Cryptic journalism: news reporting of encryption

Einar Thorsen
School of Journalism, English and Communication
Bournemouth University
United Kingdom

ethorsen@bournemouth.ac.uk
ORCID http://orcid.org/0000-0002-7126-7293

This is an Accepted Manuscript of an article published by Taylor & Francis in *Digital Journalism* on 19/10/2016, available online: http://www.tandfonline.com/10.1080/21670811.2016.1243452

Abstract

In light of Edward Snowden's global surveillance disclosures, this article examines news discourses about online communication security and surveillance circumvention practices. It analyses 1,249 news reports mentioning encryption in *The Guardian* and *The New York Times*, covering a 3-year period from June 2012 to June 2015 (one year before and two years after the Snowden revelations). Whilst there was a marked increase in volume of news articles mentioning encryption post-Snowden, the context in which encryption is discussed has since shifted from an initial emphasis on "surveillance" towards "security" issues. However, the research found that greater news coverage of encryption did not necessarily mean an increase in *depth* of coverage, with most mentions of encryption vague and non-descript. In terms of source usage, the research finds an emphasis on private corporations in both publications analysed. This is problematic when many of the organisations allowed to speak on encryption were those accused of colluding with the US and UK Governments to aid covert mass surveillance - the likes of Google, Facebook, Apple, Microsoft and so forth - thus providing them with a platform to exonerate themselves from the accusations. This contradictory depiction of communication security serves the status quo and prevents advancement of the "encrypted by default" communication practice called for by Snowden. This, by extension, has serious implications for both journalistic freedom and civil liberties since it helps to perpetuate the ability of nation states and corporations to conduct indiscriminate mass surveillance.

Key words

encryption, cybersecurity, source protection, surveillance, Snowden, NSA, GCHQ

Introduction

Classified information leaked by whistleblower Edward Snowden in 2013 exposed indiscriminate mass surveillance by the NSA and GCHQ, targeting *all* citizens' communications as opposed to merely those under suspicion or investigation. This sparked global outcry and fuelled renewed attention to how citizens might protect themselves from privacy intrusion. According to Snowden, the global surveillance disclosures provided "irrefutable evidence that unencrypted communications on the internet are no longer safe", and therefore in his view, "Any communications should be encrypted by default" (Snowden, cited in *The Guardian*, 17 July 2014). This was particularly pertinent, he argued, for anyone who has a professional duty of confidentiality (such as "journalists, lawyers, doctors, investigators, possibly even accountants"). Snowden stressed the urgency of training and agreed standards about encryption, "to make sure that we have mechanisms to ensure that the average member of our society can have a reasonable measure of faith in the skills of all the members of these professions" (ibid). Singling out one profession in particular, Snowden highlighted how the work of journalists and need for source protection "has become immeasurably harder than it ever has been in the past" due to "these new surveillance technologies":

> "Journalists have to be particularly conscious about any sort of network signalling, any sort of connection, any sort of licence-plate reading device that they pass on their way to a meeting point, any place they use their credit card, any place they take their phone, any email contact they have with the source because that very first contact, before encrypted communications are established, is enough to give it all away." (ibid)

Mass surveillance, in other words, undermines journalists' ability to effectively do their work (Thorsen, 2017). Government agencies have even used the existence of digital communications as a means to collect information about journalists and their sources, by obtaining search warrants for personal emails and phone records (Taylor 2015). Lack of knowledge about how to integrate preventative measures such as encryption into everyday routinised news work is a considerable challenge - as highlighted in Henrichsen et al's (2015) international survey of journalists published by UNESCO; in Kleberg's (2015) report on digital source protection; in Bradshaw's (2015) study of UK regional journalists' source protection and information security; and in Lashmar's (2016) interviews with journalists from countries of the Five Eyes intelligence alliance (Australia, Canada, New Zealand, UK and US).

Such uncertainty is echoed in news reporting *about* surveillance, and specifically concerning the methods of *surveillance circumvention*. Tools that help evade detection or scrutiny remain clouded in mystery, associated with clandestine operations, criminal activities, or security threats. To provide systematic evidence of how such a discourse is constructed, this article examines news articles about online communication security and surveillance circumvention practices. It analyses 1,249 news reports that mentions encryption and related terms in *The Guardian* and *The New York Times*, covering a 3-year

period from June 2012 to June 2015 (one year before and two years after the Snowden revelations). Through a thematic overview of how communication security techniques are reported, the research documents what types of events trigger such considerations, what is purportedly at stake when it is reported, and who is advantaged by it.

