Citizens Deserve Privacy Even in the Big Data Age

Contents

Summary

Datasets containing information about individual people should be respected and stored securely, not made more open and liable to abuse. Increasing the availability of Government data where it relates to non-personal areas such as spending, land or legislation may be beneficial to the public, but will suffer from numerous technical difficulties. Individuals, as consumers and citizens, need greater control and access over their data, ideally in the form of property rights which would give them the right to access, correct or delete their personal information. Personal information property rights would balance an individual's privacy with data availability by allowing a person to make their data available more widely if they choose. Businesses who manage or are custodians of a person's data should therefore be required to notify them of any breach, to provide remediation, be subject to heavy penalties and open to civil litigation. Without protecting privacy, the costs of making personal information more available far outweigh the benefits.

About the Author

I am a private individual, born in Australia and university educated. I have had personal information exposed in data breaches, but luckily have not been subject to identity theft or fraud. I deal with small data sets and access, use and generate personal information about clients.

Background

Trust in organisations that manage personal information is justifiably low. A steady stream of news about hacks and data breaches, revelations about government dragnet surveillance and measures to increase that surveillance such as metadata retention have eroded the mutual trust between consumers and business and between citizens and governments. As noted in the issues paper, "individuals frequently do not understand how their personal information is currently being collected and used and, should they find out, may lose trust and stop using services that collect their personal information" (p. 23). In this climate it is counterproductive to seek to increase the availability of data where that data is personal information.

Personal information (or personal data) is defined by the *Privacy Act 1988* (Cth) as "information or an opinion about an identified individual, or an individual who is reasonably identifiable". This means that information may be personal information even when a person's name or other identifying information is not present, so long as they are reasonably identifiable.

Privacy relates to a person's ability to control access to and the use of their personal information. It is a freedom from observation or intrusion and a human right defined by article 17 of the International Covenant on Civil and Political Rights, which is recognised in Australia under the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth). Governments therefore have an obligation not to arbitrarily intrude on people's lives and must make laws to protect their privacy from intrusion. Whenever this review considers the expansion of the availability and use of personal information or data, it represents a threat to human rights.

Privacy Intrusions Are Costly

Privacy intrusions and breaches are extremely costly to individuals, business and society. Individuals suffer emotionally and financially, yet find it difficult to make privacy decisions to manage their risks. Businesses suffer financially and in the damage done to their brand. Society also suffers generally from the denial of privacy as a human right, loss of trust in its structures and chilling effects on free expression that undermine democracy.

Individuals suffer costs from privacy intrusions that are both emotional and financial. When they are victims of data breaches they may suffer emotionally (Stark, 2016) and financially through identity theft or the stress of civil litigation (Romanosky, Hoffman, & Acquisti, 2014; Romanosky, Telang, & Acquisti, 2011). One of the major risks of being a victim of a data breach is identity theft which has been estimated to affect approximately 9% of Australians within the last 12 months and one in five Australians during their lifetime (Smith & Hutchings, 2014). Although half of those victims are reimbursed in full, the other half suffer losses with a median of A$247, although a minority suffer much greater losses resulting in mean losses of over A$4,000.

Unfortunately, individual decision-making processes around privacy are far from simple and rational. For example, the methodology used to assess an individual's privacy pricing heavily influences the price that an individual would be willing to accept or to pay (Acquisti, John, & Loewenstein, 2013). Attitudinal surveys find that individuals have a strong belief in the importance of privacy, yet this frequently does not translate into privacy-enhancing

behaviours (Acquisti, Brandimarte, & Loewenstein, 2015). However, privacy-seeking is an instinctive human behaviour that has been demonstrated across cultures. More recently, data reviewed by Acquisti et al. (2015) shows that as people have become more aware of online data practices rates of disclosure on social media has decreased – in 2005 approximately 90% of college students disclosed their birthday and high school on social media profiles, but in 2011 this was less than 20% and 40% respectively.

