Surveillance Following Snowden: A Major Challenge in Spain

Andrew A. Adams
Centre for Business Information Ethics, Meiji University, Tokyo, Japan
Mario Arias-Oliva
Business and Management Department, Universitat Rovira I Virgili, Spain
Ana María Lara Palma
Ingeniería Civil, University of Burgos, Spain
Kiyoshi Murata
Centre for Business Information Ethics, Meiji University, Tokyo, Japan

Abstract

Purpose – This study analyses the impacts of Edward Snowden's revelations in Spain focusing on issues of privacy and state surveillance. Our research takes into consideration the Spanish context from a multidimensional perspective: social, cultural, legal and political.

Design/methodology/approach – The paper reviews the Spanish privacy and state surveillance situation. Responses to a questionnaire were collected from 207 university students studying at Universitat Rovira i Virgili or Burgos University. The quantitative responses to the survey were statistically analysed as well as qualitative considerations of free text answers.

Findings – The survey outcomes demonstrate that a majority of respondents are aware of Snowden´s revelations, but only a few have even considered taking serious actions to improve their online privacy. One of the most relevant findings is that Spanish citizens find it acceptable to lose privacy and be subject to state surveillance if that provides a benefit in security.

Practical implications – The research points out the importance of privacy in a multicultural environment. A sensitized society is a key stone for the healthy and balanced development of state surveillance policy and practice.

Social implications – Training programs are a critical dimension to ensure awareness across society regarding privacy and digital technologies. Suitable educational policies and curricula at all levels should be fostered.

Originality/value – Privacy and state surveillance based on ICT is an emerging research topic with important consequences for social values and ethics. This study provides an overview of Spanish higher education students' attitudes in these areas.

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

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 Spain.

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 Spain

Spain is one of the NATO nations that has been the target of indiscriminate violence by extreme Islamists, with the Madrid train bombings on 11th March 2004. The subsequent investigations, trials and convictions found no significant evidence of direct links to Al Qaeda or any other group beyond those directly involved (Nash, 2006). Evidence from the trial (ABC, 2007) shows that some of those convicted of planning the attack had been under police surveillance before the attacks, although that surveillance had recorded no evidence of planning or preparations for the attacks. Such issues can be used to argue either for more state surveillance (the prior surveillance was insufficient to prevent or mitigate the attack) or for less (despite being under surveillance the perpetrators managed to carry out their plans, so efforts should be directed to other mechanisms for mitigating causes of attacks or the impact of attacks). The Spanish elections immediately following the 2004 attacks were considered to have been significantly altered by those events (Chari, 2004). In 2016, Spain has again been in political turmoil, with elections in December 2015 failing to lead to a new government being formed, a second election in June 2016 resulting in little change and a minority government only finally formed in late October 2016.

Spain's Centro Nacional de Inteligencia was revealed as a collaborator of the UK's GCHQ (Borger, 2013) in the Snowden documents. Allegations by Spanish newspaper El Mundo that 60 million telephone calls per month were being monitored by the NSA led to demands by the Spanish government for an explanation by the US (BBC News, 2013).

2 History, social and legal contexts of state surveillance in Spain

This section presents an analysis of the history and evolution of social and political Spanish context regarding civil rights, particularly as it concerns state surveillance and privacy protection (García and Gonzalez, 2012). A sequence of changes of government type through the 20th century has led Spain and Spanish society from its cultural roots to laws and a legal context which define what government surveillance is, and what is permitted or forbidden.

2.1 Pre-Dictatorship: To 1939

Spain had a deeply unstable political and social environment during the end of 19th century and the beginning of the 20th, even without involvement in the 1st World War. The First Republic (1873-4) lasted only eleven months but had four different presidents, and was followed by a restored monarchy with conservative and liberal elected governments but then a monarchy-backed military dictatorship (Primo de Rivera). A Second Republic (1931-1936) was then declared but lacked stability and broad social acceptance of election results.

2.2 Dictatorship government: 1939-1975

On July 18th 1936 Francisco Franco led a military coup against the second Republic, beginning the Spanish Civil War, which lasted for four years (1936-1939). Despite having received backing from both Hitler in Germany and Mussolini in Italy during the civil war, under Franco's victorious regime (from April 1st of 1939), Spain remained neutral during the 2nd World War and became an inward-looking state quite at odds with its previous international imperial power, gradually losing its remaining North African colonial territories, having lost most of its American territories in the 19th Century. Its neutrality allowed the regime to survive the defeat of the Axis Powers.

Franco persecuted political opponents, censored the media and otherwise exerted totalitarian control over the country, driven by intense surveillance from multiple government agencies, in particular of trade unions (Sánchez, 2009) and students (Rodríguez Tejada, 2014).

2.3 Transition to democracy: 1975-1982

After the dictator's death in 1975, Spain entered a democratic transition, with Franco designating the formerly exiled heir to the throne, Juan Carlos I, as his replacement head of state and government. An official coronation ceremony was held on 27th November, followed two days later by a broad Royal Pardon releasing 5,655 political prisoners, such as Marcelino Camacho, a union leader imprisoned in 1957 for his trade union activities. In 1976, a Law on freedom of assembly was passed. The 1977 democratic elections and the new Spanish Constitution (1978) included explicit protections for privacy in Article 18, including privacy of communications.

1. The right to honour, to personal and family privacy and to the own image is guaranteed.
2. The home is inviolable. No entry or search may be made without the consent of the householder or a legal warrant, except in cases of flagrante delicto.
3. Secrecy of communications is guaranteed, particularly regarding postal, telegraphic and telephonic communications, except in the event of a court order.
4. The law shall restrict the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.

A failed coup in 1981 showed that Spain had progressed beyond accepting military dictatorship, while the peaceful transfer of power to a new party in 1982 demonstrated acceptance of the democratic processes by the political class. The cost of a relatively peaceful transition to democracy, however, was acceptance of amnesty for virtually all of the activities of the government during Franco's regime (Rodríguez Tejada, 2014).

