Following Snowden, German uncertainty about monitoring

Andrew A. Adams
Centre for Business Information Ethics, Meiji University, aaa@meiji.ac.jp

Sarah Hosell
HMKW University of Applied Sciences, s.hosell@hmkw.de

Kiyoshi Murata
Centre for Business Information Ethics, Meiji University, kmurata@meiji.ac.jp

Abstract.

Purpose – As part of an international study of knowledge of and attitudes to Snowden's revelations about the activities of the NSA/GCHQ, this paper deals with Germany, taking its socio-cultural and political environment surrounding privacy and state surveillance into account.

Design/methodology/approach – A questionnaire was answered by 76 German University students. The quantitative responses to the survey were statistically analysed as well as qualitative considerations of free text answers.

Findings – Snowden's revelations have had an important influence over German students' attitudes toward privacy and state surveillance, and shows concerns over the privacy risks associated with Internet activity.

Practical implications – The study results imply a need to build a collective awareness of the importance of the right to privacy and its responsibilities, the available technological options for individuals to exert their own privacy and security and the democratic means to agree and enforce appropriate legal restrictions on state surveillance.

Social implications – Young Germans support Snowden's actions and would be more willing to emulate him in Germany than the US. While many believe that people must give up some privacy and freedom for security, few seem to believe that current US or German approaches are valid and justified.

Originality/value – This study is the first attempt to investigate the social impact of Snowden's revelations on German students' attitudes toward privacy and state surveillance as part of cross-cultural analyses between eight countries.

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

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 Germany.

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 about/in Germany

Snowden's revelations have been heavily covered in the German press, particularly since the revelation on 24th October 2013 that German Chancellor Merkel's mobile phone was being monitored (Rosenbach and Stark, 2014). In an unprecedented move, the German Federal Foreign Minister Westerwelle summoned the US Ambassador to communicate their severe displeasure (Barkin and Chambers, 2013; Bierling, 2014). Germany, along with a number of other EU countries, raised the possibility of a mutual non-espionage pact or "no-spy agreement" both directly with the US and publicly as reported by O'Donnell and Baker (2013). Chancellor Merkel was later accused of talking up the possibility, knowing it was unrealistic, ahead of German Federal elections in November 2013 (Deutsche Welle, 2015a), playing to the gallery of German public opinion and trying to avoid hard questions about Germany's secret intelligence service BND's collaborations with the NSA and GCHQ (Deutsche Welle, 2015b) and its own murky past in monitoring democratic political dissent and journalists.

The German Federal Government does not regard Snowden's actions as politically motivated, so they claim that if Snowden were to enter Germany they would be required to allow him to be extradited to the US (Gazeas, 2014) and so have refused his requests for asylum there (Rosenbach and Stark, 2014).

However, a number of German NGO's have continued to push for the granting of asylum (Werkner, 2014). In March 2014, all parties in the Bundestag agreed to form a parliamentary board of enquiry in regard to the NSA in a rare occasion of unanimity (German Bundestag Drucksache, 2014). As of writing, two and a half years later, no full report has been issued by the committee, although evidence it has seen and its internal deliberations have been subject to multiple leaks (Uchil, 2016).

2. Background: Historical Surveillance in Germany

Germany has one of the most problematic histories in the world surrounding governmental surveillance. Between the activities of the Nazi regime from 1933-45 in Germany and its occupied territories, and the communist German Democratic Republic (GDR; DDR or Deutsche Demokratische Republik in German; often referred to as "East Germany" in regular English parlance, hereafter GDR), German experiences remain some of the best-known examples of surveillance coupled with authoritarian violence against the populace.

2.1 Surveillance in Nazi Germany

The Nazi identification of those deemed a threat to the purity of the people (primarily Jews, but also other groups such as Roma and homosexuals) and their incarceration in concentration camps and often execution is a case study in both the banality of evil (Arendt, 1971) but also of the force multiplication factor of dataveillance (Clarke, 1988) in the pursuit of government programs aimed at the oppression of minority groups. In Germany and then in occupied territories in Austria, Belgium, France, the Netherlands, Poland, etc. the Nazi regime used both existing census data and other government documents such as birth, marriage and death certificates, to build punched card databases on the populations under their control. Jews in particular, but other ethnic groups such as Roma and blacks (Lusane, 2003), were identified to the sixteenth degree, i.e. those with one great-great-grandparent of the targeted group (Black, 2012), although only those with one quarter such ancestry were officially classified as non-Aryan.

