desired and perceived control over privacy on OSNs before and after using *Scramble!* (Beato et al., 2011), a cryptographic tool that provides greater control over privacy than current OSN privacy settings. Although purely qualitative, the study results suggest that users lack a proper understanding of the benefits and advantages of this kind of tools, and especially what these tools can provide them in terms of privacy protection. However, we also find qualitative evidence that users may be *unwilling* to take on greater responsibility in exchange for greater privacy control.
2 Background

2.1 Privacy Preserving Tools for OSNs

In the last few years, computer security researchers have devised various tools for privacy protection on OSNs. Most of these tools have a common denominator: they provide users with a means to control who has access to their data online, e.g., their personal data, communication data, such as posts or messages, and other content, such as photos, independently of the OSN provider. Moreover, many of these tools take advantage of the robust security properties provided by cryptography to enforce the protection guarantees required by the kind of sensitive information that is made available in online social networks.

Early proposals of privacy preserving tools for OSNs include ImageLock (Tootoonchian & Hatahet, 2007), a Firefox extension that allows users to protect the photos they upload online. The way ImageLock protects the users’ photos is by replacing them on the social networking site with a fake photo and storing the real ones in a trusted server, i.e., a server that the user confides in, such as her own server or her account in a cloud server. When authorized users request to see the user photos, ImageLock loads them from the trusted server to replace the fake photos. That way, users do not need to trust any service provider with their intimate photos and have a higher degree of control over who actually can access those photos. Another tool, Lockr (Tootoonchian et al., 2009), follows the very same principle: instead of uploading the user content to the OSN, it replaces it with fake content together with an access control list (ACL) which defines who should have access to the real content, stored in a separate (trusted) server. Yet, the main drawback of both ImageLock and Lockr is that if users do not have their own server or a server they can trust, they still have to rely on a third party server.

Cryptography comes in handy for solving this problem, allowing users to encrypt the content with independence of the service provider they choose to store their OSN data. NOYB (acronym that stands for None Of Your Business), is a tool to encrypt the users’ social network data (Guha et al., 2008). NOYB further uses a special encryption technique (substitution encryption) that prevents the social network provider (e.g., Facebook, Twitter) from learning that the users have in fact encrypted their data. Another tool, FaceCloak (Luo et al., 2009), uses cryptography to protect the users’ personal information in their social network profile. FaceCloak stores the information, encrypted, on a third party server and posts on the social networking site fake data that, thanks to complex cryptographic techniques, can be used by the authorised users to access the real data in the third party server. Note that the third party server only stores encrypted data and therefore is not able to access their content.

Scramble!

Numerous cryptography-based tools for privacy protection on OSNs have followed NOYB and FaceCloak. In our work, we focus on Scramble! (Beato et al., 2011), a Firefox extension currently under development under the framework of the SPION project. Scramble! allows users to
enforce access control rules over their data; this is, it enables users to enforce their own privacy settings over the messages they send/post on social networking sites, regardless and independently from the privacy settings already available on the site. Scramble! features a hybrid cryptosystem (based on OpenPGP) to enforce access control lists (Sandhu & Samarati, 1994). Developed as a Firefox Extension, Scramble! is publicly available for download and can be easily installed as any other Firefox extension. After installation, users need to initialise the tool, which consists in generating a pair of public-private keys (it is also possible to import them, in case the user already has a key pair). Users can then add their friends’ public keys to Scramble!’s key ring, which can be done either by asking Scramble! to perform a lookup in a public key server or loading it from a local file. After that short initialisation, Scramble! is ready to use. Users just have to select the messages they would like to encrypt in the social networking site of their choice, and the friends with whom they wish to share the content, and Scramble! automatically replaces the unencrypted text with its corresponding encrypted version, which is then posted on the OSN site. That way, all users communications are stored encrypted on the server of the social networking site. This provides several benefits: users do not need to trust the social network provider to guarantee the confidentiality of their content, they do not need an alternative trusted server to store their data, and they can easily manage who is able to access their information. Furthermore, Scramble! provides automatic decryption for those users who have the right cryptographic keys to decrypt content, releasing users from the burden of having to deal with the manual decryption of messages.

As previously mentioned, none of the tools described in this section - including Scramble!, have experienced significant adoption.

2.2 Usability Studies of Cryptographic Tools

Our work combines both elements of behavioural economics research and usability studies. On the one hand, we try to find patterns between the attitudes of users towards their privacy and their perception of and attitude towards tools that try to provide a solution to various privacy problems online. On the other hand, we explore the usability issues that users find on one of such tools: Scramble!. We do so, in part, to find out whether usability issues are behind the lack of adoption of these systems and, ultimately, to provide general or specific design principles that help designers improve the usability of their tools, therefore increasing the chances of successful adoption.

Previous research has studied the usability of cryptographic tools. In the context of our work, two studies are of special importance. The first work is Whitten and Tygar (1999)’s seminal study of usability of a cryptographic tool, PGP 5.0. Whitten and Tygar used a cognitive walkthrough analysis and a laboratory user test to assess whether PGP 5.0 could be successfully used by a broad audience, or whether it could only be understood by security-savvy users. Whitten and Tygar pointed out several design flaws that prevented the general Internet user from being able to successfully use PGP 5.0 and therefore achieve the desired level of security. The authors blamed the inadequacy of general user interface design principles for security mechanisms, that result in dangerous mistakes, such as users sending secrets without protection. In our study, we aim to
identify issues that would prevent people from using Scramble! and discuss the adequacy of possible solutions to alleviate those issues.

Secondly, Fahl et al. (2012) performed an analysis of privacy preserving tools for OSNs and a usability study of the main existing approaches. They proposed a set of certain key decisions that may aid users while using these type of tools, including automatic key management and key recovery capabilities. An interesting finding of their study is that the users tend to prefer tools that disrupt or change as little as possible their user experience, i.e., with respect to the way they would normally use the system without the tool. However, this is a tricky design decision in the field of cryptography solutions, as automatisation involves a loss of control or lack of involvement and responsibility in the process by the users. For instance, a key recovery mechanism would often require delegating to external parties copies of the key, or parts of the key that could later be combined from different parties to recover the original key (distributing pieces of the key among several parties is more secure as no single party has a copy of the key, but still parties may be able to collude to recover the key). In any case, this would have a negative effect on the security of the system. Similarly to Fahl et al. (2012), in our study we also found evidence that users have a clear desire for automatisation, such as a tool where the only thing they need to do in order to encrypt is to click a single button, a tool with minimal or no management. However, this desire for automatisation and waiving of responsibility is in clear conflict with the carefulness and attention that most security tools require.
3 A Usability Evaluation of Scramble!