2.4 Democratic Period: from 1982

Although subject to continued internal political violence around the Basque region, Spain has

developed into a secure democracy, joining the European Economic Community (EEC) in 1986 and it is now a full EU member, using the Euro as its currency and submerging its borders into the Schengen Zone. Much of Spain's privacy and surveillance legislation therefore follows EU requirements, although state surveillance in the name of "national security" remains a contentious issue within the EU, as seen by the overturning of the Data Retention Directive (Directive 2006/24/EC) by the European Court of Justice (ECJ) on the grounds of incompatibility with the EU's Charter of Fundamental Rights' provisions on privacy and the need for proportionality and necessity of any government action impinging on such rights (Digital Rights Ireland v. Minister for Communications, 2012). Spain's implementation of the directive was primary legislation, unlike for example the UK which (as it often does) used secondary legislation to implement that directive. Such a secondary legislation approach avoids UK parliamentary debate on the issue, but the overturning of the directive by the ECJ removed the legal basis for the legislation in the UK, which has since adopted a similar regime under national primary legislative authority. Further court cases are pending at the ECJ to decide if national primary legislation (whether implementing the directive or replacing it) is allowed under EU rules, which may force Spain to alter its approach once decided.

The aforementioned Section 18 of the Spanish Constitution is given force by specific "Organic Laws" (a term of Spanish jurisprudence referring to laws which are not simply ordinary statutes but which are necessary embodiments of constitutional principles). For example, Organic Law 15/99 on Personal Data Protection (LOPD) states that in Spain everyone is entitled to know by whom, for what purpose and when their personal data is being used, and entitles them to decide about such use. Royal Decree 1720/2007 (the Spanish version of an Executive Order) approved the specific current regulations regarding data subjects' rights to access, have rectified, have deleted or oppose processing of their personal data (Government of the Principality of Asturias, 2015) which are referred to in Spain as ARCO rights:

- **A**ccess: Right to know what personal data are contained in a file.
- **R**ectification: Right to rectify incorrect or incomplete data in a file.
- **C**ancellation: Right to have data deleted from a file.
- **O**pposition: Right to oppose certain, specific processing of personal data within a file.

These rights have the following characteristics:

- They are personal rights. They may only be exercised by the affected party, a legal representative of the affected party or a voluntary representative of the affected party.
- They are independent rights. It is not necessary to exercise any of these rights (such as access or rectification) before exercising another (such as deletion or preventing processing)
- They are free rights. Exercising these rights may not incur any fees for the data subject.

2.5 Government SIGINT Surveillance in Spain

In Spain, as in many industrialised countries, the Internet has become part of ordinary everyday life. In 2014, 76.2% of the Spanish population had Internet access, and 74.4% of Spanish households had Internet access. Most of that is broadband (73%) with mobile devices becoming one of the most important accessing tools. 81.7% regard smartphones as their main device for accessing the Internet (INE, 2014).

In addition to the benefits offered by access to the Internet, of course, this all comes with risks to users' privacy. As the European Parliamentary Research Service pointed out in their Mass Surveillance, Risk, Opportunities and Mitigation Strategies report (European Parliamentary Research Service, 2015), the risks of data breaches for users of publicly available Internet services such as email, social networks and cloud computing, are substantial. The report considered the latest technology advances allowing the analysis of user data and their meta-data on a mass scale for surveillance reasons as one of the main risks faced by users.

Following the Snowden revelations various countries have updated their legislation covering SIGINT activity by their national security services. These regulations are often regarded by civil liberties proponents as retroactively authorising prior and ongoing activities which either had no explicit previous authorisation or were even explicitly illegal (Bowcott, 2015). France, for example, approved a law regulating national and international espionage, legalizing the use of methods and "exceptional" technologies (including the use of space antennas and a tracking algorithm for communications) to control, monitor and prevent crimes and attacks of various kinds (Arrieta, 2015). According European Parliamentary Research Service (2015), most EU Member States' Government Intelligence Agencies intercept an enormous amount of information about their citizens. They use direct access to transmission systems, hacking techniques and demands to technology companies that hold user data for copies of that data or direct access to the databases of the companies.

While it has been generally accepted that governments spy on each other's activities, most had not expected that citizens in the liberal democracies were under general surveillance by their own governments (or indeed those of allied countries) without warrants and specific targeting (Campbell, 2015; Delle, 2014).

In Spain these issues came out long before Snowden's revelations about the NSA and GCHQ. The Centre for Defence Information (CESID) spent 11 years recording private conversations, including those of politicians, diplomats, businesspeople, journalists and even the King of Spain (Galiacho, 2007). The scandal was discovered by press, and it had important consequences in Spain's legal and political system. Following revelation of these activities, CESID morphed into the Centro Nacional de Inteligencia (National Intelligence Centre/CNI) in 2001 (CNI, 2015) with a revised structure, including a civilian director, rather than the prior military officer. Spanish judges and politicians were blunt: listening to telephone conversations (wired or wireless) without judicial authorization

deserves criminal sanction (Galiacho, 2007).

Despite these changes to the secret intelligence services in Spain, however, other powerful government authorities see surveillance becoming an ever more pervasive part of modern life. José María Blanco, director of the Centre for Analysis and Forecasting of the Civil Police (Guardia Civil), has said that they expect we will live in a more controlled state, not just increasing the number of video cameras on public zones, but through mobile devices and the Internet (Ballesteros, 2013).