Individual privacy decision-making is extremely difficult because it involves dealing with unknown risk and invisible processes. As noted previously, the issues paper acknowledges that individuals do not understand current practices of data collection and use and so cannot be expected to make rational decisions. Many privacy questions require a fairly high level of understanding of both technical information technology and legal issues – for example, is an individual's privacy better protected by using unsecured SMS or by a third-party instant messenger? In the first case, the individual needs to evaluate the data retention policy of their telecommunications provider because their message is transmitted in plaintext and the privacy risks associated with Australia's two-year metadata retention scheme. In the second, message content may or may not be protected by an encryption protocol which may or may not be open source and metadata may be logged for an indefinite period by a private company.

Cognitive biases also play a role, as demonstrated by Brandimarte, Acquisti, and Loewenstein (2013) who found that when individuals had a perception of control they disclosed more, thus increasing their privacy risks. Further, according Acquisti et al. (2015), many privacy decisions are frequently influenced by contextual cues rather than rational processes. It is therefore exceedingly difficult for individuals to make rational cost-benefit based privacy decisions because they are not usually in a position to understand either side of the cost-benefit equation.

Businesses also incur costs from data breaches, but these are lower than for individuals. According to the Ponemon Institute (2015b), the global average cost of a data breach is US$3.5 million and in Australia, the average cost per record lost is A$144 with an average breach size of almost 20,000 records (Ponemon Institute, 2015a). Breaches also affect market capitalisation, with an average loss of 2% of market value over the two days following a data breach announcement (Cavusoglu, Mishra, & Raghunathan, 2004), demonstrating the negative perceptions of investors. However, these losses represent only short-term market volatility and the cost of a lost record ($A144) is less than what an individual subject to misuse of their personal information and who is not reimbursed is likely to lose (>A$247).

The cost of privacy intrusions to society generally is intangible, but no less important. The collection, retention and use of large sets of personal information or data is effectively surveillance and triggers self-censorship. Government-sponsored mass surveillance produces a chilling effect on free expression as citizens self-censor for fear of retribution (Bauman et al., 2014; Hughes, 2012). Writers in countries considered 'free' now have similar levels of concern about surveillance as writers in countries that are not considered free (75-80%) and a third of writers have self-censored because of mass surveillance (PEN America, 2015). When people are made aware of surveillance, they become less likely to speak out, especially if they perceive their opinion to not be in agreement with the majority (Stoycheff, 2016). Thus public trust and the robustness of democracy is degraded by intrusions into privacy.

Personal Data Protection Suffers from Market Failure

The disparity between the costs suffered by a business and the potential costs to individuals from data breaches and the misuse of personal information creates an externality where the privacy costs associated with businesses are not priced into their products and are paid for by society. Businesses, rather than individuals, experience benefits from the use of large sets of personal data and information. The issues paper highlights the expansion of Australia's credit reporting regime and its supposed "gains to individual borrowers", but neglects the dual use potential of larger datasets (p. 17). For individuals, the efficient pricing of credit may mean that credit is more or less expensive and so they may or may not benefit. The only clear beneficiaries are credit reporting agencies who can expand their product offerings and lenders who may benefit from expanding and segmenting their customer-base.

The rewards available to business for exploiting data and the low costs of associated with failing to protect it, have meant that an individual's data is unlikely to be well protected. The Privacy Rights Clearing House (http://www.privacyrights.org) has accumulated a searchable online database which shows that from 2010 to 2015 there were over 3000 breaches, covering nearly 400 million records in the United States. In Australia, malicious actors account for only a minority of breaches, with 30% involving a negligent employee or contractor and 30% involving system glitches (Ponemon Institute, 2015a). It is clear that organisations are taking insufficient care with the personal data that is entrusted to them and cannot be trusted to protect data as malicious actors increase the frequency and sophistication of hacking attempts.

Open Non-Personal Data is Beneficial

What public sector datasets should be considered high-value data to the: business sector; research sector; academics; or the broader community?

Public datasets which are not personal data will be beneficial to the community. The issues paper has noted that public sector data on public spending, legislation and the environment is not as open as it is in the United Kingdom (p. 13). As a member of the broader community, I am interested in this information being more publicly available.