3.1 The Study

Our study was divided in three phases: an entry questionnaire, a guided tour to Scramble! and an exit questionnaire. The goal of the entry questionnaire was to get a glimpse of the participants’ attitudes towards privacy on social networks (in practice, Facebook), with a special focus on matters such as the amount of control and responsibility over one’s privacy, the surveillance performed by the service provider, and data disclosure to other unintended recipients. The goal of the guided tour to Scramble! was to provide participants hands-on experience using a privacy preserving tool for social networks that would enable them to enforce their own privacy settings independently of the service provider. Our hope was that this in turn would allow us to gain some insight into the issues and problems that users experience using these tools, the trade-offs involving greater control and greater responsibility (and potentially increased management complexity) for better privacy, in order to, ultimately, infer a set of principles that would help developers design better privacy preserving tools for OSNs.

Note that in our study we investigate both users’ attitudes towards the fundamental benefits that privacy preserving tools such as Scramble! provide, and specific issues and problems that Scramble! presents. Therefore, even if some of our results would only apply to the specific goal of improving Scramble!, we also provide insight on how to improve any cryptographic tool for privacy protection in OSNs.

In the remainder of this section we explain in detail each of the different phases of our study.

The entry questionnaire. The entry questionnaire consisted of 6 initial questions about general Facebook usage (frequency, number of friends, and so on) that helped us better understand our pool of participants (described in the next subsection); 5 questions about desired and perceived control and responsibility over privacy on Facebook; 9(+5) questions about the general perception of privacy protection on Facebook and of Facebook’s privacy settings; 3 questions hinting at the lack of control over and limitations of Facebook’s privacy settings; and finally 13(+6) questions about the feeling of protection from and concern about unintended recipients on Facebook. The complete list of questions can be found in Appendix A.

Based on the responses provided by participants to this questionnaire, we were able to better understand the attitudes of the participants towards Scramble!, as we could link and compare reported attitudes before and after using Scramble!.

Guided tour to Scramble!. The goal of this phase was to expose participants to an actual privacy preserving tool for OSNs that provides robust security and greater control over their privacy on OSNs. As previously mentioned, we chose Scramble! because it is being developed under the framework of the SPION project and it has the basic features and attributes typical of cryptography-based privacy preserving tools for OSNs.

The tour involved each and every step that a new Scramble! user would have to perform to
be able to use the tool. Therefore, we provided participants with a manual to download, install and use Scramble!, together with some specific instructions to motivate them to thoroughly test the tool. It is true that a guided tour may not give users enough freedom to explore themselves, make mistakes, and fully experience the tool. However, given logistical constraints, we considered it would be best to walk the users through the most important and basic tasks - i.e., installing the tool and learning how to use the interface in order to send encrypted messages - rather than having them spending time with less informative features (such as, for instance, saving their private keys to a USB stick or creating groups of friends).

The exit questionnaire. The goal of the exit questionnaire was twofold. On the one hand, we wanted to find out whether there are serious usability issues that would prevent participants from having an even minimally informative experience of how privacy preserving tools like Scramble! operate. To this end, we included, as the first part of the exit questionnaire, the system usability scale (SUS), a standardised usability questionnaire (Brooke, 1996) based on a 10-item attitude Likert scale widely used in usability studies. This allowed us to perform a simple, quick check on the difficulties that users had experienced using the tool.

The second part of the questionnaire was a set of 11 questions specifically addressed to evaluate the attitudes of users towards tools such as Scramble!, based on their experience using this tool. We enquired users about their general experience using Scramble!, what they had liked and disliked of this tool, whether they thought it was a secure way of protecting their privacy, and whether they would use the tool in the future, for which cases or purposes. The complete list of questions can be found in Appendix B.

This three-phase structure allowed us to collect general attitudes of users before using one of these tools, and link and compare them with the perceptions and opinions after they had used one of these tools. All three phases occurred in the lab. At arrival, participants were instructed to log into one of the 8 available computers in the lab and received an email with a link to the entry questionnaire. They were given 15 minutes to complete it, at which point they received a paper copy of the manual to download and install Scramble!. They had a chance to experience the use of Scramble! for 30 minutes. When they were done, they received a second email with the link to the exit questionnaire. Everybody followed this sequence except for the first 8 participants, who did not have sufficient time to take the exit questionnaire, and were therefore asked to take it at a later time.

3.2 Experimental setup

We invited 52 students (42% female, average age = 21.5, SD = 2.6) from the Center for Behavioral Decision Research Pool at Carnegie Mellon University to participate in a study to “Test Scramble! - A Facebook app” and compensated them with $10. From those participants, 48 completed the whole study, although only 43 participants were able to complete it in our lab: the remaining five participants had to complete the exit survey at home and, given that surveys were online and anonymous, we cannot link them back to the entry questionnaire. Therefore, whenever
we describe the results with respect to variables in the entry questionnaire, the sample size to consider is 52; for the analysis of the exit questionnaire, the sample size is 48, and for variables that combine both the entry and the exit questionnaires the sample size is 43. Note that, for a usability study, as little as 4 or 5 participants are usually enough to discover 80% of a product’s usability problems (Virzi, 1992). In fact, previous similar usability studies relied on as little as 12 and 15 participants (Whitten and Tygar, 1999 and Fahl et al., 2012, respectively). Given that our study is not just a usability study, but rather a qualitative, extended, in-depth study with plenty of interaction with the participants, the three-fold increase in the accustomed sample size should be sufficient to provide meaningful, reliable results.

Participants’ Facebook usage. In order to understand how knowledgeable and Facebook-savvy the participants were, we asked them a series of questions related to their Facebook usage. All participants had been using Facebook for at least 2 years, with the vast majority (90%) using Facebook for more than 3 years. All participants declared to be active Facebook users. Almost all of them (95%) declared to use Facebook daily, with some of them (27%) declaring to be always online and checking the site regularly. Amongst the activities we suggested in the entry questionnaire, the most popular were classic Facebook activities, such as sending private messages to friends, checking what my friends are up to, share photos, “Like” stuff, and commenting on posts. Activities such as tell people how I am feeling or attract people’s attention were far less popular amongst the participants.

Specifically, when asked about the way they preferred to communicate on the site, most participants (60%) declared to have a significant inclination for public posting over private messages (10%), with around a third of them using both equally often. As for their number of friends, most participants (90%) declared to have more than 200 friends on Facebook, and more than half of them (60%) declared to have more than 500 friends. However, many participants (75%) declared to communicate with less than 50 of their friends. This supports previous studies that report that most users only communicate with a subset of their friends (Huberman et al., 2008).
4 Evaluation

In this section we provide a detailed account of the main findings of our study.

