Snowden's revelations and the attitudes of students at Swedish universities

Iordanis Kavathatzopoulos
Uppsala University. iordanis@it.uu.se

Ryoko Asai
Uppsala University and Meiji University. rynjyu@gmail.com

Andrew A. Adams
Meiji University. aaa@meiji.ac.jp

Kiyoshi Murata
Meiji University. kmurata@meiji.ac.jp

Abstract.

Purpose – Mapping of Swedish students' attitudes toward Snowden's revelations and their effects in the political and socio-cultural environment of Sweden.

Design/methodology/approach – A questionnaire was answered by 190 Swedish University students. The quantitative responses to the survey were statistically analysed as well as qualitative considerations of free text answers.

Findings – Swedish students had a high level of knowledge of Snowden revelations, they actively searched for information, they gave a positive judgement of Snowden's actions and they were willing to follow his example in Sweden but not the US. They trusted their country and most of its institutions and authorities except for secret service agencies and Internet and computer software companies.

Practical implications – Design of education for university students, especially in Information Technology programs.

Social implications – Developing and applying policies on privacy, surveillance and whistleblowing.

Originality/value – This study is part of a bigger international study to map students' attitudes toward Snowden's revelations and their opinions about privacy, surveillance and whistleblowing opening up for cross-cultural analyses.

Keywords Edward Snowden, privacy, state surveillance, social impact, Sweden

Paper type Research paper

1. Introduction

In June 2013, The Guardian in the UK and The Washington Post in the US began publishing internal electronic documents from the US' signals intelligence (SIGINT) organisation the National Security Agency (NSA), provided to them by Edward Snowden who had obtained the documents while employed as a systems administrator at the NSA for contractor Booz Allen Hamilton. As they have done previously, the NSA and other parts of the US government generally will not confirm or deny the

validity of the documents, however on 21st June 2013, the US Department of Justice charged Snowden with violating the Espionage Act. The activities detailed in the documents included activity undertaken by the NSA and its main SIGINT partner the UK's Government Communications Headquarters (GCHQ), and with the SIGINT agencies of three former British colonies (Canada, Australia and New Zealand), as well as joint activities with similar agencies in other countries such as Germany's Bundesnachrichtendienst (BND).

In 2014, the Pew Research Center (Madden, 2014) undertook the first of a number of surveys of US citizens' attitudes to Snowden and the documents he revealed. In particular, they asked questions such as whether respondents believed that Snowden's revelations had served or harmed the public good, whether Snowden should be prosecuted or not. Inspired by these surveys, a group of academics at Meiji University in Tokyo developed a pilot survey deployed in Japan and Spain using students as the primary research population (for reasons of resource constraints) and conducted follow-up interviews. The results of this pilot survey are presented in Murata, Adams and Lara Palma (2017). Having revised the survey after analysis it was deployed with the cooperation of local academics in Mexico, New Zealand, Spain and Sweden (in English), and in translation in Japan and Germany. With the aid of graduate students studying in Tokyo, it was also translated into Chinese and deployed in Taiwan (using traditional Chinese characters) and the People's Republic of China (using simplified Chinese characters). The choice of countries was a combination of deliberation and pragmatism. The following countries had suitable resources available: New Zealand was chosen as a Five Eyes member; Germany, Spain and Sweden provide an EU perspective; Mexico provides a US neighbouring perspective as well as a Spanish-influenced culture outside Spain; and Japan, China and Taiwan provide a South East Asian viewpoint. This paper presents the results of the survey in Sweden.

1.1 Roadmap

This paper focusses on the local content of Snowden's revelations in the rest of this introduction section. In Section 2 an overview is given of the general cultural and historical context of government surveillance. Section 3 gives an overview of the survey and of respondent's demographic information, while section 4 provides the detailed survey results. Section 5 presents the political and cultural impacts of Snowden as perceived by the authors, while the final section gives some conclusions and identifies avenues for future research.

1.2 Snowden's Revelations and Sweden

People in Sweden have a high level of knowledge about new technology as well as a strong conviction about their society being supportive of individual rights and freedom. A combination of these two generates a strong interest in issues of the relationship of technology, society and human life, especially among younger people in the country. Sweden is one of the oldest countries in Europe with strong traditions and a rather homogenous culture. Snowden's whistleblowing and revelations have been perceived rather positively on an ideological and moral level. He was awarded the Swedish Right Livelihood Award 2014, which is described as an alternative Nobel Prize, with the description: "... for his courage and skill in revealing the unprecedented extent of state surveillance violating basic democratic processes and constitutional rights." (Right Livelihood Award, 2014). This general positive attitude did not, however, lead to any concrete political action, for example, the granting of political asylum. Snowden was not even able to visit Sweden and attend the prize award ceremony in person.

This is illustrative of something of a double standard in Sweden regarding individual rights: on the one hand a high profile and outspoken supporter of freedom; on the other hand a country with a long history of surveillance in the service of preserving its ideological and political homogeny.

2. Background: Historical Surveillance in Sweden

Systematic surveillance in Sweden started in the 19th century by the government to handle certain risks connected to the rising labour movement and to a growing number of foreign citizens entering and living in the country. However, this surveillance organization soon sought and gained more independence from its principal, the government of the day, promoting its own importance and necessity (Langkjaer, 2011).

Later on, the Bolshevik power taking in Russia and the establishment of fascist and Nazi regimes in several European countries acquired many sympathizers in Sweden which had to be under surveillance.