Secrecy, risk and resistance

Since varying definitions of intelligence services places secrecy at its core, Hillebrand (2012) argues that "their work do not fit comfortably into a democratic framework and clash with the basic requirements of openness and participation" (2012, 691). Because the intelligence apparatus seems to operate on the edges of, or even in opposition to, such values, democratic societies end up finding creative ways to accommodate both. Being part of the state apparatus assumes a degree of accountability, whilst "at the same time, the intelligence sector is typically granted considerable exemptions from regulations, such as freedom of information policies" (ibid). Central to both Snowden and Manning's revelations is a recurring concern that *secrecy* is in fact an operational mechanism designed to protect established forms of power (see Hintz et al 2017; Thorsen et al 2013). Snowden poignantly proclaiming that: "If we can't understand the policies and the programs of our government, we cannot grant our consent." (Snowden's Sam Adams Award speech, 11 October 2013). This echoes Manuel Castell's assessment of power in contemporary society, where he notes that "if we do not know the forms of power in the network society, we cannot neutralize the unjust exercise of power" (Castells 2009, 431). In such an environment, competing assertions about what constitutes whistleblowing, for example, is a constant source of tension - especially where it undermines established forms of power. Indeed Snowden himself makes a similar point, and contends that we are witnessing a "temporal compression" that dramatically reduces "the time frame in which unconstitutional activities can continue before they are exposed by acts of conscience" (Snowden 2016, xi). This, he argues, "empowers an informed citizenry to defend the democracy that 'state secrets' are nominally intended to support" (2016, xii).

Bakir and McStay (2016, 36) follows a similar logic, noting that "Post-Snowden the surveillant state appears to be moving from a position of forced transparency towards one of radical translucency". The former suggests a situation of "maximal visibility of all citizens […] but without their knowledge or consent", while the latter "advocates the opening up of both public and private processes for the general good, but with socially or legally agreed limits to the extent of oversight of the surveillant entity and the extent of citizens' visibility" (Bakir and McStay 2016, 27, 35–36). That is, the global surveillance disclosures have contributed to increased awareness about signal intelligence powers, and by extension attempts at curtailing and legally defining (thus rendering visible) those powers. This also goes beyond state power, as the corporations named in Snowden's global surveillance disclosures adopt radical translucency by identifying "commercial opportunities in privacy":

> "as they simultaneously enforce the privacy of their customers (in regard to state surveillance) yet seek to make extensive use of non-personally identifiable data (for

commercial ends). Critically, opacity decisions are primarily being made by corporations rather than citizens." (Bakir and McStay 2016, 36)

This interoperability of state and private interests, and indeed use of secrecy for their preferment, dramatically complicates efforts to hold these powers to account. Accountability is increasingly interchanged with and even "operationalized as transparency", whereby transparency is "supposed to *generate* accountability" (Christensen and Cheney 2015, 71). Yet, as Christensen and Cheney point out, this convulsion is deeply flawed since citizens lack both interest in (unless there are demonstrable suspicions about wrongdoing) and understanding of how to interpret transparency disclosures. Citizens are subsequently dependent on "intermediaries" – journalists, community representatives, political pundits and so forth - that help make sense of and contextualise information attained through transparency.

Barnard-Wills (2011), meanwhile, argues that "surveillance is an active concept in news discourse" and as such "news media [is] a useful starting point for mapping wider discursive assemblages of surveillance" (Barnard-Wills 2011, 550). In his examination of UK newspapers, he identified two different evaluating schemas in which to position the various frames identified: firstly, "a discourse of appropriate surveillance, which mobilizes discourses of crime, terrorism, and national security" and secondly "a discourse of inappropriate surveillance, mobilizes discourses of privacy, Big Brother, and personal liberty" (Barnard-Wills 2011, 554). Lischka (2015) identified a similar pattern in relation to surveillance discourse in UK broadcasters post-Snowden, with surveillance encapsulated by the major themes of terrorism versus privacy. News media's legitimisation of mass surveillance, under the guise of preventing terrorist attacks, stemmed largely from political and government sources who predominantly used "authorisation and rationalisation strategies" (Lischka 2015, 16). Delegitimisation strategies are limited to challenging surveillance *practices* rather than challenging surveillance in general. Moreover, sources whose utterances aid framing of the delegitimisation of surveillance, tend to vary for each case. Oppositional voices *are not* given a voice by default, as is the case for government, pro-surveillance actors (Lischka 2015, 17). Moreover, media representations are often steeped in "myths", designed to normalise "a certain organization of life and discourse in modern societies", stemming from "the intense concentration of symbolic power" yielded by "centralized media institutions" (Couldy 2015, 609). To this end, Couldry warns that "we need to be cautious about the specific contribution to political explanation of the rhetorics associated with large-scale media institutions" (Couldry 2015, 614), particularly in a context of permanent surveillance.

