

Schulich School of Law, Dalhousie University

Schulich Law Scholars

Articles, Book Chapters, & Popular Press

Faculty Scholarship

2017

Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study

Jonathon Penney

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/scholarly_works



Part of the [Constitutional Law Commons](#), [Human Rights Law Commons](#), [Internet Law Commons](#), [Legislation Commons](#), and the [Privacy Law Commons](#)



Internet surveillance, regulation, and chilling effects online: a comparative case study

Jonathon W. Penney

Citizen Lab, University of Toronto, Canada

Published on 26 May 2017 | DOI: 10.14763/2017.2.692

Abstract: With internet regulation and censorship on the rise, states increasingly engaging in online surveillance, and state cyber-policing capabilities rapidly evolving globally, concerns about regulatory “chilling effects” online—the idea that laws, regulations, or state surveillance can deter people from exercising their freedoms or engaging in legal activities on the internet have taken on greater urgency and public importance. But just as notions of “chilling effects” are not new, neither is skepticism about their legal, theoretical, and empirical basis; in fact, the concept remains largely un-interrogated with significant gaps in understanding, particularly with respect to chilling effects online. This work helps fill this void with a first-of-its-kind online survey that examines multiple dimensions of chilling effects online by comparing and analyzing responses to hypothetical scenarios involving different kinds of regulatory actions—including an anti-cyberbullying law, public/private sector surveillance, and an online regulatory scheme, based on the Digital Millennium Copyright Act (DMCA), enforced through personally received legal threats/notices. The results suggest not only the existence and significance of regulatory chilling effects online across these different scenarios but also evidence a differential impact—with personally received legal notices and government surveillance online consistently having the greatest chilling effect on people’s activities online—and certain online activities like speech, search, and personal sharing also impacted differently. The results also offer, for the first time, insights based on demographics and other similar factors about how certain people and groups may be more affected than others, including findings that younger people and women are more likely to be chilled; younger people and women are less likely to take steps to resist regulatory actions and defend themselves; and anti-cyberbullying laws may have a salutary impact on women’s willingness to share content online suggesting, contrary to critics, that such laws may lead to more speech and sharing, than less. The findings also offer evidence of secondary chilling effects— where users’ online activities are chilled even when not they, but others in their social networks receive legal processes.

Keywords: Chilling effects, Online surveillance, Government surveillance, Corporate surveillance

Article information

Received: 15 Aug 2016 **Reviewed:** 01 May 2017 **Published:** 26 May 2017

Licence: Creative Commons Attribution 3.0 Germany

Funding: Social Science Humanities and Research Council (SSHRC), Government of Canada.

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:

<http://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case>

Citation: Penney, J. W. (2017). Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, 6(2). DOI: 10.14763/2017.2.692

***Note by the editor:** Three references have been added and one minor adjustment has been made to one sentence in the text, post-publication (on 13 June 2017).*

1. INTRODUCTION

With internet regulation and censorship on the rise, states increasingly engaging in online surveillance, and state cyber-policing capabilities rapidly evolving globally (Nye, 2011; Zittrain, 2008; Deibert, 2013; Deibert et al., 2012; Schneier, 2015) concerns about regulatory “chilling effects” online - the idea or theory that laws, regulations, or state surveillance can deter people from exercising their freedoms or engaging in legal activities on the internet have taken on greater urgency and public importance. But just as notions of chilling effects are not new, neither is skepticism about its legal, theoretical, and empirical basis (Kaminski and Witov, 2015: 480-482; Schauer, 1978; Blasi, 1985; Kendrick, 2013: 1657). And while several recent studies have helped provide new insights on chilling effects (e.g., Stoycheff, 2016; Penney, 2016; Townend, 2014; Marthews and Tucker, 2014; PEN America, 2013; 2015; Pew Research Center, 2015a; 2015b), significant gaps remain in its empirical underpinning and theoretical understanding, particularly how such laws, regulations, and state surveillance impact activities online (Kaminski and Witnov, 2015: 517; Townend, 2014).

One such gap in research is the *comparative* dimensions of chilling effects online, both in terms of different forms of chilling effects and their impact across different populations (Townend, 2014). This case study helps address this lack of empirical evidence with a first-of-its-kind online survey that examines multiple dimensions of chilling effects online by comparing and analysing responses to four different hypothetical “chilling effect scenarios”, that is, hypothetical scenarios involving different kinds of regulatory actions that may, in practice, “chill” or deter internet users from engaging in legal activities online, to different or greater or lesser extents (if at all).

CHILLING EFFECTS THEORY: FRAMING THE CASE STUDY

Though notions of self-censorship in the face of coercive threats are quite old—historian Quentin Skinner, for example, identified comparable themes in early strains of republican political thought (Skinner, 2002: 257)—more modern notions of regulatory “chilling effects” emerged out of the tumultuous Cold War regulatory context and gained their most high profile expression in traditional free speech law and First Amendment jurisprudence of the US Supreme Court (Horwitz, 1997; Barendt et al., 1997: 189-190; Kenyon, 2010). Concerns about chilling effects have not remained a relic of early American constitutionalism, but have evolved as these concerns have emerged in law, research, and public policy debates in Canada, Australia, the United Kingdom, Europe, and many other jurisdictions, including “blogger and journalists’ everyday discourse” (Townend, 2014; Kenyon, 2010). Chilling effects concerns have also been investigated and pursued in other disciplines like sociology and psychology (Kaminski and Witov, 2015).

Schauer (1978) and Solove (2006; 2007) provide the primary theoretical foundation for this case study, which is also informed by leading works on intersecting subject matter such as surveillance (Lyon, 2015; 2006; 2001; 1994; 1991; Zureik et al., 2010; Graham and Wood, 2003; Marx, 2002), privacy (Nissenbaum, 2009; Acquisti, 2004), libel chill (Barendt et al., 1997) and self-censorship/self-presentation online (Das and Kramer, 2013; boyd and Marwick, 2010). This theoretical framework is also informed by, and aims to build on, recent research on chilling effects online (Stoycheff, 2016; Penney, 2016; Marthews and Tucker, 2014; Townend, 2014; PEN America, 2013; 2015; Pew Research, 2015a; 2014b; 2014c).

Schauer (1978) is generally considered the leading account of chilling effects theory (Zacharias, 1986). For Schauer, a “chilling effect” is at its core an “act of deterrence” and the fear, risk, and uncertainty built into laws, regulations, and the legal system more generally, can deter people from exercising their rights (Schauer, 1978: 689). Solove, drawing on the insights of surveillance studies (Lyon, 2006; 2001), builds on Schauer’s account to encompass concerns about how “modern” privacy problems associated with such information practices as state surveillance and data gathering can create an atmosphere of “risk” and self-censorship, a kind of society-wide chilling effect comparable to “environmental harms” or “pollution” (2006: 487). This chilling effects theory is operationalised here by measuring and comparing internet users predicted responses to four “chilling effects scenarios”. More specifically, the survey describes certain hypothetical scenarios and then asks questions to understand and measure how the respondent and his or her *legal* online activities would be impacted by the regulatory act or issue in question. It offers both *comparative* and more general empirical and theoretical insights, such as, what sort of state or non-state action would have a comparatively greater chilling effect on user activities and behaviour. The four scenarios, around which the survey is designed, are elaborated in the next section.

2. CASE STUDY DESIGN AND METHOD

2.1 RECRUITMENT AND DESIGN

The participant pool for the survey was recruited using an online crowdsourcing service,¹ a platform purposefully chosen as its participant pools have been found to be relatively representative of the US internet using population, the target population for this study (Paolacci

et al., 2010: 412; Chen and Yeh, 2013; Wolfson and Bartkus, 2013: 119; McDonald and Cranor, 2010: 5). Chilling effects have also been previously studied using survey methods (Barendt et al., 1997; Renas et al., 1989; Townend, 2014; PEN America, 2013; 2015; Pew Research Center, 2015a; 2015b; 2014a; 2014b; 2014c). To strengthen the internal and external validity of results, rather than have participants merely self-report attitudes, this survey measures and compares responses to hypothetical online “chilling effects” scenarios. Each scenario is described separately to respondents followed by subsequent questions designed to elicit likely behavioral responses to each scenario described rather than basic self-reports or stated attitudes about privacy, surveillance, or regulatory chilling effects.

Though they do have limitations,² such hypothetical scenarios (and behavioral questions) were used not only used in Renas et al. (1989), a leading previous empirical chilling effects study on libel laws, but have also been used widely to by researchers in a range of fields, including recent studies on privacy and online behavior (see, e.g., Mamonov and Koufaris, 2014; Keith, Ngo, and Babb, 2014; Seih, Buhrmester, and Lin, 2013). Furthermore, the leading survey-based studies on surveillance-related impact and harms in recent years have all employed hypothetical questions and scenarios: PEN America (2013; 2015); Pew Research Center (2015a; 2015b; 2014a; 2014b; 2014c). In short, this is a common research technique used in leading privacy surveys with the defined scenarios employed based on extensive literature review. Other measures taken to address validity and reliability are set out in **Appendix 1**.

This survey is structured around four primary hypothetical scenarios. The first (1) primary scenario employed in the survey, much like the laws Schauer (1978) largely examined, involves a vague or uncertain statute or regulation enacted to regulate or prohibit an online activity, with a significant penalty or punishment for transgressions or violations of the statute or regulation is traversed or broken. For this scenario, a form of “anti-cyberbullying” statute—that criminalises the “intent” to “harass or intimate another person” online—was used, as such laws been increasingly used to regulate forms of online speech and activities by lawmakers in the US and internationally and are often criticised for chilling online speech, including constitutionally protected speech.³ Despite such criticisms, there is little empirical research on the impact of such legislative efforts implemented in the United States and elsewhere to criminalise and deter online harassment and cyberbullying (Asam and Samara, 2016: 138-139; Hazelwood and Koon-Magnin, 2013: 156; Henry and Powell, 2016). This scenario explores this proposition. Online surveys have previously been used to study cyberbullying and online harassment (Cederborg et al., 2016: 138), including the few studies exploring the impact of relating legal interventions (See Kasgupta, 2016; Sung, 2016).

The second (2) scenario involves state or non-state surveillance (and related practices like data collection or gathering), consistent with Solove (2006; 2007)’s concerns about chilling effect associated with these forms of data and information gathering. A third (3) scenario is related to the first two, in that vague laws and uncertainties in the legal process are part of what creates a chilling effect, but differs in how the threat of legal penalty is delivered—here it is delivered personally via legal notice to the individual targeted. This scenario is based on libel chill concerns (Renas et al., 1989; Barendt et al., 1997) as well as “next generation” internet regulatory efforts like the Digital Millennium Copyright Act (DMCA) notice and takedown system for enforcing copyright law online.⁴ It is thus referred herein as the “DMCA” scenario. A fourth (4) scenario primarily concerns a kind of *secondary* chilling effect in online environments. Here, an internet user is “chilled” or deterred from certain legal activities after learning, perhaps by a post on social media, that friends or other members of their network (online or otherwise) have been targeted or received a legal threat.⁵

This case study's survey is primarily designed around these scenarios, with some modification in certain contexts to explore different comparative elements or dimensions of chilling effects. Each scenario, once briefly described, is followed by a series of questions exploring how this new law would impact each respondent's (future or predicted) behaviour. It is from these responses that any potential or expected regulatory chilling effects are observed.⁶ Questions are generally based on a five point Likert scale and repeated for each of the hypothetical scenarios to allow for comparisons, with a few additional questions (based on slightly modified scenarios) for additional insights.

2.2 OPERATIONALISING CHILLING EFFECTS THEORY

Chilling effects theory is operationalised in the design via questions exploring how each "chilling effects" scenario may impact different online activities, specifically, how each regulatory act or action described may render the respondent less likely to engage in one or more activities online, such as speaking, searching, and sharing content online. This is consistent with both Schauer (1978) and Solove (2006; 2007)'s accounts of chilling effects, whereby certain regulatory actions may deter or chill activities. Additional questions (on how internet users may be rendered more "careful" or cautious in their activities) are likewise designed to explore what Sklansky (2014) calls the "stultification thesis", that is, the notion that certain state (and non-state) regulatory actions (particularly surveillance) promotes self-censorship, conformity, and inhibition among citizens, rendering them more cautious, careful, and less willing to seek out and engage with controversial views and ideas or exchange in "robust" and "candid discussion"; things necessary to "deliberative democracy" and "self-determination" (Solove, 2007: 123-124). This form of chilling effect is more subtle and more difficult to measure or explore, but is nevertheless an essential harm relating to chilling effects, menacing "society's foundational commitments to intellectual diversity and eccentric individuality" (Richards, 2013: 1948). Sklansky (2014) argues there is little empirical evidence supporting the "stultification thesis" despite it being an "article of faith" among surveillance and privacy theorists (p. 1097). This case study is designed to address this lack of empirical support.