3. Overview of the Surveys

207 respondents studying at two universities in Spain (University of Burgos [UBU] and University of Rovira I Virgili [URV]) were presented with a 37-question online survey, with responses on a likert scale, a yes/no selection or a free-text box. The questions begin with general attitudes to questions of privacy and perception of threats to privacy from groups or technologies. Respondents were then asked if they knew about Edward Snowden's revelation about the activities of the US' NSA and the UK's GCHQ. If they had they were asked how they obtained this information. Whether they had heard of them or not, they were then given a brief neutral presentation of the revelations. They were asked to indicate their evaluation of Snowden's actions (specifically whether they had harmed or helped the public good) and whether they would emulate Snowden themselves (including their reasons). All questions were optional, but all respondents who completed the survey gave answers to most questions.

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.

3.2 Participant Details

Of the 207 respondents, 87/42% were UBU students, and 120/58% were URV students. 95% of the respondents were Spanish nationals. The age of respondents is heavily weighted younger, even within the expected student range: 66% were 18–20 years old, 22% 21–24 years old, and only 12% 25 or older. 47% were male and 53% female (see Table 1). 59% of respondents were studying Social Sciences, Law and Humanities, and 35% technology/engineering.

Table 1: Respondent Attributes

Gender	**Male**				**Female**			
	47%				53%			
Age	18	19	20	21	22	23	24	25+
	20%	29%	17%	7%	3%	9%	3%	12%

4. Survey Results and Discussion

4.1 Attitude towards Privacy

Respondents overwhelmingly regard the Right to Privacy as important, with none replying “Not important at all”, only 1.4% (3) selected “Not so important”, 25.7% (57) selected “Important” and 72.1% (160) chose “Very important” (14 opted out of giving an evaluation, 12 by skipping the question and 2 by selecting “prefer not to answer”). However, as presented below, although they self-reported regarding the right to privacy as (very) important, relatively few indicated that they take significant actions to preserve that right.

Textual analysis of the free-text responses asking for an explanation of their evaluation provides a diverse set of reasons, as shown in Table 2. Some respondents’ responses contained more than one of the categories identified.

Table 2: Reasons for the importance of the right to privacy

Reason	Percentage
Freedom of Intimacy and Association	29.0
Feeling Safe	18.2
Respect	14.5
Being Let Alone	8.6

INTECO (2014) reported that, from a study of Spanish household's cybersecurity and privacy awareness/activity "26.7% of Internet users expose their profiles to strangers and 4.3% of the users do not know anything about privacy settings for their profiles". It also showed that "16% of the users of social nets share their information only with some friends; 52% say that their information only can be seen by their friends; 19.3% share with their friends and friends of their friends; 7.4% share with all users".

Having made strong claims about their view on the importance of the right to privacy, respondents also claimed a good understanding of the right, though less strongly than their belief in its importance. Only 11.1% (23) of respondents reported "hardly understanding" the right to privacy, and only 1.9% (4) reported not understanding at all. All of these had claimed that the right was important or very important. 65.7% (136) of respondents claimed to understand the right, while 42 claimed to understand it very well. Table 3 shows the answers to these two questions separately while Table 4 shows the cross-tabulation of answers.

Table 3: Frequency table of Q10 and Q12

Q10. Is your right to privacy important?		Q12. How well do you understand what the right to privacy is?	
Answers	Frequency (%)	Answers	Frequency (%)
Very important	153 (73.9%)	Understand very well	42 (20.3%)
Important	51 (24.6%)	Understand	136 (65.7%)
Not so important	2 (1.0%)	Hardly understand	23 (11.1%)
Not important at all	0 (0.0%)	Don't understand at all	4 (1.9%)
Total	206	Total	205

Table 4: Contingency table of Q10 and Q12

	Q12. How well do you understand what the right to privacy is?		
Q10. Is your right to privacy important?	Understand (very well)	Hardly/Don't understand	Total
(Very) important	176	26	202
Not (so) important (at all)	2	0	2
Total	178	26	204

Free text responses were also requested, asking respondents to give their definition of the right to privacy. Five common elements emerged from a textual analysis of the responses, which are given in table 5, along with the frequency with which respondents mentioned each.

Table 5: Analysis of Free Text Responses on Defining the Right to Privacy

Please describe what the right to privacy is.	
Freedom	30.9%
Personal choice	28.1%
Security	20.3%
Control	9.2%
Life without problems	1.4%

Despite their belief in the importance of the right to privacy and their claim to understanding (partially borne out by the free text answers shown above) other research on Spanish people shows that few take active measures to protect their privacy. INTECO (2014) reported "42% of the users do not use active security measures; 69.4% of the users say that the updating of security is done automatically in their PC's, while 57.8% of the users never check their devices for virus infections, trusting their anti-virus program to perform perfectly and automatically" and "12.4% of the users do not password protect their home Wi-Fi". Perhaps a belief in the abstract "right" gives respondents a false feeling that they have no related responsibility, but that others (the government, corporations, etc.) will do it all for them.

4.2 Threats to Privacy

Since the majority of Snowden's revelations are in regard to NSA/GCHQ surveillance of Internet-based information, respondents were asked about how much they feel their Internet and non-Internet activities require them to take risks with the privacy. As can be seen from the comparative graph in Figure 1, respondents in this survey regarded Internet activities as much higher risk than non-Internet activities

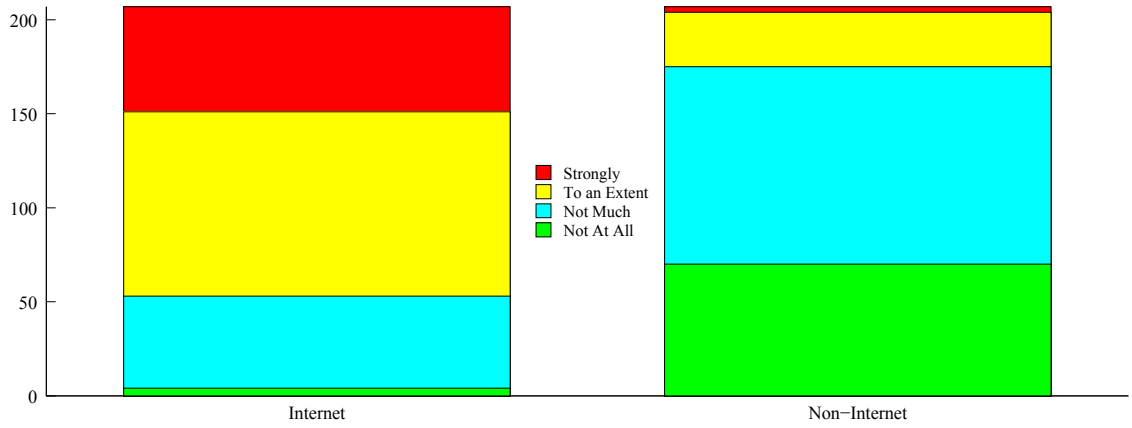

Figure 1: Do you feel that you are taking risks with your privacy? (N=207)