Even after the Second World War until today there are plenty of reasons for the government to continue with the surveillance activities, like the spread of Communism in the fifties, radical political movements in the sixties and seventies, left-wing terrorism in the seventies, right wing extremism later, and now Islamist terror (Eliasson, 2006).
This has been easily accepted and integrated into normal life in Sweden although it wants to see itself as a progressive and open society. Probably the reason is that this was not anything new from the start. Sweden is, and in the 19th century it was even more, a Lutheran society in which the detailed surveillance of individual life was seen as something normal. The priests of the church kept track of the behaviour and the thoughts of their parish members by regular catechetical meetings in their homes. On the societal level no other beliefs or even Christian churches were allowed, with some few exceptions like Judaism (Kent, 2008).
Regarding surveillance, Sweden has had for decades a close cooperation with American security agencies, despite being a neutral country. Sweden locates in a geo-strategically important position to access data traffic in the Baltic Sea, which has been very important since the 1940s. Sweden was supported by US military technology and received far-reaching security guarantees in the 1960s (Agrell, 2000, 2013). In the documents revealed by Snowden, Sweden is "one of the countries that's the closest to the US when it comes to surveillance" (The Local Sweden, 2013). This cooperation has been expanded significantly over the past five years. The common operations are about surveillance on Russian military and other activities of interest, but there is also cooperation on surveilling the Internet and other civilian communications (Reuters, 2013; Shilton, 2013).
Surveillance and control of citizens is the one side of the coin. The other side is the individuals' trust in society and state. Although trust in society and government have been declining globally in recent years, Swedish people still strongly believe their country is trustworthy (Holmberg, 1999; OECD, 2013). In Sweden people perceive the state as a kind of parent figure and they expect intervention in order to resolve important issues and to support them in various ways. Therefore surveillance can be tolerated, if not fully accepted. Since community is understood as something principal or at least superior to the individual, collectivism as ideology and political correctness play an important role in supporting the community and keeping together the group, which benefits the individuals.
Egalitarianism, homogeneity and collectivism are salient features of the Swedish society, with a long tradition. The individual is loyal to the group. It may be that the cold climate or the harsh conditions of the Nordic country made the group so important. Anyway, diverging ideas or behavior by an individual risk the cohesion or the actions of the group and threaten the well-being of its members, therefore they cannot be tolerated (Daun, 1996).
Political correctness has its roots in Lutheran tradition but it is still dominating Swedish society today. It is important to keep in mind that political correctness refers to whatever for the moment is established as the right thing, morally, ideologically or politically.
Homogeneity and political correctness make it very difficult for dissent voices to be uttered or to be listened to. Anyone who dares to utter anything provocative to the established order may be treated as a disloyal, a traitor or even as a lunatic. Still Sweden has passed a law making it compulsory for government private employees to report to the media irregularities, wrongdoings and bad conditions in their working place. Furthermore, the law protects the whistleblower and makes it illegal for the government to search for the leak (Regeringskansliet, 2014; Transparency International, 2012).

2.1 Individual rights

Despite the fact Sweden being a homogeneous society, individualism and a strong feeling of privacy have also a long tradition in Sweden. Sweden is a big country with a small population. Today more people live in the cities, previously the great majority lived in farms spread all over the huge country, often in a relatively long distance from each other and isolated by forests. This situation became the ground for a feeling of independence and uneasiness of interference by any outsider, particularly governmental or religious authorities.
Double standards and hypocrisy, related to the individual's façade vis-à-vis official positions, is very common in Sweden. This works as the other side of homogeneity and Lutheranism. Double standards and hypocrisy are very useful in a society where the cohesion of a group is very important. They become the defense and the protection of the individual's privacy and the individual's choices and behavior,

whenever they do not comply with the moral, ideological and political correctness of society. By adopting hypocrisy the individual can be free to act as he finds best without the risk of threatening the cohesion of the group or the risk of being seen as disloyal or traitor.
Sweden is a country where workers' movement and unionism started early and became very successful and strong. This movement questioned traditional values and promoted new ideas. Openness, democracy, free speech, individual freedoms and rights played a central role in the ideology of labor unions and of Social-democratic party, who governed Sweden for half a century. These new ideas helped to build the workers' unions and party, and eventually became themselves an established institution dominating political ideology in Sweden (Haug, 2004).
Starting from this ideological base at home, Sweden has been very influential in the work to spread these ideas internationally. It took the role of promoting individual rights and freedom. Sweden acquired a high profile as the moral conscience of the world directed not only outside but also inside the country. Swedes perceive their country as the most open, tolerant and respectful of individual rights (Joenniemi, 2013).
Sweden is also a high technological country. New and advanced information technologies are developed at universities and in industry, and they are used in almost every aspect of working or private life. One telling example is the broad use of cards for payment which is highest in Europe (Economist, 2016), and the use of electronic on-line medical records easily accessed by doctors and patients. The government and the people support this technological excellency, and they are proud of it. Focus on information technology and its importance, discussing freely and intensively all ideas connecting to the use of IT, and the culture built around it lead in a high awareness of Swedes regarding IT's effect on individual rights, both positive and negative (Lehnbom, McLachlan & Brien, 2013).

2.2 Individuals and society

All this affects the thoughts of Swedish people believing that they live probably in the most open, democratic and tolerant society of the world, where individual rights are of outmost importance and therefore they are supported fully by the government and society. And this strong belief dominates people's minds in a collectivistic, invariable and rather uniform society, which has great difficulties to handle ideas contesting political correctness, and which has a long tradition and culture of control and surveillance.
These two opposing traditions of Swedish society have led to contradicting policies: Sometimes supporting privacy and whistleblowing, sometimes imposing control and surveillance. For example, Sweden offers a strong protection for whistleblowers, which will soon be even stronger; people can access all unclassified government data anonymously; there is an influential movement for individual rights; and Swedes have a culture of openness and respect for the individual. But on the other hand we have many scandals spoiling this nice picture of individual rights: FRA conflict and later accusations of cooperating with NSA; earlier the IB affair about spying on leftist workers union members by the Social-democratic party; the Bofors and Tsesis scandals about punishing whistleblowers; recently the Roma registration scandal about the police registering persons illegally; and many more (Hedin & Månsson, 2012).

2.3 Summary

According to all the above, students in Sweden, especially university students of Information Technology are expected to show a strong feeling for privacy and for whistleblowing combined with trust to their society. They are involved in IT, they are either active themselves into the privacy movement or they have a very good interest and knowledge about these issues, and they support actions protecting privacy like whistleblowing. Older students who have more experience in these activities have a better understanding of the right to privacy. However, students in Sweden are expected to have an idealistic picture of Sweden, and to accept its profile at face value, including the official presentation of the country as solidly supporting privacy and whistleblowing.