Indeed, as Munro (2015) rightly points out, organisations such as WikiLeaks have been able to develop a form of resistance to State and corporate power due in large parts to its 'deterritorialisation'. In so doing, it has sought to inverse "existing hegemonic systems of surveillance" by creating "its own anti-secrecy havens" (Munro 2015, 2). This has been met with fierce attempts by States at re-exerting control, through 'reterritorialisation' by both legal and 'extra-judicial' means. Indeed WikiLeaks is not just challenging established form

of power, but also reversing the operational mechanisms of power - supporting “privacy for the weak and transparency of the powerful” (Munro 2015, 15). These anti-secrecy havens are operationalised through communication security and encryption which effectively ensure vectors of deterritorialisation, to borrow Munro’s term, and are able to circumvent state and private surveillance efforts.

Mass use of encryption is important to aid the effectiveness of surveillance circumvention, a logic referred to by Penney (2013) as the “economics of privacy and mass surveillance”. While he argues "there are very few ways to avoid compromise in the face of an advanced persistent threat”, such as the NSA or GCHQ, "for the vast majority of Internet users, incorporating basic security measures and encryption use can ensure privacy and security even today” (Penney 2013, 747–748). Increasing both the volume and complexity of messages intelligence or spy agencies have to decipher makes surveillance more expensive, and "the more costly the surveillance is for the watchers, the safer regular users will be from mass forms of surveillance” (Penney 2013, 749). This is particularly important since selective use of encryption may attract unwanted attention to the communication that it is designed to protect. The danger here is that if communication security is occasionally used by a journalist, for example, they may inadvertently draw attention to themselves and put a source at risk - especially where the metadata is not protected (Kleberg 2015, 5-6). Penney's (2013) deduction about mass encryption is posited in part to combat this very problem, since cloaking every piece of communication would avoid singling out for eavesdropping only that which is sensitive.

In light of such deeply contested spaces, this study seeks to understand how news media report on surveillance circumvention technologies and practices. That is, to what extent are discourses specific to encryption reflecting the dichotomous tensions exhibited in news reporting about surveillance generally, and how does this shape our understanding of and potential for adopting measures to circumvent private and state intelligence intrusion?

Sample and methodology

This article draws on an analysis of online news reporting mentioning encryption in *The Guardian* and *the New York Times* over a three-year period, due to their direct involvement in the Snowden global surveillance disclosures. *The Guardian* was the primary partner for Snowden and devoted significant resource to publishing details from the data it had obtained[1]. In August 2013 it formally partnered with *the New York Times* to ensure it could continue to publish materials from the Snowden leak, as a direct consequence of a “climate of intense pressure from the UK government” (Official statement, *The Guardian*, 23 August 2013). Both these newspapers have a prior track record for collaborating on highly sensitive material, notably publishing the US military and diplomatic cables released by WikiLeaks (Brevini et al. 2013).

Given *The Guardian* and *the New York Times*' extensive involvement in publishing classified material from whistleblowers and the communication security procedures

required to facilitate this (Thorsen, 2017), it can be presupposed that they are more likely to inflect concerns about this in their news reporting than other publishers. Both newspapers' broadly liberal tradition underpins the expectation that their reporting is more likely to be concerned with the ability of citizens (and indeed journalists) to communicate freely without Government interference. This study is therefore designed to establish a comprehensive understanding of the discursive constructs related to encryption, in publications where mentions of encryption are likely to be advanced and even possibly supported, to enable further comparative studies in the future.

This study is specifically concerned with the newspapers' respective websites, since online news transcends traditional space restrictions associated with print editions. Websites offer publishers opportunities to provide expanded context and intertextuality, for example by linking out to tools or information that can mitigate barriers to uptake of encryption practices. Indeed the modern use of encryption is inherently associated with digital communication, and online news can therefore be considered an optimum place to provide additional context for audiences about encryption in the environment where it is relevant.