What benefits would the community derive from increasing the availability and use of public sector data?

Information about government activities is fundamental to democracy. Increasing the availability of non-personal data on public sector spending, legislation and environment would enhance the ability of citizens to understand their government's actions and to make up their minds about which policies they do and do not support.

What are the main factors currently stopping government agencies from making their data available?

I hope that privacy legislation continues to stop government agencies from making personal information or data available to others. Collection of personal information by government agencies involves consent that is usually spurious (i.e. consent is required to interact with the service and interaction is necessary to function normally).

Should the collection, sharing and release of public sector data be standardised?

This seems unlikely for technical reasons. Even the issues paper, a text document, was released in two formats (Word and PDF). Standardising data is notoriously difficult. Attempts to create standards are often derided as just producing an additional standard.

Which datasets, if linked or coordinated across public sector agencies, would be of high value to the community, and how would they be used?

This question, as it relates to personal information or data, would be a serious threat to privacy. Linking datasets inherently involves identification. As noted earlier, personal information according to the *Privacy Act 1988* (Cth) is defined as information where a person is identified or reasonably identifiable. Therefore, if data can be linked, it is identified and its release should not occur.

What are the reasonable concerns that businesses have about increasing the availability of their data?

Businesses increasing the availability of their data creates competitive, privacy, security and legal risks. Apart from potentially benefitting competitors, additional methods of accessing data that was not previously available creates new avenues for malicious actors or negligent organisations to breach the personal information or data of their employees or clients. As noted previously, system glitches and employee or contractor neglect account for approximately 60% of data breaches in Australia (Ponemon Institute, 2015a) and this would create additional reputational risks and the possibility of litigation. Any increase in the

sharing of data would have to come with careful implementation and hardening of network infrastructure to prevent this from occurring.

Who should have the ownership rights to data that is generated by individuals but collected by businesses? For which data does unclear ownership inhibit its availability and use?

Individuals should have a high degree of ownership rights to data that is about them but collected by business. As noted in the issues paper, data can sometimes be considered the property of both the individual to whom it relates, and the business which collects it (p. 6). Both the individual and the business have clear interests in owning the data.

There are ethical problems with businesses having complete ownership of the data that they collect about individuals. As Sax (2016) has identified, big data companies often operate using a set of "finders keepers" ethical assumptions, where the data they collect is solely theirs to exploit and to benefit from, regardless of whether there are other stakeholders who might have an interest. Ethical and privacy concerns also exist within the field of computer science, where researchers are trying to develop privacy-preserving data mining techniques (Matwin, 2012).

Individuals should therefore have property rights to the data about them that is collected by businesses and businesses should be able to benefit from the use of that data under revocable *licensing* arrangements. This would enhance the availability and use of that data by giving individuals the right to have access to and analyse data that is about themselves or license its use to other organisations. The Hub of All Things (http://hubofallthings.com) is an example of a project intended to empower individuals to access, use, analyse and exchange their own data. Projects like the Hub of All Things would benefit from giving individuals property rights to their personal information and data.

Individuals Need Access and Control Over Their Data

What impediments currently restrict consumers' access to and use of public and private sector data about themselves? Is there scope to streamline individuals' access to such data and, if there is, how should this be achieved?

Individuals are impeded in their access to and control over data by a lack of knowledge and understanding that the data exists, their rights, access procedures and ease of access. As noted by the issues paper, individuals often do not understand how their information is collected, stored and used (p. 23). Data collection is often invisible by design and requires specialised tools to detect and visualise. For example, Mozilla Firefox users can use the Lightbeam add-on to visualise the third-party tracking cookies that are placed on their computer by advertisers while they browse the internet. Other tracking technology, such as web beacons and browser fingerprinting are even more insidious, tracking users based on technical aspects of their browser and device.

Once an individual learns about the data that exists about them, they may or may not have the knowledge or understanding of the procedures that they need to use to access it. Data access usually involves making formal requests under privacy legislation, which most individuals are unlikely to have ever done. In the case of data collected online, jurisdiction presents an additional barrier as an organisation which is collecting data may be located in another country.