3. Overview of the Survey

The survey consists of 40 questions (in English) with a variety of answers forms including yes/no; Likert scales and free text responses (which could be given in English or Swedish). It is part of an international comparative study using the same questions except for some very minor local alterations such as the names of a country's law enforcement and secret intelligence service organisations, and in some cases traanslation of the questions and answer options.

Participants were recruited from undergraduate and graduate (Master and PhD) students who had studied an IT and Ethics course at Uppsala University during the previous two years. They were invited to participate in the online survey by e-mail. Participation was entirely voluntary and not compensated. Respondents participated between 5th October and 11th November 2014.

The total number of respondents was 190 (male 142, female 47 and other 1), with 46 "25+ years old", 6% teenagers (18-19). Most (173; 91%) were studying at Uppsala University, 15 (8%) at another Swedish university and 2 (1%) at universities outside Sweden. Two thirds (126; 66%) were studying technology/engineering and another 27 (14%) were studying natural/physical sciences. Respondents were mostly Swedish (149; 78%) with two a mix of Swedish and non-Swedish descent. Others nationalities represented included other European countries, African countries, Asian Countries and North American Countries.

Table 1: Respondent attributes (N=190)

Gender	**Male**			**Female**			**Other**	
	142 (75%)			47 (25%)			1 (1%)	
Age	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25+**
	2	10	10	16	22	19	24	87

The platform of the questionnaire was the free online survey software SurveyMonkey. All responses have been stored in a common data base from which they could be retrieved and analyzed. No follow-up interviews were conducted.

3.1 Analytical Approaches

Much of the data from the surveys consists of Likert Scale responses, usually on a four option scale. For all such questions, respondents could skip any question they did not wish to answer, either giving an explicit "I do not wish to answer this question" response, or by simply not selecting an answer. For those questions requesting an evaluation or opinion in response, a "no opinion" box was also shown separately (to the right hand side of the "opinion-exposing" answers to avoid the well-known problem of median answers). The answers varied depending on the question, including zero-to-positive indications from "none" to "a lot" or negative/positive evaluations "disagree a lot" through to "agree a lot".

These Likert scale responses are then analysed using continuous statistical approaches to answer questions about their relationship to respondents' attributes or other answers. While not a universally accepted approach (Kuzon *et al.*, 1996) it is quite common and if done appropriately is accepted by many as a robust approach (Labowitz, 1967; Norman, 2010). In particular the use of Likert scale responses in this paper are primarily used for explanatory purposes and to show relationships between attributes/responses, and are not used as numerical input data for further analyses.

The following abbreviations for statistical terms are used in presenting quantitative analyses: SD: Standard Deviation; M: Mean; SE: Standard Error; D: (average) Difference; CI: Confidence Interval; t: t-test result.

4. Survey Results and Discussions

4.1 Attitudes to Privacy

The vast majority (177; 93%) of respondents felt that the right to privacy is "Very important" or "Important", with only ten responding that it is "Not so important", and none that it is "Not important at

all"(three preferred not to answer). When asked how well they understood the right to privacy, most (139; 73%) indicated that they understood it ("Understand very well"/"Understand") while 39 (21%) indicated that they did not understand ("Hardly understand"/"Don't understand at all") and 12 preferred not to answer (see Table 2 for detailed breakdowns)

Table 2: Frequency table of Q11 and Q14

Q11. Is your right to privacy important?		Q14 How well do you understand what the right to privacy is?	
Answers	Frequency (%)	Answers	Frequency (%)
Very important	108 (57%)	Understand very well	41 (22%)
Important	69 (36%)	Understand	98 (52%)
Not so important	10 (5%)	Hardly understand	37 (19%)
Not important at all	0 (0%)	Don't understand at all	2 (1%)
Total	187	Total	178

Collapsing these answers into "Important"/"Not important" and "Understand"/"Not Understand" produces the Contingency table shown in Table 3, in which can be seen that 34 respondents regard the right to privacy as important even though they do not understand it. Despite this, a Fisher Exact test shows a significant correlation at the 5% level between valuation of importance and understanding of the right to privacy (Fisher Test statistic: 0.042, $p<0.05$).

Table 3: Contingency table of Q11 and Q14

		Q 14 How well do you understand what the right to privacy is?		
		"Understand very well" or "Understand"	"Hardly understand" or "Don't understand at all"	Total
Q 11 Is your right to privacy important?	"Very important" or "Important"	134	34	168
	"Not so important" or "Not important at all"	5	5	10
	Total	139	39	178

Respondents were asked to give free text answers explaining why the right to privacy is important or not. The three who felt that the right was not important, all gave answers indicating that they had nothing to hide (two said this only while one indicated a possible problem with "insurance companies or organizations that go against my personal beliefs and opinions"). Of the two who felt that they understood the right but felt that it was not important, one answered that they had nothing to hide, and the other that too much privacy could make society feel cold . This second answer was echoed by one of those who felt that they hardly understood the right, but that it wasn't important, using the phrase from Egger's novel "The Circle" that "Sharing is Caring. Two others again indicated nothing to hide, another that privacy was impossible with modern technology, and the final one gave no answer.

Amongst thoe who felt that the right was (very) important a number of key themes emerged from their free-text answers (some gave more than one of these answers). The most common element was that privacy is a fundamental right indicated by 43 respondents. The right to a personal life was mentioned by 35. Control/consent over the collection, processing and use of personal information came up in 30 answers. Personal security/safety was an element in 23 answers, while 22 included concern about misuse. The necessity of privacy for wellbeing appeared in 11 answers, while nine mentioned the importance of privacy for democracy.

Respondents were asked whether their Internet and their non-Internet activities involve taking risks with their privacy. Internet activities were seen as a greater risk. Internet involves taking risks with privacy: strongly (53/190; 28%) or to an extent (95/190; 50%) together almost 78%, whereas non-Internet activities involves taking risks with privacy: strongly (7/190; 4%) or to an extent (60/190; 32%) together only just over a third (35%).