More than seven out of ten respondents (74.4%; 154 of 207) answered that their use of the Internet involved taking risks with their privacy either "strongly" (27.1%; 56 of 207) or "to an extent" (47.4%; 98 of 207), whereas less than one in six (15.5% 32 of 207) felt at high risk in the non-Internet context: "strongly" (1.45%; 3 of 207) or "to an extent" (14.0%; 29 of 207). The average responses to these questions were 2.00 (SE = .05) (Internet) and 0.86 (SE = .05) (non-Internet). The difference between these averages was 1.133 and the results of the t-test indicate this difference is statistically significant at the 1% level ((95% CI [1.024, 1.244]); t: (110) = 20.316, $p < .01$). So, respondents regarded Internet-based activities as significant privacy risks compared with non-Internet activity.

To understand respondents' views on the privacy threats they face online, respondents were also asked to rate the privacy threats posed by various groups or organisations, including people (split into individuals they know well, individuals they know but not well and individuals they don't know), various types of for-profit and non-profit organisations and government organisations including intelligence agencies and others. They were also requested to similarly rate the threats posed by various technologies such as smart phones, home automation which sense human activity, and video game consoles. The same scale was used as for the Internet/non-Internet activity questions. For the ranked list of the privacy threat posed by groups see Table 6 and by technologies see Table 7. It should be noted that some respondents (in most cases less than 10%, and never above

15% of respondents) offered no opinion or had not heard of some groups or technologies, and these respondents' answers are not reflected in these calculations.

Table 6: 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?		
Group	Mean	S.D.
Internet companies	2.59	0.668
Telecom companies/ Internet providers	2.22	0.814
Secret service government agencies	2.10	0.993
Law enforcement government agencies	1.86	1.017
Computer software companies	1.83	0.930
Computer hardware companies	1.80	0.908
Other for-profit companies	1.68	0.884
Other government agencies	1.68	0.950
System Integrators	1.59	0.965
Individuals who you don't know	1.36	0.971
Individuals who you know but not well	1.17	0.749
Health-care organisations	1.17	0.829
Educational institutions	1.16	0.755
Other not-for-profit organisations	1.08	0.816
Individuals who you know well	0.98	1.024

Internet companies such as Google, Twitter, Facebook were considered to post the greatest risk, with an average of 2.59 (out of 3), two-thirds of respondents (138/207) ranking them "very much" a threat to privacy and another quarter (55/207) considering them a threat "to an extent". Telecom companies/Internet providers and both secret service and law enforcement government agencies were also regarded as highly threatening to respondents' privacy. Individuals (known or unknown) and non-profit organisations including health and education institutions were regarded as least threatening to privacy, all with a mean of less than the median value of 1.5.

Table 7: Ranked means (0: low; 3: high) of 17 technologies as perceived privacy threat

Q9. How much do you feel that the following technologies threaten your privacy?		
Technologies	Mean	S.D.
Smart phone	2.29	0.774
Making payments online	2.12	0.837
Online shopping	1.97	0.823
GPS	1.87	0.911
Personal computer	1.73	0.935
Social media services	1.69	0.974
Online auction	1.56	0.907
Online games	1.39	0.907
Survey TV cameras	1.29	0.942
Smart meter	1.25	0.943
Behavioural targeting	1.14	0.984
Home video game console	0.99	0.969
Smart card	0.87	0.999
Portable video game console	0.85	0.982
RFID	0.76	0.947
Personal body monitoring	0.69	0.979
Home automation which senses human activities	0.45	0.938

Smart phones, online payments and online shopping were deemed the riskiest technologies. Despite the poor showing of social media companies such as Facebook in the organisations' question, social media services were close to the median with a mean of 1.69. Home automation technologies such as the NEST thermostat and personal body monitoring devices such as the Fitbit all registered as low level threats with means of 0.45 and 0.69 respectively.

The low perception of a threat to privacy from those known to respondents, shown by the following analysis:

Individuals who you know well:

Very much: 23/207(11.1%); To an extent: 34/207 (16.4%);

Not much: 59/207 (28.5%); Not at all 85/207 (41.0%))

Individuals who you know but not well:

Very much: 7/207(3.4%); To an extent: 56/207 (27.05%);

Not much: 103/207 (49.8%); Not at all 35/207 (16.9%))

contrasts with the results of other surveys regarding non-privacy harms online among young people. A study of US teens in 2007 by the National Crime Prevention Council (2007) reported that 43% of male teens and 57% of female teens (aged 13-17) studied reported being victims of cyberbullying. Microsoft (2009) reported that almost a third of European teenagers had been cyberbullying victims. According to (Kirwan and Power, 2012) these attacks can come from well-known people, casual acquaintances or strangers.

So, on the one hand, a significant majority perceive various technologies as threats to their privacy, but on the other hand they still use them, INTECO (2014): "86.8% of the cyber users with a high frequency of Internet usage had a Smartphone or similar electronic device". This reflects the near-impossible situation that many users are placed in with regards to modern technologies and privacy, that there are no good privacy-preserving options or solid legal protections available yet the benefits are such that users end up using them anyway as discussed by Adams (2014).

