Monetary valuation of people's private information

Vashek Matyas
Faculty of Informatics
Masaryk University
Brno, Czech Republic
matyas@fi.muni.cz

Marek Kumpost
Faculty of Informatics
Masaryk University
Brno, Czech Republic
kumpost@fi.muni.cz

ABSTRACT

In this paper we present the results of an experiment with the primary goal to assess the economic value that people attach to their private information. The private information considered in this experiment was related to the usage of online communication tools (emails and instant messaging), which would be collected by a proprietary monitoring software. People were asked to bid for the remuneration they would require for participating in such an experiment. We estimated the monetary value of private information in three general scenarios – data collected for academic research, for commercial purposes, and for governmental purposes.

Categories and Subject Descriptors

K.4 [**Computers and Society**]: Public policy issues—*privacy*; K.6 [**Management of Computing and Information Systems**]: General—*economics*

General Terms

Privacy, value.

Keywords

Privacy, online communication, value, auction, survey, experiment.

1. INTRODUCTION

The price of privacy is a notion used quite often, but there are always doubts about the correctness of the price itself. Privacy is a very complex notion and as such it is very difficult to evaluate it in the whole complexity. We therefore took an approach of defining one rather simple facet of privacy and came out with the following study, focusing on the use of online communication tools like emails or instant messaging.

The main goal of the study was to find out how people value information about their usage of online communication tools like emails or instant messaging. We organized this study for the FIDIS[1] project we were part of. This fact allowed us to organize another experiment quite similar to the one organized in 2006. Results of our first experiment were published in [9], our second experiment was presented in FIDIS deliverable D13.12[2] [14].

Even though people are increasingly aware of the need to secure and control their private information, they seem to be willing to disclose information for a very modest reward. A typical example is the popularity of loyalty cards, allowing superstore chains to monitor customer purchases regardless of the store used for shopping. In exchange, customers may get discounts for regular shopping or collect bonus points that are exchangeable for goods.

Privacy requirements are very hard to satisfy in information systems. One can implement access control mechanisms in trusted systems, but once the data leaks it is very hard to track their usage. There are two very different approaches to privacy problems. The first one uses the legal system to punish unlawful breaches of privacy. The second approach is to implement technical measures to guard the privacy of data stored and processed in information systems. The latter takes into account that law enforcement might be too slow or ineffective (due to the complexity of information technology) to enforce privacy requirements.

However, the technology needed to preserve privacy is very expensive. This is reflected in computational complexity, communication overheads and delays. Despite declaring some sensitivity to their personal information, users are often not prepared to accept the overhead or cost of privacy enabled technologies. The market failures of flagship products like the Freedom network [1, 2], an anonymous web browsing solution, illustrate this.

Online communication tools such as email or instant messaging systems offer no privacy protection towards the service provider. Network administrators can observe, analyze and track users while they are active in their networks. The availability of these very detailed data opens concerns with respect to abuse, of which many users are not aware since

[1]FIDIS – "Future of Identity in the Information Society" was a 5-year Network of Excellence research grant of the EU 6th Framework Program (www.fidis.net). Its objective was to research the changes that the concept of identity has been undergoing in the developing European information society.
[2]Document is accessible via http://www.fidis.net.

the data collection is invisible to them. Tools for online communication are widely used and our assumptions were that people can sense the value of their privacy in the online world.

The way in which people describe their attitude to information technology alone cannot give us the full picture of their real attitude to privacy [12]. For this reason we turn to experimental psychology and economics to establish the "value" that individuals attach to their privacy. We first generalize the study by Danezis, Lewis, and Anderson [3] on the value of location information, considering a larger and more varied population across multiple EU countries – the original location privacy study [3] was done at Cambridge University and was of a considerably smaller scale. By measuring the same aspects of privacy, we can compare our results, and establish whether people's attitudes to privacy are uniform across the EU.

In the light of our first experiment, which was conducted in 2006 [9], we prepared a new study to analyze other types of private information. The second study focused on the usage of online communication tools such as email and instant messaging. Both studies together allow us to observe trends in people's privacy perception.