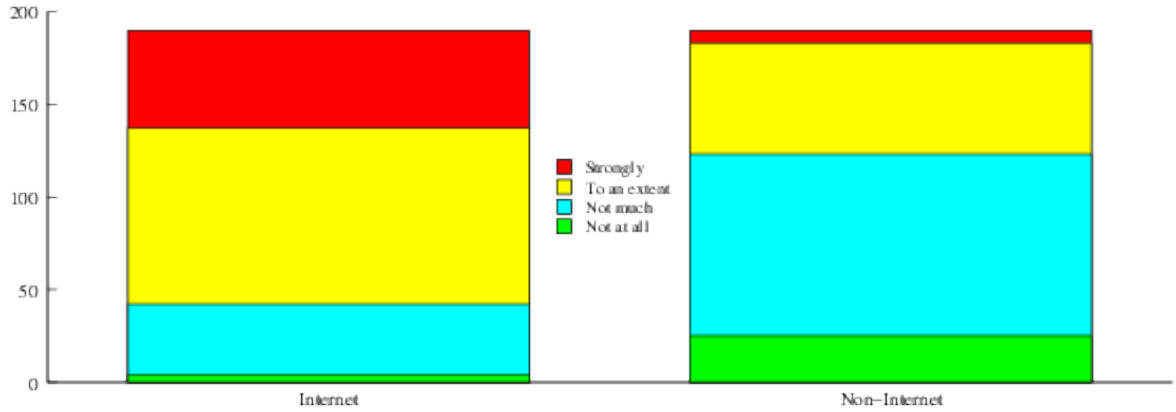

Figure 1: Do you feel that you are taking risks with your privacy? (N=190)

Figure 1: Do you feel that you are taking risks with your privacy? (N=190)

These results show that respondents are generally concerned about their privacy online and generally not concerned about their privacy offline. The mode for the privacy risks of Internet activity is "To an extent" but for Non-Internet activity is "No much" Using a two-tailed paired means t-test analysis with a numeric interpretation (0: "Not at all"; 1: "Not much"; 2: "To an extent"; 3: "Strongly"), respondents were more concerned about their privacy in Internet activity than non-Internet activity, significant at the 1% level: ($t=-12.813$; $p< 0.00001$).

This is borne out again when they were asked about the level of privacy threat posed by various groups and technologies. Respondents were asked to rate the level of threat to their privacy posed by 15 groups and 19 technologies on levels of "Not at all"; "Not Much"; "To an Extent"; "Strongly". Allocating numeric values to these of 0 (Not at all) to 3 (Strongly), allows calculation of a mean privacy risk associated with each item, and the production of a ranked list of each. These are shown in Tables 4 (groups) and 5 (technologies). The mean value for all group is 1.43 (with a SD of 1.011) and for all technologies is 1.5 (with a SD of 1.017). Since the mid-point of the scale is 1.5 this shows that respondents were concerned about many groups and technologies, but unconcerned about others (a standard deviation of approximately 1 around an average of the mid-point).

Internet companies were clearly seen as the most dangerous type of organisation, with a mean of 2.44: 106 respondents regarded them as a strong threat to their privacy and another 33 as a threat to an extent. Secret Service government agencies, telecom companies, other for-profit companies and computer software companies were all also regarded as threats with a mean of more than 1.75. Law enforcement government agencies had a mean just above the mid-point of 1.5, while Systems integrators and other government agencies were just below that mid-point, computer hardware companies were down in the less risky area. All groups of individuals were in the low risk zone, with the more well-known, the lower the risk. Health-care and other non-profit organisations were also low risk (average of below 1) while educational institutions were tied with well-known individuals at the lowest risk.

Smartphones and social media services were regarded as the most risky technologies, the only ones with an average of above 2. 86 respondents regarded smartphones as a strong threat and 69 as a threat to an extent,while 80 regarded social media as a strong threat and 64 as a threat to an extent. Behavioural targetting and online shopping were regarded as moderate threats. RFID, home-based health monitoring, personal body monitoring, home automation and video consoles were all regarded as low risks.

Table 4: Ranked means (0: low; 3: high) of 15 groups as perceived privacy threat

Q8. How much do you feel that the following groups threaten your privacy?		
Types of organisations	Mean	SD
Internet companies	2.44	0.722
Secret service government agencies	2.11	1.036
Telecom companies/ Internet providers	1.95	0.799
Other for-profit companies	1.82	0.865
Computer software companies	1.79	0.945
Law enforcement government agencies	1.59	1.039
System Integrators	1.47	0.873
Other government agencies	1.38	0.947
Computer hardware companies	1.21	0.905
Individuals who you don't know	1.10	0.879
Individuals who you know but not well	1.04	0.817
Health-care organisations	0.93	0.861
Other not-for-profit organisations	0.91	0.783
Individuals who you know well	0.81	0.869
Educational institutions	0.81	0.745

Table 5: Ranked means (0: low; 3: high) of 19 technologies as perceived privacy threat

Q9. How much do you feel that the following technologies threaten your privacy?		
Technologies	Mean	SD
Smart phone	2.23	0.844
Social media services	2.19	0.881
Behavioural targeting	1.94	0.990
Online shopping	1.81	0.898
Personal computer	1.75	0.914
GPS	1.71	0.948
Making payments online	1.63	0.885
CCTV	1.56	0.971
Online auction	1.42	0.948
Smart meter	1.41	0.994
Smart card	1.36	0.976
Online games	1.27	0.939
RFID	1.23	1.006
Home-based health monitoring	1.12	0.997
Personal body monitoring	1.11	0.964
Home video game console	1.01	0.876
Home automation which senses human activities	0.90	0.931
Portable video game console	0.80	0.854

4.2 Knowledge of Surveillance

Respondents were asked to assess their level of knowledge of Swedish organisations involved in Signals intelligence (SIGINT) as well as the US and UK organisations. They were asked

Do you know much about the following organisations?