We have used emergent coding (Lazar et al., 2010) to analyse the responses provided by the participants to the numerous open-ended questions in the questionnaires. Emergent coding is specially useful when working on a topic that has a limited amount of literature to build on, as it is the case of usability studies of privacy preserving tools for OSNs. The categories that emerged in the coding process are a combination of research-denoted concepts, i.e., concepts that we, as experts, often use and are familiar with, given their importance in the field; and in-vivo codes, namely, terms provided by the participants themselves that summarise particularly accurately and well the concept they are referring to. Moreover, in numerous cases throughout this section we will quote the very comments of the participants, in order to illustrate how the categories surfaced and as a way to support our coding scheme.

4.1. General Survey on Attitudes towards Privacy on Facebook (Before Scramble! -- Entry Questionnaire)

As mentioned earlier in Section 3, part of our study was devoted to learn about the attitudes and practices of the participants in our study. This would help us better find an explanation for how they perceive privacy preserving tools, and concretely Scramble!. In this section we report on our analysis of the participants’ responses to the questions of the questionnaire they took before using Scramble!.

Desired and Perceived Control and Responsibility over Privacy on Facebook.

We asked participants who should have control over a set of decisions related to the visibility of and access to their data on Facebook. For each decision, users were able to choose you (namely, they were the ones to have control over the decision), Facebook, or Others (and asked to specify who those others were). Multiple choice selections were allowed. For all decisions but one, most users thought that they should have control over those decisions themselves, consistent with previous literature in the privacy field suggesting that users desire control over personal information, even though they may not actually make use of that control (see, e.g., Brandimarte, Acquisti, and Loewenstein 2013). Only for Who should decide which ads show up on Facebook most users thought Facebook should be in control of such decision. We conjecture that this may be due to the fact that users have a shallow understanding of how Facebook tracks them online and processes their content and behavioural data to provide them with targeted advertising. This should be explored in future studies. Interestingly, even though multiple participants considered that both Facebook and themselves should have control over some decisions, in no case were these participants as numerous as those who thought only themselves should have control over those decisions.

This desire for control seemingly clashes with the unwillingness of participants to actually
be responsible for many of the privacy related issues we proposed to them. We enquired participants “Who should be responsible for the following decisions?”, proposing decisions that would affect their privacy, such as “setting the proper privacy settings on your profile” or “making sure private companies do not have access to the data you post to the site without your permission.” Most participants considered that Facebook should be responsible for issues such as making sure that privacy settings work, making sure strangers cannot see their photos/posts online, or making sure private companies do not have access without their permission to the data they post. These may seem quite reasonable, but a few participants declared that Facebook should be responsible for setting proper privacy settings or even “making sure your friends do not post photos of you that you do not like.” In general, most users attributed to Facebook greater responsibility than control. Furthermore, we noticed certain trends in how users assigned responsibility. Firstly, it seems that Facebook’s status quo influenced the way participants responded to the question regarding who should be responsible for various issues. For example, responsibility for “preventing strangers from logging in to your account” and “preventing people other than your friends from reading your messages and seeing your photos” (and more generally, issues which Facebook is indeed currently responsible for) was attributed to Facebook, whereas responsibility for “what your friends can see in your profile” (and more generally, matters for which users may have felt current responsibility) was attributed to the users themselves. However, we caution that different people may have given different interpretations to the meaning of “responsibility.” Therefore, more studies are needed in order to find further evidence to the dichotomy control-responsibility and, ultimately, find the causes underpinning this phenomenon.

We then asked participants “what would you say is the amount of control you have over your privacy on Facebook?” On a scale from 1 (Extremely low) to 7 (Extremely high), most users declared to have a low to medium amount of control (M = 3.64, SD = 1.25). No one had a perception of “extremely high” control over their privacy on Facebook. This general perception of low control clashes with the fact that participants reported to be in control themselves or in combination with (rather than) Facebook for a series of activities related to the management of their privacy. We asked participants “On Facebook, who gets to make the following decisions?” Almost half the participants (42%, and 8% --of all participants-- in combination with Facebook) responded they were able to decide who will have access to your data if Facebook stops its service. Similarly, a third of the participants (33%) responded they were able to decide where your data goes if Facebook stops its service. Even for those activities over which many participants acknowledged to hardly have power of decision, some other participants still reported to be able to decide upon, e.g., which data in your account the police can access in case of an investigation (27/10%) or which ads show up on Facebook (35/8%). Many participants responded to decide who is able to see and access everything you do/see/post on Facebook (80/27%) and who is able to see the photos you are tagged in (85/27%) even when they have no control over the former and limited control (mediated through Facebook and people who tag them) over the latter. This makes us wonder about the degree of understanding users have of how often they are in fact delegating control to Facebook through a set of defined preferences and trusting that Facebook will enforce them. This should also be further explored in future studies.

Lastly, we asked participants “what do you feel responsible for with respect to your own privacy?” The answers were varied but can be classified in two main categories. Firstly, what they
Post, and secondly, how they use the tools provided by Facebook to manage their privacy. Participants in the first category were the majority (47%). They generally referred to control over the content or nature of the posts, photos or comments they post and make on Facebook and, specifically, to self-censorship practices, such as not posting very intimate and personal photos, not [...] talk bad about public figures or not posting confidential information. Participants in the second category (17%) referred to practices such as getting my privacy settings right, the access I set for each of my photos/posts, make sure not all info is public and other options provided by Facebook, such as block people I don’t want to have contact with or make sure my profile cannot be searched on Google. Some participants’ responses (15%) fell in both categories.

Interestingly, the vast majority of respondents (85%) framed these practices (what is posted and how it is controlled with the tools provided by Facebook) within Facebook’s public domain. In other words, participants referred to photos, links, comments they post but not to the private communications they take part in. In fact, some participants explicitly mentioned how Facebook’s private domain falls out of the scope they consider under their responsibility, waiving it and charging Facebook instead, e.g., “I feel responsible for the content of my public posts/comments and photos posted to the public. I feel I should not have to further manage private messages [...] which I want to remain private and have selected as such”. Another participant responded “I am not the one who can guarantee the execution of [the privacy settings], Facebook does it. At this level what choice do I have? To trust Facebook”.

It is interesting to note the way users feel responsible for social privacy problems and barely mention the surveillance problem (Gürses & Díaz, 2013). Users said to be responsible for the configuration of the privacy settings, disregarding the fact that it makes no difference from the point of view of the service provider (Facebook); and limited their self-censorship practices to the “public” domain (“what I post”). The response of a participant summarises well this pattern: “I would rather friends send me private messages if they want to share something fun with me”.