Beyond the use of IBM tabulation machines to sort the census and other genealogical records in an unprecedented dataveillance mechanism, the Nazi regime employed multiple other forms of surveillance including surveillance of communications and regular and irregular informants

> While the Gestapo tapped phones and intercepted mail, it was the army of informers, willing to plumb any depth of mundanity, that gave the force its psychological potency, down to apartment-block concierges reporting on the comings and goings of every tenant. These volunteers would often denounce people less out of political fervour than to ingratiate themselves with the authorities.
>
> (Tudge, 2010)

> My analysis of 175 case files involving efforts to enforce the social and sexual isolation of the Jews concluded that 57 percent began with an identifiable denunciation from the population at large.
>
> (Gellately, 1996)

Despite their anti-communism, the Nazi regime were inspired by and emulated or expanded upon the Soviet NKVD's (the fore-runner of the KGB) surveillance techniques for control of the population (Tudge, 2010). In the Soviet zone of occupied Germany which became the GDR, therefore, it is hardly surprising that state surveillance was a key element of the regime.

2.2 Surveillance in the GDR

The secret police of the East German state, the Ministry of State Security – commonly referred to as *The Stasi*, employed one of the most comprehensive population surveillance systems ever developed, doing so primarily using paper and analogue sound and video recordings rather than mechanical or electronic

computation (Ash, 1997), although indexing of the paper material was done using an electronic databank, (perhaps unfortunately) destroyed in February 1990 by the group charged with dealing with the Stasi's legacy (Miller, 2002). In addition to a huge workforce of direct employees (91,000 by 1989) and informers (174,000 by 1989) (Miller, 2002), like the Nazi regime, the Stasi gathered data not only from its specific employees but also encouraged the general populace to engage in denunciation of their fellows, both for personal gain and for "the good of the community" (Gellately, 1996), with Gellately also pointing out (p. 955) that the 170k+ unofficial employees had a high turnover rate in the 80s (around ten percent per year). Gellately concludes that "one in every eight person in the country was formally involved in the effort to generate Stasi files, and that perhaps a third of the population, more or less, had worked for the Stasi".

A specific department within the Stasi was responsible for audio recordings and telephone wiretapping. Department 26 eventually became one of the best-funded and important elements of the Stasi (p. 187, Ghouas, 2004), with another department (M) responsible for surveillance of surveillance of posted mail. Department 26 also used photographic and video cameras, and even infrared cameras, in its search for as much information as possible, and therefore as much control as possible, over citizens in the GDR (Ghouas, 2004). Departments 26 and M routinely broke the laws of the GDR, but the powerful position of the Stasi and the lack of any significant mechanism of oversight, even by other senior members of the GDR politburo, made those laws effectively inapplicable to these departments.

2.3 Surveillance and Privacy in the FRG (pre-1990)

Following the defeat of the Nazis, the US and UK immediately turned their attention to the threat of Soviet expansion. The occupation of eastern Germany, what would soon become the GDR, by Soviet forces, and of other Eastern European countries liberated from Nazi occupation, led to the recruitment of former German military and intelligence personnel by the US. In particular this centred on the CIA's funding of the "Gehlen organisation" led by former Wehrmacht (Nazi German military) general Reinhard Gehlen, who had served on the Eastern front against the Soviets for the Nazis. Krieger (2011) and Zolling & Höhne (1972) both claim that Gehlen's operation employed former SS and Gestapo officers after their release from Allied detention. Under Gehlen's command it became the Federal Intelligence Service of West Germany (Bundesnachrichtendienst, commonly known as the BND) and remains the foreign intelligence agency of the current German Republic (with both military and civilian areas of interest under its remit). Gehlen was the BND's first president, serving until 1968.

Given West Germany's "frontline" status in the Cold War, and the enclave position of West Berlin within the GDR, the "foreign" focus of the BND was less clear cut than the supposed split of US agencies' remits (FBI for domestic issues and the NSA/CIA for overseas). Incidents and threats on German soil such as the Munich Olympics bombings in 1972 and the 1986 bombing of a West Berlin Disco, mean that the BND's activities within the FRG have always been significant (Zolling andHöhne, 1972).

2.4 Surveillance in Post-1990 Germany

This domestic activity of the BND extended to the illegal practice of spying on German journalists, revealed in 2005 as taking place from 1993, primarily aimed at identifying possible sources of leaks from within the BND to journalists. A German parliamentary inquiry into the affair which concluded in 2009 (Deutscher Bundestag, 2009) confirmed the reports and identified poor oversight of the organisation from senior management as the primary cause but did not single anyone out for individual sanction.

As detailed below, Snowden's revelation were heavily covered in the German press and resulted not only in revelations about the NSA's actions within Germany and aimed at German targets, but revealed or

caused the revelation of details of the BND's activities on its own behalf and in collaboration with the NSA and GCHQ.

3. Overview of the Survey

The survey consisted of 37 questions (in German) with a variety of answers forms including yes/no; Likert scales and free text responses (which could be given in English or German, and which were almost all answered in German). It used the same questions as the other surveys (in this case translated into German) with some very minor local alterations such as the names of Germany's law enforcement and secret intelligence service organisations.