Our studies were conducted in the context of, and with the help of, the FIDIS network. Besides the fact that partners in different European countries have been instrumental in allowing us to gather data across Europe, this also allowed us to undertake a large-scale study.

Previous studies on people's attitudes to privacy [3, 4] have shown that quantifying the value that people attach to their information privacy is a difficult problem. We chose, in the tradition of the earlier study [3], to use an auction, in which people are offered to sell their private information. The selected auction is based on the "multiple sales by sealed bid" principle described in [11] (participants have no information about the bids of others). In this type of auction, participants are more motivated to report the true monetary value that they attach to their privacy because bidding too high may exclude them from the study and its rewards, while too small bids may not make it worth it to take part in the experiment.

The key idea behind the auction methodology used in our experiment was to create conditions that push the upper and lower bounds of bids (sums for which participants agree to provide their data) as close as possible. The lower bound is pushed up by the participants' interest in getting as much money as possible, while the upper bound is squeezed by a possibility to be left out from the auction. The sum that the selected bidders obtain is equal to the amount of the lowest not accepted bid – this may bring in some bias (primarily because of the two potential types of bidders – those being motivated by money on one hand and those being motivated by the possibility to take part in such experiment on the other hand) but this is unavoidable.

It has also been observed that, if asked directly, individuals tend to overemphasize their privacy concerns [5]. As a result, asking subjects about their privacy sensitivity may provide data that is generally not matched by their actions. For this reason we *deceived* the participants of our studies, and made them believe that they were applying to take part in a study of mobile phone usage (our first study). The fictitious study required participants to agree to be tracked for a period of a month, by allowing us to record their location in five minute intervals.

The cover story for this experiment was a study of the usage of online communication tools for email and instant messaging through an installed application certified by a third party (audit firm), and the information recorded would be all the traffic data (no content) of these communications. We further told participants that there was a limited budget for the studies, and that we would use an auction to select the participants. The lure of real financial returns, and the auction structure of the studies, gives participants incentives to state their real privacy valuation.

Our goal has been to provide a quantification of personal information (self-)valuation in monetary terms. Sociological analysis is out of the scope of this paper.

The rest of this article is organized as follows. Section 2 describes the preparation of the experiment – the auction principle, the cover story that we used and the technical details of the online web questionnaires on which the experiment was based. The main contribution of this paper is presented in Section 3. Section 4 concludes the article.

2. DESIGN OF THE STUDY

It is very hard to find a way that would allow to obtain realistic data about the privacy value. When you let people say a number (in euros, pounds, or crowns) they will quite probably give you a number that is relatively high. Firstly, they know what you are interested in and naturally they do not want to look like someone ignorant about her/his privacy. Secondly, there is no motivation to keep the delivered number low – it is very hard to say – "Hey friend, it is too much what about just half of what you said?" – without introducing another bias.

We have expected that the approach (the similar approach as in our previous experiment targeting the price of location privacy) – auction for participation in an experiment related to a quality of mobile phone networks – could eliminate both problems mentioned above and allow us to obtain quite realistic data.

We have therefore also decided to use a small deception – claim that we are interested in research of usage of online communication tools – namely the email and instant messaging systems. We believed that we would get reasonable data. On the other hand, we were also very concerned with ethical issues of this approach. We have consulted the issue with experts in social sciences and the responsible universities' bodies for ethical issues. To make it short, we were told that it is quite usual to use deceptions if these are explained afterwards.

The whole study was thus hidden under a cover story stating that it is going to be a sociological study about the use of online communication. A similar introductory e-mail was

sent out to university students in four countries (translated to local languages and with proper name of local partners of the study). Our potential participants were mainly from the academic environment since we asked our partners to spread the information about the experiment within their institutions. We may also expect some non-academic participant, but there was no clear question in the web questionnaire asking for academic/non-academic status of the participant.

The questionnaire was online for two weeks and we recorded a majority of responses during the first week. We think that there will not be any considerable increase of answers if the questionnaire would have been online for one or two more weeks.