**General Feeling of Privacy on Facebook and Usage and Perception of Privacy Settings.**

We asked participants “What would you say is the level of privacy protection on Facebook?”. On a scale from 1 to 7 (Extremely low and Extremely high, respectively), most participants rated Facebook’s privacy protection as medium or low (M = 3.6, SD = 1.10). Only six participants (12%) rated privacy protection on Facebook as high. No one gave a better rating than that. However, when asked “Which privacy problems, if any, do you encounter using Facebook?”, 25% of the participants actually replied None. One could expect those participants who declare to encounter no privacy problems to find privacy protection on Facebook to be rather high. However, as previously noted, very few participants were of this opinion. One may wonder whether participants were too lazy to provide a response or rather have a general feeling of low privacy protection despite any specific, concrete privacy issues they have on Facebook. The rest of participants (70%) pointed out to issues regarding Facebook’s privacy settings, such as its complexity or limitations, e.g., “it is hard to figure out how to change the privacy settings”, or “being unable to hide profile picture” or “cover page is always public”.

We further asked participants “How often do you check your privacy settings on Facebook?”. Most participants (70%) declared to check their privacy settings once a month or more often. Fewer
participants (17%) declared to never check their privacy settings. No participants answered that they checked their privacy settings more than once a week. Regardless of how frequent those periodic checks are, almost all participants (90%) had changed their privacy settings at least once. Regarding the suitability of FB's privacy settings (i.e., how well the settings address privacy protection), most participants declared to find Facebook's privacy settings (FBPS) “appropriate” or “somewhat appropriate”. Only 8 participants (20%) positioned FBPS in the “inappropriate” range (i.e., from Very inappropriate to Somewhat inappropriate). Interestingly, when we asked them “What privacy issues you have, if any, that you are not able to solve with Facebook's privacy settings?”, 5 out of 10 participants that reported to have privacy issues they were unable to solve using FBPS had rated FBPS as “somewhat appropriate”, others having each given a different rating from each other (both in the positive and negative range). A significant large group of participants (35%) reported to find no privacy issues that they could not solve using FBPS and, still, 3 amongst those participants had given a negative rating to the suitability of FBPS. In any case, most participants responded they “did not know” about privacy issues they could not solve using FBPS. These participants had mostly deemed FBPS suitability to solve their privacy problems as “appropriate”.

Many participants (83%) declared that they would be “moderately concerned” if Facebook was to change the privacy settings. Other responses were evenly distributed between “slightly”, “very” and “hugely concerned”. As for changes on FB’s privacy policy, participants seemed to be generally more concerned, with a shift of opinion from “moderately concerned” to “very” and “hugely concerned”. On the other hand, 3 users reported to miss the difference between FB’s privacy settings and privacy policy.

About the level of protection afforded by FBPS against people who are not “Facebook friends”, most participants (60%) perceived it to be either “neither low nor high” (35%) or “high” (25%). Interestingly, whereas no one deemed the protection to be “extremely low”, 2 participants found it to be “extremely high”. Around a third of participants (30%) thought that no one other than the intended recipients was able to access their messages or posts on Facebook, whereas other participants thought that that was not the case or replied that they “did not know” (40% and 30%, respectively).

Awareness of alternative privacy controls not provided by FB

When we asked participants “Are you aware of any strategies or mechanisms, currently not provided by Facebook, that can help you better protect your privacy?”, all users but one reported to be unaware of any such strategies or mechanisms. When asked “Which ones?” the only one who had reported to be aware of any such mechanisms pointed out to “DoNotTrack”, which does not fall under the category of what we consider privacy preserving tools for OSNs but is rather a technique to express a preference towards online tracking (Soghoian, 2011).

Privacy Protection from Facebook itself

We found an interesting trend in the participants’ answers to the question “On Facebook, what would you say is the level of privacy protection from Facebook itself?”. On a scale from 1 to 7 (Extremely low and Extremely high, respectively), the average response was “low” (M=3.01, SD=2). However, this conceals an interesting trend. In fact, the majority of participants responded either
"Neither low nor high" (30%) or "Extremely low" (27%), with the remaining options being selected only by a few participants. From the researchers’ perspective, the intent of the question was to find out whether users are aware of the fact that Facebook has complete access and control over all the data they provide to the site. In this way, participants that replied “Extremely low” gave the “correct” answer to the question (there is little (or no) protection for the data towards the very entity that collects, stores and manages it). We hypothesise, then, that the existence of these two “peaks” in “Neither low nor high” and “Extremely low” is caused by the existence of two groups within the participants. One group is aware of the fact that they cannot afford any privacy towards the service provider itself (in this case, Facebook), and one group which is still unaware.

We asked participants “How worried are you by the fact that intelligence and law enforcement agencies (such as the NSA, the FBI) may have access to your Facebook data?”. On a scale from 1 to 5 (from Not at all concerned to Hugely concerned) most participants declared to be slightly or moderately concerned (M = 2.78, SD = 1.40). Around a fifth of the participants (20%) responded to be Not at all concerned while a third other participants responded to be very (15%) or hugely concerned (15%).

Finally, we asked users “How interested are you in any tool to prevent all unintended recipients (Facebook, law enforcement agencies, etc.) from having access to your data on Facebook?”. On a scale from 1 to 5 (i.e., Not at all interested to Extremely interested) most users declared to be moderately or very interested (M = 3.14, SD = 1.03) in such a tool.

### 4.3 User experiences using Scramble! (Exit Questionnaire)

In this section we report on the experiences and opinions of participants after having gone through the guided tour of Scramble! We start providing results for the general usability test and later provide further insight with respect to the experience of the participants using Scramble!, their opinions, the issues they had and what they liked and did not like about the tool. Furthermore, we provide an analysis of how these responses relate to their prior attitudes as reported in the entry questionnaire.

**System Usability Scale (SUS)**

In the first part of the exit questionnaire, participants were asked to reply to a standard questionnaire designed to provide a general system usability score (SUS) for tools tested in usability studies (see Appendix B). SUS is a usability score based on a 10 item Likert scale that yields a score between 0 and 100 thus allowing a quick, coarse comparison of completely different systems. SUS has been widely used by the usability research community and because of its popularity we decided to include it as part of our post-experience questionnaire. The average score for Scramble! fell barely above the middle score (M = 52.9, SD=18.35, MAX=95, MIN=15). This can be considered a remarkably good result, given it is a tool still under development with many limitations and a rather rudimentary and clunky interface. On the other hand, one may have to account for potential experimenter effects (the participants being less likely to provide negative valuations of the tool to
the researchers if they thought the latter may have been the ones to develop it).

Opinions and perceptions on Scramble!

We asked participants to “describe, in a few words, your experience using Scramble!”. Responses were rich and varied, providing comments to many different features of the tool. In a very broad sense, we can classify responses of the participants as negative (25%), positive with reservations (28%) and positive (25%). Other users pointed to particular details without passing any judgement on their experience using the tool.