In exploring how different regulatory scenarios may deter, inhibit, prevent, or render more cautious or self-censoring internet users in relation to a range of different online activities (speech, search, engagement, etc.), this case study examines what Barendt et al. (1997) call "structural" chilling effects. This is different from instances where specifically targeted content is altered as a result of specific legal concerns (e.g., a news story is changed after receiving a libel threat relating to it) (Townend, 2014). This form of impact, which Barendt et al. (1997) approached as a more "direct" chill, is also explored here via several additional questions posed in relation to the third scenario (e.g., respondents are asked how they would respond to the legal notice received if they felt it was incorrect; including if they would alter/re-post content).

Moreover, consistent with Schauer (1978), the four primary scenarios are employed to explore any potential impact or chilling effect on presumptively *legal* activities, that is, activities such as speaking online, searching online, or sharing personally created content online; all activities presumptively legal under US law. This is important, as Schauer notes, for while a "chilling effect" is at its core an "act of deterrence", *some* deterrent effects are actually intended by laws - such as deterrence of criminal activities - thus, his theoretical account concerns how laws or state regulatory actions may chill or deter legal activities and how laws and regulations might have a chilling effect upon such legal and permissible activities (1978: 6890-6990), particularly speech. This case study, then, is similarly designed to capture chilling effects on presumptively *legal* activities, not facially criminal or illegal ones.

Of course, any research design will be imperfect on this count, as uncertainties in the law and legal process about the legality of certain activities, coupled with the threat of harsh penalty or punishment associated with an activity, can often, as Schauer (1978) theorised, be the very cause of chilling effects. Additionally, designing research illustrating chilling effects, that is, what a user would have said or did but for some state or regulatory activity is difficult enough (Schauer, 1978; Solove, 2007: 121); adding a requirement that such hypothetical activity is also definitively *legal* adds an additional layer of complexity to an already demanding methodological challenge. Nevertheless, to address these challenges, the scenarios and related questions explored here were designed to explore how regulatory actions like a vague statute, online surveillance, or delivering a threatening legal notice (among other scenarios) may impact on an internet user's more *general* activities (speaking/writing/sharing/searching online) that may not necessarily be definitively legal in all cases, but normally would be so. This is the concern of chilling effects theory.

2.3 IMPLEMENTATION AND METHOD OF ANALYSIS

The survey itself was hosted and field tested using online survey software.⁷ Data was collected over the course of a week in March 2014. The dataset thus constituted 1,212 total surveys.⁸ Responses to questions are first analysed (percentages, summary, and descriptive statistics) to understand any apparent “chilling effect”, including comparisons between results for each scenario, for comparative insights. To explore and identify potential factors that may impact or influence any apparent “chilling effects” (e.g. being less likely to speak or share online, due to knowledge of online surveillance) results were statistically analysed using Goodman and Kruskal's gamma (γ) and Pearson's chi-square (X^2) test statistics.⁹

2.4 ETHICAL CONSIDERATIONS

The ethical dimensions of this study were informed by the recent Menlo Report (Dittrich and Kenneally, 2012) as well as the Association of Internet Researchers (AoIR) ethical guidelines (2002; 2012). The research also received ethical approval from the Oxford Internet Institute's departmental Central University Research Ethics Committee (CUREC) at the University of Oxford. A central ethical concern in this research was ensuring participant confidentiality as this study also deals with sensitive issues and data, such as the legality of certain kinds of online actions. For this reason, extra precautions were taken to ensure data was kept safe, secure, and confidential, including preventing survey software from tracking IP addresses and allowing respondents to complete the online survey anonymously. All results/data obtained was stored anonymously as there was no need to identify or link information obtained with the specific identities of any participants to achieve the aims of the research. Another ethical consideration was obtaining the consent of human research subjects. Informed consent was obtained from respondents through the online survey itself prior to participation (that consent form can be viewed at **Appendix 8**).¹⁰

2.5 HYPOTHESIS

This survey's design was centered on four “chilling effect” scenarios. If these hypothetical scenarios lead internet users to be less likely to engage in certain legal activities online or are more careful about how they do so, this is evidence of such regulatory chilling effects. It is predicted that *due to regulatory chilling effects internet users will be less likely to engage in certain legal online activities (across the different scenarios designed into the survey) or will be more careful about how they engage in such online activities*. Consistent with Schauer (1978) and Solove (2006; 2007) this prediction speaks to potential chilling effects on legal activities online, as indicated by respondents being less willing to engage in such activities, as well as evidence of the stultification thesis, about how chilling effects may also promote self-

censorship, inhibition, and conformity, by encouraging internet users to be more careful and cautious while engaging in these activities.

3. PARTICIPANT POOL

In the final dataset, there were 1,212 total participants with characteristics similar to other crowdsourced participant pools, which have been found to be “relatively representative of the population of US Internet users” with a few biases, mainly, that samples are somewhat younger, more female, and have slightly lower incomes than the general US internet population (Paolacci et al., 2010: 412). That is all approximately true of this sample, except on gender where it is much more balanced, with 608 participants male (49.7%) and 608 female (50.3%).¹¹ Like most internet user samples, this participant pool also included heavy internet users overall, but with some variability in other aspects of internet use. Almost half (49.5%) of participants indicated they were “continually” connected to the internet, while another 46.1% reported connecting several times a day. A slight majority (51.9%) shared content or posted things online at least “several times a week”, and almost 17% sharing content several times a day.¹² For more details, graphs, and visualisations on participants, see **Appendices 2** through **6**.

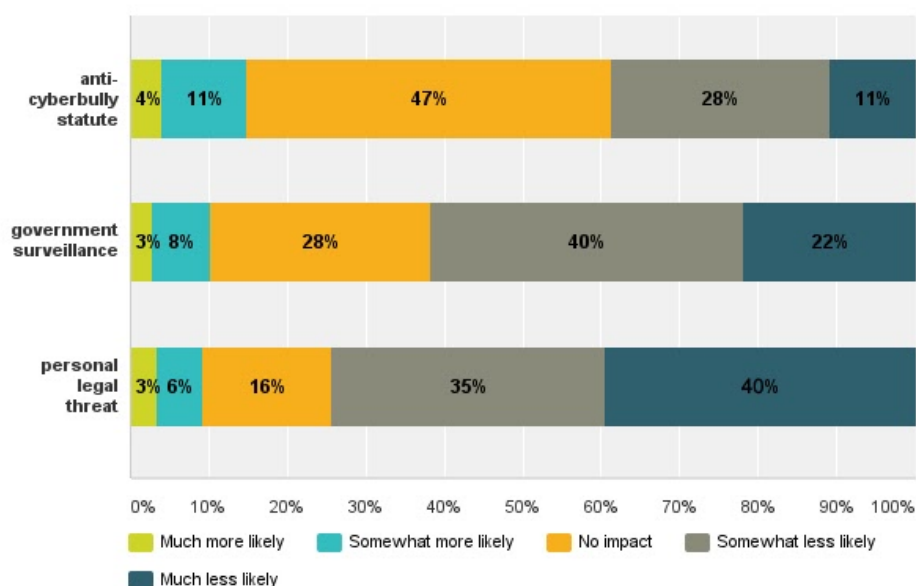
4. RESULTS

4.1 ONLINE SPEECH

All scenarios evidence a chilling effect on online speech and expression. A comparison of results from the three primary hypothetical scenarios concerning any potential “chill” on speech is charted in **Figure 1**:

Figure 1: Impact on online speech I (more or less likely to speak/write)

Respondents were asked whether they would be “more likely or less likely to speak or write about certain topics online” in response to each hypothetical scenario. This chart collates and compares the responses. The cumulative percentage of responses is mapped on the x-axis in relation to the three primary hypothetical “chilling effect” scenarios on the y-axis.

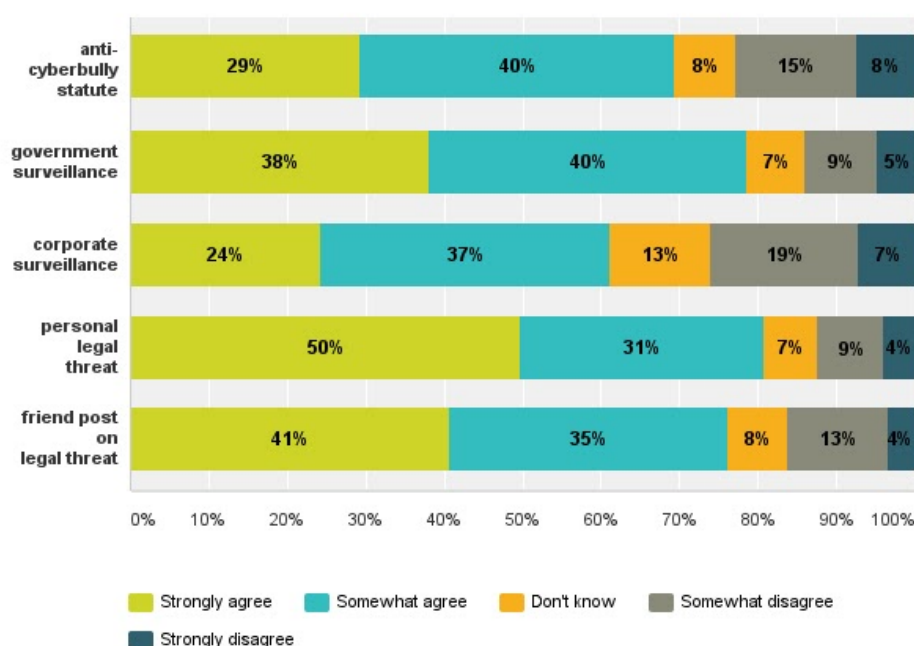


The results show that for respondents, personally receiving a legal threat from a third party about some online activities had the greatest chilling effect, with 75% of respondents being “much less likely” (40%) or “somewhat less likely” (35%) to “speak or write about certain topics online” as a result. The next most “chilling” was government surveillance, with 62% of respondents “much less likely” (22%) or “somewhat less likely” (40%) “speak or write about certain topics online” due to such online monitoring. Interestingly, the vague anti-cyberbullying statute did have some chilling effect (39% much less or somewhat less likely) but a near majority (47%) indicated the law would “have no impact” on their online speech.

In a comparison of all four scenarios concerning any potential “chill” on speech, again, personally receiving a legal threat from a third party about some online activities had the most impact, with 81% of respondents indicating they “strongly agreed” (50%) or “somewhat agreed” (31%) with the statement that receiving such a legal notice would make them “more careful” about what they “say or discuss in certain contexts online” (see **Figure 2**).

Figure 2: Impact on online speech II (carefulness about speech)

Respondents were asked to indicate their level of agreement with the following statement, “I would be more careful about what I say or discuss in certain contexts online” in response to each hypothetical scenario. The cumulative percentage of agreement or disagreement with the statement is mapped on the x-axis in relation to each hypothetical “chilling effect” scenario on the y-axis.



Government surveillance, consistent with earlier results, was the next most chilling, with 78% of respondents “strongly” agreeing (38%) or “somewhat” agreeing with that statement. A close third was the scenario where the respondent sees a friend posting online about receiving a personal legal notice warning the friend about the legality of certain online activities. Here, 76% of respondents “strongly” (41%) or “somewhat” agreed (35%). Next in terms of impact is the anti-cyberbullying statute scenario followed by corporate surveillance - with a 69% either “strongly” (29%) or “somewhat” agreeing (40%). The results suggest corporate surveillance may have the least impact or chilling effects. Here, in the questionnaire, respondents were asked the same question as those in the government surveillance scenario, but with the small change that it was an internet company monitoring online activities instead of the government. 61% either “strongly” (24%) or “somewhat” (37%) agreed with the statement that such corporate surveillance would make them “more careful” about what they “say or discuss” online.

A few observations would be helpful here. First, results from both comparisons are certainly consistent with chilling effects theory and all suggesting some chilling effect on the online speech and expression of respondents. The results from the second comparison (**Figure 2**) - involving the three primary scenarios: statutory, government surveillance, and individualised legal notice - as well as the two additional exploratory ones (corporate surveillance and secondary/networked “chill” or regulation) suggest a greater impact than the findings from the first (**Figure 1**). This makes sense, as arguably chilling effects often work in subtle ways; these results indicate that the “chill” might be that respondents become more careful in their online speech, rather than simply being chilled or deterred from speaking at all or rendered much less likely to do so. Still, **Figure 2** also reveals substantial chilling effects, with noteworthy percentages of respondents rendered “much less” or “somewhat less” likely to “speak or write about certain topics online”.

