

# The social impact of Snowden's revelations on Mexican youngsters.

Andrew A. Adams  
Meiji University. [aaa@meiji.ac.jp](mailto:aaa@meiji.ac.jp)

Juan Carlos Yáñez-Luna  
Universidad Autónoma de San Luis Potosí. [jcyl@uaslp.mx](mailto:jcyl@uaslp.mx)

Pedro I. González Ramírez  
Universidad Autónoma de San Luis Potosí. [pedro.gonzalez@uaslp.mx](mailto:pedro.gonzalez@uaslp.mx)

Mario Arias-Oliva  
Universitat Rovira I Virgili. [mario.arias@urv.cat](mailto:mario.arias@urv.cat)

Kiyoshi Murata  
Meiji University. [kmurata@meiji.ac.jp](mailto: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 Mexico, taking its socio-cultural and political environment surrounding privacy and state surveillance into account.

**Design/methodology/approach** – A questionnaire was answered by 160 Mexican 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 a limited influence over Mexican youngsters' attitudes toward privacy and state surveillance, although there is a great awareness by Mexican young people of individual rights issues.

**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** – The results of this study based indicate an urgent necessity for providing Mexican youngsters with opportunities to learn more about privacy, liberty, individual autonomy and national security.

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

**Keywords** Edward Snowden, privacy, state surveillance, social impact, Mexico

**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 Mexico.

### **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 Privacy, Surveillance and Snowden in Mexico**

SIGINT agencies such as the NSA are no longer focussed solely on foreign government and military targets, but now routinely regard everyone in the world as a legitimate target and every type of communication as legitimate means of surveillance (Connolly, 2015; Johnson, 2015; Jiménez Barca, 2015). The documents revealed by Snowden included a number of specific references to Mexico, which is used as an example in case studies in internal newsletters and training documents (Fromkin, 2015), as well as the target of espionage aimed at Mexican trade negotiators:

“The Western European and Strategic Partnerships division primarily focusses on foreign police and trade activities of Belgium, France, Germany, Italy and Spain, as well as Brazil, Japan and Mexico.”  
The International Security Issues Build-Out (2012)

As Pfeffer Urquiaga (2000) suggests, modern technology creates personal data in a broad variety of forms including text, voice and video, through CCTV surveillance systems, smartphones and personal computer webcams, but most people have a very limited understanding of the scope of potential privacy invasions this allows.

Citizens of countries which currently have relatively democratic systems of government but which have within living memory experienced authoritarian regimes tend to overestimate the ability of regulatory mechanisms to restrict surveillance. They also tended (before Snowden) to be unaware that the US and UK in particular (but also other countries) have brought their cold war SIGINT capabilities to bear on a broad range of targets without significant technological, resource or ethical restrictions.

## **2 State Surveillance in Mexico.**

### **2.1 Historical Overview.**

Like many former colonies, Mexico as such did not exist as a single country historically. However, the dominant political powers in that geographic area are believed to have depended on espionage techniques to maintain their military and political power. The Aztec empire is reported to have employed traders and merchants to detect signs of dissent or organising opposition to their rule and to expand their influence: "New markets, supplies and trading routes were established by violent means, with the information on where to apply the violence provided by merchants acting as spies. However, the military used others to spy on these merchants in turn." (Rivera Cabrieles, 2012, p. 51).

The Spanish colonial invaders used members of the subordinate populations as interpreters, informants and spies to aid in their battle for control against the incumbent, local, Aztec empire (González Hernández, 2002), eventually forming the colony of New Spain, covering all of modern Mexico, and extending both north into what is now the USA, and south into Central and South America.

The early nineteenth century saw multiple attempts to divide New Spain from Spain. As with other such independence movements, espionage played a significant role on both sides in a conflict that lasted decades and had multiple iterations, with some groups switching sides between continued support for the status quo and support for separation. One famous example of a supporter of independence was Leona Vicario de Quintano Roo, who acted as a central information hub for early independence movements, using her high social standing and wealth to build a spy network, distribute rebel correspondence, and support meetings with families of prisoners (Manzanera, 2008).

### **2.2 Revolution and Surveillance**

From 1910-20 Mexico was embroiled in political turmoil, revolution and civil war. The US continued to target Mexico for surveillance as it always had (Katz, 2006, p. 275), given extra impetus by links to surveillance of Germany in the lead up to and during the First World War, and during the brief US invasion of Mexico in 1916 (Benítez Manaut, 2012). The final outcome of this period was the establishment of single party rule under an evolving set of "revolutionary parties", culminating with the Partido Revolucionario Institucional (PRI: Institutional Revolutionary Party) created in 1946.