76 valid responses were collected from students and a few non-students of similar age, between November 2014 and January 2015. Almost all of the respondents were German citizens (92%) with a moderately balanced gender distribution of 59% females and 41% males. The age of respondents ranges from 18-30, but skewing younger: 31% (24/76) were 18-20 years old, 38% (29) 21-24 years old and 30% (23) 25 years or older (the survey did not ask for age beyond 25 but even in Germany where students in general are older than in many countries, it is unlikely that many were very mature). A majority of 83% (63) of the respondents were currently studying, 8% (6) were working and the rest were both working and studying.

Table 1: Respondent attributes (N=76)

Gender	**Male**				**Female**			
	31%(41%)				45(59%)			
Age	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25+**
	5	7	12	14	10	4	1	23

Most student respondents were at either Hochschule Niederrhein or Hochschule Fresenius, the remainder from other universities in the same region. The sample has a good spread of subject areas including respondents studying Humanities, Engineering, Psychology,Industrial Engineering, and Social Sciences, with no subject representing more than 20% of the group. 89% of student respondents were studying for a Bachelor's degree, the remaining 11% for a Masters.

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

Privacy was important to respondents, as can be seen from answers to the question "Is your right to privacy important?", with over 90% regarding it as "Very important" (40.8%; 31/76) or "Important" (50.0%; 38). Only six thought is "Not so important" and none thought it "Not important at all" (one respondent preferred not to answer). Respondents' self-reported understanding of the right to privacy was lower than their evaluation of its importance, although still the vast majority believed they understood it: 15 (19.7%) claiming to understand it very well and 52 (68.4%) claiming to understand it well. See Table 2 for the details of the answers to these two questions. Seven respondents thought that the right to privacy was important even though they did not understand it, see Table 3 for the full contingency table.

Table 2: Frequency table of Q12 and Q15

Q12. Is your right to privacy important?		Q15. How well do you understand what the right to privacy is?	
Answers	Frequency (%)	Answers	Frequency (%)
Very important	31 (40.8%)	Understand very well	15 (19.7%)
Important	38 (50.0%)	Understand	52(68.4%)
Not so important	6 (7.9%)	Hardly understand	8 (10.5%)
Not important at all	0 (0.0%)	Don't understand at all	0 (0.0%)
Total	75	Total	75

(Two different respondents preferred not to answer one each of these questions.)

Table 3: Contingency table of Q12 and Q15

		Q 15 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 12 Is your right to privacy important?	"Very important" or "Important"	61	7	68
	"Not so important" or "Not important at all"	5	1	6
	Total	66	8	74

When asked to explain the importance of the right to privacy most respondents gave a free text answer. Frequent types of response include “afraid to be a naked citizen”, “safety is an important feeling”, “fundamental right”, “personal freedom” and “freedom of choice”. All six who believed the right was not important also gave free text answers explaining their position. The most characteristic ones were: “I see my privacy is already lost” and “I do not experience threats my privacy”. The first appears to be a surrender to the loss of effective privacy, giving up a right to something impossible to achieve.

Further analysis of the free text answers on the importance of the right to privacy provided more detailed insight into the feelings of respondents (the following groups are not discrete: some respondents mentioned more than one of the observed categories of response). The largest group linked privacy directly to “freedom” and said that they do not want to be observed in their lives (29%). Just under a quarter (24%) “feared the consequences” if their right to privacy is not upheld, in particular being afraid of companies and others who could use their data. A group of 18% of the respondents said that they want to keep their “private activities private” and that no one else should know about these things.13% want to maintain “control over their personal data”. Another 7% said that they feel more “secure” when their right to privacy is upheld. A further 5% gave a positive law response: the right to privacy is so important because it is in the “law” and should be available for everyone.

When asked about the risks that Internet and non-Internet activity poses to their privacy, the vast majority of respondents were very concerned about the risks of their Internet activity, while a more modest majority were concerned about their non-Internet activity, see Figure 1 for details.