Second, it also makes sense that the scenario involving individualised and personally received legal notices (threatening legal repercussions for online activities) had the greatest apparent chilling effect, since such an “individualised” legal or regulatory measure would send the message that the targeted person is already targeted, or being watched closely, thus raising the

risk of punishment or penalty for any online activities they pursue. This would likely lead to a more pronounced chilling effect apparent in the results. And there is probably a good reason why government surveillance appears to have a more chilling effect than corporate surveillance, given that respondents would likely assume that a company is monitoring activity online to protect only a narrow set of corporate interests (e.g., financial), while government monitoring is more sweeping and sophisticated, and thus respondents would be more chilled as a result.

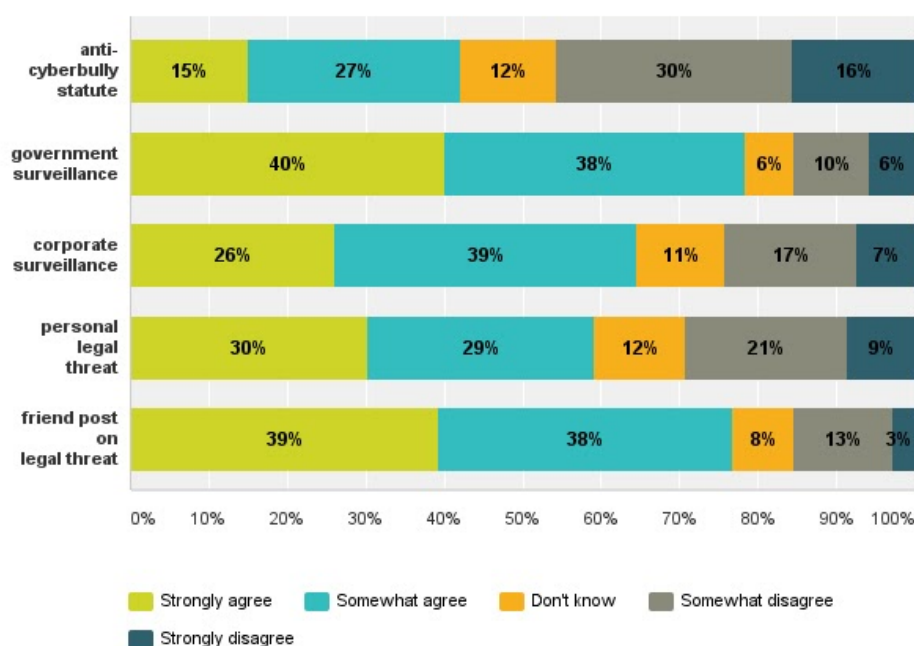
Third, the reaction among respondents to the hypothetical anti-cyberbullying statute is interesting for, as will be seen from other results, this “statutory” scenario often appears to have less of an impact, at least comparatively speaking, than other kinds of scenarios explored. Not here, however. Rather, the response is fairly consistent with, and comparable to, results from the other scenarios, with the findings for the anti-cyberbullying statute suggesting it has more of a chilling effect than corporate surveillance. This, too, might be explained by respondents perceiving action by state authorities to be more of a threat than private entities with only corporate or profit motives.

4.2 ONLINE SEARCH

Responses suggested online search activities may also be affected, as apparent in **Figure 3**, a comparison of all four scenarios concerning any potential “chill” on online search activities. Government surveillance had the greatest likelihood to chill respondents’ future internet search activities, with 78% of respondents either “strongly” (40%) or “somewhat” (38%) agreeing with the statement that government monitoring of online activities would make them “more careful” about what they “search for online”. Interestingly, seeing a friend posting online about receiving a personal legal notice warning the friend about illegal activities online (e.g., downloading copyrighted material) had the next most effect, with 77% of respondents “strongly” (39%) or “somewhat” (38%) agreeing with the statement that seeing such a post would make them “more careful” about what they “search for online”.

Figure 3: Impact on online search

Respondents were asked to indicate their level of agreement with the following statement, “I would be more careful about what I search for online” in response to each hypothetical scenario. This chart maps the responses consistent with previous graphs.



The next in terms of potential chill on internet search is corporate surveillance, with 65% either “strongly” (26%) or “somewhat” (39%) agreeing, and the personal legal notice, with 59% of respondents indicating they “strongly agree” (30%) or “somewhat agree” (29%).

These results are also consistent with chilling effects theory, with the relatively stronger chilling effect of some of the hypothetical regulatory acts or actions - like government surveillance - likely explained by the aspects of such government monitoring earlier; people would be deterred from certain online search queries assuming government may be monitoring for illegal or antisocial and even non-conforming behaviour, which might suggest future illegal conduct. However, the results also suggest a strong measure of potential “chill” relating to the secondary or “networked” regulatory chilling effects scenario, where the hypothetical involves the respondents being made aware, via a friend’s Facebook posting, that the friend has received a personal legal notice warning them about potentially illegal online activities. This scenario had the second most substantial impact after government surveillance. One possible explanation for this comparatively greater “impact” for this hypothetical scenario on search, is that the legal notice (as described in the scenario) was targeting illegal downloading of copyrighted material. Given that seemed to be the target, it makes sense that respondents would be much more careful about what they search for (copyright content), so as not to attract attention or penalty for likewise accessing or following links to pirated material via search. Moreover, consistent with Schauer (1978) legal uncertainties about the legality of accessing or downloading certain content online may be contributing to this subtle chilling effect, apparent in a more careful and cautious approach to activities online more generally, in this case speech.

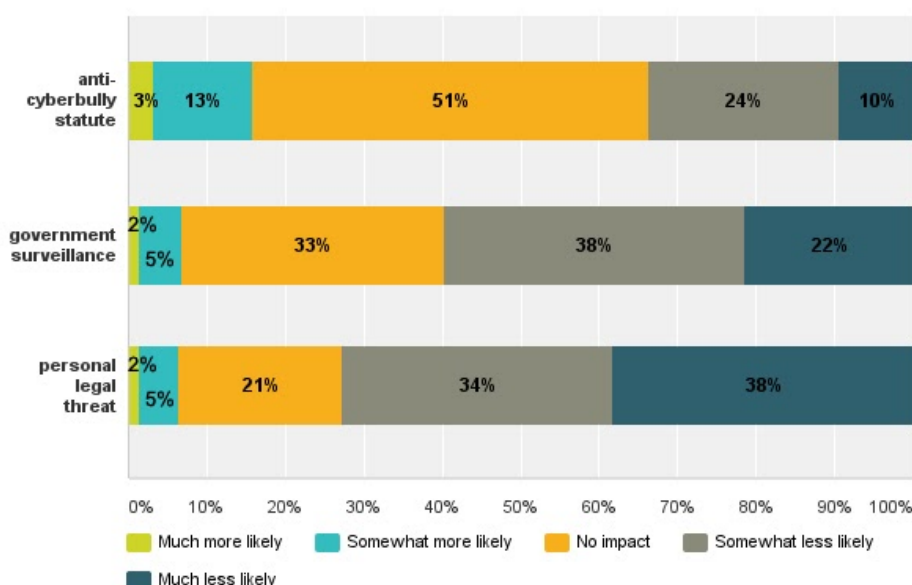
Also, by contrast to online speech (in **Figure 2**) the anti-cyberbullying statute here is, interestingly, a distant fourth with answers almost evenly distributed across the spectrum of possible responses. This can probably be explained by the fact that the anti-cyberbullying statute here would appear to target speech and other forms of communication online - it is vague and has uncertain application and *aims* to prevent “harassment” or “intimidation” online. Online search, as a discrete and non-communicative online activity, would expectedly be far less impacted.

4.3 ONLINE SHARING / SOCIAL MEDIA CONTRIBUTIONS

Online sharing of content personally created by the respondent in question was also demonstrably chilled in each of the scenarios, though not as much as either online speech or search chill noted earlier, but certainly more so than time spent online. This is an important category of activities, because they concern creativity, authorship, and even innovation on the part of the person being potentially “chilling”. The results (see **Figure 4**) show that, again, personally receiving an individualised legal notice about online activities (72% of respondents either “much less” or “somewhat less” likely to share) and government surveillance (60% of respondents “much” or “somewhat” less likely to share) would have had the greatest chilling effect on such legal online activities. The anti-cyberbullying statute also suggested some chilling effect (34% of respondents were either “much less likely” or “somewhat less likely”), though a majority (51%) indicated that their sharing would not be impacted by the statute.

Figure 4: Impact on online sharing (personally created content)

Respondents were asked whether they would be “more likely or less likely to share content on the internet that [the respondent] personally created, authored, or made (e.g., a digital photo, song, blog post, Facebook status update, etc)” in response to each hypothetical scenario. This chart maps the responses consistent with previous graphs.



Again, these results also provide support for chilling effects, especially so since the content in this hypothetical scenario concerns creative output (“personally created” content), which also means such content would almost always be legal (e.g., does not raise any copyright concerns in most cases, unlike content being shared that has been created by someone else). The comparative ranking in terms of chilling effects here, with the personally received legal threat and government surveillance much more significant than the anti-cyberbullying statute, can likely be explained for similar reasons noted for the “online speech” section above (See **Figure 1** and **Figure 2** and accompanying interpretation) - for example, more targeted enforcement (like individualised notice) will have a more profound impact; government surveillance, rather than simply a vague law, has more impact. That seems to be the case with creative output as well.

4.4 TARGETED CONTENT (AND USER RESISTANCE)

Consistent with Barendt et al. (1997)'s notion to 'direct' chill (how people are impacted with respect to specifically targeted content or activities, and how they respond). Questions were also posed concerning the third scenario - the personally received legal notice concerning content posted online - about how likely the respondents would take steps to legally challenge the notice they received if they believed it was wrong or mistaken. Here, responses were fairly evenly distributed, with 34% saying they would challenge; 36% saying no they would not; and 30% saying they "Don't know". For those who indicated they would not challenge the legal notice, or did not know, the potential costs of (legally) challenging the legal notice was the most significant factor with 81% of respondents citing it as a reason not to take such steps. Other concerns were time costs (66%), wishing to avoid trouble (legal or otherwise) (53%) not understanding the legal issue at stake (28%), or not knowing how to legally challenge the notice (34%).¹³ Also, these legal notices were mostly effective in deterring re-posting or re-sharing of content that the notice had targeted - 70% of respondents were "very unlikely" (54%) or "somewhat unlikely" (16%) to re-post or re-share. However, a notable percentage of respondents (15%) also said receiving the notice would actually make them "very likely" (4%) or "somewhat likely" (11%) to re-post or re-share.

5. DISCUSSION AND ANALYSIS

5.1 EVIDENCE FOR CHILLING EFFECTS MORE GENERALLY

More generally, these findings strongly support a theory of *online chilling effects* on internet users legal activities due to a range of regulatory activities (statutory, corporate/state surveillance, individualised legal notices/enforcement, and secondary (or network) chilling effects, where users are chilled simply due to becoming aware that a friend or other member of their social network have been targeted by such regulatory actions.

5.2 COMPARATIVE CHILLING EFFECTS

There are also *comparative* insights. When examining the chilling effects evidence comparatively, the results also provide insight into what sort of regulatory acts or actions may have the *greatest* online chilling effects. On a comparative angle of view, scenario three, that is, the individualised and personally received legal notice, containing a legal threat about content posted online, consistently suggested greater levels of chilling effects among respondents across the different scenarios - rendering respondents less likely to speak or write in certain contexts online (or more careful about what they say or write online), less likely to share of personally created content online, less likely to contribute to social networks and other online forums, and less likely to spend time on the internet more generally. This finding was consistent across all online activities tracked, except online search - here, government surveillance had a slightly greater impact, with a full 78% of respondents agreeing with the statement that knowing that the government was monitoring online activities they would be "more careful" about what they search for online. Though even here, the personally received individualised legal notice also had a substantial impact with 77% responding agreeing they would be "more careful". Indeed, comparatively, government surveillance consistently had the second most "chill" or impact across all forms of online activities explored.

Neither of these findings are unexpected given that chilling effects theory hypothesises that people are deterred both by the threat of punishment pursuant to vague or unclear laws or rules but also, as Solove (2006) suggests, a chilling effect due to a kind of "environmental pollution"

wherein regulatory actions like state surveillance chill or deter certain legal activities. In such cases, the chilling effect might arise out of concern for privacy, fear of potential government targeting, and/or social conformity (e.g., to avoid being associated with unpopular ideas or causes). The individualised legal notice and the government surveillance scenarios both implicate such chilling effects. With individualised or personally received legal notices (disclosing legal claims or threats), people would feel specifically targeted and would thus increase the likelihood of punishment or penalty greater, leading to more of a chilling effect as noted in the results. In terms of online speech and online search activities, corporate surveillance also had a chilling effect comparable to, but not as significant as, government surveillance. This could be explained by the respondents viewing corporate surveillance as less broad or effective as government; or, perhaps, the findings may also reflect the Weberian view of state power, where only the state has a legitimate claim to the use of force and violence (Weber, 1965); here, the “violence” is done through corporate surveillance.