2.1 Design of the web questionnaire

The study was implemented using web forms with questionnaires. We advertised it using email, university information systems, and posters addressed to a university audience. The text we used for propagating the study can be found in the Appendix A. The text was published to university students in five countries, translated into the local languages. Access to the questionnaire in the experiment was without any additional authentication. We changed the requirement for authentication after the first experiment as we got some indication that the necessity of authentication might have discouraged some participants.

On the first page of the web application, users could choose the language of the questionnaire (the available languages were Czech, English, Slovak, German and Flemish). The web forms were up for two weeks. The introductory text (similar to the text used for propagating the experiment) presenting the experiment was followed by the question "Do you want to take part in this study?", and four possible answers:

1. Yes, with a PC only.
2. Yes, with any mobile device(s).
3. Yes, with both PC and mobile device(s).
4. No, I do not want to participate.

If the subject selected any of the first three options the first set of questions was displayed. These were designed to support the cover story of the fictitious study but also to obtain data we were interested in. We asked the participants about their age, gender, device possession (own or shared hardware) and the level of IT knowledge. The key question was: "How much money do you want for being monitored for two weeks (please put only a number in € and specify only those scenarios you are interested in)?"

1. For email traffic data (no message body) (€):
2. For instant messaging traffic data (no message body) (€):
3. For all traffic data (€):

After the first set of questions (and the first scenario), two additional special scenarios for the experiment extension were introduced. Participants had the possibility to opt out on any of these two scenarios. We also asked participants to fill in their email address so that we can contact them in case they will be selected for participation in our experiment.

1. We will consider to process the data within the FIDIS research consortium and provide some answers to queries or summaries in an aggregated form to a commercial subject who entered in a contractual relation with us. (No direct access to the data). What amount of money (in €) would you request for your participation in such case?
2. This is a hypothetical issue: As you might be aware, our data collection might be of some use for system training and improvement in detecting terrorist activities. Imagine that we could provide the data to your national government (only) to let them improve their terrorist activity detection and tracking tools. Although we do not plan to do this, how much money (in €) would you ask for participating under these circumstances?

Option 4 in the introductory part was for those visitors who did not want to participate in our study. After selecting this option, users were asked about the reasons why they did not want to participate in the experiment. The possible options were:

1. I do not have appropriate hardware equipment.
2. I do not have time.
3. I do not see the value of such study.
4. Such study is not ethical.
5. I do not trust your intentions with this study – but I would trust another institution, namely:
6. Other reasons: <Text array for free comments.>

3. RESULTS

There were 1080 people (or robots) who saw the introductory text of our second study. These visitors were given the choice from five language versions: Flemish, Czech, German, Slovak and English. The numbers in the Table 1 reflect the popularity of each language version.

Lang.	BE	CZ	DE	SK	EN	All
Share	2.8%	33.5%	6.6%	43.5%	13.5%	1080

Table 1: Chosen questionnaire language.

Lang.	BE	CZ	DE	SK	EN
Share	3%	40.7%	7%	31.8%	17.5%

Table 2: Percentage of participants willing to participate in the study.

The number of visitors willing to participate (regardless of the device selection) for each of the available languages are

in Table 2. The total number of participants was 428, which is 40% of those who saw the introductory text. 26% of participants filled at least the first tracking scenario, in which the data would only be used for academic purposes. 80% of the participants who filled the first scenario were males. If we compare the drop-out rate with that of our first experiment (location privacy), we can see that the percentage of visitors willing to participate (48%) was higher in the first experiment. Such decrease can be caused by two factors: 1) visitors were more sensitive to disclosing this kind of information than location data; or 2) similarity with our previous experiment (we noticed several why-did-you-not-participate reasons explicitly stating this fact).

Lang.	BE	CZ	DE	SK	EN	All
Share	3.5%	33.4%	15.8%	36.8%	10.5%	57

Table 3: Percentage of participants who explicitly said that they did not want to participate in the study.

The percentage of visitors who explicitly said that they did not want to participate in the study is shown in Table 3 (the numbers reflect the chosen language version). We further analyze the answers provided as reasons for not participating at the end of this section.