To streamline individuals' access to data, individuals should be notified that data exists about them (for example, notified that a credit reporting agency has opened a file on them) and informed on how to access that data. Making data more readily accessible via online processes would streamline this, but may also enhance the risk of unauthorised access.

Are regulatory solutions of value in giving consumers more access to and control over their own data?

Yes, regulatory solutions like granting property rights to individuals regarding their data would give a guarantee that individuals have access to and control over their own data or data property.

Privacy and Security Concerns are Often Inadequately Addressed

What types of data and data applications (public sector and private sector) pose the greatest concerns for privacy protection?

All sufficiently rich data about a person or their behaviour poses a potential privacy risk, but data about an individual's health, welfare or financial situation is particularly concerning. For example, the Australian Bureau of Statistics has decided that the 2016 Census of Population and Housing will retain names and addresses for data linkage. This is intrusive to privacy because sufficiently rich datasets are difficult to anonymise. Re-identification has been shown to be possible many times in the academic literature, for example, by de Montjoye, Radaelli, Singh, and Pentland (2015) who showed that just four spatiotemporal points are required to re-identify 90% of credit card metadata records. Any release of unit-level data about health, financial transactions or enriched census information has the potential to be identifiable. As noted by the Office of the Australian Information Commissioner's (2014) guidelines on de-identification, de-identification is not as simple as deleting names and addresses. Other techniques such as modifying data or generating synthetic data are necessary to truly de-identify personal information or data.

How can individuals' and businesses' confidence and trust in the way data is used be maintained and enhanced?

As outlined previously, organisations do not deserve confidence or trust in the way they handle data. The difficulty of making good privacy decisions, combined with the perverse economics of the costs of data protection and the costs of data breaches have resulted in frequent and massive data breaches.

Confidence and trust in the way data is used can be enhanced in the following ways:

1. Mandatory data breach notifications and remedial actions
2. Heavy penalties for organisations that are subject to data breaches
3. A privacy tort that would give individuals grounds for civil litigation

Unlike other developed nations, Australia does not have mandatory data breach notification laws. While successive governments have planned data breach notification laws, they have not actually passed the legislation. Additionally, data breach notification must be accompanied by remedial action, funded by the organisation which was breached. It has been shown that data breach notifications reduce identity theft caused by these breaches by 6% (Romanosky et al., 2011) and that providing free credit monitoring with these notifications reduces the odds of being sued by six times (Romanosky et al., 2014). To enhance trust, breached organisations must be legally obliged to provide a breach notification and remedial action such as credit monitoring or replacing leaked identification documents.

Due to the market failure in the protection of personal information or data, heavy penalties are required to correct organisational approaches to IT security. For example, Telstra was fined just $10,200 for a breach involving 15,775 customers in 2014 – a fine of just 65c per customer (ABC News, 2014). Heavier penalties are clearly needed to deter negligent IT security practices that lead to the majority of Australian data breaches, let alone to promote the hardening of network security that will stop malicious actors.

A privacy tort would also give individuals grounds to sue for serious invasions of privacy. As the Australian Privacy Foundation (2015) has argued, a privacy tort would close a gap in the law, allowing individuals to sue for the invasion of their privacy and for damages to be awarded according to the scope and nature of the breach.

Trust can be restored and enhanced by regulating to end the market failure that results in poor information security through mandatory data breach notification, remediation and penalties.

What weight should be given to privacy protection relative to the benefits of greater data availability and use, particularly given the rate of change in the capabilities of technology?

A heavy weighting should be given to privacy protection relative to greater data availability and use. As previously discussed, privacy is a human right and in supposedly free Western democracies, we should not discard human rights simply for economic gain. In fact, protecting privacy increases public trust and emboldens individuals to disclose information about themselves (Acquisti et al., 2015). It is under conditions where large datasets are used for surveillance, especially where that surveillance does not appear justified, that failure to respect privacy leads to a reduction in disclosure and other privacy-protective behaviour such as identity-masking and therefore a reduction in the value of datasets (Chen, Beaudoin, & Hong, 2016; Stoycheff, 2016).