Participants that made a negative evaluation pointed out issues such as Scramble! being difficult to use, others responded it was confusing or cumbersome. Two participants referred specifically to the complexity of the initialisation process and one participant responded “[Scramble!] seems unnecessary”. Another participant mentioned that [Scramble!] didn’t seem worth the effort, presumably an alternative way of saying it was cumbersome and difficult to use. One participant also questioned its advantages by saying that it was “Easy, interesting, not sure about the benefits, though”. This hints at the fact that users would have needed more time and experience to properly grasp and understand the benefits and advantages of using such a tool. This potentially steep learning curve is definitely a major handicap towards the adoption of this type of privacy enhancing technologies.

Many participants had an overall positive experience but pointed to major issues that ostensibly undermined their experience using Scramble!. Among those issues, we found two main groups. One group of participants (15% of the total) thought that it was a nice tool but not worthy to use; and provided a variety of reasons such as not efficient enough / not easy / I wish it was [...] easier to use / it does not have a good interface / cumbersome / it's a second app [...] rather than a seamless integration on Facebook. Another group of participants valued it positively but dismissed it because they thought the tool would only be useful for extremely private/sensitive information, e.g., it’s [...] only useful for messages that really need to be protected / you would rather use this when something should be kept secret / for paranoid people or people that want to conduct illegal activities without being traced / I would only use it in the most sensitive cases.

These two are recurrent perceptions throughout all the responses to the exit questionnaire. On the one hand, users wish Scramble! was more automatic, integrated on the platform. In our own terms, we interpret this as a desire of the users for Scramble! to be more stealthy and less apparent, a desire to get rid of the need to deal with it. In fact, it is a tool that increases the number of steps that users need to communicate. On the other hand, users perceive that Scramble! is “too much” for them. The nature of the information they post on Facebook is not sensitive enough for them to need such robust cryptographic techniques. They perceive cryptography as a means to deal with top secret information, rather than trivial, daily communication between peers. This disregards the fact that access control can be achieved in several different ways and that the very service provider could be using cryptography to enforce access control for their communications in a transparent way to the users.

Those participants that gave a plain positive evaluation of Scramble! did not generally provide extra comments. Those who did referred to Scramble! with little remarks such as easy to learn and worth the effort.
In order to gain a better understanding of the participants’ perceptions and opinions, we also included more specific questions that would encourage participants to point out those features that they valued and those that they disfavoured. We asked participants “What, if anything, did you like about Scramble!?”. Many participants (35%) pointed out to the concept behind Scramble! itself, although in different ways. Some participants (8%) plainly replied that they liked the idea or the functionality or the novelty it provides. Another group of participants (15%) referred to the fact that Scramble! is able to provide protection against Facebook itself, as well as other unintended recipients, e.g., one participant replied: *It's a novel idea and it's nice to not be under the thumb of organizations like Facebook*. Other participants (8%) pointed to its simplicity, e.g., one participant responded: *It's easy to just right click and encrypt a message*. Another group of participants (8%) specifically pointed to the fact that Scramble! uses encryption to provide access control. Finally, within this group of participants that liked “the idea”, two participants noted specific features of the tool such as the use of “tinylinks” or the fact that the private key is stored locally.

On the other hand, a different group of participants (27%) reported that they liked the security and privacy provided by Scramble!. Within this group, an important subdivision can be made: those participants that praised the feeling of security created by Scramble! (8%) and those that did not refer to a feeling but rather assumed or took for granted the fact that Scramble! provided the security it promises (19%).

Finally, one participant reported to like “nothin really”.

This connects to a different, complementary question we asked the participants: “What, if anything, did you dislike about Scramble!?”. Almost all participants complained about practical issues such as the interface, the steps required to encrypt a message or the complexity of the whole process. Participants pointed out that Scramble! was cumbersome (13%), difficult (4%) and complex (13%). They also referred to the amount of time it took to install and encrypt or decrypt a message, saying it was slow (13%) or that there were too many steps (13%), concretely, one participant complained that it was necessary to “add people to the list [every time I send a message]”. Some participants (10%) complained about the interface, saying it was “clunky”, “unattractive”, “unpolished” or “real bad”. There were specific comments about the amount of automatisation. Some participants (8%) suggested that Scramble! should have “a handy button just to encrypt” or that “if the key can be generated by itself it would be awesome”.

Only a couple of participants mentioned issues regarding the security, reliability or transparency of Scramble! In particular, one participant worried that “Because messages sent to me were automatically scrambled, I wasn’t sure if the person sent a scrambled message or a normal one. I’m also not sure if anyone with scramble would be able to read a scrambled message, or I would have to have them on my contacts list first.” Another participant worried if “would it be possible for third parties to figure out the encryption mechanism”.

Naturally, when we asked participants “What features did you miss in Scramble! or you think that such a tool should have?” most of their answers related to what they had not liked. Some participants (25%) suggested that it should be easier to use and faster, e.g., “it should be easy and fast”, “it should be predictable to use”, “it should be faster and maybe a lil bit easier [...]”.

Other participants (13%) referred to what they perceived a lack of automatisation, e.g., they
mentioned that they missed “automatic encryption”, or “adding the contacts from Facebook to a group automatically”. Also one user suggested automatic detection of the person the user wants to encrypt messages for as suggested by one participant who responded “it should not have me select the person I am sending to once I am in a private message thread”

Yet another group of participants let their imagination flow and suggested improvements such as an “on/off switch so that once a conversation is started, i can type normally without having to scramble each line”, “a built in guide/ help menu on how to use it” or the availability of the plug-in for other platforms (“I use chrome, hopefully a plugin for chrome can be developed too”). Two users wondered whether Scramble! could also be used to encrypt photos. One user suggested to allow for the encryption of previous messages (“[..] does it scramble any past messages?”).

A few users (13%) responded either it had already the features they needed (“I think it’s got the features I would want from it”) or could not think of anything else that would improve the tool.

About cryptography

Cryptography is often a rather obscure and invisible feature that Internet users do not deal with directly. Because of the technical complexity of modern cryptographic protocols, most users are not familiar with how these work or why they are secure, if they are at all. Scramble! requires users to deal with cryptography. In particular, in the manual provided to the participants, we asked them to install and initialise the plug-in, and in this process they needed to create, import and export the cryptographic keys Scramble! uses to encrypt and decrypt messages.