Let us also summarize the results from questions that were not principal for our study. These questions (devices used in the experiment, age of a participant, IT knowledge and shared vs. own hardware) were part of the questionnaire primarily to support the idea of the cover story. The split of the results of these three additional questions are in Tables 4, 5 and 6. 89.5 % users indicated own/dedicated and 10.5 % shared hardware. Majority of our participants were between 18-24 years old. This corresponds to the fact, that the experiment was promoted primarily in the academic environment and therefore majority of our participants were university students. The level of stated IT knowledge again corresponds to the academic environment, because majority of our participant stated medium or advanced level of their IT knowledge.

Lang.	PC only	Mobile devices only	Both types
Flemish	7	2	4
Czech	114	16	44
German	21	2	7
Slovak	106	12	18
English	42	9	24

Table 4: Devices selected for participation.

Under 18	18-24	25-34	35-44	55-64	over 65
0.7 %	85.6 %	10.2 %	3.1 %	0.4	0 %

Table 5: Age of participants.

3.1 Why not participating in the study

There were 57 visitors who explicitly stated that they did not wish to participate in our study. We prepared a short list of questions to find their reasons for not being interested. We received 45 answers from those visitors. Offered options as well as numbers of received answers were:

Basic	Medium	Advanced	Professional
4.9 %	28.2 %	48.6 %	18.3 %

Table 6: Stated IT knowledge of participants.

	First bids – males			First bids – females		
	email	messag.	all	email	messag.	all
1st qt.	10	9.5	12	10	10	15
2nd qt.	32.5	25	50	30	35	50
3rd qt.	100	100	200	275	150	300

Table 7: First scenario – academic use of data.

1. I do not have appropriate hardware equipment (3).
2. I do not have time (13).
3. I do not see the value of such study (12).
4. Such study is not ethical (11).
5. I do not trust your intentions with this study (6).

3.2 The main results

Our main goal was to evaluate the monetary value that people ask in exchange for being monitored by a special software ("spyware"). We collected bids for three scenarios: (1) data collected for academic purposes only; (2) data may be used to assist a set of commercial partners; and (3) data may be used to assist national governments for national security purposes. In each of these scenarios the information that would be recorded consisted of: email traffic data; online messaging traffic data; or all available traffic data.

We already discussed numbers of participants and the split of languages. Table 8 shows the relative numbers of participants with regard to answers (individual scenarios) they provided during the study.

Table 7 shows the distribution of the monetary compensation (all values are in euros) asked in the first scenario. In Table 7, the "email" column represents the email traffic monitoring option; the "messaging" column the online messaging traffic monitoring, and the "all" column represents monitoring all traffic data. Table 7 shows these values separately for males and females. It is interesting that in a majority of the cases the sum of email and messaging monetary compensations is higher than all traffic data. We can also observe that in case of the academic use of data females were bidding a little bit higher in the second and third quartiles. This could be an indication of a stronger feeling about privacy among females, but we must keep in mind that there were only 20% of females who filled the questionnaire for the first scenario.

We decided to use quartiles for comparing bids instead of minimal, maximal and average values. The reason is the existence of extreme values that would negatively influence medium values. For instance for the first bid such extreme monetary compensation was €1 000 000.

Regarding the number of visitors who filled the first scenario bids, we can see that there is not much difference between the bids placed by males and by females, except for the third quartile. 23 participants (10%) explicitly expressed in the

	will participate	1st form	2nd form	3rd form
Percentage w.r.t. intro text numbers	40 %	26.3 %	20.8 %	20.7 %
Percentage w.r.t. participants	100.0 %	57.0 %	45.2 %	44.9 %

Table 8: Percentage of participants, who saw the intro text (or confirmed participation) and percentage of answers in each scenario.

	First bids (€)			Second bids (€)			Third bids (€)		
tracking data	email	messaging	all	email	messaging	all	email	messaging	all
1st quartile	8.8	8.5	11.1	10	10	15	10	10	15
2nd quartile	20	25	40	40	40	50	50	50	60
3rd quartile	100	80	150	100	100	200	200	200	400

Table 9: Bidders in all three scenarios (academic, commercial and governmental).

	First bids (€)			Second bids (€)		
	email	messag.	all	email	messag.	all
1st qt.	10	8.3	10.4	10	10	15
2nd qt.	20	22.5	40	40	40	50
3rd qt.	100	80	150	100	100	200

Table 10: Second scenario – commercial use of data.