Results concerning the fourth scenario deserve some additional attention, as this was more of an exploratory aspect of the case study. These findings provide a novel contribution in providing empirical foundations for *networked chilling effects*; that is, people who simply read, or are made aware of, online regulatory actions are themselves chilled or deterred. Comparatively speaking, across the range of online activities explored (in relation to different potential “chilling effects” scenarios), this networked impact was consistently comparable to the impact or effects caused by hypothetical scenarios involving other kinds of regulatory acts or actions. There were instances, in fact, where this secondary or networked impact was greater than most others. In the comparative results for online search (**Figure 1**), this scenario had the second most substantial impact just behind government surveillance, with 39% “strongly” agreeing and 38% “somewhat” agreeing with the statement that they would be “more careful” about what they search for online; even outstripping a personal legal threat. And in the comparative results for online speech across five scenarios (three primary and two more exploratory in **Figure 2**), the results suggest that this kind of networked regulatory effect (here, seeing a friend posting on Facebook about receiving a personal legal notice may have a greater “chill” than both corporate surveillance or even effects caused by a vague statute or regulation enacted in relation to online activities (though, this will likely depend on the nature of the statute in question and the context of the activities).

Again, these findings are consistent with chilling effects theory - knowing that someone in your social network is being targeted by public or private legal threats concerning their online activities - could raise concerns of similar legal targeting, mistaken punishment, pressures to conform, or guilt by association; thus, causing a “chill” on otherwise legal activities. And as earlier noted, with respect to online search, it may be that respondents understood the legal notice in the hypothetical scenario (e.g., sent to a friend about potentially illegal downloads) most likely concerned online searches for copyrighted material, hence the greater number of respondents being “careful” about searching for such content online.

5.3 CHILLING EFFECTS FACTORS: ANALYSING UNDERLYING RELATIONSHIPS

Beyond the analysis of percentages and comparisons above, factors underlying or influencing the “chilling effect” evidenced in the hypothetical scenarios (e.g., being less likely to speak, search, or share online, due to knowledge of online surveillance) were statistically analysed in relation to a range of demographic and comparable variables such as age, gender, level of education, level of income, level of internet use, whether they have followed the news about online surveillance (e.g., news about the NSA surveillance programmes), how often they share

personally created content online, how often they contribute to social network sites and other online forums, and, the respondents' familiarity with laws that regulate the internet (assessed by the respondents on a scale).

This analysis was done to identify any potential background factors or variables that influence, or have an association with any potential chilling effects suggested by the responses. The core statistical test results for the three primary scenarios analysed are set out in **Table 1**, **2**, and **3**, respectively. Two other scenarios analysed - though not extensively as they are more exploratory - was the impact of online surveillance by a private internet company as well as a friend (of the respondent internet user) posting on a social network about receiving a legal notice about unauthorised or illegal downloading online. Those results are set out in **Table 4** and **5**, respectively.

Table 1 – Anti-cyberbullying scenario (#1): chi-square (X^2) and gamma (γ) test results predicting respondent's willingness to discuss, search, or share content online after government enacts vague law criminalising cyber-bullying.			
	Less likely to speak/write online	More caution in online search	Less likely to share online
Predictor			
Age	$X^2(df) = 37.8(16)^*$ $\gamma = -0.07^*$	48.6(16)** -0.19**	28.5(16)* -0.07*
Gender	9.1(4) -0.0805	3.1(4) -0.04	8.8(4) -0.14*
Education level***	13.5(4) -0.09	22.4(8)** -0.16**	13.9(8) -0.12*
Income level	33.1(16)** -0.06	17.9(16) -0.06	12.8(16) -0.03
Internet usage level***	20.3(8)** -0.02	26.2(8)** 0.03	16.2(8)* -0.03
Followed news about NSA***	39.3(16)** 0.06	28.4(16)* 0.01	26.9(16)* 0.05
Frequency of online sharing	11.1(16) -0.03	17.9(16) -0.00	17.6(16) -0.00
SNS engagement level	30.6(16)* -0.02	5.8(16) -0.00	33.3(16)** -0.00
Legal awareness level***	24.4(16) 0.00	9.6(16) 0.00	31.1(16)* -0.03

* $p < 0.05$, ** $p < 0.01$, *** = Recoded

bold = significant gamma results (chi-square also highlighted where gamma also significant)

Table 2 – Government online surveillance (#2): chi-square (X^2) and gamma (γ) test results predicting respondent's willingness to discuss, search, or share content online after made aware of government online surveillance

	Less likely to speak/write online	More caution in online search	Less likely to share online
Predictor			
Age	X ² (df) = 36.2(16)** $\gamma = -0.07^*$	41(16)** -0.17**	24.4(16) -0.08*
Gender	6.5(4) -0.00	2.1(4) -0.01	1.8(4) -0.00
Education level***	15.3(8) 0.07	10.8(8) -0.05	11.3(8) -0.00
Income level	15.9(16) -0.03	17.7(16) -0.00	14.5(16) -0.04
Internet usage level***	16.3(8)* 0.00	24.3(8)** 0.06	33.5(8)** 0.02
Followed news about NSA***	79.2(16)** 0.12**	32(16)* 0.10**	42.3(16)** 0.13**
Frequency of online sharing	18.1(16) -0.02	9.6(16) -0.00	21.1(16) -0.06
SNS engagement level	17.7(16) 0.03	32.3(16)* 0.00	15.6(16) -0.02
Legal awareness level***	48.2(16)** 0.03	21.5(16) 0.03	31.7(16)* 0.01

* $p < 0.05$, ** $p < 0.01$, *** = Recoded

bold = significant gamma results (chi-square also highlighted where gamma also significant)

Table 3 – Personally received legal notice/threat (#3): chi-square (X²) and gamma (γ) test results predicting respondent's willingness to discuss, search, or share content online after personally receiving a threatening legal notice

	Less likely to speak/write online	More caution in online search	Less likely to share online
Predictor			
Age	X ² (df) = 12.9(16) $\gamma = 0.03$	14.8 (16) -0.09**	22.7(16)* -0.02
Gender	23.4(4)** 0.19**	14.9(4)** 0.13**	5.7(4) 0.09*
Education level***	11.8(8) 0.05	6.9(8) -0.07	6.7(8) -0.00
Income level	19.1(16) 0.05	19.2(16) 0.04	20.45(16) 0.02
Internet usage level***	35(8)** 0.00	11.4(8) -0.03	33.9(8)** 0.01

Followed news about NSA***	33.2(16)** -0.05	37.3(16)** 0.03	24.1(16) -0.00
Frequency of online sharing	14.8(16) -0.04	9.5(16) 0.00	17.9(16) -0.03
SNS engagement level	28.1(16)* -0.10**	21.5(16) -0.03	15.6(16) -0.10**
Legal awareness level***	49.9(16)** 0.11**	29.9(16)* 0.03	23.5(16) 0.08*

* $p < 0.05$, ** $p < 0.01$, *** = Recoded

bold = significant gamma results (chi-square also highlighted where gamma also significant)

Table 4 – Online surveillance by a private internet company (#4): chi-square (X^2) and gamma (γ) test results predicting respondents being more careful in their online speech and searches after made aware of online surveillance by a private internet corporation

	More cautious/careful in online speech	More cautious/careful in online search
Predictor		
Age	$X^2(df) = 27.9(16)^*$ $\gamma = -0.05$	38(16)** -0.08*
Gender	8.3(4) 0.10*	0.5(4) 0.03
Education level***	8.6(8) -0.05	12.8(8) -0.08
Income level	11.8(16) 0.00	11.3(16) 0.03
Internet usage level***	11.1(8) -0.03	14(8) -0.00
Followed news about NSA***	45.6(16)** 0.11**	32.6(16)** 0.07*
Frequency of online sharing	18.1(16) -0.00	16.3(16) 0.00
SNS engagement level	18.1(16) -0.02	24.4(16) -0.00
Legal awareness level***	30.4(16)** 0.09**	17.8(16) 0.07*

* $p < 0.05$, ** $p < 0.01$, *** = Recoded

bold = significant gamma results (chi-square also highlighted where gamma also significant)

Table 5 – Friend posting about receiving legal notice/threat (#5): chi-square (X^2) and gamma (γ) test results predicting respondents being more careful and cautious in their online speech and searches after made aware a friend has received a threatening legal notice for unauthorised/illegal downloading online

	More cautious/careful in online speech	More cautious/careful in online search
Predictor		
Age	X ² (df) = 20.2(16) γ = 0.08	19.2(16) -0.02
Gender	9.8(4)* 0.18**	4.3(4) 0.11
Education level***	10.7(8) -0.15*	9.48) -0.21**
Income level	12.7(16) 0.10*	12.8(16) 0.03
Internet usage level***	4.4(8) 0.02	11.4(8) 0.00
Followed news about NSA***	10.7(16) -0.05	20.8(16) -0.03
Frequency of online sharing	14.4(16) -0.06	26.2(16) -0.00
SNS engagement level	34.5(16) -0.18**	21.8(16) -0.11*
Legal awareness level***	18.7(16) -0.03	18.4(16) 0.08

* $p < 0.05$, ** $p < 0.01$, *** = Recoded

bold = significant gamma results (chi-square also highlighted where gamma also significant)

Younger internet users more likely to be chilled

There are some interesting results here as well. In the findings set out in **Tables 1, 2, and 3**, age had a statistically significant negative association in relation to all three forms of chilling effects in the first hypothetical scenario that involved the vague anti-cyberbullying statute (with harsh penalties attached). That is, as the age of respondents increased, chilling effects in relation to the anti-cyberbullying statute decreased.¹⁴ It also had a statistically significant negative association with all three forms of chilling effects for the government surveillance scenario (hypothetical scenario two).¹⁵ It should be noted that these associations were weak to moderate, but the pattern, nevertheless, is noteworthy. Interestingly, that pattern breaks with the third hypothetical scenario (individualised and personally received legal notice). It should be noted that these associations were weak to moderate, but the pattern, nevertheless, is noteworthy. In the scenario involving corporate online surveillance (**Table 4**), there was also a mild negative statistically significant association between the age of respondents and respondents being more careful and cautious about their online searches once made aware about an internet company conducting online surveillance; this, again, suggests more chilling effects for younger respondents.

Interestingly, that pattern breaks with the third hypothetical scenario (individualised and personally received legal notice). Here, age only has a statistically significant relationship with chilling effects with *one* activity (online search), also a negative association.¹⁶ One explanation is that the first two hypothetical scenarios - the anti-cyberbullying statute and the government

surveillance - both involve a measure of vagueness and uncertainty - respondents are not personally targeted and so must make a judgment as to whether they think they might be targeted, and this would have an impact on their searching, speaking, and sharing online. On that count, it seems youth may be more impacted or cautious in their activities, assuming they are more likely to be targeted as compared to older respondents, who are less concerned. By the third scenario, that uncertainty is significantly reduced in the sense that the legal notice is personally delivered; so youthful cautiousness is no longer a factor in most cases with people being “chilled” more uniformly, other than online search.

Female internet users more likely to be chilled

A second notable point concerns gender. Findings in **Tables 1, 2, and 3**, show gender had no effect in the second (government surveillance) scenario but becomes a noteworthy factor in the third scenario - where a threatening legal notice is received.¹⁷ Due to the way in which the gender variable was coded, the positive association suggests that female respondents were “chilled” in relation to all three forms of activities in this hypothetical scenario (less likely to speak or write online in certain contexts, less likely to share personally created content, and would be more careful in their online search activities). There was also a gender effect in the scenarios involving corporate online surveillance and where a friend is targeted with a personal legal notice (**Tables 4 and 5**), with a mild positive association between female respondents and their being more cautious/careful about their online speech for both of these scenarios.

It is difficult to say why female respondents were more affected in these scenarios, but the results no doubt suggest females in this sample were much more cautious and chilled once they were personally targeted or, as with the scenario where a friend is targeted, someone close to them are targeted. The gender effect in the corporate surveillance scenario, but not the government surveillance scenario, may also suggest women distrust or feel they are more likely to be targeted by corporate employers or employees than government agencies. Consistent with Lenhart et al. (2016)— who found women were more likely to be negatively affected by online harassment (which can include forms of threats)— these findings suggest women may also be more negatively impacted and chilled by personal legal threats concerning online activities as well.