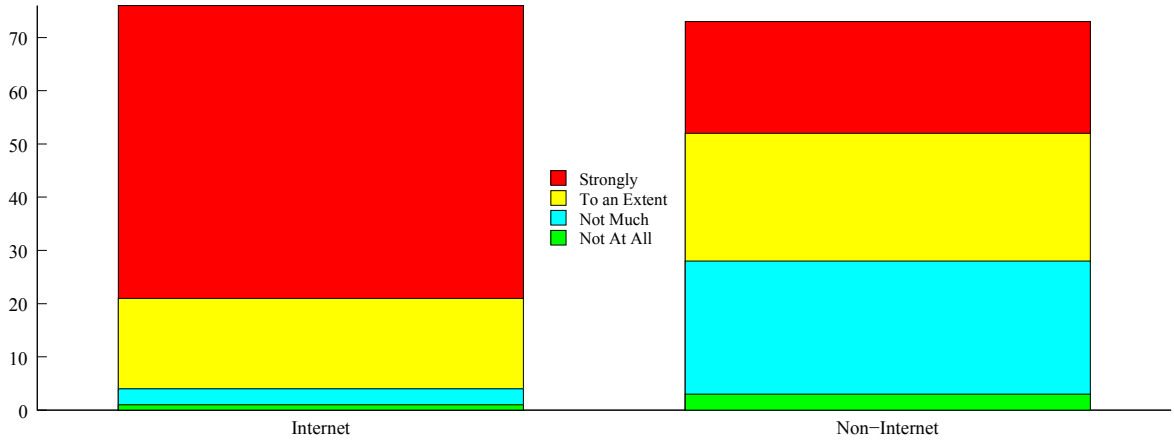

Figure 1: Do you feel that you are taking risks with your privacy? (N=76)

These results show that the respondents to this survey are generally quite nervous about their privacy. 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 groups is 1.67 (with a SD of 0.99) and for all technologies is 1.86 (with a SD of 1.01). Since the mid-point of the scale is 1.5 this shows that respondents are in general concerned about the privacy implications of the groups and technologies presented.

Internet companies are clearly seen as the most dangerous type of organisation, with a mean of only just under 3: 82% (62/76) of respondents regarded them as a strong threat to their privacy. Secret service government agencies, telecom companies and computer software companies were all also regarded as a

significant threat with a mean of just over 2. All government agencies and for-profit groups in the list had a mean of over 1.5, although “Other for-profit companies” and “Systems integrators” are only just in “risky” territory. Respondents did not regard individuals as particularly a threat to their privacy, with unknown or not well-known individuals rating just below the mid-point and well-known individuals ranking lowest with a mean of 0.92, with 38% (29) of respondents rating them as “Not at all” a threat and 36% (27) as “Not much” of a threat.

Smartphones and GPS systems were seen by respondents as the most privacy-threatening technologies, with online shopping, CCTV, Social Media, behavioural targeting, online payments and personal computers all rating a mean threat level of over 2. Home-based health monitoring, home automation systems and personal body monitoring are all seen as causing limited privacy concern.

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?		
Groups	Means	SD
Internet companies	2.79	0.522
Secret service government agencies	2.28	0.901
Telecom companies/ Internet providers	2.15	0.805
Computer software companies	2.15	0.711
Computer hardware companies	1.81	0.855
Other government agencies	1.77	0.878
Law enforcement government agencies	1.76	1.024
System Integrators	1.63	0.875
Other for-profit companies	1.58	0.813
Health-care organisations	1.54	0.901
Individuals who you don't know	1.31	0.928
Individuals who you know but not well	1.25	0.857
Educational institutions	1.07	0.777
Other not-for-profit organisations	1.03	0.785
Individuals who you know well	0.92	0.933

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	Means	SD
Smart phone	2.69	0.565
GPS	2.56	0.599
Online shopping	2.32	0.790
CCTV	2.27	0.754
Social media services	2.25	0.807
Behavioural targeting	2.21	0.859
Online Payments	2.16	0.901
PC	2.14	0.777
Smart card	1.90	0.860
Online auction	1.90	0.953
Online games	1.86	0.952
Automated Road Tolls	1.57	1.009
RFID	1.51	0.929
Home-based health monitor	1.48	1.065
Home vid. game	1.35	0.920
Home automation	1.30	1.016
Smart meter	1.25	0.858
Portable vid. game	1.13	0.882
Personal body monitoring	1.11	1.137

4.2 Knowledge of Surveillance

Respondents were asked to assess their level of knowledge of German 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)
- BND (Bundesnachrichtendienst)
- MAD (Amt für den Militärischen Abschirmdienst)

- BSI (Bundesamt für Sicherheit in der Informationstechnik)

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". Two respondents preferred not to answer about their knowledge of any of these organisations. One other preferred not to answer about GCHQ but gave answers for the others (this may have been a mistake and they meant to select "I have not heard of this organisation").

As can be seen from Figure 2 many respondents believe they know what the NSA and BND do. This perhaps reflects the level of attention paid to these organisations in the Germany news since Snowden's revelations. However, the CIA and FBI are also well-known to respondents, perhaps reflecting those organisations' profile in popular media. Few respondents claimed to understand the role of the UK's SIGINT agency GCHQ (and the NSA's junior partner in much of Snowden's revelations) and most had not even heard of it. More had heard of the other German agencies (MAD and BSI) although again claimed knowledge of what their role and operations are is very limited.