- FBI (Federal Bureau of Investigation)
- CIA (Central Intelligence Agency)
- NSA (National Security Agency)
- GCHQ (Government Communications Headquarters)
- Säpo (Säkerhetspolisen)
- FRA (Försvarets radioanstalt)
- MUST (Militära underrättelse- och säkerhetstjänsten)
- Datainspektionen

with answer options of "I have heard of this organisation and understand what it does"; "I have heard of this organisation but do not understand what it does"; "I have not heard of this organisation"; "I prefer not to answer this question".
As can be seen from figure 2, most respondents know about the three US agencies (FBI, CIA and NSA), with fewer, but still a majority knowing the Swedish groups Säpo and FRA. Swedish groups MUST and Datainspektionen are little known and most have not even heard of the UK's GCHQ and very few believe they understand what it does.

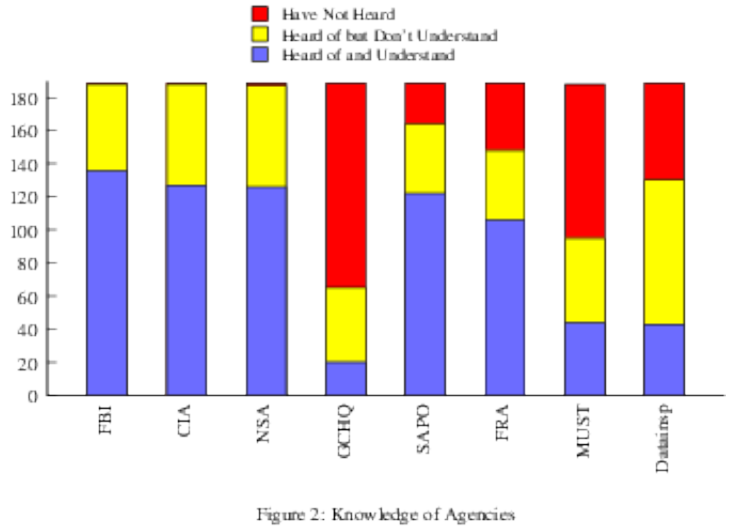

Figure 2: Knowledge of Agencies

Figure 2: Knowledge of Agencies

Almost all respondents had heard about Snowden's revelations: 94% (179/190). Their reported level of knowledge was mixed, with around half (52%, 93/179) claiming to know "A lot" or "A fair amount" about the revelations, with the other half knowing "Not much" or "Little" (three preferred not to answer). The US government's reactions were a little better known (perhaps reflecting the amount of information available as much as interest in the topic) with 65% (116 of 179) claiming to know "A lot" (15) or "A fair amount" (101), but only just over a third (39%; 70/179) were well-informed on the current status of Mr Snowden. See Table 6 for a detailed breakdown.

Table 6: Level of Knowledge of Snowden's Revelations

Q.24. How much do you know about the contents of Snowden's revelations? Q.26. How much do you know about the US government's reactions to Snowden's revelations? Q.27. How much do you know about the current status of Mr. Snowden?						
	Q24		Q26		Q27	
A lot	15	8%	15	8%	7	4%
A fair amount	78	41%	101	53%	63	33%
Not much	67	35%	40	21%	78	41%
Little	16	8%	20	11%	28	15%
Nothing/No Ans	14	7%	14	7%	14	7%

The main channels of information (Q21: How did you get and have updated your knowledge about Snowden's revelations? (Multiple answers allowed)) were reading news reports on the Internet (150; 84%,), reading newspaper articles (113; 63%), social media (103; 58%) and watching TV news reports (97; 54%). Just under half had heard about them from friends or acquaintances (81; 45%). Hearing about Snowden during lectures at university did not play any important role (6; 3%).As might be expected given that almost half had heard about the revelations from friends or acquaintances, 71% (127/179) reporting having talked about them with others. Only half (89/179; 50%) reported searching for information about the revelations. A fisher exact test on the contingency table showed a correlation between those who had discussed the revelations and those who had searched, significant at the 1% level (two-tailed p: $0.006 < 0.01$)

Table 7: Contingency Table for Discussed/Searched Snowden's revelations

Discussed? Searched?	Yes	No	Total
Yes	72	16	88
No	53	32	85
Total	125	48	173

4.3. Evaluation of Snowden's Actions

Respondents in this survey were very positive about Snowden's actions. After being presented with a brief neutral description of Snowden's revelation all respondents (including those who had not previously heard about his actions) were asked "Did Snowden's revelations serve or harm the public interest?" seven had no opinion. 162 of those who offered an opinion gave a positive evaluation: 86 selecting "Served it a lot" and 76 "To some extent". Six felt that he had "Harmed it to an extent" and one that he had "Harmed it a lot". Unsurprisingly, given this positive evaluation of his actions, 121 respondents thought that the US should not pursue a criminal case against him, while only 17 thought that they should (39 had no opinion and 13 chose not to answer).

Respondents were then asked two hypothetical questions about whether they would follow Snowden's lead and emulate his actions. They were asked whether they would act as he did if they were US citizens and found out the same information that he had (QUS), and they were also asked about whether they would do the same had they found out about a similar situation in Sweden (and were Swedish citizens –

remember that approximately one in six participants were not Swedish, comprised of 30 nationalities) (QSE). Table 8 shows the contingency table for answers to QUS and QSE.

Table 8: Would you Follow Snowden?