Anti-cyberbullying statute has salutary impact on women’s sharing

Also, notably, there was a statistically significant negative association between being female and chilling effects on personal sharing online in relation to the first scenario involving the anti-cyberbullying statute.¹⁸ One way of reading this, is that men were more likely to be chilled from personal sharing due to the anti-cyberbullying statute in scenario one. However, given that the statute had little chilling effects overall, another way of interpreting this, is that the anti-cyberbullying statute had a salutary or positive impact on sharing personally created content among female respondents. In other words, with new legal measures to protect or deter cyberbullying and harassment online, women were more willing to share

This is noteworthy as a substantial body of legal literature argues that statutes regulating or criminalizing online harassment or cyberbullying proscribe or deter constitutionally protected online speech (Volokh, 2016; Kayyali and O’Brien, 2016; Diaz, 2016; Buchhandler-Raphael, 2015; Hayward, 2011; King, 2010). The analysis may change, however, if these laws encourage greater online speech and sharing, while minimally impacting other speech (results suggested a chilling effect on some user activities but far less than in other scenarios). While not absolving other important concerns about enforcement or impact on other online activities (Marwick and Miller, 2014; Kayyali and O’Brien, 2016), these findings are consistent with what advocates like Danielle Citron argue; that such legal interventions can help preserve the “expressive autonomy”

of past or potential targets of such abuse by facilitating their speech, expression, and participation online (2014: 196-197)..

Knowledge of NSA news leads to greater chill

A third observation of note concerns the impact that respondents' familiarity with news stories concerning surveillance by the "NSA" has on comparative chilling effects. Respondents were asked to indicate how closely they were following news stories concerning NSA surveillance; as it turns out, at least for the second hypothetical involving government surveillance, how closely the respondent follows NSA news helps predict how much respondents were "chilled" in relation to the three online activities in this scenario. The gamma values are all positive here, indicating a statistically significant positive measure of association.¹⁹ This is not surprising; it makes sense that those respondents following the news about the NSA's pervasive and invasive surveillance practices would be more likely to be "chilled" by the government surveillance in hypothetical scenario two. These findings are also consistent with recent studies finding evidence of chilling effects associated with awareness of NSA online surveillance in Wikipedia article traffic data (Penney, 2016) and Google search trends (Marthews and Tucker, 2016). They are also consistent with recent experimental findings of the same (Stoycheff, 2015).

This statistically significant "NSA knowledge" effect also held for the scenario involving online surveillance conducted by a private internet company. These findings also make sense—someone sensitive about government surveillance due to awareness about the NSA's overreaching activities would likely be similarly sensitive about similar surveillance practices carried out by a private company. That is reflected again here.

Other factors

There are other noteworthy observations (for graphs and data on the demographics of the participant pool, see **Appendices 2** through **5**). First, education level was largely a non-factor in most cases, except in the first scenario (involving the anti-cyberbullying statute). Here, where there was a mild negative association between education level and respondents being less likely to share, and showing more caution in their online search activities. In other words, as the education level increased for respondents, chilling effects decreased, at least in these two instances. Also, the respondents' self-assessed level of awareness of regulations and relevant laws was largely a non-factor, except in the third factor, involving the personally received legal notice, where legal awareness had a statistically significant weak to mild association with being less likely to speak or write after receiving the notice, or showing more caution in online searching. This makes sense, as with additional legal awareness, a respondent may be more cautious or careful in their online activities, being more aware of the potential legal risks at stake. Also interesting are those things that turned out to not be associated with chilling effects. While education and income levels had a statistically significant (negative) association with chilling effects in a handful of cases, overall, they were simply not a notable factor.

Also, amount of time spent online, level of personal sharing, level of regular contributions to social network sites and other online forums, and even familiarity with laws applying to the internet, were, apart from one or two instances, mostly non-factors in terms of responses to hypothetical chilling effect scenarios. It should be noted, however, that the latter (legal awareness) did have a negative association concerning the impact the personally received legal notice (scenario three) had on online speech and content sharing (personally created content). This also makes sense, as familiarity with the law would lead respondents to feel less threatened. The fact that these factors ended up having little relationship with chilling effects in most cases is similar to the findings by Stoycheff (2016), who also found education levels, income levels, attention to news, and political knowledge had no statistically significant relationship with

participants willingness to speak out in the face of known surveillance.

As with results in **Table 1, 2, and 3** those set out in **Table 4 and 5** are interesting for those things that turned out to not be associated with chilling effects. Income levels, internet usage levels, frequency of online sharing, were all, once again, mostly non-factors. Again, these demographic and other factors having no significant relationship with chilling effects similar to the findings by Stoycheff (2016).

Interestingly, however, education level and level of social network engagement had a mild to moderate negative association for respondents being more cautious or careful with online speech and search in relation to scenario #5 (friend posting about receiving a legal notice); this is not easy to explain, but may simply be a proxy for some other variable or measure, like sensitivity postings on social network sites. Perhaps respondents with higher levels of education are more likely to have attended universities, and thus gained more social network connections and online social network “friends”, and are more desensitised (and so less chilled) due to postings by friends, including where legal concerns are involved. Similarly, respondents who are more engaged with social network sites may also be less sensitive to such postings simply because they encounter such postings more often in their higher levels of use and are thus less chilled. These findings are similar to Stoycheff (2016), who also found the higher levels of social media use was associated with respondents being more willing to speak up (and thus be chilled less).

Younger and female internet users less likely to resist chilling effects

Respondents were also asked in relation to hypothetical scenario three (receiving the personal legal notice, like a DMCA copyright notice) how likely they would take steps to legally challenge the legal notice they received if they believed it was wrong or mistaken (to explore notions of more specific or direct chilling effects). Additional statistical analysis was conducted to explore what demographics (and related variables) may be a factor or be associated with respondents’ willingness to legally challenge the notice. Here, there was a mild negative association between age and willingness to challenge ($\gamma = -0.10$; $p < 0.05$) suggesting younger respondents were less likely to “resist” or fight back against the legal threat/notice received. There was also a small negative association between respondents being female and willingness to challenge suggesting females were also mildly less likely to do so as well ($\gamma = -0.12$; $X^2 = 3.95$; $df = 1$; $p < 0.05$).

Engaged internet users more likely to resist chilling effects

There was also a positive association between willingness to challenge and two internet “engagement” variables: time spent online ($\gamma = 0.19$; $X^2 = 11.7$; $df = 2$; $p < 0.01$) and level of social network site (and related) engagement ($\gamma = 0.13$; $X^2 = 11.4$; $df = 4$; $p < 0.05$). Notably, there were also somewhat stronger positive associations between willingness to take steps to challenge the legal notice in this scenario and two other variables - familiarity with internet laws ($\gamma = 0.34$; $X^2 = 50.83$; $df = 4$; $p < 0.01$) and how closely respondents were following NSA news ($\gamma = 0.23$; $X^2 = 35.4$; $df = 4$; $p < 0.01$). These make sense, if you believe you have a stronger grasp of the law, you may feel more confident in a legal challenge. In the case of the NSA news knowledge, this may reflect reality that respondents more engaged with the issue (greater knowledge of surveillance challenges) are also more likely to take concrete steps to defend themselves.

Also interesting to note: despite respondents citing the potential costs of (legally) challenging the legal notice received as the most significant deterrent for taking steps to legally challenge a note that they receive (81% citing it), annual income of respondents had no statistically significant association with respondents’ indication that they would challenge the legal notice.

Education levels also disclosed no significant association. These results suggest that notwithstanding what respondents might say to self-report as their reasons for deciding to challenge a legal notice or not, it would seem that other factors may be more influential in their decisions either way. Certainly, knowledge of the law would likely encourage a person to challenge a notice; and, similarly, someone who spends a lot of time online or contributes heavily to social network sites and other online communities may be more motivated to challenge in order to defend a practice they do regularly (and thus feel is important).

CONCLUSION AND LIMITATIONS

Chilling effects on legal and democratic activities, online or off, as Bruce Schneier has implore, are an insidious force for conformity and are thus corrosive to “political discourse” (2015: 95-99; Deibert, 2013: 130-132) and the “democratic processes” (Parsons, 2015: 2) that lead to an “extrinsic losses of freedom” (Nissenbaum, 2009). And this article has discussed the results of a new and original survey-based case study that offer strong support for the suggestion that state and non-state action, such as laws, regulations, or state actions like surveillance, can, and do, have a chilling effect on people’s activities online. The study provides comparative insights as well, suggesting, not surprisingly, that greater chilling effects arise when individuals are personally targeted by legal threat (as with a DMCA notice received for content posted online) (scenario #3) while government surveillance (scenario #2) was consistently associated with the second highest level of chilling effects; though findings suggested chilling effects in every scenario examined. This study also suggests younger people and women are more negatively chilled in certain circumstances and are less likely to take steps to defend themselves from regulatory actions and threats. Some findings, however, suggest certain legal interventions may have salutary effects to encourage online speech and sharing by women, but more research needs to be done on this point. Additionally, findings suggest a range of other factors, like education, legal training, and knowledge of the US National Security Agency’s online activities also influence the nature and extent of regulatory chilling effects.

Of course, this study also had a number of limitations. First, using an online crowdsourcing platform for recruitment means that this survey does not use randomised probability sampling (a method ideal for a representative sample) (Berg, 2009; Bryman, 2008). Rather, the strategy was purposive sampling, in that while the sample included only willing user participants (and thus introduces concerns about self-selection and sampling bias), though this is common not only to case study but also survey-based studies more generally. Indeed, the participant pool was “relatively representative” of the US internet user population and, additionally, measures were taken to strengthen the validity of findings. Future work, with more representative and probability sampling, would be optimal. Second, this case study employing an original survey, developed specifically for this research, meaning it the scales and methods used have not be “validated” by other research. But this limitation is mainly a product of the fact that there are *no* such validated scales or metrics to employ, especially on the comparative dimensions of chilling effects online; as noted, the survey used here was specifically designed for this research, and provides a methodological contribution as a model, template, or foundation for further studies and measures, building on, and improving, its findings and design. Third, this survey was primarily quantitative in design and employed Likert scale questions creating categorical variables. This was to allow greater ease of comparison as examining chilling effects across different scenarios with different forms of regulatory actions was a key aim; however, it also meant more qualitative data (and accompanying insights) were not obtained. A future study,

focusing on these qualitative elements, would be invaluable.

No doubt, there is far more work, employing a range of methods, necessary to substantiate and explore chilling effects online. This study, however, has aimed to address existing gaps and has done so in providing both general and comparative insights, as well as a methodological design to improve upon, and employ, in new contexts.

REFERENCES

- Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification*. Paper presented at the Proceedings of the 5th ACM conference on Electronic commerce.
- Acquisti, A., John, L. K., & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, 49(2), 160-174.
- Agir, B., Calbimonte, J.-P., & Aberer, K. (2014). *Semantic and Sensitivity Aware Location Privacy Protection for the Internet of Things*. Paper presented at the Privacy Online: Workshop on Society, Privacy and the Semantic Web Privon 2014.
- Allam, A., Schulz, P.J., & Nakatmoto, K. (2014). The Impact of Search Selection and Sorting Criteria on Vaccination Beliefs and Attitudes: Two Experiments Manipulating Google Outputs. *Journal of Medical Internet Search*, 16(4): e100.
http://www.jmir.org/article/viewFile/jmir_v16i4e100/2
- Barendt, E., Lustgarten, L., Norrie, K., & Stephenson, H. (1997). *Libel and the Media: The Chilling Effect*. New York: Clarendon Press; Oxford: Oxford University Press.
- Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, 48(4), 101-106.
- Berg, B. L. (2009). *Qualitative research methods for the social sciences* (7th ed.). Boston; Montreal: Allyn & Bacon.
- Bernheim, B. D., Bjorkegren, D., Naecker, J., & Rangel, A. (2013). Do Hypothetical Choices and Non-Choice Ratings Reveal Preferences? National Bureau of Economic Research.
- Blasi, V. (1981). Toward a Theory of Prior Restraint: The Central Linkage. *Minn. L. Rev.*, 66, 11.
- Bonetto, M., Korshunov, P., Ramponi, G., & Ebrahimi, T. (2015). *Privacy in Mini-drone Based Video Surveillance*. Paper presented at the Workshop on De-identification for privacy protection in multimedia.
- boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8).
- Bryman, A. (2008). *Social research methods* (3rd ed.). Oxford ; New York: Oxford University Press.
- Buchhandler-Raphael, M. (2015). Overcriminalizing Speech. *Cardozo L. Rev.* Vol 36.
- Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-quality, Data? *Perspectives on psychological science*, 6(1), 3-5.
- Cobia, J. (2009). Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process, The. *Minn. JL Sci. & Tech.*, 10, 387.
- Carter, R. R., DiFeo, A., Bogie, K., Zhang, G.-Q., & Sun, J. (2014). Crowdsourcing Awareness: Exploration of the Ovarian Cancer Knowledge Gap through Amazon Mechanical Turk. *PLoS ONE*, 9(1), e85508. doi: 10.1371/journal.pone.0085508