During World War II Mexico was again the target of espionage. Nazi Germany established a very effective spy network in European and North American countries, including Mexico, as mentioned by Katz (2006, p.377) "The Nazis expanded their spy networks in Latin America, its main targets Argentina, Chile and Mexico." Other countries also sought to expand their spy-networks in Mexico, such as the Soviet Union "...whose interests in Mexico focused on the one hand on trade and on the other hand on espionage: the country [Mexico] was one of the most important bases of Soviet espionage in America" (Katz, 2006).

According to Riva Palacio (2013), during the mid-twentieth century the government of Mexico and the CIA engaged in joint surveillance of communist countries using a base in the US Embassy in Mexico. However, he also claims that the CIA sabotaged Mexican companies to destabilise both the economy and political system, to clear the way for US subsidiaries, and engaged in corruption payments to union leaders, journalists, politicians and diplomats to advance the interests of the United States.

The PRI monopolized all major political offices in Mexico until 1988, holding all Mexican Senate seats, State Governorships and the Presidency. Gradual political and electoral reforms and discontent within the party in the late 80s and through the 90s led to a non-PRI president in 2000. In the following few years economic and social instability related to the drug trade increased, and the election process has not proven robust, leading to accusations that the return to power of the PRI in 2012 was not through democratically valid means (Weisbort, 2012).

### **2.3 Recent Politics and Surveillance: the Drug War**

The US War on Drugs (Friman, 1996) had a significant impact on Mexico throughout the twentieth century. However, as Lindau (2011) explains, the weakening of formal executive power in Mexico following the introduction of democratic reforms has led to a political expansion of judicial and law enforcement activities justified by reference to the war against the drug cartels. This has included expansion of physical, electronic and economic surveillance programs.

Similar to the data retention regime for telecommunications providers instituted by the European Union's Data Retention Directive of 2006 (annulled by the CJEU in 2014), in 2010 the Mexican government proposed a number of reforms to the national telecom law, including the requirement for carrier companies to store their customers' metadata for two years (Bogado, 2016). As in other countries, these requirements, and the lack of oversight of access to the data by law enforcement and other government authorities, have been controversial and the subject of objections by ordinary people, civil and digital rights groups and opposition political parties. Mexican citizens in general, however, have limited understanding of their information rights and how to protect themselves from online crime, fraud, etc. (Ornelas Núñez and Higuera Pérez, 2013).

According to Vite Pérez (2015), Mexican government surveillance is primarily conducted by the Mexican military in the service of public safety, and the scale of violence in Mexico due to drug cartels is indeed significant. However, there are few safeguards in place to prevent misuse of these capabilities for other purposes, and the Mexican government cooperates with the US, allowing the installation of equipment in Mexico, with the intention of intercepting communications and accessing computer equipment (Vargas, 2013). Following Snowden's revelations, information has come out from other sources revealed about government hacking and interceptions, including activities in Mexico. One of these was the release in of documents (ironically obtained by hacking) from the Italian surveillance and computer intrusion software provider "Hacking Team". The released data indicated that Mexico was the largest state client of the company (De Castro, 2015).

### **3. Outline of the survey**

The survey consists of 37 questions (in English) with a variety of answers forms including yes/no; Likert Scales and free text responses (which could be given in English or Spanish). The survey begins with questions about demographic information such as age, gender and study subject. The second set focusses on respondents' attitudes to the right to privacy and views on threats to privacy. Respondents are then asked about their knowledge of and attitudes towards Edward Snowden's revelations about NSA and GCHQ operations.

Respondents in Mexico were all studying Economics or International Trading and Business in the Faculty of Economics at the Autonomous University of San Luis Potosi, including both recently enrolled

and upper year students. Minors were excluded from taking the survey. Responses were collected between 17th and 31st of October 2014.

Although the survey was conducted using the SurveyMonkey online system, respondents were given the appropriate URL and asked to complete it during a classroom session, rather than sent a link in email and asked to fill it in on their own time.

### 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 Overview of Respondents

163 respondents took the survey but three sets were incomplete, giving 160 complete surveys for analysis. The age and gender balance of respondents is show in Table 1.