		QUS			
		Yes	No	N/A	Total
QSE	Yes	56	21	13	90
	No	2	40	2	44
	N/A	4	8	44	56
	Total	62	69	59	190

Of those who gave an answer a clear majority (Yes: 90 v 44: No) would emulate Snowden in Sweden while a smaller majority (Yes: 62 v 69: No) would not emulate him in the US (statistically significant at the 1% level according to a z-test (z: 53.260, 95% CI [38.52; 56.21]; $p<0.0001$). Of those who expressed an answer for both hypotheticals (119 respondents) most were consistent Yes/Yes: 56 and No/No: 40 between emulating him in both or emulating him in neither country. 21 would emulate him in Sweden, but not the US, while just two would emulate him in the US but not in Sweden. A two-tailed Fisher exact test shows a correlation significant at the 1% level between the answers to QUS and QSE ($p< 1e^{-12}$)
Respondents were asked to explain the reasons for their choices. All 21 of those who would follow Snowden's lead in Sweden but not the US gave free text answers for their unwillingness to follow Snowden's lead in QUS and for their willingness to follow him in QSE. In explaining their reasons for not emulating him in the US hypothetical all but one said that they would be too afraid of reprisals from the government. The other said "If I was an American citizen I would probably be brainwashed about the importance of collecting information on people to prevent 9/11-like attacks against the Nation." All the response as to why they would emulate Snowden in Sweden indicted less fear of reprisals, many stating their greater faith in the Swedish protection of whistleblowers and fairness of the Swedish courts.
29 of the 44 respondents who would not emulate Snowden in QUS or QSE gave positive evaluations of Snowden's effect on the public interest. In their free-text responses explaining their unwillingness to emulate Snowden, 20 were too afraid of reprisals from both the US and Swedish governments, although a few said that they were less frightened in the Swedish hypothetical. Three said they did not know why, two said that they felt it would have no impact, while three said that it would be wrong to do so because of loyalty to the state or the organisation even though they had answered that Snowden's revelations had helped the public good.

4.4. Perceptions of The Impact of Snowden's Revelations

The 179 who had heard about Snowden's revelations were asked if they had changed their own online behaviour afterwards. 71 (40%) said that they had made no change. Seven preferred not to answer. The remaining 101 selected one or more changes, shown in Table 9 with percentages of both the 101 who had made changes and the 179 who answered the question. A free-text option for "other changes" was also provided, through which four mentioned VPNs/Tor/Encryption.

Table 9: Changes in Behaviours in Response to Snowden's Revelations
N=101/179; multiple selections permitted

Action	No.	% of 101	% of 179
Think more about postings on SNS	68	67%	38%
Reduced the use of some services	61	60%	34%
Change privacy settings on some systems	56	55%	31%
Deleted personal data and content from SNS	41	41%	23%
Stopped using some systems	26	26%	15%

All respondents were asked whether they believed Snowden's revelations had had any broader social impact. Just over a fifth (40/190; 21%) said they believed no social changes had occurred. A further 52 (27%) had no opinion, while 13 (7%) preferred not to answer. The 85 (45%) who believed that some social change had happened were asked to provide a free text response about those changes. 56 respondents mentioned that Snowden's revelation had increased awareness of privacy and surveillance issues. Only 18 felt that people had done something about it by changing their behaviour online. Two mentioned a general decrease in trust in governments.

When asked whether Swedish citizens need to give up their privacy and freedom in order to ensure the security of society and the individual, 6 selected "no opinion" and 8 preferred not to answer. Of the 176 expressing an opinion there was a preponderance (65%; 115/176) against agreeing with the statement, statistically significant at the 1% level according to a z-test (z: 85.787, 95% CI [57.81; 72.34]; $p<0.0001$) but a qualified rather than wholehearted rejection, with 49% (86/176) selecting "Not much" and 16% (29/176) selecting "Not at all". See Table 10 for the detailed results.

Table 10: Give up Privacy and Freedom for Societal and Individual Security?

Answer	Number	%
Yes: Very much	8	5%
Yes: To an extent	53	30%
Yes (combined)	61	35%
No (combined)	115	65%
No: Not much	86	49%
No: Not at all	29	16%

4.5. Calculations of The Impact of Snowden's Revelations

In addition to the perceptions of those who had heard about Snowden's revelations on their personal activities or more broadly, differences in attitudes between those who had heard of them (the "Heard" group) and those who had not (the "Not Heard" group) were analysed to identify significant differences. Of course, any such significant difference is simply correlation and not necessarily causation. it is possible that those who are more privacy conscious, for example, might well be more aware of news reports on surveillance and therefore have heard of Snowden. Nevertheless, these correlations are worth exploring.

So, did the Heard group demonstrate a higher level of concern about the privacy risks involved in Internet/non-Internet activity, or regarding the right to privacy? Table 11 shows the contingency tables for these correlations, along with the results in each case of a Fisher Exact test for correlation. The scales for importance have been collapsed to binary rather than four-way selections.

Table 11: Contingency Tables for Q7/8/11 and Q20

	Q20. Heard about Snowden's revelations		
Q7. Privacy Risk from Internet Activity?	Yes	No	All
Strongly or to an extent	141	7	148
Not much or not at all	38	4	42
All	179	11	190

A Fisher exact one-tailed test fails to show a correlation between Heard Group and Evaluation of Privacy threat from Internet Activity at 1% level (p=0.205).

	Q20. Heard about Snowden's revelations		
Q8. Privacy Risk from non-Internet Activity?	Yes	No	All
Strongly or to an extent	66	1	67
Not much or not at all	113	10	123
All	179	11	190

A Fisher exact one-tailed test fails to show a correlation between Heard Group and Evaluation of Privacy threat from Internet Activity at 1% level (p=0.053).

	Q20. Heard about Snowden's revelations		
Q11. Is your right to privacy important?	Yes	No	All
Strongly or to an extent	167	10	177
Not much or not at all	9	1	10
All	176	11	187

A Fisher exact one-tailed test fails to show a correlation between Heard Group and Importance of the right to Privacy at 1% level (p=0.463).

This suggests that the Heard group are no more generally privacy-conscious than the Not Heard group. Given this, then analysis of other differences between the groups with respect to privacy attitudes suggest a possible causative link between attitudes and Snowden's revelations. Since Snowden's revelation were mostly about government surveillance, but also implicated some online services, Heard/not Heard respondents' evaluations of the privacy threats posed by Telecom companies (Q9d), Internet companies (Q9e), Law enforcement government agencies (Q9m), Secret Service Government Agencies (Q9n) and social media services (Q10n) are compared in Table 12. Because five comparisons are being calculated, a 1% significance level has been chosen.