- Cederborg, A., Swlwander, K.R., & Blom, K.A. (2015). Research Expanding Current Understandings of Bullying in Sweden. *Pensamiento Psicológico*, Vol 14, No 1, 2016, pp. 131-146.
- Chen, D. L., & Yeh, S. (2013). The Construction of Morals. *Journal of Economic Behavior and Organization*.
- Citron, D. (2014). *Hate Crimes in Cyberspace*. Cambridge: Harvard University Press.
- Clifford, S., Jewell, R. M., & Waggoner, P. D. (2015). Are samples drawn from Mechanical Turk valid for research on political ideology? *Research & Politics*, 2(4). doi: 10.1177/2053168015622072
- Cochran, W. G. (1954). Some methods for strengthening the common χ^2 tests. *Biometrics*, 10(4), 417-451.
- Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). *Location Disclosure to Social Relations: why, when, & what people want to share*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.
- Coolican, H. (2014). *Research Methods and Statistics in Psychology*: Psychology Press.
- Coviello, L., Sohn, Y., Kramer, A. D., Marlow, C., Franceschetti, M., Christakis, N. A., & Fowler, J. H. (2014). Detecting emotional contagion in massive social networks. *PLoS ONE*, 9(3), e90315.
- Crump, M. J. C., McDonnell, J. V., & Gureckis, T. M. (2013). Evaluating Amazon's Mechanical Turk as a Tool for Experimental Behavioral Research. *PLoS ONE*, 8(3), e57410.
- Das, S., & Kramer, A. (2013). Self-censorship on Facebook. *Proc. of ICWSM 2013*, 120-127.
- Dasgupta, K. (2016). *Youth response to state cyberbullying laws* [Working Paper No. 2016-05]. Department of Economics, Auckland University of Technology. http://www.aut.ac.nz/__data/assets/pdf_file/0009/695259/Economics-WP-2016-05.pdf
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access contested: security, identity, and resistance in Asian cyberspace*: MIT Press.
- Deibert, R. J. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal.
- Diaz, F.L. (2016). Trolling & the First Amendment: Protecting Internet Speech in the Era of Cyberbullies and Internet Defamation. *Journal of Law, Technology, and Policy*.
- Dittrich, D., & Kenneally, E. (2012). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. In M. Madden & L. Rainie (Eds.), *Tech. rep., U.S. Department of Homeland Security*.
- El Asam, A. & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. *Computers in Human Behavior*. Vol 65, pp. 127-141, <http://www.sciencedirect.com/science/article/pii/S0747563216305775>
- Faris, R., Ashar, A., Gasser, U., & Joo, D. (2016). Understanding Harmful Speech Online.

Berkman Klein Center Research Publication 2016-21,

<https://cyber.harvard.edu/publications/2016/UnderstandingHarmfulSpeech>

Ferguson, C. J. (2009). An Effect Size Primer: A Guide for Clinicians and Researchers.

Professional Psychology: Research and Practice, 40(5), 532.

Göktas, A. & Işci, O. (2008). A comparison of the most commonly used measures of association for doubly ordered square contingency tables via simulation. *Metodološki zvezki* 8(1), 17–37.

Graham, S. & D. Wood. (2003). "Digitising Surveillance: Categorisation, Space, Inequality", *Critical Social Policy*, 23(2): 227-248

Hamby, T., & Taylor, W. (2016). Survey Satisficing Inflates Reliability and Validity Measures: An Experimental Comparison of College and Amazon Mechanical Turk Samples. *Educational and Psychological Measurement*. doi: 10.1177/0013164415627349

Harper, J., & Singleton, S. (2001). With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us. *Competitive Enterprise Institute*.

Hayward, J. O. (2011). Anti-Cyber Bullying Statutes: Threat to Student Free Speech. *Clev. St. L. Rev.*, 59, 85.

Hazelwood, S.D. & Koon-Magnin, S. (2013). Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. *International Journal of Cyber Criminology*. Vol 7, No. 2, <http://www.cybercrimejournal.com/hazelwoodkoonmagninijcc2013vol7issue2.pdf>

Henry, N. & Powell, A. (2016). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, and Abuse*. Vol 14, No 1., <http://journals.sagepub.com/doi/pdf/10.1177/1524838016650189>

Hinduja, S. & Patchin, J.W. (2016). State Cyberbullying Laws A Brief Review of State Cyberbullying Laws and Policies. *Cyberbullying Research Center Report*, <http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf>

Hinduja, S. & Patchin, J.W. (2014). Cyberbullying Identification, Prevention, & Response, *Cyberbullying Research Center Fact Sheet*, http://cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf

Healey, J. (2012). *The Essentials of Statistics: A Tool for Social Research*: Cengage Learning.

Horwitz, M. J. (1997). In Memoriam: William J. Brennan, Jr. *Harvard Law Review*, 111(1), 1-50. doi:10.2307/1342130

Kaminski, M. E., & Witnov, S. (2015). The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech. *University of Richmond Law Review*, 49.

Kaspar, B. L. (2012). Beyond the Schoolhouse Gate: Should Schools Have the Authority to Punish Online Student Speech.

Kayyali, D. & O'Brien, D. (2015). Facing the Challenge of Online Harassment, *EFF Deeplinks Blog*, <https://www.eff.org/deeplinks/2015/01/facing-challenge-online-harassment>

Keith, M., Ngo, N., & Babb, J. (2014). The Effects of Consumer Self-regulation on Information

Disclosure Over Mobile Devices.

Kenyon, A. T. (2010). Investigating Chilling Effects: News Media and Public Speech in Malaysia, Singapore, and Australia. *International Journal of Communication*, 4, 440–467.

King, A.V. (2010). Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech. *Vand. L. Rev.* Vol 65,
<https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx>

Korshunov, P., Melle, A., Dugelay, J.-L., & Ebrahimi, T. (2013). *Framework For Objective Evaluation of Privacy Filters*. Paper presented at the SPIE Optical Engineering+ Applications.

Korshunov, P., Nemoto, H., Skodras, A., & Ebrahimi, T. (2014). *Crowdsourcing-based Evaluation of Privacy in HDR images*. Paper presented at the SPIE Photonics Europe.

Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016). Online Harassment, Digital Abuse, and Cyberstalking in America, *Data & Society Institute Report*.
<https://datasociety.net/output/online-harassment-digital-abuse-cyberstalking/>

Levay, K. E., Freese, J., & Druckman, J. N. (2016). The Demographic and Political Composition of Mechanical Turk Samples. *SAGE Open*, 6(1). doi: 10.1177/2158244016636433

Liljas, B., & Blumenschein, K. (2000). On Hypothetical Bias and Calibration in Cost–benefit Studies. *Health Policy*, 52(1), 53–70.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). *Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing*. Paper presented at the Proceedings of the 2012 ACM Conference on Ubiquitous Computing.

Lyon, D. (2015). *Surveillance After Snowden*. Cambridge, MA: Polity Press.

Lyon, D. (2006). *Theorizing surveillance: The panopticon and beyond*. Cullompton, Devon: Willan Publishing.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Lyon, D. (1991). “Bentham’s Panopticon: From moral architecture to electronic surveillance,” *Queen’s Quarterly*, volume 98, number 3, pp. 596–617.

Malheiros, M., Preibusch, S., & Sasse, M. A. (2013). “Fairly truthful”: The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. *Trust and Trustworthy Computing* (pp. 250–266): Springer.

Mamonov, S., & Koufaris, M. (2014). The Impact of Perceived Privacy Breach on Smartphone User Attitudes and Intention to Terminate the Relationship with the Mobile Carrier. *Communications of the Association for Information Systems*, 34(1), 60.

Marshall, C. C., & Shipman, F. M. (2013). *Experiences Surveying the Crowd: Reflections on Methods, Participation, and Reliability*. Paper presented at the Proceedings of the 5th Annual ACM Web Science Conference.

Marthews, A., & Tucker, C. (2014). Government Surveillance and Internet Search Behavior. *MIT Sloane Working Paper No. 14380*.

Marwick, A.E. & Miller, R.W. (2014). Online harassment, defamation, and hateful speech: A primer of the legal landscape, *Fordham Center on Law and Information Policy Report*, <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1002&context=clip>

Marx, G.T., (2002). "What's New About the 'New Surveillance'? Classifying for Change and Continuity". *Surveillance & Society*, 1(1), pp. 9-29.

McDonald, A. M., & Cranor, L. F. (2010). *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*. Paper presented at the Proceedings of the 2010 Research Conference on Communication, Information and Internet Policy.

McDonough, P. E. (2013). Where Good Intentions Go Bad: Redrafting the Massachusetts Cyberbullying Statute to Protect Student Speech. *Suffolk UL Rev.*, 46, 627.

Morrison, M., & Brown, T. C. (2009). Testing the Effectiveness of Certainty Scales, Cheap Talk, and Dissonance-minimization in Reducing Hypothetical Bias in Contingent Valuation Studies. *Environmental and Resource Economics*, 44(3), 307-326.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*: Stanford University Press.

Nye, J. (2010). Cyber power. *The Future of Power in the 21st Century*. Belfer Center for Science and International Affairs.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running Experiments on Amazon Mechanical Turk. *Judgment and Decision Making*, 5(5), 411-419.

Paolacci, G., & Chandler, J. (2014). Inside the Turk: Understanding Mechanical Turk as a Participant Pool. *Current Directions in Psychological Science*, 23(3), 184-188. doi: 10.1177/0963721414531598

Parsons, C. (2015). "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance". *Media and Communication*, 3(3), 1-11.

PEN America (2013). Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor. New York: PEN American Center.

PEN America (2015). Global Chilling: The Impact of Mass Surveillance on International Writers. New York: PEN American Center.

Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Tech. L.J.*, 31, 117-182.

Pew Research Center. (2014a). Global Opposition to U.S. Surveillance and Drones, But Limited Harm to America's Image.

- Pew Research Center. (2014b). Social Media and the 'Spiral of Silence'.
- Pew Research Center. (2014c). Public Perceptions of Privacy and Security in the Post-Snowden Era.
- Pew Research Center. (2015a). Americans' Privacy Strategies Post-Snowden.
- Pew Research Center. (2015b). Americans' Attitudes About Privacy, Security and Surveillance.
- Rea, L.M. & Parker, R.A. (2014). *Designing and Conducting Survey Research: A Comprehensive Guide*, 4th ed.
- Renas, S. M., Hartmann, C. J., & Walker, J. L. (1989). An Empirical Analysis of the Chilling Effect. In E. E. Dennis & E. M. Noam (Eds.), *The Cost of Libel: Economic and Policy Implications* (pp. 41-68). New York: Columbia University Press.
- Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review*, 126, 1934-1965.
- Ross, J., Irani, L., Silberman, M., Zaldivar, A., & Tomlinson, B. (2010). *Who are the crowdworkers?: Shifting Demographics in Mechanical Turk*. Paper presented at the CHI'10 Extended Abstracts on Human Factors in Computing Systems.
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*: WW Norton & Company.
- Schauer, F. (1978). Fear, Risk, and the First Amendment: Unraveling the 'Chilling Effect'. *Boston University Law Review*, 58, 685-732.
- Seih, Y.-T., Buhrmester, M. D., Lin, Y.-C., Huang, C.-L., & Swann Jr, W. B. (2013). Do People Want to be Flattered or Understood? The Cross-cultural Universality of Self-Verification. *Journal of Experimental Social Psychology*, 49(1), 169-172.
- Seltzer, W. (2010). Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment. *Harvard Journal of Law and Technology*, 24, 171-232.
- Shapiro, D. N., Chandler, J., & Mueller, P. A. (2013). Using Mechanical Turk to Study Clinical Populations. *Clinical Psychological Science*. doi: 10.1177/2167702612469015
- Skinner, Q. (2002). 'A Third Concept of Liberty'. Paper presented at the Proceedings of the British Academy.
- Sklansky, D.A. (2014). Too Much Information: How Not to Think About Privacy and The Fourth Amendment. *Stanford Law Review*, 102(5), 1069-1121.
- Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154, 477-564.
- Solove, D. J. (2007). The First Amendment as Criminal Procedure. *New York University Law Review*, 82, 112.
- Stamatis, D. H. (2003). *Six Sigma and Beyond Statistics and Probability, Volume III*: New York: St Lucie Press.

Steinhauer, J., Delcambre, L. L., Lykke, M., & Ådland, M. (2013). Do User (Browse and Click) Sessions Relate to Their Questions in a Domain-Specific Collection? In T. Aalberg, C. Papatheodorou, M. Dobрева, G. Tsakonas & C. Farrugia (Eds.), *Research and Advanced Technology for Digital Libraries* (Vol. 8092, pp. 96-107): Springer Berlin Heidelberg.

Stoycheff, E. (2016). Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. *Journalism & Mass Communication Quarterly*. doi: 10.1177/1077699016630255

Sullivan, D. (2016). Google Now Handles At Least 2 Trillion Searches Per Year. *Search Engine Land*, <http://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247>

Sung, W. (2016). A Study of Cyberbullying Policies in the Smart Age. *International Journal of Applied Engineering Research*. Vol. 11, No. 2, 1171-1176, http://www.ripublication.com/ijaer16/ijaerv11n2_73.pdf.