**Table 1: Respondents' attributes (number (%))**

Gender	Male				Female			
	72 (45.%)				88 (55%)			
Age	18	19	20	21	22	23	24	25+
	83 52%	33 21%	26 16%	10 6%	2 1%	2 1%	2 1%	2 1%

## 4 Survey results and discussion.

### 4.1. Mexican Circumstances Related to Snowden's Revelations

#### 4.1.1. Attitudes towards the Right to Privacy in Mexico

When asked, without being given a definition, whether the right to privacy is important, respondents overwhelmingly (89.4%; 143/160) selected “Very important”, and another 8.1% (13) choosing “Important”. Only two felt it was “Not so important” and none that it was “Not important at all” (two preferred not to answer). They were less sure of their understanding of what the right is with only 26.9% (43) claiming to “Understand it very well” and 61.9% (99) reporting that they “Understand”. Only 15 reported “Hardly understand” and just three “Don't understand at all” (see Table 2). An oddity in the contingency table (see Table 3) for these two questions is that 13 respondents regard the right to privacy as “Very important” but “Hardly understand it”.

**Table 1: Frequency table of Q10 and Q13**

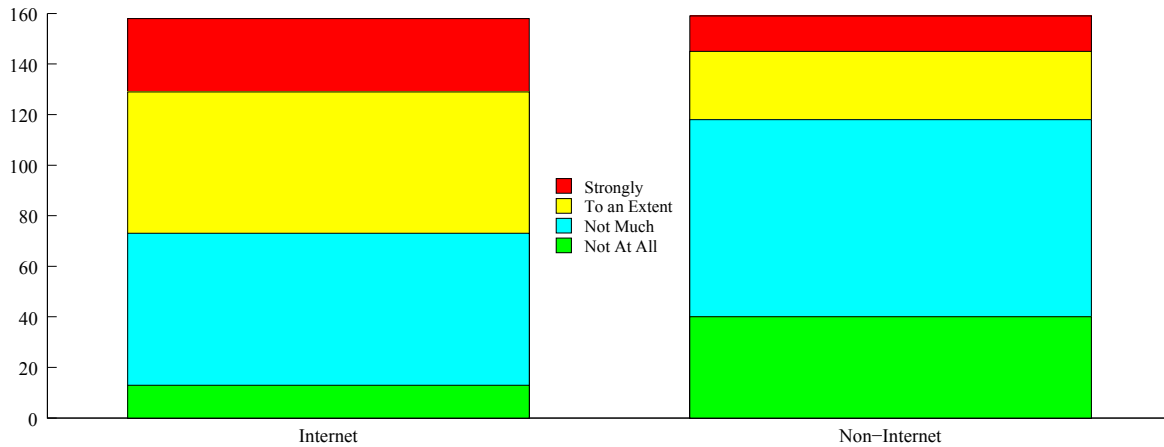
Q10. Is your right to privacy important?		Q13. How well do you understand what the right to privacy is?	
Answers	Frequency (%)	Answers	Frequency (%)
Very important	143 (89.38 %)	Understand very well	43 (26.88%)
Important	13 (8.13%)	Understand	99 (61.88%)
Not so important	2 (1.25%)	Hardly understand	15 (9.38%)
Not important at all	0 (1.25%)	Don't understand at all	3 (1.88%)
Total	158	Total	160

**Table 3: Contingency table of Q10 and Q13**

Q10. Is your right to privacy important?	Q13. How well do you understand what the right to privacy is?				Total
	Understand very well	Understand	Hardly understand	Don't understand at all	
Very important	40 (25.31%)	88 (55.70%)	13 (8.23%)	2 (1.27%)	143 (90.51%)
Important	3 (1.90%)	10 (6.33%)	0 (0.00%)	0 (0.00%)	13 (8.23%)
Not so important	0 (0.00%)	1 (0.63%)	1 (0.63%)	0 (0.00%)	2 (1.27%)
Not important at all	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Total	44 (27.85%)	99 (62.66%)	14 (8.86%)	2 (1.27%)	158 (100.00%)

Respondents were also asked to explain the importance (or lack of it) of the right to privacy in a free-text answer. Both of the respondents who regarded the right as not so important gave variations on the “nothing to hide, nothing to fear” comment so beloved of politicians attempting to justify state surveillance (Solove, 2011). All 156 respondents who indicated that privacy was an important right gave a free text answer, almost all providing recognisable answers that fall into one, or more, standard justifications for privacy: 50 presented it as a fundamental right; while 46 referred to the problem of misuse of personal information, some with specific examples such as credit card fraud but most with general concern about misuse; the security benefits of good privacy were referred to by 29 respondents; the right to a personal life was mentioned by 21; while 14 gave some version of a need or desire for autonomy; a small minority of four explicitly mentioned concern about their reputation with respect to maintaining privacy.

Respondents were also asked to evaluate whether their Internet and non-Internet activities involve taking risks with their privacy. The results are shown in Figure 1.