What are the benefits and costs of allowing an individual to request deletion of personal information about themselves? In what circumstances and for what types of information should this apply?

There is a clear privacy benefit in allowing individuals to request deletion of their personal information or data. Since most data is collected and stored electronically, its deletion, or at least the scheduling of deletion, should be built into the system and with minimal associated costs. Deletion is a feature of most social networking and other online accounts. Individuals expect to be able to delete their data from online services and it is a principle of all privacy legislation that organisations retain information only for as long as necessary or as required by law. Deletion also frees up data storage infrastructure from keeping information on inactive or unwanted accounts and so could actually reduce costs or enhance the quality of datasets while simultaneously providing privacy benefits.

Individuals should be able to request deletion of all of their personal information or data. Where that information must be kept because it forms part of a business record or is necessary for the provision of government services, deletion should be scheduled for action. For example, a recruitment agency may need to retain information on a candidate for a period of up to year in case they require the same psychometric evaluations for another job position, but the individual should be able to schedule their information to be deleted once that time period has elapsed.

This would interact well with privacy property rights, where personal information or data is owned by the individual but licensed to an organisation. In these cases, minimum licensing arrangements may apply, but individuals should be able to revoke the license granted to an organisation by deleting their data or scheduling data for deletion after the minimum licensing or retention period.

What competing interests (such as the public interest) or practical requirements would indicate that the ability to request deletion should not apply?

Competing interests such as other human rights or the public interest should limit or prevent deletion requests from applying. I am not arguing for the "right to be forgotten" as is being established in Europe. Where an individual's privacy property rights conflict with another's right to free expression, it may be a situation where a right to deletion should not apply. For example, individuals should not have the right to request deletion of media articles about themselves apart from current legal processes involving defamation and libel.

The right to delete (or schedule deletion) should apply to personal information or data that is collected by organisations such as customer records, behavioural profiling, recruitment information, health or financial information. Information that may be of commercial value but does not have a public interest value, should be subject to deletion after appropriate business record-keeping and statutory record-keeping requirements have been met.

Are security measures for public sector data too prescriptive? Do they need to be more flexible to adapt to changing circumstances and technologies?

Given the breach to the Bureau of Meteorology in 2015, it seems that security measures for public sector data are inadequate, not necessarily too prescriptive.

How should the risks and consequences of public sector and private sector data breaches be assessed and managed? Is data breach notification an appropriate and sufficient response?

The risks of public and private sector data breaches can be managed first by accepting their existence and prioritising them appropriately. As noted by the issues paper, the Office of the Australian Information Commissioner received 110 voluntary breach notifications in 2014-15. If these breaches were the average of 19,788 records reported by the Ponemon Institute (2015b), that would mean that in one year over 2 million records were breached. The risks are therefore very high that data breaches will occur and affect a substantial number of people.

Public and private sector data breaches can then be managed by integrating security into every level of data collection and storage. Networks which are secure-by-design are likely to use well-validated authentication and encryption methods to protect data. In these systems, the minimum amount of data necessary is collected and it is not retained for longer than needed, which is also a requirement of Australian privacy legislation. It is assumed that users will make errors and so the security of the system is made as robust as possible to user error (e.g. clicking on a phishing link from an email).

Data breach notification is an appropriate, but not sufficient response. Data breach notifications have not stemmed the tide of data breaches, which involves tens millions of records a year in the United States alone. Notifications only have a small effect on mitigating the risk of identity theft (Romanosky et al., 2011). A sufficient response would include providing mitigation services to affected individuals, including free credit monitoring and the replacement of affected identification documents. For example, if a telecommunications provider suffers a data breach which exposes contact information and drivers licence numbers, it is appropriate for its customers to receive a breach notification, a period of free credit monitoring and a voucher to pay for a new licence being issued. The breached organisation should also be subject to a fine, based on the nature and size of the breach.

Conclusions

The aim of increasing data availability and use when it applies to information about people is a serious threat to the human right to privacy. The rich datasets available to big data enterprises can too easily allow individuals to be identified (de Montjoye et al., 2015). As such, a massive increase in data availability would likely be an equally massive breach of personal information and privacy.