	Second bids – males			Second bids – females		
	email	messag.	all	email	messag.	all
1st qt.	10	10	15	10	10	10
2nd qt.	40	40	50	40	35	40
3rd qt.	100	100	200	150	70	127

Table 11: Second scenario – males vs. females.

questionnaire that they will not participate in the scenario extension (the data would be used to assist a commercial subject we have a business contract with) but the real drop-out rate was 27% (i.e., including participants who closed the questionnaire and decided not to continue, but did not provide an explicit indication in the questionnaire).

Table 10 shows the bids placed in the second scenario, in which the gathered data would be used to assist a commercial subject with whom we have a business contract. We also show the first scenario bids of those visitors who decided to participate in the second scenario of our experiment. The highest increase can be observed in the second quartile (about 50% from academic to commercial data usage). Table 11 shows the bids classified according to the gender of the participant.

Finally, the data for the third scenario considered the possible use of data by the national governments to improve their terrorist-activity-detection techniques. 41 participants (18%) explicitly stated that they did not wish to participate if the data was to be provided to their national governments. The real drop-out rate for this experiment was 28%.

The data in Table 9 shows the results for the third bid as well as for the two previous bids, taking into account those participants who provided answers to the third experiment scenario. Table 12 again provides the comparison of male and female bids. And again, we can observe males bidding higher than females.

3.3 Diagrams of bids

In this section we provide diagrams of bids for the first and third scenarios. Diagrams are quite helpful in observing trends of bids and allow for quick comparisons. The y-axis in the diagrams shows % of the saturated bidding population. We decided not to split all bids according to national variants since those sets are too small to provide conclusive results.

Figure 1(a) shows the results of the first bid in all three scenarios for those visitors who provided answers in all three scenarios. These are the visitors who did not explicitly state the I-do-not-want-to-participate option. Line 1 shows the results for the academic use of data (neither the data nor the results will be revealed to any other subjects); Line 2 for the commercial use of data (the data could be used to assist a commercial entity); and Line 3 for the scenario in which data could be used to assist national governments (to improve mechanisms for terrorist detection). We can see that the value of bids is increasing as the use of acquired data changes from academic to national government.

The diagram for the 2nd bids (online messaging) in all three scenarios is very similar to the email monitoring case. In order to examine this observation, we performed the Kolmogorov-Smirnov test for testing probability distributions of two samples (whether both sets have the same probability distribution or not) [13]. We first tested the distributions of the first bids (email tracking) and second bids (online messaging). The hypothesis that these two sets have the same distribution was not rejected on a significance level $\alpha = 0.05$. Average values for both sets were almost the same – 166.96 and 160.16, respectively. Based on this information, we can say that the value of both types of information is on the same level for our participants. The expected change occurred in the diagram of the 3rd bids (tracking all communication data) where we expected the highest bids (Figure 1(b)). We performed the same test (Kolmogorov-Smirnov) for the second bids (online messaging) and third bids (all traffic data) to observe the expected increase of required monetary compensation required by participants. The hypothesis, that both sets have the same distribution was not rejected on a significance level $\alpha = 0.05$, but the average values in this case were significantly different – 160.16 and 288.39, respectively. Based on this observation, we can conclude that the overall required monetary compensation for all traffic data is significantly higher than for the email or instant messaging.

	Third bids – males			Third bids – females		
	email	messag.	all	email	messag.	all
1st qt.	10	10	17.5	9	9	14
2nd qt.	50	50	80	30	32	46
3rd qt.	200	200	450	162	162	332

Table 12: Third scenario – males vs. females.

If we compare Figures 1(a) and 1(b), we can observe that the majority of visitors do not differentiate between the types of tracking data as the differences at the beginnings of all diagrams are very small. As we described in the previous paragraph, there are no differences between the first and second bids. More significant differences in the price can be visually observed in the upper half of the participants.