**Figure 1: Do you feel that you are taking risks with your privacy? (0="Not at All"; 3="Strongly")**

Collapsing “Strongly”/“To an Extent” into “Yes” and collapsing “Not Much”/“Not At All” into “No”, 53.8% (85/158) felt that Internet activity posed a risk to their privacy while only 25.8% (41/159) felt that non-Internet activity posed a risk.

Taking the four point likert scale as a quantitative evaluation by respondents of the level of perceived risk from 0 (“Not at all”) to 3 (“Strongly”), the mean score of perceived privacy risk of the Internet use (1.64) was higher than that of non-Internet activities (1.09), and the difference ( $D = 0.55$ ) was significant at the one percent level via a t-test ( $t(159) = 5.809, p < 0.01$ ).

Respondents were asked to indicate the level of risk associated with different groups of people and technologies. Table 4 shows the mean score of groups as a threat of privacy invasion (0: “Not at all”; 3: “Strongly”). The top privacy invasive groups were “Internet companies” (2.15), “telecom companies/Internet provider” (1.89) and “Secret Service Government Agencies” (1.88) and Law Enforcement government agencies (1.84). The least worrying groups were “Individual well-known to respondents” (0.97), “Health-care organisations” (1.00) and “Educational institutions” (1.09).

**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?		
Group	Mean	SD
Internet companies	2.15	0.885
Telecom companies/ Internet providers	1.89	0.872
Secret service government agencies	1.88	1.096
Law enforcement government agencies	1.84	1.062
Individuals who you don't know	1.67	1.040
Other government agencies	1.51	1.047
Computer hardware companies	1.46	0.965
Other for-profit companies	1.41	0.948
Computer software companies	1.38	0.973
System Integrators	1.32	0.886
Individuals who you know but not well	1.19	0.763
Other not-for-profit organisations	1.15	0.839
Educational institutions	1.09	0.947
Health-care organisations	1.00	0.865
Individuals who you know well	0.97	0.973

For evaluations of the threats posed by technologies (see Table 5): “GPS” (2.01), “Smartphone” (1.99), “Online Shopping” (1.77) and “Making payments online” (1.76) were ranked highest, with video game consoles, behavioural targeting and home automation systems ranked lowest. The difference between online shopping and behavioural targeting is odd and perhaps indicates that respondents did not understand behavioural targeting, or the extent to which things like smartphones, GPS and online shopping are related to behavioural targeting.



**Table 5: Ranked means (0: low; 3: high) of 17 technologies as perceived privacy threat**

Q8. How much do you feel that the following technologies threaten your privacy?		
Technology	Mean	SD
GPS	2.01	0.961
Smart phone	1.99	0.997
Online shopping	1.77	0.966
Online payments	1.76	1.051
PC	1.71	0.959
Social media services	1.62	1.002
CCTV	1.58	0.994
Online auction	1.54	0.931
Smart meter	1.49	0.813
Online games	1.41	1.017
Personal body monitor	1.39	0.968
Smart card	1.33	1.024
RFID	1.20	0.879
Home vid. game	1.13	1.039
Portable vid. game	1.10	0.992
Behavioural targeting	1.08	0.890
Home automation	0.97	0.969

Taken together, the results of the “Internet” versus “non-Internet” activity question, the groups that threaten privacy and the technologies that threaten privacy, it is clear the Mexican students all feel that Internet-related activities, groups and technologies are their greatest concerns in respect of privacy invasion

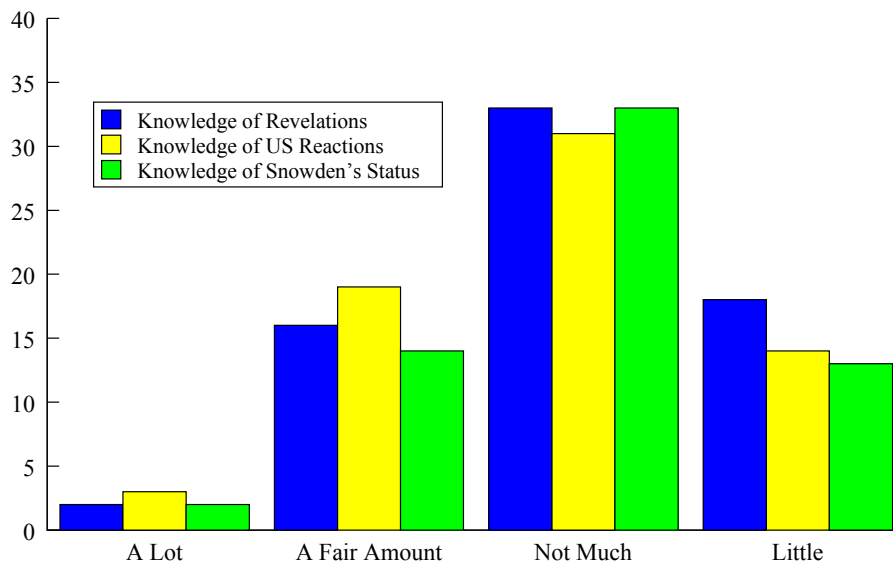
#### **4.1.2 The Degree of Recognition of and Interest in Snowden’s Revelations in Mexico.**