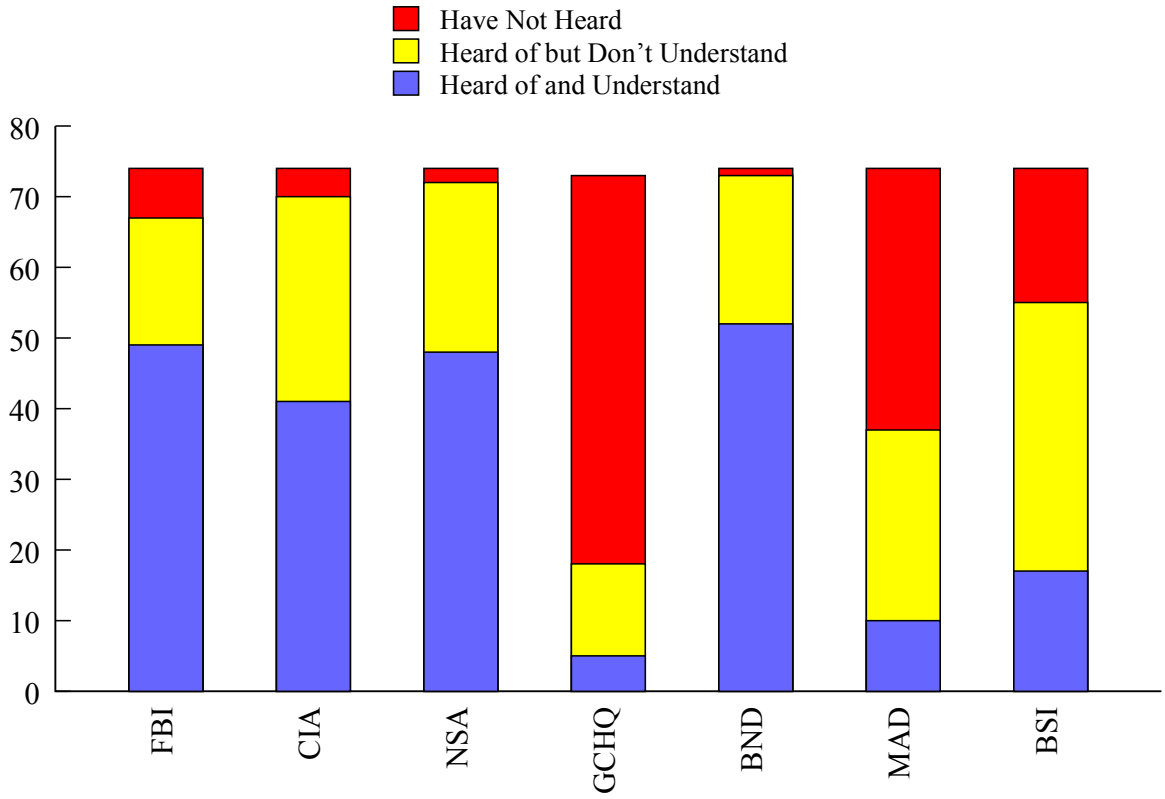

Figure 2: Knowledge ofAgencies

Almost all respondents had heard about Snowden's revelations: 97% (74/76). However, their reported level of knowledge was fairly low, with none claiming to know "A lot" and most claiming to know "Not much" or "Little". Similarly limited levels of knowledge were claimed about the US government's reaction and the current status of Mr Snowden. See Table 6 for a detailed breakdown. These results are consistent with a poll conducted by KRC Research (2015) on behalf of the ACLU in which 95% of "Millennials" (defined by them as 18-34 years old at the time of the survey) in Germany had heard of Snowden and his revelations.

Table 6: Level of Knowledge of Snowden's Revelations

Q.25. How much do you know about the contents of Snowden's revelations?
Q.27. How much do you know about the US government's reactions to Snowden's revelations?
Q.28. How much do you know about the current status of Mr. Snowden?

	Q25		Q27		Q28	
A lot	0	0%	2	3%	1	1%
A fair amount	6	8%	14	19%	6	8%
Not much	41	54%	31	41%	25	33%
Little	27	36%	26	35%	42	55%
Nothing (have not heard)	2	3%	2	3%	2	3%

Despite their limited knowledge of the revelations, a clear majority of respondents who had heard of the revelations (55/74; 74%) had discussed them with their friends, but a similar majority (57/74; 77%) had not searched for more information. A Fisher Exact Test on the contingency table data (see Table 7)for these questions revealed a difference significant at the 1% level ($p<0.001$) showing that despite the difference in majorities, those who had talked about Snowden with their friends were more likely to also search and that those who had not talked about Snowden were less likely to search.

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

Discussed? Searched?	Yes	No	Total
Yes	15	39	54
No	1	18	19
Total	16	57	73/74

One respondent preferred not to answer about discussions (but had searched).