4.3 The Degree of Recognition of and Interest in Snowden's Revelations

Almost 60% (121/207) of respondents had heard about Snowden's revelations. Respondents were asked about their sources of information. They could select "all that apply" of the options given. Most (76.0%; 93/121) had seen TV news reports, 62.0% (75) had read about it on the Internet, 48.8% (59) had read newspaper articles and 45.5% (55) through social media platforms. Only 18.2% (22) had heard about it from friends and only 7.4% (9) had heard about it via university lectures.

Half of those who had heard about Snowden's revelations (51.2%; 62/121) had discussed the topic with other, and half had 46.3% (56) had searched for further information. Those who had spoken about it to others were also more likely to have searched for information and vice versa (those who had not spoken to others were less likely to have searched for information) at a 1% significance level, according to a Fisher Exact Test (see Table 8 for the contingency table).

Table 8: Contingency table of Q21 and Q22

	Q22. Have you ever searched for information about Snowden's revelations??		
	Yes	No	Total
Q21. Have you ever talked about Snowden's revelations with others? Yes	38	24	62
Q21. Have you ever talked about Snowden's revelations with others? No	16	38	54
Q21. Have you ever talked about Snowden's revelations with others? Total	54	62	116

Despite most respondents (78/121) who had heard of Snowden's revelation looking it up and/or discussing it with friends, their claimed level of knowledge was limited. Only a small minority claimed to know "A lot" (4/121), 46 claimed "A fair amount" of knowledge, but a majority indicated "Not much" (51) or "Little" (19) knowledge.

4.4 Evaluation of Snowden's Conduct

The vast majority (67.1%; 139/207) of respondents felt that Snowden's revelation had served rather than harmed the public interest (29.5%/61 indicated "Served it a lot" while 37.7%/78 said "Served it to an extent"). Only 16.9% (35) felt that the public interest had been harmed (6.3%/13 "Harmed it a lot" and 10.6%/22 "Harmed it to an extent").

Free text answers to the question "Why do you think Snowden determined to make those revelations?" produced similarly strong positive evaluations. While 26 explicitly stated "don't know" and 39 provided no clear response, 67 clearly reported that Snowden had concerns for the privacy of ordinary people, 52 that he felt people needed to know what was happening, 26 that he was acting under his belief in an ethical imperative, and ten mentioned defence of democracy (some respondents mentioned more than one of these issues). Only nine suggested it was for some personal gain, such as fame or money. (Some respondents gave more than one positive reason.)

4.5 Empirical Consideration of the Impact of Snowden's Revelations

Both Snowden's supporters and opponents have claimed that his revelations had an impact. Supporters have claimed that it has stimulated debate and legal actions, though in the case of the legal situation in various countries the outcome is a mix of some limited restrictions to the activities of security services, or expansion of judicial redress (Childress, 2015), but in other cases an explicit legalisation of actions previously illegal or of unclear legality (Travis, 2016). There has been limited research on ordinary people's direct responses in terms of their behaviour and use of technology.

This survey asked respondents about these issues with both selection and free-text answers. The level of claimed knowledge of Snowden's revelations was also compared to statements about changes in behaviour.

In addition, the question of whether those who had heard about Snowden's revelations have a greater perception of the privacy threats posed by government agencies is also considered. Of course correlation is not causation and it is possible that those with an existing greater mistrust of government agencies were more likely to hear about and pay attention to Snowden's revelations because it confirms their existing bias.

4.5.1 Personal Changes in Communication Behaviour

Respondents were asked "Have you changed your way of communicating online using systems such as social media (e.g., Twitter, Facebook), Messenger (WhatsApp), YouTube, blogging, Skype, email and instant messaging since you heard about Snowden's revelations?". A majority (58.7%; 71/121) indicted that they had made one or more changes. The numbers indicating which change are shown in Table 9. A Chi-squared test shows that the number of respondents reporting a change is significant at the 1% level: Chi-Squared (71/50) 42.572, $p<0.01$.

Table 9: Have you changed your way of communicating online?

Answer (N=121)	N	%
Have not changed at all	46	38.0%
Stopped using some systems	9	7.4%
Have tried to cut down my use of some systems	25	20.7%
Have deleted (some of) personal data and contents I had posted on social media	22	18.2%
Have paid more attention to personal data and contents posted on social media	41	33.9%
Have changed my privacy settings on some systems	34	28.1%
Prefer not to answer	4	3.3%
Other changes...Please specify	6	5.0%

Other changes given included starting to use Tor (the Onion Router), installing the CyanogenMod community build of Android, and setting up three accounts on social media: personal/professional/fake.

A Fisher Exact Test examining the link between the claimed level of knowledge of Snowden's revelations (High/Low) and whether or not respondents had changed their ways of communicating

online failed to show a correlation.

4.5.2 Social Changes Due to Snowden's Revelations

Only 29.0% (60/207) of respondents felt that Snowden's revelations had led to social change (25.1%/52 said there had been no change; 31.0%/6 had explicitly no opinion on changes; 15.0%/31 preferred not to answer). Of these 60, 30 thought that people had become more careful of their privacy (though only two specifically mentioned the development or increased use of privacy technology). Ten thought that it had increased awareness of the risks of online activity, and another nine that it had increased awareness of the activities of spying agencies. A few others mentioned increased mistrust of technology, states and agencies.

4.5.3 Privacy Threat Perceptions Compared to Knowledge of Snowden's Revelations

In general, respondents regarded Secret Service Government Agencies, Law Enforcement Government Agencies and Other Government Agencies as a threat to their privacy (see Table 7 above). Responses were further analysed to check for correlation between knowledge of Snowden's revelations and these perceptions of privacy threat. Although in each case the mean threat perception was greater amongst respondents who had heard about Snowden's revelations there was no statistical significance to this difference for any of the three government groups. See Table 10 for the detailed statistics.