Before the survey, only 43.8% of respondents (70 of 160) had heard about Snowden’s revelations (50% indicated that they had not while 10/160 (6.3% preferred not to answer).. Furthermore, the knowledge level of those respondents who had heard was very low. Of the 70 who had heard about the revelations only two claimed to know “A lot” and 16 to know “a fair amount” with 33 knowing “not much” and 18 knowing “little” (one respondent preferred not to answer). Only a minority had ever discussed Snowden’s revelations with others (39.4%; 28/70), and a similar minority (38.6%; 27) had searched for further information about the revelations. There was a statistically significant correlation at the 1% level, between those who had talked about Snowden’s revelations and those who had searched for more information, confirmed by a Chi-Squared test on the cross-tab (see Table 6) of the two questions (Chi-squared: 21.5575, df(3);  $p < 0.01$ ).

**Table 6: Cross-tab of Qs 21 (Have you ever talked about Snowden's revelations with others?) and 22 (Have you ever searched for information about Snowden's revelations? )**

	Searched	Not Searched
Talked	20	8
Not Talked	6	41

Respondents' knowledge of the US reaction to Snowden's revelation and his current status were similar to their weak level of knowledge about the revelations themselves, as shown in Figure 2.



**Figure 2: Knowledge of the Revelation/US Reactions/Snowden's Status**

Respondents were also asked to indicate where they had received their information about Snowden's revelations, with a "select all that apply" set of answers. Mass media such as TV news (66.2%; 47), news on the Internet (53.5%; 38) were the most common sources, with Social Media close behind (50.7%; 36). Newspaper articles (28.17%; 20) were mentioned by just over a quarter, whereas direct from friends or acquaintances was reported by under a fifth (19.7%; 14) with university lectures coming in last (7.0%; 5).

#### 4.1.3 Evaluation of Attitudes in Mexico to Snowden's Activities.

On a question directly copying the Pew survey "Have Snowden's revelations served the public interest or harmed it?" a majority of 91/160 felt that he has served the public interest (25.6%/41 – "Served it a lot"; 31.3%/50 – "Served it to an extent") while only 33 felt that he had harmed the public interest (13.8%/22 – "Harmed it to an extent"; 6.9%/11 – "Harmed it a lot"). 27 explicitly indicated no opinion and nine preferred not to answer. Reflecting this positive evaluation of the consequences of his revelations, only 24 respondents believed the US government should pursue a criminal case against Snowden, while 72 believed they should not (49 claimed no opinion and 15 preferred not to answer). However, of those who felt the US should pursue a criminal case, 15 had given a positive evaluation of the consequences of Snowden's actions, while five who felt he had harmed the public interest nevertheless thought the US should not pursue a criminal case.

In free text responses to the question of why they believed that Snowden made his revelations, 56 respondents stated that they believed his reason was to inform people of the fact that the NSA was monitoring them. Another 50 indicated that they thought he wanted to protect people’s privacy, from either or both of the NSA itself or others who might have/gain access to material gathered by/because of the NSA. 15 thought he had acted on a personal ethical imperative, while six thought he had acted for personal gain. Three indicated that he believed he was defending democracy. 11 specifically said they did not know and 16 gave no answer or nothing that can be reasonably interpreted.

Respondents were asked about their willingness to “Follow Snowden”, i.e. emulate his actions in revealing details of such activities by secret intelligence agencies, in two situations: imagining themselves as a US citizen and having access to the same information as Snowden about the NSA/GCHQ operations; imagining themselves as a Mexican finding similar things out about Mexican SIGINT agencies. A significant minority preferred not to answer either hypothetical : 34.4%(55/160) (US) and 20.6% (38) (Mexico), though only 22 preferred not to answer both. Of those who gave an answer those willing to follow Snowden were in approximately a two-to-one majority in each hypothetical (see Table 7 for details)

**Table 7: If you were faced with a similar situation to Snowden in US/Mexico, would you, as a US/Mexican citizen, do what he did? (Number/160; % of answered)**