Table 12: Contingency Tables for Q9x and Q20

Privacy threat from...	Heard about Snowden's revelations (Q20)		
Q9d. Telecom companies/ Internet providers	Yes	No	All
Strongly or to an extent	134	6	140
Not much or not at all	44	5	49
All	178	11	189

A Fisher exact one-tailed test fails to show any correlation between the Heard/not Heard group and the perceived level of privacy threat from Telecom companies/Internet providers at 1% level (p=0.123).

Q9e. Internet companies	Yes	No	All
Strongly or to an extent	159	10	169
Not much or not at all	19	1	20
All	178	11	189

A Fisher exact one-tailed test fails to show any correlation between the Heard/not Heard group and the perceived level of privacy threat from Internet companies at 1% level (p=0.67).

Q9m. Law enforcement government agencies	Yes	No	All
Strongly or to an extent	95	1	96
Not much or not at all	74	9	83
All	169	10	189

A Fisher exact on-tailed test shows a correlation between the Heard Group and the perceived level of privacy threat from Law enforcement government agencies at the 1% level (p=0.005).

Q9n. Secret service government agencies	Yes	No	All
Strongly or to an extent	121	3	124
Not much or not at all	47	5	52
All	168	8	176

A Fisher exact one-tailed test fails to show any correlation between the Heard/not Heard group and the perceived level of privacy threat from Secret service government agencies at 1% level (p=0.050).

Q10n. Social media services	Yes	No	All
Strongly or to an extent	139	5	144
Not much or not at all	31	5	36
All	170	10	180

A Fisher exact on-tailed test shows a correlation between the Heard Group and the perceived level of privacy threat from social media services at the 1% level (p=0.029).

So, the only group which the Heard Group have a statistical correlation with higher privacy threat levels are law enforcement government agencies.

Only those who already knew about Snowden's revelations were asked about whether they had changed their behaviour because of it. Did the self-reported level of knowledge of Snowden's revelations correlate with self-reported change of behaviour?

Table 13: Contingency Table for Q24 and Q25	Changed Behaviour (Q25)		
Level of Knowledge (Q24)	**Yes**	**No**	**All**
A lot	13	2	15
A fair amount	51	27	78
A lot or A fair amount	**64**	**29**	**93**
Not much or Little	**41**	**42**	**83**
Not much	35	32	67
Little	6	10	16
All	**105**	**71**	**176**

A one-tailed Fisher exact test on the collapsed answers to Q24 shows a correlation at the 1% level between level of knowledge and likelihood of changing behaviour ($p<0.007$)

5. Surveillance in Sweden Following Snowden

Sweden has a strong legal support for whistleblowers, first introduced in the 1949 law on freedom of the Press, updated in 2014 (Regeringskansliet, 2014). Whistleblowers have the same rights whether they are employees of government authorities or private organisations, including the right to anonymity, and immunity from prosecution. This immunity holds even for revealing classified data unless a case of treason can be made, or if the revelation constituted a breach of medical or priestly confessional confidentiality. Following Snowden's revelations, in 2016 the Swedish parliament improved protection for whistleblowers (Riksdagen, 2015). The new law, which came into force on 1st of January 2017, forbids employers in both the private and public sectors from retaliating against whistleblowers. If they do so, the employer is liable for compensation to the whistleblower for economic losses and for the insult.

However, existing government surveillance policies and practices have not changed in Sweden following Snowden's revelations: the surveillance activities described above continue operating as before.

6. Conclusions

Our hypothesis was that university students of Information Technology in Sweden would be very conscious about the value of privacy, they would appreciate the practice of whistleblowing. Furthermore, it was expected that Swedish students would trust their society regarding privacy issues and would perceive it as supportive of whistleblowing. Swedish society sees itself as respectful to privacy, sensitive to the Snowden case and therefore ready to strengthen its human rights and openness profile.

The great majority of the participants reported that they understand both the importance and the meaning of the right to privacy. Information technology plays an important role for privacy according to the participants. Use of the Internet was seen as involving risks to privacy whereas other activities were seen as less risky. This was consistent with their view of the threats to privacy which were felt to come mainly from Internet, private telecom and computer software companies and from government secret service agencies.

The level of knowledge of students at Swedish universities about the Snowden case was very high. Almost all participants reported that they had heard about Snowden's revelations. The main sources of information were online and traditional media as well as friends. Furthermore, the participants reported that they discussed Snowden's revelations with their friends or other people and many of them searched actively for information about this case. These findings support our expectations about students at Swedish universities having a high level of knowledge and interest about Snowden's actions.

Respondents showed a positive attitude to Snowden's revelations since they were seen as serving the public interest, and believed that some social changes had been caused, mainly higher awareness of surveillance and caution regarding online activity. The fact that Sweden strengthened whistleblower protection in recent years indicates that this support for Snowden's actions has broad social support in Sweden beyond the limited group participating in this survey.

Students at Swedish universities trust their society. Those who had heard about Snowden's revelations did not display any significantly higher concern about the privacy risks involved in using the

Internet. They felt that Swedish individuals do not need to give up privacy and freedom in order to ensure safety and security.

However, those respondents who knew more about Snowden's revelations were more likely to report having changed their online behaviour. Although this is a correlation and not causation it means there is some distrust, perhaps particularly of foreign companies and agencies such as the NSA.

The idea of following Snowden's example was clearly more attractive to the participants if they were placing themselves as Swedes or living in Sweden compared with placing themselves as American citizens. This means participants trust Sweden more than United States. This conclusion is reinforced by the correlation between willingness to emulate Snowden in both or neither case. The free text responses about why they would or would no emulate Snowden support these conclusions strongly, with most referring to risk to their lifestyles as the main reason for emulation or not.

To summarize, the results support our initial hypotheses that Swedish students had a high knowledge of the Snowden case, they actively searched for information, they gave a positive judgment of Snowden's actions and a majority would be willing to follow his example, at least in Sweden. They also trusted their country and most of its institutions and authorities except for secret service agencies and telecommunications companies. They also distrust Internet companies, many of which are based overseas, and particularly in the US (such as Facebook and Google).