Table 10: Threat Perception of Government Agencies Between Heard/Not Heard Group.

Q19x	Group	N	Mean	SD	SE
m. Law enforcement government agencies (Police)	Heard	126	1.8700	.97967	.08728
	Not-Heard	82	1.7800	1.11138	.12273
n. Secret service government agencies (CNI)	Heard	126	2.1700	1.00462	.08950
	Not-Heard	76	1.9600	1.01247	.11614
o. Other government agencies (Health, Interior, Tax, etc.)	Heard	118	1.7034	.92736	.08537
	Not-Heard	72	1.6111	1.01476	.11959

Independent Samples Test

		Levene's Test for Eq of Var		t-test for Equality of Means						
									95% CI of Diff	
Q19.	Equal Var	F	Sig.	t	df	Sig. (2-tail)	M Diff	SE. Diff	Lower	Upper
m.	assumed	4.640	0.032	0.631	206.00	0.529	0.093	0.147	-0.197	0.382
	not ass.			0.614	157.53	0.540	0.093	0.151	-0.205	0.390
n.	assumed	0.144	0.705	1.463	200.00	0.145	0.214	0.146	-0.074	0.503
	not ass.			1.460	157.26	0.146	0.214	0.147	-0.076	0.504
o.	assumed	1.662	0.199	0.642	188.00	0.522	0.092	0.144	-0.191	0.376
	not ass.			0.628	139.77	0.531	0.092	0.147	-0.198	0.383

Chi-squared tests on the cross-tabulation of Q6 (Do you feel that your use of the Internet involves taking risks with your privacy?) and Q19 (Have you heard about Snowden's Revelations?) reveal no statistically significant differences.

4.6 Would Respondents Follow Snowden's Lead?

Respondents were asked two hypothetical questions about whether they would seek to emulate Snowden. First they were asked if they would do what he had done if they were also US citizens and had such knowledge about the NSA (the US hypothetical or QUS). Second, they were asked a similar question about being a Spanish citizen and finding out that Spain's government agencies were acting similarly (the Spanish hypothetical or QESP). In each case respondents were asked for free-text responses explaining their positive or negative choice (those who "preferred not to answer" were not asked for an explanation).

For the US hypothetical, 42.0% (87/207) claimed they would act similarly to Snowden. 28.5% (59) said they would not and 29.5% (61) preferred not to answer. For the Spanish hypothetical, 47.3% (98) claimed they would act similarly to Snowden, 28.0% (58) said they would not and 24.6% (51) preferred not to answer. The differences in answers were not a simple matter of those who would not follow Snowden's lead in the US being willing to follow it in Spain as shown by the contingency table in Table 11.

Table 11: Contingency table of QUS and QESP

QESP \ QUS	Yes	No	No Answer
Yes	70	11	17
No	8	42	8
No Answer	9	6	36

A Chi-squared test for consistency between the answers to the two questions showed that there was a correlation between the two sets of answers at the 1% level (Chi-squared=131.869; df=4; $p<0.01$). So, the slightly higher percentage of those willing to emulate Snowden in the Spanish hypothetical than in US hypothetical was not significant.

Comparing respondents' evaluation of Snowden's actions to their willingness to emulate him provides some varying results. By collapsing the answers to Question 28 (Have Snowden's Actions Served or Harmed the Public Good?) from "Served it a lot" and "Served it to an extent" into a "positive" evaluation and from "Harmed it to an extent" and "Harmed it a lot" into a "negative" evaluation (with others placed into canonical missing values), and producing contingency tables (Table 12) for the US and Spanish hypotheticals, a greater tendency to be willing to follow Snowden's example among those with a positive view of his actions can be seen in both cases, and a tendency to be unwilling to follow Snowden's example among those with a negative view of his actions.

Table 12: Contingency Tables for Q28 and QUS/QESP

Q28 \ QUS	Yes	No	Total
Served	71	42	113
Harmed	11	14	25
Total	82	56	138

Q28 \ QESP	Yes	No	Total
Served	82	35	117
Harmed	10	14	24
Total	92	49	141

However, a Chi-squared test shows that for the US hypothetical there is no statistical significance to this relationship between evaluation and willingness to emulate (Chi-squared(1)=3.011, $p > 0.1$). In the Spanish hypothetical case, however, there is a correlation at the 5% significance level (Chi-squared(1)=7.093, $p<0.05$).

Responses to the free text questions as to why they would emulate Snowden tended to repeat similar reasons to those respondents had given as to why they believed Snowden himself had made his revelations: to safeguard the privacy of citizens (18%), because citizens need to know more about the spying they are subjected to (16%), because it is the right thing to do/is ethical (8%)

4.7 Gender Differences

As the survey respondents were split approximately equally between males and females, various questions were analysed to check for significant differences in outcome for these two groups: Level of knowledge of Snowden's revelations; Evaluation of Snowden's actions; Willingness to emulate Snowden's actions in the US or Spanish hypothetical. Only in the level of knowledge was a statistically significant difference identified. Collapsing "A lot" and "A fair amount" into a "High Knowledge" group and "Not much" and "Little" into a "Low Knowledge" group and comparing that with reported gender, males were more likely to report "High Knowledge" than females at the 1% significance level (Chi-square (1)=7.87, $p < 0.01$). Of course, this is an untested self-report and this difference may simply be due to overconfidence rather than an actual higher level of knowledge (as per Bhandair and Deaves (2006) which showed overconfidence in highly educated males about their investment decision-making ability).