4. CONCLUSIONS

Let us summarize the most important results of our experiment. We received almost 300 responses for at least the first scenario (academic use of data) from at least five countries (in terms of the selected language variant of the web questionnaire). The claimed goal of the experiment was to deploy a special piece of software on participants' hardware that would observe the use of online communication tools. We asked the participants for the monetary compensation they require for taking part in such experiment. We evaluated the results and provided several tables and graphs for better understanding.

The second quartiles in the first scenario (non-commercial use of data) may be considered as the main result. The median monetary compensation for being observed through the email traffic data is €30 and the same price is for instant messaging. All tracking data together is "more expensive", namely €50 (median). We can also see that in some cases instant messaging traffic data is priced higher than email traffic data. All traffic data is always the most expensive case. We provided a comparison between male and female bidding and the results showed no considerable differences between these.

The price for being monitored for two weeks was €50 (all tracking data for academic purposes). If we consider the commercial use of data (second scenario) then the required monetary compensation (median) was €50 (all tracking data). It may look like the values did not change much in the experiment, yet let us consider the drop-out effect of those privacy sensitive when considering commercial use of the data. With valuations of only those who would participate in both scenarios we can observe a change from €40 to €50.

We observed an increasing tendency to opt out as the purpose of data collection changed from academic to commercial (1/10 of participants did not wish to continue) and from commercial to governmental usage (1/5 of participants). The real drop-outs were actually a little higher (nearly 30% in each step). If we look at the required monetary compensation for all tracking data (academic purposes) of those, who did not wish to continue (explicitly stated or left the questionnaire uncompleted) with the commercial option, then the value was €40. €50 is the required compensation for the commercial option of those who decided not to continue with the governmental variant.

We also compared bids of those answering more than just for the first scenario (the other scenarios were: data will assist some commercial subject or the national governments) and the result confirmed our expectations. The required value for participation has an increasing tendency as the scenario changed from academic use of data to commercial use of data and finally to the scenario where we hypothetically provide the data to national governments. This shows a clear increase in traffic data valuation and a decrease in willingness to provide such data when changing the purpose from academic research, through commercial exploitation, to the use by governments. We believe that this also indicates a decrease in trust of subject to various types of data processing agents.

One may argue that a different order of the three scenarios can lead to different biases (monetary valuations). We were aware of this risk but we are still convinced that the used structure and order of scenarios was the best compromise for our purposes. Personal interviews with all involved participants could help to get unbiased information regarding the value of their privacy on one hand, but this approach would not allow us to make the study that wide.

Let us also briefly compare the results with our previous experiment (the price of location privacy). In the location privacy experiment, we received 1214 answers out of almost 2600 visitors. In the communication traffic study, the numbers were 1080 visitors and 284 participants who provided their answers. Regarding the monetary value, the median in the first experiment was €25 for one-month tracking. In the second experiment, the price for being monitored for two weeks was €50 (all tracking data).

5. ACKNOWLEDGMENTS

The authors would like to thank Jozef Vyskoc, Claudia Diaz, Sandra Steinbrecher, Dan Cvrcek and Eleni Kosta for their fruitful discussions while preparing the questionnaire for the experiment and for their help with translations of the web GUI into national languages.

6. REFERENCES

[1] Boucher, P., Shostack, A., Goldberg, I.: Freedom system 2.0 architecture. Whitepaper, Zero-Knowledge Systems, Inc. (2000)

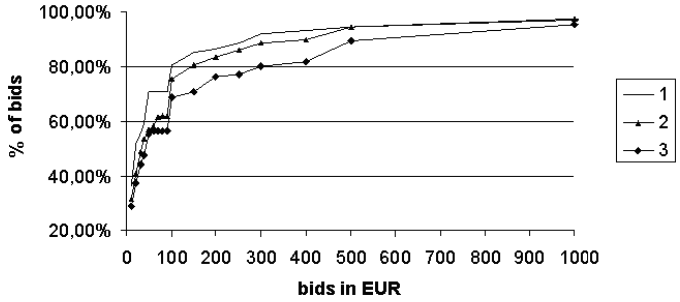
[2] Law, G.: Anonymity declines as zero-knowledge ends web service. PC World. (2001)

[3] Danezis, G., Lewis, S., Anderson, R.: How much is location privacy worth? In: Fourth Workshop on the Economics of Information Security. (2005)