We acknowledge the fact that the vast majority of the participants in our study were not familiar with cryptography. Furthermore, given the superficial and short instructions given to them (enough to do a basic test of the tool), as well as the little time they had to really stop to think and try to grasp and comprehend the rationale behind using cryptography and the trade-offs of data security, we decided to ask them directly if they thought that cryptography was a proper way of preventing unintended recipients from having access to their data. We asked the participants “Scramble! encrypts messages before you send or post them on Facebook. Do you think this is a secure way to prevent unintended recipients from having access to them?”. Almost all participants (77%) replied with a simple and plain “Yes”; often with no further commentary. Some other participants (17%) replied “Yes” but had some reservations about how really secure cryptography is. Among the comments provided by these participants we can find, e.g., “a simple private and public key mechanism may not be robust enough”, another participant mentioned that “Probably yes, but remember we don’t know whether scramble is a government control plug-in or actually developed by Facebook itself.” A couple of participants were sceptical about the inability of third parties to actually decrypt the messages, e.g., “I am sure they will find another way to decode it”; another responded “someone can figure it out and de-crypt it”.

One participant replied “No”, with, in our opinion as experts, a very good reason: “no, till proper and full information about, what scramble is, how and why it encrypts our data”. It was interesting to find that, the response that we expected was far from popular and only one participant gave it. Three other participants replied “No” providing reasons that hint at the fact that they are not familiar with cryptography and the guarantees it provides, e.g., one participant wrote “what if you
accidentally send a message to someone who has scramble but they were an unintended recipient can they still read your message? or do you have to add them to your contact list first?” which clearly reveals that she or he does not know that it does not matter who you send an encrypted message to as long as the recipients do not have the corresponding key to decrypt it. In the scenario described by this participant, if the message was encrypted for a certain friend, let’s say Alice, and the participant sent a message encrypted for Alice to Bob, Bob would be unable to decrypt the message unless he was able to get Alice’s private key. This is a reasonable misconception for people who are not familiar with the workings of cryptography. Another participant wrote “No, because if someone is able to hack into your account, then they would still be able to read your messages”, which ignores the fact that Scramble! does not store any information on the user account, therefore access to the account provides an adversary no information or power to decrypt encrypted messages. For a person to be able to decrypt the messages of the user it would need to have access to the very computer of the user and log in to the user account in the operating system, e.g., log in to the user’s account on Windows. (Alternatively, an adversary could steal the private key, which in turn would be far from trivial, as it is stored encrypted, protected with password). A third participant wrote that “That would require a second, and third level of encryption, which I think is illogical”. Adding layers of encryption could definitely provide stronger security, but it is unclear to us why a single layer of encryption seemed weak to this participant, and which mechanisms the participant would suggest to manage all the keys involved in a multi-layer encryption scheme.

Despite the overwhelming amount of participants that perceived cryptography as a secure way to prevent unintended recipients from having access to their messages and posts, we are unsure whether they really understood why Scramble! could help them protecting their messages or posts or they took our word for it. Also, our description of Scramble! in the manual for testing the tool described the benefits of using encryption. This, and a strong acquiescence bias might have caused the majority of users to simply respond “Yes”. Further studies should enquire users about why they think so or challenge their perception of the amount of security provided by cryptographic techniques.

Using Scramble! “out of the lab”
We asked participants “Do you see yourself using a tool such as Scramble!?”. On a scale from 1 to 5 (Never and All the time, respectively), participants confessed they would rarely use such a tool (M = 2.70, SD = 1.05). Only one participant responded “I don’t know”.

We further asked participants “Which cases, purposes or people do you think a tool like Scramble! could be useful for?” in order to know whether there would be any cases for which they would find a tool like Scramble! suitable. Most of the participants (52%) thought Scramble! would be useful to send “really private information”, “confidential information”, “for people who want to send sensitive information, like addresses or phone numbers”, for “extremely secretive information”, or “sending messages that are very private and important” or when “people need to send top-secret messages”. Some participants (15%) went even further and placed the utility of Scramble! in the domain of the military, intelligence and (counter)terrorism, e.g., “inside a military base” responded one participant. “Criminals, intelligence, […]” responded another participant. “Illegal activities” was also mentioned by one of the participants. A couple of people referred to “people who fear being
observed” or “paranoid people”. All in all, the domain of the very private, top secret or confidential accounted for 71% of the participants.

Only a rather small group (17%) thought Scramble! would be suitable for everyone and everyday activities. Interestingly, one user thought it would not be suitable for youngsters “I don’t think younger people are curious about their privacy”, whereas another one thought that would be the ideal segment of population that would benefit the most - presumably because young people are not careful about what they post online, even if previous research has shown that youngsters are certainly aware of the risks of having sensitive personal information online and carefully decide what to post online (Lenhart & Madden, 2007). Scramble! would allow younger users to post anything while protecting them against unintended recipients that could abuse their information. In fact, one user thought Scramble! would be useful for “Regular people who aren’t cautious of what they post on facebook”.

This may suggest that participants rely heavily on self-censorship as a means of protecting their privacy online, and that only in the event that they really need to post something very secret would they feel the need to use a tool such as Scramble! For example, one participant mentioned that “If people really need to make sure that their information is safe, it would be a good tool to use. But for me, I don’t have a lot of extremely secretive information that I put on facebook.” This establishes a nice future research direction, namely, try to elucidate where do users place the boundary of sensitiveness that would prevent them from posting or sending certain information on Facebook. However, if we relate to the entry questionnaire, where we asked people “How concerned are you about the fact that Facebook may suffer from a security breach and all or part of your messages, posts and photos become publicly available?”, many people declared to be very concerned about their private messages leaking out, e.g., a participant responded “I have nothing on facebook that I am ashamed of or need to hide. If my stuff is on facebook, then I am already okay with it being public. Not the inbox messages though, that would freak me out.”
5 Conclusions and discussion

In this section we provide a summary of the main findings from our study and a set of recommendations for the improvement of privacy preserving tools based on cryptography such as Scramble!

To begin with, it is important to note that most users liked the concept behind Scramble! - namely, to encrypt messages so that the service provider cannot access them or they remain private in the event of an unintended disclosure. However, they perceived that the robust security this tool provides is not matched by their real needs. Most participants thought Scramble! would be mostly useful for secret information, with some participants even framing its purpose and utility in the realm of government intelligence and (counter)terrorism.

This was motivated by the explicit use of cryptography, which participants generally perceived as secure, but way too excessive a protection means for the type information they post on social networks, i.e., not that sensitive. It is interesting to note that some participants reported that they refrain from posting very sensitive information on Facebook. This suggests the widespread use of self-censorship to mitigate the amount of information collected by the social networking site. Hence, it would be very interesting to explore in future studies whether the adoption of robust privacy enhancing technologies such as Scramble! enables or motivates less repressed communication practices. In fact, it would be needed to check to what extent participants are faithful about their self-reported self-censorship practices or instead they disclose the kind of very sensitive information they thought Scramble! would be useful for.