4.3. Evaluation of Snowden's Actions

Other polls have shown that young people in Germany have a relatively high opinion of Snowden, for example The ACLU poll mentioned above (KRC Research, 2015) reported that 86% of Millennials who had heard of Snowden had a positive opinion of him (14% very positive, 72% somewhat positive). Respondents in this survey were similarly positive. After being presented with a brief neutral description of Snowden's revelation all respondents (including the few who had not previously heard about his actions) were asked "Did Snowden's revelations serve or harm the public interest?" Four declined to answer, and another four had no opinion. 59 of those who offered an opiniongave a positive evaluation: 31 selecting "Served it a lot" and 28 "To some extent". Seven felt that he had "Harmed it to an extent" and only two that he had "Harmed it a lot". Unsurprisingly, given this positive evaluation of his actions, 50 respondents thought that the US should not pursue a criminal case against him, while only six thought that they should (13 had no opinion while seven declined to answer/skipped the question).

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 Germany (and were German citizens) (QDE). Table 8 shows the contingency table for answers to QUS and QDE.

Table 8: Would you Follow Snowden?

		QUS			
		Yes	No	N/A	Total
QDE	Yes	18	4	7	29
	No	0	18	1	19
	N/A	1	6	19	23
	Total	19	28	27	74

Of those who gave an answer a clear majority (29 v 19) would emulate Snowden in Germany while a clear majority (28 v 19) would not emulate him in the US. Of those who expressed an answer for both hypotheticals (40 respondents) most were evenly split 18/18 between emulating him in both or emulating him in neither country. Four would emulate him in Germany, but not the US. Respondents were asked to explain the reasons for their choices. The four who would follow Snowden's lead in Germany but not the US all gave answers for their unwillingness to follow Snowden's lead in QUS and for their willingness to follow him in QDE:

- "Fear of punishment"; "More security and support"
- "Fear of losing work etc."; "Germany is more open than the US, paying more attention to the law"
- "I would be too scared"; "In Germany the legal situation is better, or at least I would have more confidence that I have no danger."
- "I do not want to live in Russia."; "In Germany I feel safer."

So, three explicitly mentioning fear and the other implying fear for life circumstances as reasons not to follow Snowden in the US, with all of them stating that they would feel more secure being whistleblowers in Germany.

15 of the 18 respondents who would not emulate Snowden in QUS or QDE gave positive evaluations of Snowden's effect on the public interest. 11 of those 15 explained that they would not have acted through fear of the consequences. The other four all referred to loyalty in some way: to the organisation, to the state more broadly, or to any oath of secrecy they would have needed to take before starting work for such an agency.

4.4. The Impact of Snowden's Revelations

When the 74 who had heard about Snowden's revelations were asked whether they had changed their own online behaviour after hearing about Snowden's revelations, over a third (41%; 30/74) reported no change, while one declined to answer. Three explained that they had not changed their behaviour because they were already privacy conscious in their use of online systems. Of the 45 who reported a change in their behaviour, their responses are shown in Table 9, with percentages of the 45 who had noted changes and of the 74 who had heard of Snowden's revelations both given.

Table 9: Changes in Behaviours in Response to Snowden's Revelations
N=45/74; multiple selections permitted

Action	No.	% of 45	% of 74
Change privacy settings on some systems	28	62%	38%
Think more about postings on SNS	23	51%	31%
Reduced the use of some services	22	49%	30%
Deleted personal data and content from SNS	19	42%	26%
Stopped using some services	8	18%	11%

When asked whether Snowden's revelations have had any broader social impact over a third (27/74; 36%) indicted that they thought there had been none. Another seven (9%) had no opinion, while ten did not reply. The 32 (46%) who believed there had been some change were asked to give examples in a free text response. See Table 10 for an analysis of their responses: again, percentages are given both of those who indicated a change [34] and of all those who had heard about Snowden's revelations before taking the survey [74].

Table 10: Social Changes Due to Snowden's Revelations
N=34/74; multiple selections permitted

Change	No.	% of 34	% of 74
Increased awareness of privacy	19	56%	26%
Action on self-protection against surveillance	10	29%	14%
Increased awareness of government surveillance	3	9%	4%
Degraded US/German relations	2	6%	3%
Corporate pushback against government surveillance	1	3%	1%

When asked whether German citizens need to give up their privacy and freedom in order to ensure the security of society and the individual five respondents gave no answer (two explicitly preferred not to answer and three skipped the question) and two explicitly had no opinion. Of the remaining 69, there was a preponderance towards agreeing with the statement, but a qualified rather than wholehearted agreement. See Table 11 for the detailed results.

Table 11: Give up Privacy and Freedom for Societal and Individual Security?