Townend, J. (2014). Online chilling effects in England and Wales. *Internet Policy Review*, 3(2). DOI: 10.14763/2014.2.252

Volokh, E. (2016). Challenge to Maryland law banning speech that intentionally seriously distresses minors. *Washington Post (Volkh Conspiracy Blog)*, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/29/challenge-to-maryland-law-banning-speech-that-intentionally-seriously-distresses-minors/?utm_term=.5c491cbf2b39

Waclawski, E. (2012). How I Use It: Survey Monkey. *Occupational Medicine*. Vol. 62, 477, https://www.researchgate.net/profile/Eugene_Waclawski2/publication/230723255_How_I_use_it_Survey_Monkey/links/56c32bec08aeeaf199f8bfec.pdf

Wolfson, S. N., & Bartkus, J. R. (2013). An Assessment of Experiments Run on Amazon's Mechanical Turk. *Mustang Journal of Business and Ethics*, volume 5, 119.

Zacharias, F. C. (1986). Flowcharting the First Amendment. *Cornell L. Rev.*, 72, 936-1024.

Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven Conn.: Yale University Press.

Zureik, E. (2010). (ed.) *Surveillance, Privacy and the Globalization of Personal Information*. Available at: <http://www.mqup.ca/surveillance--privacy--and-the-globalization-of-personal-information-products-9780773537071.php>

APPENDIX 1: SUMMARY OF METHODOLOGICAL LIMITATIONS AND STEPS TAKEN

Methodological limitation	Steps taken to address
Survey design (construct validity / internal validity / reliability)	

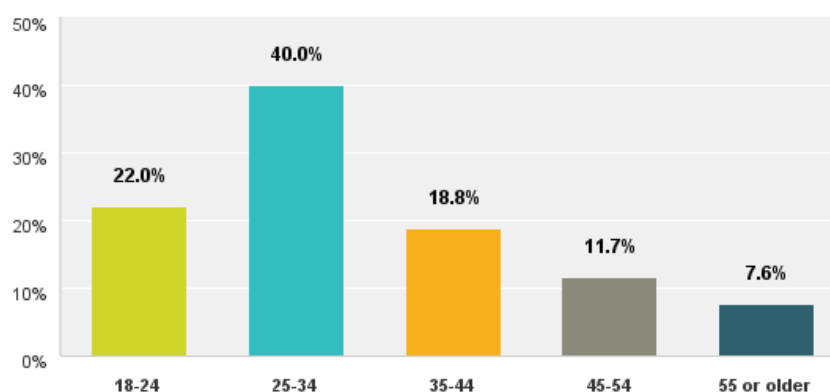
Biased survey design	<p>Survey design tracks successful methodological features of prior leading surveys</p> <p>Extensive field-testing</p> <p>No mention of “chilling effects” or related concepts in survey</p> <p>Neutrally-designed questions 5pt Likert scale design, with multiple response categories for questions</p> <p>To avoid “priming” respondents and biasing responses, demographic questions were posed near the end of the survey, rather than the beginning</p> <p>Survey design primarily based on hypothetical scenarios to measure behavioral response to chilling effects, not self-reports of concern</p>
Self-reports in surveys not always reliable	<p>Using Amazon’s crowdsourcing platform to recruit sample: self-reports by respondents in recruited samples have been shown to be “psychometrically valid” and appear to be “truthful” (Paolacci and Chandler, 2014: 186; Buhrmester, Kwang, and Gosling, 2011)</p>
Validity/accuracy of survey responses	<p>“Attention checks” incorporated into questions</p> <p>Avoids provocative questions and scenarios that may deter respondents from providing honest and accurate answers</p>
Recruitment / Sampling / Data Collection (External validity)	
Representativeness	<p>Recruited sample using online crowdsourcing platform that recruits participant pools that reflect characteristics and demographics of internet user populations in the US better than traditional recruitment methods;</p> <p>Sample collected at different times during days, to capture a wider cross-section of respondents</p>
Self-selection bias	<p>Survey information and description neutrally designed with no mention “chilling effects” or related concepts</p>
Replication	<p>Transparency about rules / protocols / eligibility for recruitment</p>
Procedure / Implementation (internal validity/reliability)	
Validity/accuracy of survey responses	<p>Recruitment restricted to Mechanical Turk users with a 95% approval rating for past tasks</p> <p>Respondents recruited compensated at high end of range for rates paid on similar tasks</p> <p>Incomplete surveys and surveys completed too quickly excluded</p>
Analysis (internal validity/reliability)	
Replication of findings	<p>Created data sets, including all variables and re-coded variables, to allow easy reproduction</p> <p>In-text reporting of relevant statistical values</p>
Accuracy in identifying relationships in data	<p>Used proven statistical tests and statistical software</p>

APPENDIX 2: AGE DISTRIBUTION

The x-axis is the age category and the y-axis is the percentage of the total sample

Q36 What is your age?

Answered: 1,209 Skipped: 3

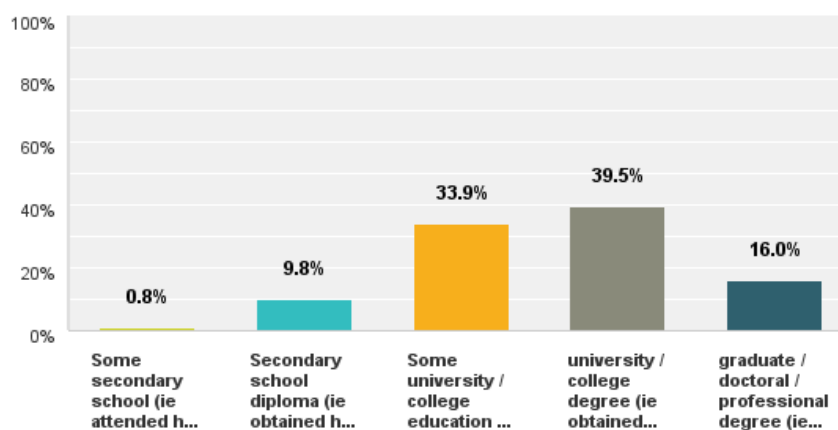


APPENDIX 3: EDUCATION LEVEL DISTRIBUTION

The x-axis is the education level category and the y-axis is the percentage of the total sample

Q39 What is your level of education?

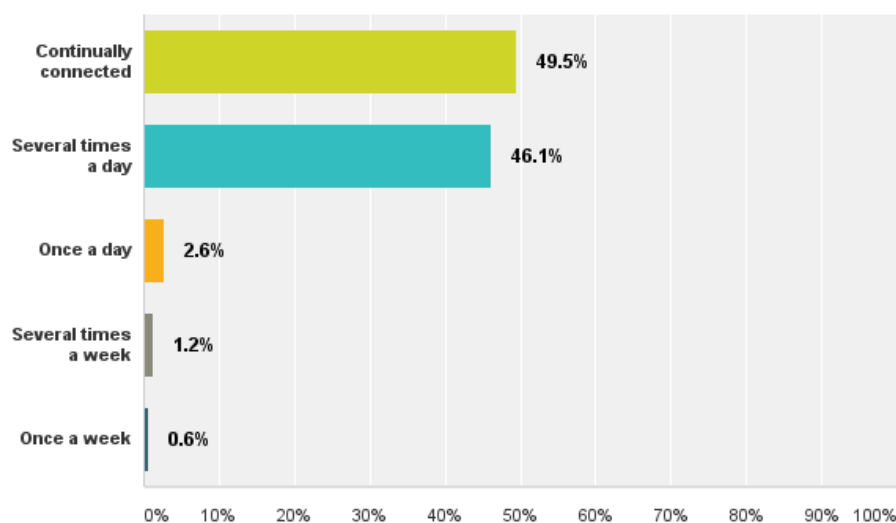
Answered: 1,210 Skipped: 2



APPENDIX 4: LEVEL OF INTERNET USE

Q30 How often do you access the internet?

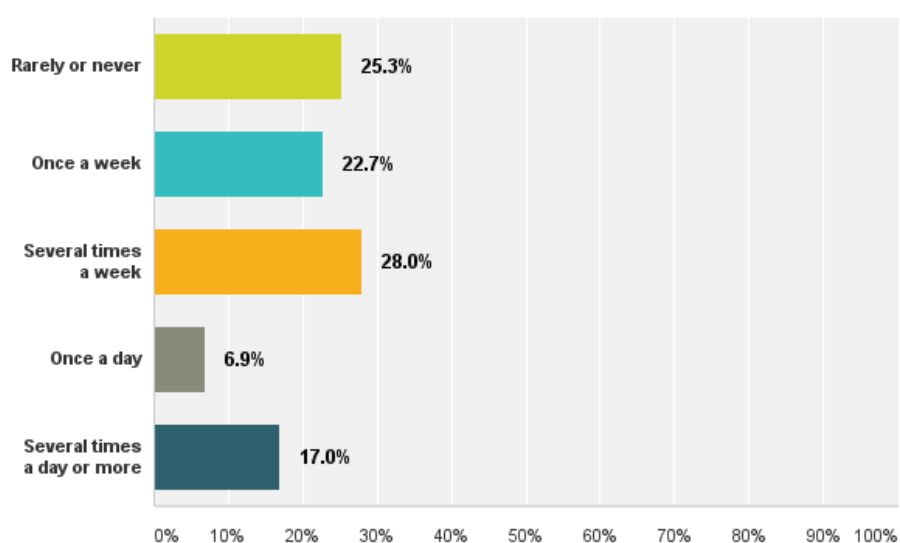
Answered: 1,209 Skipped: 3



APPENDIX 5: SHARING ONLINE

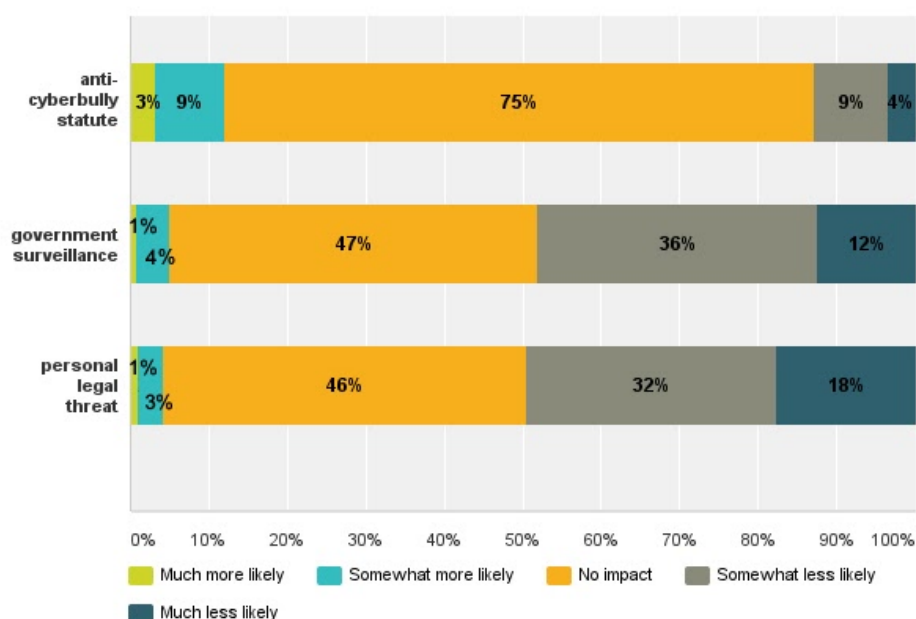
Q33 How often do you share content or post things on the internet more generally? This sharing could be public (e.g., on a blog) or private (e.g., via email).

Answered: 1,209 Skipped: 3



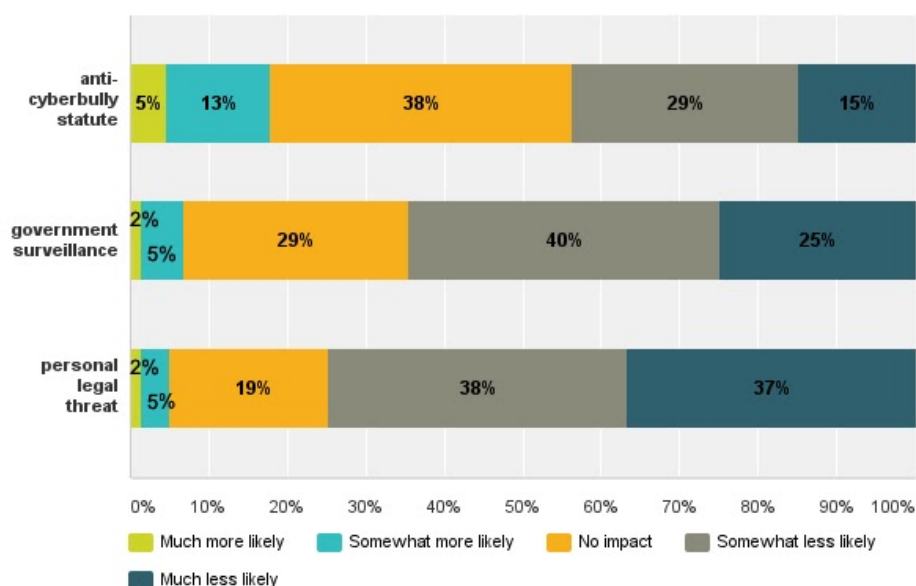
APPENDIX 6: IMPACT ON INTERNET USE

Respondents were asked whether they would be “more likely or less likely to spend time on the Internet” in response to each hypothetical scenario. This chart collates and compares the responses. The cumulative percentage of responses is mapped on the x-axis in relation to the three primary hypothetical “chilling effect” scenarios on the y-axis.