<b>US \ Mexico</b>	<b>Yes</b>	<b>No</b>	<b>Sub-Total</b>	<b>No Ans</b>	<b>Total</b>
<b>Yes</b>	<b>48</b> <b>(52.75%)</b>	<b>12</b> <b>(13.19%)</b>	<b>60</b> <b>(65.93%)</b>	7	<b>67</b> <b>(63.81%)</b>
<b>No</b>	<b>11</b> <b>(12.09%)</b>	<b>20</b> <b>(21.98%)</b>	<b>31</b> <b>(34.07%)</b>	7	<b>38</b> <b>(36.19%)</b>
<b>Sub-Total</b>	<b>59</b> <b>(64.84%)</b>	<b>32</b> <b>(31.16%)</b>	<b>91</b>	14	<b>105</b>
No Ans	20	11	31	24	55
<b>Total</b>	<b>79</b> <b>(64.75%)</b>	<b>43</b> <b>(35.25%)</b>	<b>122</b>	38	160

For the 12 respondents who would emulate Snowden in the US hypothetical but not in the Mexico hypothetical, in their free text answers to the question as to why they would not emulate him in Mexico many indicate greater fear of reprisals from the Mexican government than from the US government. For the 11 respondents who would emulate him in Mexico but not the US, many again explained their actions as fear of government power. Nine respondents gave a positive evaluation of Snowden’s actions (“served the public good” “a lot” or “to an extent”) but would not emulate him in either hypothetical. Their free text explanations similarly include a number (though far from all) expressing fear of government reprisals as the main reason for their reluctance.

**4.2. Empirical Consideration about Influence of Snowden’s Revelations**

When asked what if any social changes Snowden’s revelations have caused, only 19.4% (31/160; ) of respondents could identify any changes. 23.1% (37) explicitly said that no change had happened, 40.6 %

(65) had “no opinion” and 16.9% (27) preferred not to answer. Free text answers to what social change they have observed include 14 mentions of increased privacy awareness or care in revealing information, seven suggestions that people feel less secure, two that Snowden has given an example of dissent, and five suggestions of a reduced trust in government (some gave more than one of these answers and others gave confusing or limited answers).

The 70 respondents who had indicated that they had heard about Snowden’s revelations before taking the survey were asked if they had changed their own approaches to online communications as a result. 25.7% (18) said that they had not made any changes, 4.3% (3) preferred not to answer, with the other 70.0% (49) selecting one or more changes from the suggested list (and none giving other suggestions) as shown in Table 8.

**Table 8: Changes in Communicating Online Following Snowden.**

Change	No.	%
stopped using some systems	16	22.9%
tried to cut down my use of some systems	17	24.3%
deleted (some of) personal data and contents I had posted on social media	18	25.7%
paid more attention to personal data and contents posted on social media	24	34.3%
changed my privacy settings on some systems	23	32.9%

Did respondents who already knew about Snowden’s revelations before taking the survey show more (or less) concern about the risks of Internet activity to their privacy or about the privacy threats of groups or technologies than those who had not heard? Respondents were divided into two groups based on their answer to “**Q19. Have you heard about former NSA contractor Edward Snowden revealing large amounts of information about the activities of the NSA and GCHQ, through the UK's The Guardian newspaper and the US's The Washington Post newspaper starting in June 2013?**”: Yes (43.8%; 70/160) becoming the “Heard” group and “No” (50.0%; 80/160) becoming the “Not Heard” group (the other 10 respondents preferred not to answer and were ignored for the following calculations).

RQ1: Did respondents who had heard about Snowden’s revelations tend to recognise more risk of privacy invasion compared to those who did not know the revelations?

**Table 9. Q6 (Do you feel that your use of the Internet involves taking risks with your privacy?) Contingency table with Q19 (Have you heard about Snowden’s Revelations?)**

Risk	Strongly	To an extent	High	Not much	Not at all	Low
Heard	15	27	42	24	4	28
Not Heard	13	25	38	33	8	41

A Chi-squared analysis of Heard/Not Heard versus High/Low gives a Chi-squared result of 2.1134 (df=1) p=0.146, so there is no significant difference at the 5 percent level between the Heard and Not Heard group in their perception of the privacy risks of their Internet activity (a more detailed chi-squared

test on the full categorisation of level of risk also fails to show any significant difference at the 5 percent level).