Answer	Number	% of 69	% of 76
Yes: A great deal	5	7%	7%
Yes: To some extent	38	55%	50%
Yes (combined)	43	62%	57%
No (combined)	26	37%	34%
No: Not much	19	28%	28%
No: Not at all	7	10%	9%

5. Surveillance in Germany Since Snowden

Snowden's documents contain significant revelations about both NSA/GCHQ operations aimed at German citizens, and about BND activity collaborating with them and a desire on behalf of the BND to extend that cooperation. This has led to a major public discussion about the role of SIGINT in Germany society (Biermann, 2016; Dehmer and Haselberger, 2015; Rosenbach and Stark, 2014). Although it was in some ways instrumental in generating disquiet amongst the German populace, the revelations that the NSA had access to the mobile phone calls made by German Chancellor Merkel, the focus this brought to the debate in Germany is perhaps distracting. Even though Germany is a strong US ally, spying on other governments' communications can be regarded as one of the roles of an external SIGINT agency. targeting all citizens of a democratic and allied nation, however, is more debatable, and this is clearly what has been happening, both by BND and the NSA (with BND's cooperation and separately, sometimes sharing access and results with the BND and sometimes not).

Despite being created in February 2014, the German parliamentary inquiry into the Snowden revelations has not yet issued a public report as of writing (early 2017). As with many other countries (particularly the US and the UK) retroactive authorisation of the existing practices of the BND are being proposed or have been passed by the Germany government, although alongside some reforms to increase oversight from parliament. Internet activists such as the blog Netzpolitik.org warned that these proposals represent a significant increase of the power of the German intelligence service (Der Spiegel, 2016), while the experience of most countries is that robust yet confidential oversight of secret service agencies is very hard to achieve.

Three years following Snowden's revelations the German Federal Cabinet agreed on a so-called anti-terrorism package with the title: "Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus" (Draft Law for a better exchange of information in the fight against international terrorism). It seems that the fear of terrorism is being offered as a justification for broader data access and monitoring functions (Biermann, 2016).

The recent refugee issue in the EU, primarily driven by the civil war in Syria, combined with a number of terrorist attacks by ISIS-linked groups in EU capital cities (Brussels, Paris, Berlin) have led to an increased call by both politicians and some citizens for expanded government surveillance powers. Civil rights groups have responded that these would restrict the privacy of law-abiding citizens without reducing the danger of terrorism (Human Rights Watch, 2016).

The respondents in this survey were among the best informed about Snowden's revelations in terms of the countries studied. They also had a relatively high opinion of the impact of his actions generally, although they reported limited personal responses to improve their own privacy. As with respondents in

many other countries the fear of government reprisals rather than lack of belief that it is the right thing to do, is the main reason offered for not being willing to emulate Snowden.

6. Conclusions

Snowden's revelations clearly informed German citizens about US, UK and German government activities which had far from universal support, indeed shocking some out of a sense that the US was a close ally with the same regard for the rights of ordinary Germans that they expect from their own government . However, respondents think that these have had limited impact on most people's communication practices, although a modest number reported having done so themselves. The types of changes they made indicate a desire to continue using their favoured online systems, but that they will make attempts to be more careful with their settings and usage.

The results of this survey are in keeping with others which indicate that German citizens are highly concerned about their privacy and support Snowden, but struggle to find ways to meaningfully implement their desire for privacy. While respondents generally agreed that to some extent privacy and freedom must be sacrificed to gain security (for society and individuals) they are not convinced that current systems strike that balance correctly.

6.1 Further Research

Free-text responses to the question "Why is your right to privacy important?" raise some interesting lines for deeper interview-based explorations. Why are they "afraid to be a naked citizen"? Why do they regard privacy as so strongly connecting to "personal freedom" and "freedom of choice"?

The responses to the question "Why is your right to privacy not important?" also raise some intriguing issues: "I see my privacy is already lost."and "I see no threat to my privacy." Are these respondents inured to, accepting of, or nihilistic about the prospect of avoiding a transparent society (Brin, 1999).

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

Arendt, H. (1971), *Eichmann in Jerusalem: A report on the banality of evil,* Viking Press, New York, NY.

Ash, T. G. (1997), *The File: a Personal History,* Atlantic, London.

Barkin, N. and Chambers, M. (2013), "Germany demands U.S. answers over Merkel bugging*", Reuters World News,* 24th October, available at http://www.reuters.com/article/us-germany-usa-spying-idUSBRE99N0LP20131024 (accessed 16th December 2016).

Bierling S. (2014), *Vormacht wider Willen: Deutsche Außenpolitik von der Wiedervereinigung bis zur Gegenwart (Supremacy against their will: German foreign policy from reunification up to the present),* C. H. Beck, Munich. In German.

Biermann K. (2016), "Selbstherrliche Überwachung soll Gesetz werden (Legalising Surveillance Organisation Self-governance)", *Die Zeit*, 7th June, available at

http://www.zeit.de/politik/deutschland/2016-06/nsa-bnd-verfassungsschutz-ueberwachung-gesetz-entwurf (accessed 16th December 2016). In German.

Black, E. (2012), *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation (2nd ed)*, Crown Books, New York, NY.

Brin, D. (1999), *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?,* Basic Books,New York, NY.