APPENDIX 7: IMPACT ON CONTRIBUTIONS TO ONLINE SOCIAL NETWORKS/COMMUNITIES

Respondents were asked whether they would be “more likely or less likely to contribute to online social networks, communities, and discussion forums” in response to each hypothetical scenario. This chart collates and compares the responses.



APPENDIX 8: ONLINE SURVEY CONSENT FORM

Online Information Study (v2)

Survey Information and Consent

STUDY INFORMATION AND CONFIDENTIALITY
 This is an academic study exploring about how people access information online. The survey should take 10-15 minutes to complete. Participation is voluntary and you can withdraw at any time. However, you must complete the entire survey in order to be compensated. You will not be asked to reveal your personal identity and all responses will be kept entirely confidential. If you have previously completed this survey, please do not do so a second time (the survey software is also designed to prevent this as well).

TO ENSURE COMPENSATION
 As previously indicated, you will be asked at the end of the survey to enter a completion code so you can be compensated. Be sure to make a note of the completion code you enter because you will have to enter it again back at the Amazon's Mechanical Turk site after you complete this survey.

If you have questions or feedback about the study you may contact the principal investigator:

Jon Penney
 Oxford Internet Institute
 University of Oxford
jon.penney@oxi.ox.ac.uk
<http://www.oxi.ox.ac.uk/people/?id=196>
https://twitter.com/jon_penney

=====

1. INFORMED CONSENT AGREEMENT

By selecting the "CONSENT TO PARTICIPATE" option below, you are agreeing to participate in this academic study and acknowledge that:

- I have read the Study and Confidentiality Information above
- I am 18 years of age or older
- I understand written English

☐ CONSENT TO PARTICIPATE
 ☐ DECLINE TO PARTICIPATE

FOOTNOTES

1. Amazon's Mechanical Turk provides an "open" crowdsourcing platform for "task creation," "recruitment," "compensation," and "data collection" (Buhrmester, Kwang, and Gosling, 2011:3). Multiple studies have canvassed Mechanical Turk's advantages for survey, experimental, and other empirical research, with the service has been empirically "validated" as a tool for a broad range of behavioral studies, including conducting "survey research" (Crump et al., 2013: 1-2) as well as research on chilling effects related concepts like privacy and privacy evaluations (Bonetto, 2015; Agir, Calbimonte, & Aberer, 2014; Korshunov et al., 2014; Korshunov et al., 2013; Lin et al., 2012). Indeed, Paolacci and Chandler recently concluded, after extensively canvassing existing research and evidence, that researchers can this platform for "virtually any study that is feasible to conduct online" (2014: 186) with recent studies by Clifford, Jewell, and Waggoner (2016) and Levay, Freese, and Druckman (2016) with similar findings.

2. Though chilling effect research is not extensive, researchers in the related field of privacy studies have found that self-reported responses in surveys do not always reflect actual privacy-related behavior (Harper and Singleton, 2001; Berendt et al., 2005; Acquisti, 2004; 2012; Consolvo et al., 2005; Malheiros et al., 2013; boyd and Hargittai, 2014;); this is due both to the complexity and contextual nature of privacy (Acquisti, 2004) but also bad survey design, where provocative or biased questions elicit biased responses (Harper and Singleton, 2001). Improperly designed or overly abstract hypothetical questions can lead to biased and unreliable responses (Bernheim et al., 2013; Morrison and Brown, 2009; Liljas and Blumenschein, 2000). This case study thus employs questions with "response categories beyond simple yes and no responses", which avoids forcing respondents into unreliable commitments with dichotomous (Morrison and Brown, 2009: 310; Bernheim et al., 2013). Moreover, the scenarios themselves also avoid complexity and abstraction to minimize bias.

3. As of 2016, all US states, except Alaska, have enacted some form of cyberbullying or online harassment specific statutes or laws (Hinduja and Patchin, 2016; Dasgupta, 2016). Such laws have been criticized and opposed on the basis that they criminalize and have a chilling effect on entirely legal internet speech, expression, and other activities online (Volkh, 2016; Buchhandler-Raphael, 2015; Kayyali and O'Brien, 2015; McDonough, 2013; Kaspar, 2012; Hayward, 2011; Brenner and Rehberg, 2010; King, 2010).

4. Under the DMCA, copyright owners can send removal or "takedown notices" (basically copyright based legal claims) to internet users for allegedly copying, posting, or sharing their copyrighted content online (Cobia, 2009; Boyle, 2009: 68; Deibert, 2013: 229-230; Seltzer, 2010).

5. The individual is not personally targeted with a legal threat or notice, but may be "chilled" because someone in their network has been targeted (presumably they feel that they may be next). This scenario is based mainly on social network related studies showing how internet users self-censor based on factors in their online networks like their (perceived) audience (Das and Kramer, 2013) and studies showing a "contagion" or network effect in online social networks and communities, where sentiments (like a chilling effect) can spread through a network (Coviello et al., 2014).

6. Chilling effects and impact are observed but also statistically analysed. See analysis in section 5.

7. SurveyMonkey was used, an online survey design and delivery service that has been “used for surveys in a number of areas including health research” (Waclawski, 2012).

8. A total of 64 survey responses were excluded for being substantially incomplete (defined by ten or more questions left unanswered; many of these were likely false-starts by respondents); another 18 excluded for being completed too quickly, and two more screened because the respondents had completed a version of survey previously (in a field test).

9. Goodman and Kruskal's gamma (γ) test statistic was used to analyse statistically significant associations between categorical ordinal variables, including the effect size (and direction) of any such associations. Chi-square (X^2) and Fisher's exact tests, also common tests of statistical significance for an association between categorical variables, were also employed for additional robustness in analysis, where appropriate, to strengthen findings of statistically significant relationships. Gamma is the preferable core test statistic as it is more sensitive to trends and patterns than chi-square tests and provides a means to demonstrate not only the existence of statistically significant associations between ordinal categorical variables like those found in this study, but also indicate the direction and effect size or strength of any such association: Rea and Parker (2014: 229-230). In fact, in comparing the most common measures of association, Göktaş and Isçi (2008) found, overall, for square tables the gamma test statistic “presents the best estimation of the actual degree of the association in average”. Here, The null hypothesis for each test is that there is no association between the variables analysed. The generally accepted standard or “rule” for chi-square testing was followed, that is, chi-square was not used where any expected frequency (in the contingency table) was less than 1 in any cell nor where the expected values were less than 5 in more than 20% of all cells: Coolican (2013); Cochran (1954). In any such case, variables were recoded to provide sufficient frequencies or Fisher's exact test was instead used to test significance. Gamma is a proportional reduction in error (PRE) statistic, which means it provides a measure of how many fewer errors we might make in predicting the value of one variable by taking into account the values of another. It is an appropriate measure of effect size when using ordinal categorical data (as here) and has an identical values range to r (Less than + or - 0.10: very weak association; + or - 0.10 to 0.19: weak; + or - 0.20 to 0.29: moderate; + or - 0.30 or above: strong) (Ferguson (2009)). Gamma is expressed on a spectrum of -1 to 1, with -1 suggesting a perfect negative association and 1 a perfect positive association; a return of 0 suggests no association between variables at all: Healey (2012: Ch. 12); Stamatis (2003). The gamma test of significance was calculated as significant at the $p < 0.05$ level where $\gamma / ASE = \pm 1.96$ (95 percent confidence) and at the $p < 0.01$ level where $\gamma / ASE = \pm 2.575$ (99 percent confidence): Rea and Parker (2014: 229-230). Results for core test statistics in relation to the three main scenarios are presented in **Table 1**, **Table 2**, and **Table 3**, with more exploratory scenarios analyses set out in **Table 4** and **5**.

10. This study also followed Winter and Suri (2012)'s recommendations for conducting behavioral research ethically and effectively with Mechanical Turk, including normal requirements for informed consent and confidentiality (15-17). Additionally, participants recruited through the service were paid no matter if they completed the survey appropriately or not, and at an hourly rate far higher than the average Mechanical Turk worker rate (paid \$6.67 USD/hour, which is over five times the average rate of pay at the time: \$1.38USD/hour) (Steinhauer et al., 2013; Shapiro et al., 2013; Buhrmester, Kwang, and Gosling, 2011). Beyond legitimate skips, to accommodate any concerns or sensitivities as to the nature of specific questions or topics covered each individual surveyed, respondents were entitled to skip questions. However, the vast majority of respondents answered all questions and most questions usually resulted in only handful of skipped or “missing” values. After agreeing to

participate in the survey, participants were provided with a unique URL to the locate the survey hosted on the SM site and further instructions on how to ensure they would be compensated through entry of a unique 5 digit code obtained at the conclusion of the survey; this technique, used in other surveys, also provided a means to verify survey completion by each participant/user that had taken on the survey task.

11. It was also comparable to participant pools in Ross et al. (2010), Marshall and Shipman (2013), and Carter et al. (2014), skewing slightly younger than the general US population and the internet user population (with the mean age approximately 30 years of age) and was well educated, with 55% of participants possessing university degrees and 88% possessing “some” university education. In short, this sample was “relatively” representative of the US internet user population (the population of interest), but retains the same biases noted in that study and subsequent ones.

12. Similarly, responses to Questions 32 and 34 indicated very nearly half (49.8%) contributed to online networks and related communities at least several times a week, with almost 16% contributing several times a day. Sharing of content respondents “personally created” was less pronounced, with 41.2% of respondents indicating “[r]arely or never” share such content, while 27% sharing such “personally created” content once a week, 21.7% answered “[s]everal times a week”, 4.8% sharing “[o]nce a day” and 5.4% sharing “[s]everal times a day or more”.

13. For this question, respondents could select “any” option that applied; hence, the percentages cited here do not add up to 100%. Not surprisingly, most respondents selected more than one factor being at play in a decision not to take steps to legally challenge the notice in the hypothetical scenario.

14. For the anti-cyberbullying statute (scenario #1), there was a statistically significant and negative association between the age of respondents and their being less likely to discuss certain things online ($\gamma = -0.07$; $X^2 = 37.8$; $df = 16$; $p < 0.05$), share online ($\gamma = -0.07$; $X^2 = 28.5$; $df = 16$; $p < 0.05$), and their being more likely to be careful in their online search activities search online ($\gamma = -0.19$; $X^2 = 48.6$; $df = 16$; $p < 0.01$).

15. For government surveillance (scenario #2), results showed a statistically significant and negative association between the age of respondents and their being less likely to speak online ($\gamma = -0.07$; $X^2 = 36.2$; $df = 16$; $p < 0.05$), share online ($\gamma = -0.08$; $p < 0.05$), and their being more likely to be careful in their online search activities ($\gamma = -0.17$; $X^2 = 41$; $df = 16$; $p < 0.01$).

16. For the personal legal notice (scenario #3), age showed a statistically significant negative association with respondents being more careful and cautious in their online searches ($\gamma = -0.09$; $p < 0.05$).

17. In this scenario, results showed a statistically significant and positive association between being female and, due to receiving a individualised legal threat, being less likely to discuss certain things online ($\gamma = 0.19$; $X^2 = 23.4$; $df = 4$; $p < 0.01$), share online ($\gamma = 0.13$; $X^2 = 14.9$; $df = 4$; $p < 0.01$), and their being more likely to be careful in their online search activities search online ($\gamma = 0.09$; $p < 0.05$).

18. Results showed a statistically significant and negative association between being female and being less likely to share personally created content online ($\gamma = -0.14$; $p < 0.05$).

19. The results showed a statistically significant positive association between being level of awareness of news concerning NSA surveillance and related revelations and chilling effects relating to government surveillance, that is, being less likely to discuss certain things online ($\gamma = 0.12$; $X^2 = 79.3$; $df = 16$; $p < 0.01$), share personally created content online ($\gamma = 0.10$; $X^2 = 32$; $df = 16$; $p < 0.01$), and being more likely to be careful and cautious in online searches ($\gamma = 0.13$; $X^2 = 42.3$; $df = 16$; $p < 0.01$).