The Heard and Not Heard groups' responses to the level of privacy threat posed by government agencies (Law enforcement government agencies (LE); Secret service government agencies (SS) and Other government agencies (OA)) were also compared. For none of the three types of government group was there a significant difference found between the Heard and Not Heard groups at the five percent significance level (see below for the detailed analyses)

(LE) T-test result: Heard:  $M=1.99$ ,  $SE=0.12$ ; Not Heard:  $M=1.72$ ,  $SE=0.13$ ;  $D=0.28$ ,  
95% CI [-0.07, 0.63];  $t(138.99)=1.597$ ;  $p > 0.1$

(SS) T-test result: Heard:  $M=2.02$ ,  $SE=0.13$ ; Not Heard:  $M=1.77$ ,  $SE=0.14$ ;  $D=0.243$ ,  
95% CI [-0.14, 0.62];  $t(128)=1.268$ ;  $p > 0.1$

(OA) T-test result: Heard:  $M=1.65$ ,  $SE=0.13$ ; Not Heard:  $M=1.39$ ,  $SE=0.12$ ;  $D=0.260$ ,  
95% CI [-0.09, 0.61];  $t(133)=1.466$ ;  $p > 0.1$

## **5. State surveillance following Snowden.**

The unstable electoral and political situation in Mexico, combined with the continuing high level of criminal violence have led to increasing government authority to conduct surveillance of electronic communications. The National Code of Criminal Procedure in the #Congreso General de los Estados Unidos Mexicanos (2014) authorises government ministries (with prior authorization) to monitor in real-time the location of any citizen suspected of a crime, irrespective of the seriousness of the alleged crime. As mentioned above recent amendments to the telecommunications law oblige communication companies to store users' usage data for at least 2 years. This data is supposed to be accessible to authorities in real-time without a warrant.

These elements, combined with the large purchases of software from "The Hacking Team" also mentioned above, add up to a pessimistic assessment of the condition of privacy, and associated human rights in Mexico at present. "When State and unlawful acts are working together, acceptance of surveillance without the establishment of democratic controls affects not only privacy but compromises the life and safety of all persons" (García, 2016). Snowden's revelations, although troubling to the survey respondents, appear to have had little impact beyond confirming some of their worst fears about their powerful neighbour to the North and undermining opposition to their own government's actions in the area of surveillance.

## **6. Conclusions and Future Research.**

Mexico is a developing country with several political situations that affect the economic and social arenas. Although Mexico adopted a transparency/freedom of information law that supposedly allows public access to government information, its implementation and limitations mean that it is more the appearance of transparency than the reality. The widespread use of surveillance and the limited rule of law in Mexico places democratic development under significant threats.

The respondents to this survey regard both major private companies and government agencies as threats to their privacy, but like most people everywhere, they still use the facilities available to them, either through choice or necessity. There is limited knowledge of Snowden's revelations, perhaps at least in part due to limited press coverage and little attention paid by Mexican politicians to the issue. Future research options include repeating the threats element of the survey to successive cohorts of students in order to identify any long term shifts in attitudes.

## 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.

## 8. References

- Benítez Manaut, R. (2012), *Historia General de La Infantería de Marina Mexicana. Tomo 2, 1a Edición.*, Secretaría de Marina-Armada de México. Estado Mayor General. Unidad de Historia y Cultura Naval, México, D.F, available at: <https://www.gob.mx/cms/uploads/attachment/file/2901/historia-general-de-la-infanteria-de-marina-mexicana-tomo-i.pdf> (accessed 5th April, 2017) . In Spanish.
- Bogado, D. (2016), “La Suprema Corte de México debe rechazar la vigilancia masiva”, *EFF - Electronic Frontier Foundation*, available at <https://www.eff.org/node/91245> (accessed 5th April 2017). In Spanish.
- Congreso General de los Estado Unidos Mexicanos. (2014), “Código nacional de procedimientos penales”, *Diario Oficial de La Federación*, available at <http://www.diputados.gob.mx/LeyesBiblio/ref/cnpp.htm> (accessed 5th April 2017). In Spanish.
- Connolly, K. (2015), “Germany summons US ambassador over new spying claims ”, *The Guardian*, 2nd July, available at <https://www.theguardian.com/world/2015/jul/02/merkel-aide-summons-us-ambassador-spying-claims> (accessed 5th April 2017).
- De Castro, R. F. (2015), “The Hacking Team leak shows Mexico was its top client, but why?” *Fusion*, 9th July, available at <http://fusion.net/story/163872/the-hacking-team-leak-shows-mexico-was-the-top-client-but-why/> (accessed 5th December, 2016).
- Friman, H. R. (1996), *Narcodiplomacy: exporting the US war on drugs*, Cornell University Press, Cornell, NY.
- Froomkin, D. (2015), “The Computers are Listening: How the NSA Converts Spoken Words into Searchable Text”, *The Intercept*, 5th May, available at <https://theintercept.com/2015/05/05/nsa-speech-recognition-snowden-searchable-text/> (accessed 30th November, 2016).
- García, L.F. (2016), “La vigilancia en México, fuera de control: R3D”, available at <http://aristeguinoticias.com/1804/mexico/la-vigilancia-en-mexico-fuera-de-control-r3d/> (accessed 5th April 2017). In Spanish.
- González Hernández, C. (2002), *Doña Marina (La Malinche) Y La Formación de La Identidad Mejicana*, Ediciones Encuentro, S.A., Madrid. In Spanish.
- The International Security Issues Build-Out (2012), Document from Snowden’s cache, available at <https://www.edwardsnowden.com/2013/12/18/the-international-security-issues-build-out/> (accessed 30th November, 2016).
- Jiménez Barca, A. (2015), “EE UU espía a 29 altos cargos del Gobierno de Rouseff en 2011”, *El País*, 4th July 2015, available at [http://internacional.elpais.com/internacional/2015/07/04/actualidad/1436039706\\_499246.html](http://internacional.elpais.com/internacional/2015/07/04/actualidad/1436039706_499246.html) (accessed 5th April 2017). In Spanish.
- Johnson, J. (2015), “WikiLeaks alleges widespread U.S. spying on Japanese government, major companies”, *The Japan Times*, 31st July, available at