7. Acknowledgements

This study was supported by the MEXT (Ministry of Education, Culture, Sports, Science and Technology, Japan) Programme for Strategic Research Bases at Private Universities (2012-16) project "Organisational Information Ethics" S1291006 and the JSPS Grant-in-Aids for Scientific Research (B) 24330127 and (B) 25285124. Meiji University's Yasunori Fukuta provide additional statistical analysis of responses.

References

Agrell, W. (2000), "Intelligence in an age of transition: The case of Sweden", *National Security and the Future*, Vol. 2, pp. 15-24.

Agrell, W. (2013), "Sweden: Intelligence the middle way", Davies, P. H. J. and Gustafson, K. C., *Intelligence elsewhere: Spies and espionage outside the anglosphere,* Georgetown University Press, Washington, DC, pp. 239-263

Daun, Å. (1996), *Swedish mentality*, The Pennsylvania State University Press, University Park, PA.

Eggers, D., (2013), *The Circle,* McSweeney's, San Francisco, CA.

The Economist (2016), "Emptying the tills: Europe's disappearing cash", available at http://www.economist.com/news/finance-and-economics/21704807-some-europeans-are-more-attached-notes-and-coins-others-emptying-tills (Accessed 23rd August 2016).

Eliasson, U. (2006), *I försvarets intresse: Säkerhetspolisens övervakning och registrering av ytterlighetspartier 1917-1945 (In Defence Interests: Security Service monitoring and recording of extremist parties 1917-1945)*, Nordic Academic Press , Lund (in Swedish).

Haug, R. (2004), "The history of industrial democracy in Sweden: Industrial revolution to 1980", *International Journal of Management*, Vol. 21, pp. 7-15.

Hedin, U. C. and Månsson, S. A. (2012), "Whistleblowing processes in Swedish public organisations—complaints and consequences", *European Journal of Social Work*, Vol. 15, pp. 151-167.

Holmberg, S. (1999), "Down and down we go: Political trust in Sweden", Norris, P., *Critical citizens: Global support for democratic government*, Oxford University Press, Oxford, pp. 103-122.

Joenniemi, P. (2013), "Disputed democratic identities: The case of Danish-Swedish discord", Morozov, V, *Decentering the West: The idea of democracy and the struggle for hegemony*, Routledge, Abingdon, pp. 175-190.

Kavathatzopoulos, I. and Asai, R. (2015), "Judging the complexity of privacy, openness and loyalty issues", *Computers & Society*, Vol. 45 No. 3, pp. 416-419.

Kent, N. (2008), *A concise history of Sweden*, Cambridge University Press, Cambridge.

Kuzon Jr, W. M., Urbanchek, M. G., & McCabe, S. (1996), "The seven deadly sins of statistical analysis", *Annals of plastic surgery*, Vol. 37 No. 3, pp. 265-272.

Labovitz, S. (1967), "Some observations on measurement and statistics", *Social Forces*, Vol. 46 No.2, pp. 151-160.

Madden, M. (2014). "Public Perceptions of Privacy and Security in the Post-Snowden Era", available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (accessed 21st March, 2017).

Murata, K., Adams, A. A., and Lara Palma, A. M. (2017) "Following Snowden: A Cross-cultural Study on Social Impact of Snowden's Revelations", *Journal of Information, Communication and Ethics in Society*, Vol 15 No.3, pp **??-??**

Norman, G. (2010), "Likert scales, levels of measurement and the "laws" of statistics", *Advances in health sciences education*, Vol. 15 No. 5, pp. 625-632.

Langkjaer, J. (2011), *Övervakning för rikets säkerhet Svensk säkerhetspolisiär övervakning av utländska personer och inhemsk politisk aktivitet, 1885–1922 (Monitoring of national security Swedish secret police monitoring of foreigners and domestic political activity, 1885-1922)*, Acta Universitatis Stockholmiensis, Stockholm (in Swedish).

Lehnbom, E.C., McLachlan, A.J. and Brien, J.A. (2013), "A qualitative study of Swedes' opinions about shared electronic health records", *Studies in Health Technology & Informatics*, Vol. 192, pp. 3-7.

The Local Sweden (2013), US 'totally dictates' Swedish surveillance, 12 Dec, available at http://www.thelocal.se/20131212/swedens-surveillance-carried-out-on-us-terms (accessed 8th August 2016).

OECD (2013), *Government at a glance 2013*. OECD Publishing, Paris, available at http://dx.doi.org/10.1787/gov_glance-2013-en (accessed 23rd August 2016).

Regeringskansliet (2014), 1949:105. Available at http://rkrattsbaser.gov.se/sfst?bet=1949:105 (accessed 23rd August 2016) (in Swedish).

Reuters (2013), "Sweden key partner for U.S. spying on Russia", available at http://www.reuters.com/article/us-sweden-spying-idUSBRE9B40Q320131205 (accessed 23rd August 2016).

Right Livelihood Award (2014), "Edward Snowden", available at http://www.rightlivelihood.org/snowden.html (accessed 23rd August 2016).

Riksdagen (2015), *Ett särskilt skydd mot repressalier för arbetstagare som slår larm om allvarliga missförhållanden: Proposition 2015/16:128 (A special protection against retaliation for workers who are sounding the alarm about the serious anomalies: Proposition 2015/16: 128),/* available at https://www.riksdagen.se/sv/dokument-lagar/dokument/proposition/ett-sarskilt-skydd-mot-repressalier-for_H303128 (accessed 23rd August 2016) (in Swedish).

Shilton, J. (2013), "Swedish intelligence service spying on Russia for US National Security Agency. Global Research", available at http://www.globalresearch.ca/swedish-intelligence-service-spying-on-russia-for-us-national-security-agency/5362967 (accessed 23rd August 2016).

Transparency International (2012), “Providing an Alternative to Silence: Towards Greater Protection and Support for Whistleblowers in the EU. Country Report: SWEDEN”, available at http://transparency-se.org/Providing-an-Alternative-to-Silence-Country-Report-Sweden-Nov-2013.pdf (accessed 23rd August 2016).