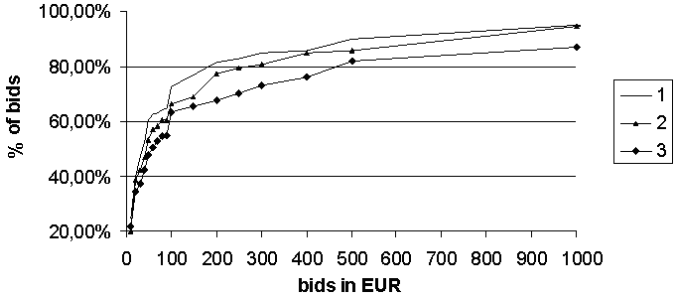
[4] Hann, I.H., Hui, K.L., Lee, T.S., Png, I.: The value of online information privacy: Evidence from the USA and Singapore. In: International Conference on Information Systems. (2002)

[5] Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security & Privacy **3**(1) pp. 26–33. (2005)

[6] Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In Breese, J.S., Feigenbaum, J., Seltzer, M.I., eds.:



(a) Diagram of the 1st bid (email tracking) in all three scenarios.



(b) Diagram of the 3rd bid (tracking all communication data) in all three scenarios.

Figure 1: Distribution of bids for all three study scenarios. The y-axis shows % of the saturated bidding population.

ACM Conference on Electronic Commerce, ACM pp. 21–29. (2004)

[7] Eagle, N.: Machine Perception and Learning of Complex Social Systems. PhD thesis, Massachusetts Institute of Technology. (2005)

[8] Danezis, G.: Government communication illegally wiretapped in Greece. EDRI-gram http://www.edri.org/edrigram. (2006)

[9] Cvrček, D., Kumpošt, M., Matyáš, V., Danezis, G.: A study on the price of location privacy. In WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 109–118. ACM. (2006)

[10] Kumpošt, M., Matyáš, V.: Location privacy pricing and motivation. In Christian Becker, Christian S. Jensen, and Jianwen Su, editors, 8th International Conference on Mobile Data Management (MDM 2007), pp. 263–267. IEEE. (2007)

[11] Vickrey, W.: Counterspeculation, auctions and competitive sealed tenders. The Journal of Finance 16:8–37. (1961)

[12] Berendt, B., Günther, O., Spiekermann, S.: Privacy in e-commerce: stated preferences vs. actual behavior Commun. ACM 48:101–106. ACM. (2005)

[13] Sheskin, David J.: Handbook of Parametric and Nonparametric Statistical Procedures. Chapman & Hall/CRC. (2007)

[14] Kumpošt, M., Matyáš, V.: D13.12: The value of tracking data. The FIDIS NoE project (online: http://www.fidis.net/resources/fidis-deliverables/). (2009)

APPENDIX

A. INTRODUCTORY LETTER

This is the homepage of a European-wide study organized within the FIDIS (Future of Identity in the Information Society - http://www.fidis.net) NoE (Network of Excellence). This study involves gathering traffic data for a number of volunteers over a period of 30 days.

We are looking for people who will be tracked for the purpose of a sociological study about the use of online communication. The study is somewhat similar to what have been done by e.g. researchers at the Northeastern University (link).

Teams from the FIDIS project in each country (mainly research and academic environment) will provide (or install if you want) a special software that will be used to collect desired data. This software will be provided to all participants in both source code and executables, and its functionality is verified by an external auditor. Data will be collected periodically and there will be regular transfers of observed traffic to our collection servers. We will provide all participants with a removal tool (or members of national teams will remove the software manually) once the experiment is over.

Each participant in the study will receive a monetary compensation, and we are running an auction to select those who will take part. We invite you to submit a bid for the amount of money you require to take part in such a study. As our budget is fixed and limited, successful bidders will be those who bid the lowest amounts, and each will be paid the amount of compensation demanded by the lowest unsuccessful bidder.

We have deployed several mechanisms to detect cheating and we reserve the right not to pay the participant if any kind of cheating is detected.

You are giving consent for this kind of observation by participating in our study in accordance with your national law on data protection.