We hypothesise that the participants’ perception of cryptography might have influenced the way they perceived Scramble!, i.e., as a tool for top-secret communication. We deliberately included in the guided tour we gave to the participants references to the cryptographic mechanisms used by Scramble! This was in part because we considered that participants needed some background information in order to gain a minimal understanding of what the initialisation of Scramble! required them to do (i.e., why they needed to generate cryptographic keys). However, had the participants not heard about cryptography and just about the benefits provided by Scramble! (i.e., protection against the service provider and unintended disclosures), would their perception still be the same? In other words, to what extent their perception of cryptography biased their opinion about the usefulness of Scramble!?

Designers could therefore aim at communicating better the workings of cryptography, through the use of mental models and metaphors, as was previously suggested in the literature (Bravo-Lillo et al., 2011, Camp, 2009); or try to communicate their benefits in different terms other than security-related terms, such as attack, secret or confidential, among others, that keep reinforcing the widespread idea that cryptography is only for top-secret use.

Participants have naturally expressed a desire for more automatisation. Automatisation would indeed release users from the burden of dealing with cryptography, which is something obscure and unknown to them. However more studies should further explore to what extent better interfaces can be designed without resorting to automatisation, as the latter would diminish users’
oversight of the security mechanisms. In fact, we must be cautious about the amount of automatisation in a security tool, as this usually comes at the expense of less control for the user, e.g., deciding which keys are to be used to encrypt a message and securely storing private keys. Developing a tool that automatically infers the recipients of a message and manages keys is a challenging problem, if not a dangerous feature from the point of view of privacy protection.

However, if users are not to get familiar with cryptographic protocols, and designers do not use proper communication strategies (e.g., mental models) that make tools intuitive and easy to manage by the general Internet user, automatisation is unavoidable. Future research should explore on the one hand how to securely automatise some tasks and on the other how to better engage users in the decision-making required by privacy preserving tools. Users need to understand the principles and basic workings of the tools they are using or they will most surely fail to use them properly. In the case of privacy and security tools, this issue is especially critical. There is still a lot of work to do in the development of user-friendly interfaces that communicate clearly to the user what she needs to do in order to properly protect her privacy.
References


Appendix

Appendix A and B provide a full description of the questions contained in the entry and exit questionnaires. Note that we used a straight type for the questions, italic type for the available response options and a series of acronyms to easier identify the type of question. Namely, [SS], which stands for single selection, i.e., respondents must select a unique response amongst the choices available; [MS], which stands for multiple selection, i.e., respondents may select more than one response amongst the choices available, and [OQ], which stands for open question, where respondents are asked to provide their own answer, i.e., no default responses are available for selection.

A Entry Questionnaire

1. How long have you been using Facebook? [SS]
   A couple of months / About a year / About 2–3 years / More than 3 years

2. How often do you use Facebook? [SS]
   Less than once a month / Once a month / 2-3 times a month / Once a week / 2-3 times a week / Daily / Always online, checking regularly

3. Which of the following activities do you do on Facebook? [MS]
   Telling my friends about important events in my life / Try to attract people’s attention / Finding out about parties and other events / Letting my friends know what I am up to / Telling people how I am feeling (happy, angry, sad... etc.) / Reading news and stay up to date / Checking what my friends are up to / Sharing links to interesting news and sites / Sharing photos / Commenting on other people’s photos / Gossip and finding info about other people / Connecting with old classmates and friends / Commenting on other people’s status / Chatting to friends (send them private messages) / “Like” stuff / Others: (Indicate which ones)

4. What do you use more often? [SS]
   Private messages / Public posts / Both private messages and public posts equally often.

5. How many friends do you have, approximately, on Facebook? [SS]
   0 – 10 / 10 – 50 / 50 – 100 / 100 – 200 / 200 – 500 / > 500

6. Of all your Facebook friends, with how many you often communicate?
   0 – 10 / 10 – 50 / 50 – 100 / 100 – 200 / 200 – 500 / > 500

7. Who should make the following decisions?
   (You may select multiple choices, including “Others”. For example, you may check both
“You” and “Facebook” and add “My friends” to “Others”)

“Who should decide...
- who is able to see the photos you are tagged in?”
- which data in your account the police can access in case of an investigation?”
- who is able to see your personal details (age, phone number, hometown, etc.)?”
- who is able to see what you post on the site?”
- when you can delete your account?”
- what kind of information (i.e., news, links to youtube videos, etc.) you post?”
- who is able to see your list of friends?”
- who is able to know whose profiles’ you have visited?”
- the configuration of your privacy settings?”
- the number of private messages you can keep in your Facebook mailbox?”
- where your data goes if Facebook stops its service?”
- who is able to read the private messages you send?”
- decide which ads show up on Facebook?”
- who will have access to your data if Facebook stops its service?”
- what information is used from your profile to deliver ads to you?”
- who can send you a friend request?“
- who is able to see and access everything you do/see/post on Facebook?”
- who is able to know which photos (of your friends or other Facebook users) you have seen?”
- for how long your data is kept available on Facebook?”
- who can send you private messages?”

You / Facebook / Others (who?) / Don’t know

8. Who should be responsible for the following? [MS]
(Regardless of whether or not that is the actual situation on Facebook).

“Who should be responsible for...
- posting photos or messages you may later regret your friends had seen/read?”
- keeping your password confidential?”
- making sure your privacy settings work?”
- making sure that photos you do not like are deleted and not available on the site anymore?”
- the grammar of your posts and messages?”
- preventing strangers from logging in to your account?”
- what your friends can see in your profile (this is, which of your photos, posts, etc., they can see?)
- making sure your friends can see your profile at any time of the day?”
- making sure strangers are not able to see your posts and photos?”
- setting the proper privacy settings on your profile?”
- making sure private companies do not have access to the data you post to the site without your permission?”
- making sure your friends do not post photos of you that you do not like?”
- preventing people other than your friends from reading your messages and seeing your
photos?”
– allowing your friends to post comments to your status updates and photos?”
– friends being upset because of what you post?”
You / Facebook / Others (who?) / Don’t know

9. Control is generally defined as “the power to change or supervise the running of something”. Given this definition, what would you say is the amount of control you have over your privacy on Facebook? [SS]
Extremely low / Very low / Low / Medium / High / Very high / Extremely high

10. On Facebook, who gets to make the following decisions? [MS]
(You can select multiple choices, including “Others”. For example, you may check both “You” and “Facebook” and add “My friends” to “Others”). “Who decides...”
[Same as question 7]

11. On Facebook, to what extent do you feel you are responsible for your own privacy? [OQ]

12. What would you say is the level of privacy protection on Facebook? [SS]
Extremely low / Very low / Low / Medium / High / Very high / Extremely high