Clarke, R. (1988), "Information technology and dataveillance", Communications of the ACM, Vol. 31 No. 5, pp. 498-512.

Dehmer D. and Haselberger S. (2015) "Unter Verdacht (Under Suspicion)", *Der Tagesspiegel*, 4th May. In German.

Der Spiegel (2016), "Geheimdienste: Koalition einig über umstrittenes BND-Gesetz (Secret Services: Coalition Agree on Controversial BND Law)", 8th June, available at http://www.spiegel.de/netzwelt/netzpolitik/bnd-koalition-einigt-sich-auf-gesetz-ueber-bundesnachrichtendienst-a-1096468.html (accessed 24th January 2017). In German.

Deutscher Bundestag (2009)."Drucksache 16/13400 – Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes (Decision and report of the 1st Committee of Inquiry under Article 44 of the Basic Law)", 18 June. In German, available at http://dipbt.bundestag.de/dip21/btd/16/134/1613400.pdf (accessed 17th January 2017). In German.

Deutscher Bundestag (2014), "Drucksache 18/483 –Einsetzung eines Untersuchungsausschusses NSA (Establishment of an NSA Investigation Committee)", 12th February, available at http://dipbt.bundestag.de/dip21/btd/18/004/1800483.pdf (accessed 24th January 2017). In German.

Deutsche Welle (2015a), "Merkel knew 'no spy' agreement with the NSA was a no-go, says German daily", 27th May, available at http://www.dw.com/en/merkel-knew-no-spy-agreement-with-the-nsa-was-a-no-go-says-german-daily/a-18477795 (accessed 16th December 2016).

Deutsche Welle (2015b), "More NSA keywords detected in German spy agency's computers", 22nd May, available at http://www.dw.com/en/more-nsa-keywords-detected-in-german-spy-agencys-computers/a-18466733 (accessed 16th December 2016).

Gazeas N. (2014) "Deutschland müsste Snowden nicht an die USA ausliefern (Germany would not extradite Snowden to the US)", *Die Zeit,* 8th May, available at http://www.zeit.de/politik/deutschland/2014-05/snowden-auslieferung-nsa-untersuchungsausschuss-gazeas(accessed 6th April 2017).

Gellately, R. (1996), "Denunciations in twentieth-century Germany: Aspects of self-policing in the Third Reich and the German Democratic Republic", *The Journal of Modern History,* Vol. 68 No. 4, pp. 931-967.

Ghouas, N. (2004), *The Conditions, Means and Methods of the MfS in the GDR: An Analysis of the Post and Telephone Control,* Cuvillier Verlag, Göttingen.

Human Rights Watch (2016), *World Report 2016: Events of 2015,* Policy Press, Bristol.

KRC Research (2015), "ACLU Edward Snowden Survey: Millennial Findings", available at https://www.aclu.org/sites/default/files/field_document/snowden_poll_results.pdf (accessed 20th January 2017).

Krieger, W. (2011), "German–American Intelligence Relations 1945–1956: New Evidence on the Origins of the BND", *Diplomacy & Statecraft,* Vol. 22 No. 1, pp. 28-43.

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.

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.

Lusane, C. (2003), *Hitler's Black Victims: The Historical Experiences of Afro-Germans, European Blacks, Africans, and African Americans in the Nazi Era,* Routledge,New York, NY.

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).

Miller, B. (2002), *Narratives of guilt and compliance in unified Germany: Stasi informers and their impact on society,* Routledge, London.

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 **??-??.**

O'Donnell, J. and Baker, L. (2013), "Germany, France demand 'no-spy' agreement with U.S.", *Reuters World News,* 24th October, available at http://www.reuters.com/article/us-eu-summit-idUSBRE99N0BJ20131025 (accessed 16th December 2016).

Rosenbach, M. and Stark, H. (2014), *Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung* (*The NSA complex: Edward Snowden and the way into total surveillance)* Spiegel Verlag,Hamburg.

Tavel, P. (2007), *Modeling and Simulation Design*. AK Peters Ltd., Natick, MA.

Tudge, R. (2010), *The No-nonsense Guide to Global Surveillance.* New Internationalist.

Uchil, J. (2016), "WikiLeaks publishes docs on inquiry into German cooperation with NSA", *The Hill,* 1st December, available at http://thehill.com/policy/cybersecurity/308407-wikileaks-drops-docs-on-inquiry-into-nsa-german-cooperation (accessed 16th December 2016).

Werkner I., Kursawe, J., Johannsen, M., Schoch, B. and von Boemcken, M. (2014), *Friedensgutachten 2014 (Peace Report, 2014)*, LIT Verlag, Münster

Zolling, H., & Höhne, H. (1972), *The General Was a Spy: the Truth About General Gehlen and His Spy Ring,* Coward, McCann & Geoghegan, New York, NY.