4.8 Privacy Versus Security

In discussions of state surveillance it is often claimed that citizens must give up privacy in order to gain security (e.g. US President Obama, reported in Spetalnick and Holland (2013)). This oppositional frame is disputed by many scholars such as Solove (2011) and Pavone and Esposito (2012) and by digital rights groups (Hintz and Dencik, 2016). At one extreme, this can be used to undermine any claim to individual privacy from state-sponsored surveillance. Since Snowden's revelations this concept has been debated on multiple fronts and in multiple fora, including for example debates around the right of non-government organisations and individuals to use strong encryption in their communications (Bay, 2017; Meinrath and Vikta, 2014). The survey asked respondents "How much do you feel that Spanish individuals must give up privacy and freedom in order to ensure safety and security of the society and individuals?" 15/207 offered no opinion and 10 preferred not to answer. The remaining 182 were mostly evenly split with 15.9% (29) saying "not at all" and 35.2% (64) saying "Not much" but another 35.2% (64) saying "To an extent" and 13.7% (25) responding Very much".

5. State Surveillance in Spain Following Snowden

There has been limited public debate in Spain about the NSA's activities and cooperation with it by the CNI. As discussed by Clavell (2014) the subject of electronic surveillance of the general population has been limited to the technology sections of the left wing press. What little parliamentary debate there has been was forced by opposition parties, while a closed door meeting between parliamentarians and CNI management resulted only in a statement claiming that CNI operates entirely within Spain's legal regime and that coordination with the NSA is part of NATO operations aimed at overseas (non-EU) targets, mostly in Africa.

Despite successfully reducing unauthorised economic migration from Africa from its high point of 8,450 (still a tiny number compared to Spain's population) in 2011, Spain has adopted significant physical surveillance of its bordering sea areas and surrounding its land enclaves in Africa, in collaboration with the European border and coastguard agency FRONTEX (n.d.). A tendency to associate surveillance issues with illegal immigrants as targets tends to distract from and delegitimise public discussion and political debate about electronic surveillance. For example, having created primary national legislation to implement the EU's Data Retention Directive, the CJEU's overturning of the directive has led to no change in Spanish law, although cases brought to the CJEU about other country's national (re)implementations may require action in Spain in the future.

6. Conclusions and Future Research

Snowden's revelations seem to have confirmed the concerns many Spanish young people had about being spied on (Murata et al, 2014). Others have commented that Snowden's revelation were often not about completely unknown operations or capabilities of the NSA/GCHQ, but that they were concrete proof of the extent of their activities including things previously dismissed by many as technically possible but highly unlikely due to the likely small benefit and the immense cost (such as regular tapping of undersea cables) (Bonney and Barnett, 2014).

This survey shows that most young people in Spain are aware of Snowden's revelations but that their ability/willingness to take actions in response is limited. The lack of continued coverage of further revelations (partly driven by political and public finance problems in Spain taking media attention but also the lack of more specifically Spanish revelations) has decreased attention to the issues over time. The acceptance of a privacy/security trade-off also militates against a strong reaction in Spain to government surveillance whether by the Spanish or foreign governments.

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. 65 academics from Universities around Japan helped in

encouraging their students to respond to our survey. There is no space to list them here, but the authors extend their sincere thanks for those efforts. Meiij University's Yasunori Fukuta provide additional statistical analysis of responses.

References

ABC (2007), "Un inspector asegura que perseguían a varios de los acusados desde enero de 2003", 21st March, available at http://www.abc.es/hemeroteca/historico-21-03-2007/abc/Nacional/un-inspector-asegura-que-perseguian-a-varios-de-los-acusados-desde-enero-de-2003_1632098197387.html, (accessed 28th October 2016). In Spanish.

Adams, A. A. (2014), "Facebook Code Social Network Sites Platform Affordances and Privacy", *Journal of Law, Information and Science,* Vol. 23 No. 1, pp. 158-168, available at http://www.jlisjournal.org/abstracts/adams.23.1.html. (accessed 17th November 2016).

Arrieta E. (2015), "¿Nos espían los gobiernos?" *Diario Expansión*, available at http://www.expansion.com/tecnologia/2015/05/23/555cc862ca474168478b45b8.html (accessed 23rd May, 2015). In Spanish.

Bhandari, G., and Deaves, R. (2006), "The demographics of overconfidence", *The Journal of Behavioral Finance,* Vol. 7 No. 1, pp. 5-11.

Ballesteros R. (2013), "El Centro de Prospectiva de la Guardia Civil pronostica una sociedad vídeo vigilada antes de 2030", *lainformacion.com, available* at http://noticias.lainformacion.com/espana/el-centro-de-prospectiva-de-la-guardia-civil-pronostica-una-sociedad-video-vigilada-antes-de-2030_WjlPAkMoqAYkoHoNbfb387/ (accessed 15th January 2015). In Spanish.

Bay, M., 2017, "The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone", *First Monday*, Vol. 22 No. 2, Article 6.

BBC News (2013), "NSA surveillance: Spain demands US explains 'monitoring'", 28th October, available at http://www.bbc.com/news/world-europe-24708410 (accessed 31st October 2016).

Bonney, W. and Barnett, A. (2014), "'We had to wait for Snowden for proof', an exchange with NSA whistleblower William Binney", *openDemocracy,* 5th June, available at https://www.opendemocracy.net/william-binney-anthony-barnett/%E2%80%9Cwe-had-to-wait-for-snowden-for-proof%E2%80%9D-exchange-with-william-binney (accessed 30th November 2016).

Bowcott, O. (2015), "*Intelligence officers given immunity from hacking laws, tribunal told"*. The Guardian, 15th May, available at https://www.theguardian.com/uk-news/2015/may/15/intelligence-officers-have-immunity-from-hacking-laws-tribunal-told (accessed 2nd November 2015).

Borger, J. (2013), "GCHQ and European spy agencies worked together on mass surveillance". *The Guardian,* 1st November, available at https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (accessed 28th October 2016).

Campbell, D. (2015), "GCHQ and Me: My Life Unmasking British Eavesdroppers", *The Intercept,* 3rd August, available at https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/ (accessed 2nd November 2016).