<http://www.japantimes.co.jp/news/2015/07/31/national/wikileaks-alleges-widespread-u-s-spying-on-japanese-government-major-companies/> (accessed 5th April 2017).

- Katz, F. (2006), *Nuevos Ensayos Mexicanos*, Primera., Ediciones Era, México, D.F. In Spanish.
- Kuzon Jr, W. M., Urbanek, 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.
- Lindau, J. D. (2011), “The drug war's impact on executive power, judicial reform, and federalism in Mexico”, *Political Science Quarterly* Vol. 126 No. 2, pp. 177-201.
- 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).
- Manzanera, L. (2008), *Mujeres Espías: Intrigas Y Sabotaje Tras Las Líneas Enemigas*, Debate, España. In Spanish.
- Murata, K., Adams, A. A., and Lara Palma, A. M. (2017) “Following Snowden: A Cross-cultural Study on Social Impact of Snowden’s Revelations”, *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. ??-??
- Norman, G. (2010), “Likert scales, levels of measurement and the “laws” of statistics”, *Advances in health sciences education*, Vol. 15 No. 5, pp. 625-632.
- Ornelas Núñez, L.G. and Higuera Pérez, M. (2013), “La autorregulación en materia de protección de datos personales: la vía hacia una protección global”, *Revista de Derecho, Comunicaciones Y Nuevas Tecnologías*, No. 9, pp. 1–32. In Spanish.
- Pfeffer Urquiaga, E. (2000), “Los derechos a la intimidad o privacidad, a la honra y a la propia imagen. Su protección frente a la libertad de opinión e información”, *Ius et Praxis*, Vol. 6 No. 1, pp. 465–474. In Spanish.
- Riva Palacio, R. (2013), “Espionaje en México , una vieja historia”, available at <http://www.razon.com.mx/spip.php?article180583> (accessed 5th April 2017). In Spanish.
- Rivera Cabrieles, L. (2012), *Historia General de La Infantería de Marina Mexicana. Tomo 1*, 1a. edición., Secretaría de Marina-Armada de México. Estado Mayor General. Unidad de Historia y Cultura Naval., México, D.F, pp. 48–52. In Spanish.
- Solove, D. (2011), *Nothing to Hide: the False Tradeoff Between Privacy and Security*. Yale University Press, New Haven, CT.
- Sánchez Onofre, J. (2015), “Vulneración a Hacking Team confirma abuso de espionaje en México”, *El Economista*, 6th July, available at <http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico> (accessed 5th April 2017). In Spanish.
- Vargas V., M.Á. (2013), “11 datos clave sobre el supuesto espionaje de EU a México”, *CNNMéxico.com*, 21st October, available at: <http://www.adnpolitico.com/gobierno/2013/10/21/11-datos-clave-sobre-el-espionaje-de-estados-unidos-a-mexico> (accessed 5th April 2017). In Spanish.
- Vite Pérez, M.A. (2015), “The social vulnerability under the surveillance from the State Mexican”, *Revista de Direito Da Cidade*, Vol. 7 No. 3, pp. 1072–1091.
- Weisbrot, Mark (2012), *Irregularities reveal Mexico's election far from fair*. The Guardian, 9th July. Available at <https://www.theguardian.com/commentisfree/2012/jul/09/irregularities-reveal-mexico->

[election-far-from-fair](#) (accessed 19th December, 2016).