13. Which privacy problems, if any, do you encounter using Facebook? [OQ]

14. Which strategies or mechanisms does Facebook provide, if any, to help you protect your privacy? [OQ]

15. How often do you check your privacy settings on Facebook? [SS]
Never / Less than Once a Month / Once a Month / 2-3 Times a Month / Once a Week / 2-3 Times a Week / Daily

16. In terms of privacy protection, how appropriate are Facebook’s privacy settings?
Very Inappropriate / Inappropriate / Somewhat Inappropriate / Neutral / Somewhat Appropriate / Appropriate / Very Appropriate / Don’t know

17. What, if anything, would you add to, modify or delete from the Facebook privacy settings? [OQ]

18. What privacy issues you have, if any, that you are not able to solve with Facebook’s privacy settings?
None / The following: [OA] / Don’t know

– (If The following:... to Q. 18) Which strategies do you use to solve those
privacy issues?
None (⇒ Why none?) / The following: [OA]

19. Have you ever changed your privacy settings? [SS]
Yes / No

– (If Yes to Q. 19) How do you make sure you configured your privacy settings to work the way that you expect? [OQ]

– (If No to Q. 19) How do you make sure the default privacy settings work the way that you expect? [OA]

20. Are you aware of any strategies or mechanisms, currently not provided by Facebook, that can help you better protect your privacy? [SS]
Yes (⇒ Which ones?) / No

21. How concerned would you be if Facebook changed the privacy settings?
Not at all concerned / Slightly concerned / Moderately concerned / Very concerned / Hugely concerned / Don’t know

22. How concerned would you be if Facebook changed the privacy policy?
Not at all concerned / Slightly concerned / Moderately concerned / Very concerned / Hugely concerned / Don’t know / I don’t know the difference between privacy policy and privacy settings

23. On Facebook, what is the level of privacy protection from people who are not your Facebook friends? [SS]
Extremely low / Very low / Low / Neither low nor high / High / Very high / Extremely high / Don’t know

24. When sharing information online, such as sending a message, posting a link to a website, etc., the term intended recipients refers all the people you would like to be able to have access to that message or piece of information. When you send a message or post something on Facebook, do you think anyone other than the intended recipients is able to access it?
Yes / No / Don’t know

– (If Yes to Q. 24) Who?

– (If Yes to Q. 24) How likely are they able to have access? Select for each recipient mentioned its likelihood corresponding box.
Very Unlikely / Unlikely / Somewhat Unlikely / Undecided / Somewhat Likely / Likely / Very Likely

27
25. Regardless of whether or not they are able to, who, if anybody, do you think wants to have access to your data on Facebook?
   Nobody / The following: [OA] / Don’t know.

26. (If Yes to Q. 24) How concerned are you about anyone other than the intended recipients being able to gain access to your Facebook data? Select your level of concern for each unintended recipients you have mentioned. [SS]
   Not at all concerned / Slightly concerned / Moderately concerned / Very concerned / Hugely concerned / Don’t know

27. Are you interested in tools or technologies that would prevent unintended recipients from having access to your Facebook data? [SS]
   Yes / No / Don’t know

28. Which strategies or mechanisms do you know, even if you do not use them, to prevent unintended recipients from having access to your messages and information you send or post on Facebook?
   None / The following: [OA]

   – (If Yes to Q. 28) Which ones do you use?
   None / The following: [OA]

29. (If None to previous question) Why would you, or would not, use such a tool? [SS]
   I would install one of those tools because... [OA] / I would not install one of those tools because... [OA]

30. How concerned are you about the fact that Facebook has control over and is able to access all the information you post on the site? [SS and explain why]
   Not at all concerned / Slightly concerned / Moderately concerned / Very concerned / Hugely concerned / Don’t know

31. Have you ever refrained from posting information on Facebook for privacy reasons?
   Yes / No / Don’t know

32. How concerned are you about the fact that Facebook may suffer from a security breach and all or part of your messages, posts and photos become publicly available? [SS]
   Not at all concerned / Slightly concerned / Moderately concerned / Very concerned / Hugely concerned / Don’t know

33. Do you know any strategy or mechanism that could prevent your data from becoming publicly available in such a case? [SS]
   No / Yes (Which ones?)
34. On Facebook, what would you say is the level of privacy protection from Facebook itself? [SS]
   Extremely low / Very low / Low / Neither low nor high / High / Very high / Extremely high / Don’t know

35. How worried are you by the fact that intelligence and law enforcement agencies (such as the NSA, the FBI) may have access to your Facebook data? [SS]
   Not at all concerned / Slightly concerned / Moderately concerned / Very concerned / Hugely concerned / Don’t know

36. How interested are you in any tool to prevent all unintended recipients (Facebook, law enforcement agencies, etc.) from having access to your data on Facebook? [SS]
   Not at all interested / Slightly interested / Moderately interested / Very interested / Extremely interested

B Exit Questionnaire

B.1 SUS

Choose the option that describes your opinion about Scramble! best:
[Strongly disagree / Disagree / Neither Agree nor Disagree / Agree / Strongly Agree]
- I think that I would like to use this plug-in frequently
- I found the plug-in unnecessarily complex
- I thought the plug-in was easy to use
- I think that I would need the support of a technical person to be able to use this plug-in
- I found the various functions in this plug-in were well integrated I thought there was too such inconsistency in this plug-in
- I would imagine that most people would learn to use this plug-in very quickly
- I found the plug-in very cumbersome to use
- I felt very confident using the plug-in
- I needed to learn a lot of things before I could get going with this plug-in

B.2 Other questions

1. Can you describe, in a few words, your experience using Scramble!? [OA]

2. What would be the advantages, if any, of using a tool like Scramble! over, or in combination with, other privacy controls? [OA]

3. Scramble! encrypts messages before you send or post them on Facebook. Do you think this
is a secure way to prevent unintended recipients from having access to them? [OA]

4. What do you think are the differences, if any, between what Scramble! does and the privacy settings of Facebook?

5. How would you grade the following tools: Facebook’s privacy settings / Scramble! with respect to:
   - safety?
   - reliability?
   - trustworthiness?

6. Overall, explain in a few words why you find a tool like Scramble! to be useful or not useful. [SS] + [OA]
   *I find tools like Scramble! useful because... / I find tools like Scramble! not useful because...

7. Do you see yourself using a tool such as Scramble!? [SS]
   Never / Rarely / Sometimes / Often / All of the Time / Don’t know

8. Which cases, purposes or people do you think a tool like Scramble! could be useful for? [OA]

9. What, if anything, did you like about Scramble!? (You will be asked about what you did not like in the question below) [OA]

10. What, if anything, did you dislike about Scramble!? [OA]

11. What features did you miss in Scramble! or you think that such a tool should have? [OA]