Chari, R. (2004), "The 2004 Spanish election: Terrorism as a catalyst for change?", *West European Politics,* Vol. 27 No. 5, 954-963.

Childress, S. (2015), "United States of Secrets: How the NSA Spying Programs Have Changed Since Snowden", *PBS Frontline,* 9th February, available at http://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/ (accessed 18th November 2016).

Clavell, G. G. (2014), "Surveillance in Spain: a slowly developing debate amid political indifference", *OpenDemocracy.net,* 15th May, available at https://www.opendemocracy.net/can-europe-make-it/gemma-galdon-clavell/surveillance-in-spain-slowly-developing-debate-amid-politica (accessed 28th November 2016).

CNI (2015), "El CNI, al servicio de España y de los españoles; Centro Nacional de Inteligencia", http://www.cni.es/es/queescni/historia/elcni/ (accessed 15th January 2015). In Spanish.

Comisión Española de Ayuda al Refugiado (2016), "Informe 2015. Las personas refugiadas en España y en Europa", available at https://www.cear.es/wp-content/uploads/2016/06/Informe_CEAR_2016.pdf (accessed 4th April 2017). In Spanish.

Constitución Española (1978), "BOE núm. 311, 29 de diciembre de 1978", available at http://www.congreso.es/consti/index.htm (accessed 5th January 2015). In Spanish.

Delle Femmine, L. (2014), "El gobierno español hace muy buen espionaje, entrevista a Eugene Kaspersky", available at http://tecnologia.elpais.com/tecnologia/2014/05/05/actualidad/1399281568_671465.html (accessed 15th January 2015). In Spanish.

Digital Rights Ireland v. Minister for Communications (2012), ECJ Joined Cases C-293/12 and C-594/12.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicl, available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

European Parliamentary Research Service (2015), "Mass Surveillance, Risk, Opportunities and Mitigation Strategies report", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf (accessed 15th January 2015).

FRONTEX (n.d.) "Western Mediterranean Route: Report from the European Border and Costguard Agency", available at http://frontex.europa.eu/trends-and-routes/western-mediterranean-route/ (accessed 28th November 2016).

Galiacho, J. L. (2007), “Las escuchas del CESID. Los espías del gobierno grababan hasta al rey, 18 historias que cambiaron España”, *El Mundo,* available at http://www.elmundo.es/especiales/2007/10/comunicacion/18elmundo/cesid.html (accessed 15th January 2015). In Spanish.

García de Cortazar, F., Gonzalez J.M. (2012), *Breve Historia de España,* Alianza Editorial, Madrid. In Spanish.

Government of the Principality of Asturias (2015), “ARCO Rights”, available at https://sede.asturias.es/portal/site/Asturias/menuitem.fe57bf7c5fd38046e44f5310bb30a0a0/?vgnextoid=290c7a0266719210VgnVCM10000097030a0aRCRD (accessed 15th January 2015).

Hintz, A., and Dencik, L. (2016), The politics of surveillance policy: UK regulatory dynamics after Snowden”, *Internet Policy Review,* Vol. 5 No. 3, pp. 1-16.

INE (2014), “Notas de presa: Encuesta sobre Equipamiento y uso de Tecnologías de Información y Comunicación en los Hogares”, available at http://www.ine.es/prensa/np864.pdf (accessed 15th January 2015).

INTECO (2014), “Estudio sobre la ciberseguridad y confianza de los hogares españoles”, *Instituto Nacional de Tecnologías de Comunicación,* available at http://www.ontsi.red.es/ontsi/sites/default/files/ciberseguridad_y_confianza_en_los_hogares.pdf (accessed 15th January 2015). In Spanish.

Kirwan, G. and Power, A. (2012), *The psychology of cybercrime: Concepts and Principles,* IGI Global, Hershey, PA.

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*, 265-272.

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

Lamb, G. M. (2009), “How we are losing our privacy online”. CS Monitor. com

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).

Meinrath, S.D. and Vitka, S., (2014), “Crypto War II”, *Critical Studies in Media Communication*, Vol. 31 No. 2, pp.123-128.

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 **??-??**

Nash, Elizabeth (2006), “Madrid bombers 'were inspired by Bin Laden address'”, *The Independent,* 7th November, available at http://www.independent.co.uk/news/world/europe/madrid-bombers-were-inspired-by-bin-laden-address-423266.html (accessed 28th October 2016)

National Crime Prevention Council (NCPC) (2007), "Teens and Cyberbullying", available at http://www.ncpc.org/resources/files/pdf/bullying/Teens%20and%20Cyberbullying%20Research%20Study.pdf (accessed 17th November 2016).

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

Pavone, V. and Esposti, S. D. (2012), "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", *Public Understanding of Science,* Vol. 21 No. 5, pp. 556-572.

Rodríguez Tejada, S. (2014), "Surveillance and student dissent: The case of the Franco dictatorship", *Surveillance & Society,* Vol. 12 No. 4, pp. 528-546.

Sánchez, A. C. (2009), *Fear and progress: ordinary lives in Franco's Spain, 1939-1975,* John Wiley & Sons, Chichester.

The Spanish Constitution (1978), available at https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf (accessed 1st November 2016).

Solove, D. J. (2011), *Nothing to hide: The false tradeoff between privacy and security,* Yale University Press, New Haven, CT.

Spanish Government (2016), "Asilo en Cifras (2008-2014)", Ministerio del Interior. In Spanish.

Spetalnick, M. and Holland, S. (2013), Obama defends surveillance effort as "trade-off" for security", *Reuters,* 7th June, available at http://www.reuters.com/article/us-usa-security-records-idUSBRE9560VA20130608 (accessed 30th November, 2016).

Travis, A. (2016), "UK security agencies unlawfully collected data for 17 years, court rules", *The Guardian,* 17th October, available at https://www.theguardian.com/world/2016/oct/17/uk-security-agencies-unlawfully-collected-data-for-decade (accessed 18th November 2016).