The conclusions of this submission are therefore:

1. Increasing the availability and use of data that is not personal information or data is relatively unproblematic and of benefit to the public, particularly in areas where data availability is low such as government spending, legislation or environment

2. Privacy legislation and privacy as a human right should continue to restrict the availability of both public and private sector datasets containing personal information or data

3. Individuals should be notified when third party businesses (such as credit reporting agencies) begin collecting data about them and informed on how they can access that data

4. Individuals should have a privacy property right to data that is about them but collected by businesses that gives them the right to revocably license the use of their data to others

5. Individuals should have the right to delete data that has commercial but no public interest value or, where that data must be retained as part of business records or for statutory reasons, to schedule that data for deletion

6. Public and private sector organisations should be required to provide mandatory data breach notifications, regardless of their size

7. Public and private sector organisations should be required to provide remediation in the event of a data breach, including free credit monitoring and replacement of identity documents

8. Public and private sector organisations should be subject to fines when a data breach occurs, in order to address the market failures associated with privacy externalities

9. Privacy rules should be strengthened by enacting a privacy tort to allow individuals to sue for serious breaches of privacy and the amount of damages scaled according to the breach

References

ABC News. (2014). Telstra fined after breaching privacy of 15,775 customers. *ABC News*. Retrieved from http://www.abc.net.au/news/2014-03-11/telstra-breaches-privacy-of-15775-customers/5312256

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*, 509-514. doi:10.1126/science.aaa1465

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*, 249-274. doi:10.1086/671754

Australian Privacy Foundation. (2015). *Privacy tort: Submission to the NSW parliamentary inquiry*. Sydney: Australian Privacy Foundation. https://www.privacy.org.au/Papers/NSWParlt-Tort-151215.pdf

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*, 121-144. doi:10.1111/ips.12048

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*, 340-347. doi:10.1177/1948550612455931

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*, 70-104. doi:10.1080/10864415.2004.11044320

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly, Advance Online Publication*. doi:10.1177/1077699016640224

de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science, 347*, 536-539. doi:10.1126/science.1256297

Hughes, S. S. (2012). Us domestic surveillance after 9/11: An analysis of the chilling effect on first amendment rights in cases filed against the terrorist surveillance program. *Canadian Journal of Law and Society, 27*, 399-425. doi:10.1353/jls.2012.0030

Matwin, S. (2012). Privacy-preserving data mining techniques: Survey and challenges. In B. Custers, T. Calders, B. Schermer, & T. Zarsky (Eds.), *Discrimination and privacy in the information society: Data mining and profiling in large databases* (pp. 209-221). Berlin/Heidelberg: Springer.

Office of the Australian Information Commissioner. (2014). Privacy business resource 4: De-identification of data and information. https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information

PEN America. (2015). *Global chilling: The impact of mass surveillance on international writers*. New York: PEN American Center. http://www.pen.org/global-chill

Ponemon Institute. (2015a). *2015 cost of data breach study: Australia*. New York: IBM. http://www-03.ibm.com/security/data-breach/

Ponemon Institute. (2015b). *2015 cost of data breach study: Global analysis*. New York: IBM. http://www-03.ibm.com/security/data-breach/

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*, 74-104. doi:10.1111/jels.12035

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*, 256-286. doi:10.1002/pam.20567

Sax, M. (2016). Big data: Finders keepers, losers weepers? *Ethics and Information Technology*, 1-7. doi:10.1007/s10676-016-9394-0

Smith, R. G., & Hutchings, A. (2014). *Identity crime and misuse in australia: Results of the 2013 online survey*. Canberra: Australian Institute of Criminology.

Stark, L. (2016). The emotional context of information privacy. *The Information Society, 32*, 14-27. doi:10.1080/01972243.2015.1107167

Stoycheff, E. (2016). Under surveillance: Examining facebook's spiral of silence effects in the wake of nsa internet monitoring. *Journalism & Mass Communication Quarterly, Advance Online Publication*. doi:10.1177/1077699016630255