Both newspapers are also national publications (UK and US respectively) that have aimed to use websites to reposition their operations and increasingly target English-speaking audiences globally. *The Guardian* has a reported print circulation of 164,630 (ABC figures as of May 2016) and theguardian.com some 341 million monthly combined page views (SimilarWeb, April 2016), while *the New York Times* has a daily print circulation of 590,000 (Sydney Ember, *the New York Times*, 3 May 2016) and nytimes.com some 505 million monthly combined page views (SimilarWeb, April 2016).

For the purpose of this study, a three-year sampling period was identified to encompass one year before and two years after the first Snowden related publication on 5th June 2013. The sample period therefore spanned: 1st June 2012 to 1st June 2015. This was done to identify patterns in news reporting of encryption over time, and the influence of the global surveillance disclosures on cybersecurity news discourses. News articles were extracted through a Google site search with www.theguardian.com/uk and www.nytimes.com using the search term *crypt*. The asterisks pre and postfix search operators acts as a wildcard to capture any word that contains the phrase “crypt”, such as encryption, decryption, cryptography, and any derivative variables.

The two Google site searches returned a total of 3,081 articles. The present study is concerned with news discourse only, thus opinion pieces, commentary, blog posts, and crosswords were removed from the initial batch of search results. Also excluded were any pages where the search syntax *crypt* was only mentioned in audience comments below the news article (for perspective on blogs and below-line comments, see Wahl-Jorgensen et al forthcoming). The final corpus for this study therefore encompassed 1,249 news articles - approximately 1/3 of the articles were from *the New York Times* (395 news articles) with 2/3 from The Guardian (854 news articles). Prioritising news articles in this way was a

purposive sampling strategy, given the resources available, to enable a longitudinal study including *all* relevant news articles over a three-year period. Whilst this offers a more complete understanding of how the news discourse relating to encryption has evolved over time, it also omits potentially important editorial explications and public interventions on the topic. The present study should therefore be considered a starting point to help guide future areas of research.

How articles in the sample constructed news discourses concerning encryption, can be understood by analysing the news framing process (de Vreese 2012; Tankard 2001; Entman 1993). That is, the way news articles emphasise certain values, facts or events in their reporting that informs possible interpretations of that text. However, references to encryption were sparse in the sample material and rarely the main purpose of any news article itself. To this end, the study modified a previous approach for analysing news framing of Manning (Thorsen et al. 2013) and Snowden (Di Salvo and Negro 2015) to examine in this study "news context" rather than frames. This thematic analysis is similar to the principles of framing, though conceptually it refers to the news article as a whole and is therefore not intended to reflect how the subject of interest (in this case encryption) specifically was framed within the article. Rather it provides an indication of the broader new contexts where encryption is mentioned. To analyse the discourse specific to encryption, the study then coded for three criteria: firstly, the described purpose of encryption as articulated within the news article; secondly, the benefactors of that encryption practice; and thirdly, any details regarding usage or adoption of encryption practices. Finally, the study analysed the news sources that were referenced in relation to encryption to examine who was afforded a voice and perceived as 'primary definers' (Hall 1973) in relation to encryption. News articles were coded using a qualitative inductive approach to enable coding categories to emerge from the analysis of the news articles.

News contexts: surveillance, security, privacy and hacking

Tracking news reporting over a three-year period, it is evident that Edward Snowden's global surveillance disclosures contributed to a significant upturn in mentions of encryption within *The Guardian* and *the New York Times*' online output. As Figure 1 illustrates, there was an immediate spike in encryption related coverage in June 2013 when the first Snowden revelations were published. This was followed by brief decline, before a subsequent steady rise in mentions of encryption later that year. Events that contributed to this increase were mostly connected or associated with the global surveillance disclosures in one way or another (see Figure 1).

Encryption was rarely the primary objective of any news article within this study. Indeed it was mentioned in the headline of only 70 articles (8% of total) by *The Guardian* and 10 articles (3% of total) by *the New York Times*. Where encryption was included in the primary news context, the stories were related to either the crypto locker ransomware or email encryption (usually connected with Snowden's use of Lavabit or discussion of PGP). Instead, encryption was typically mentioned as part of news stories with a different primary

focus. The context of these news stories were overwhelmingly centred upon security, surveillance, privacy, hacking and business which together accounted for 65% of the articles overall (see Figure 2).

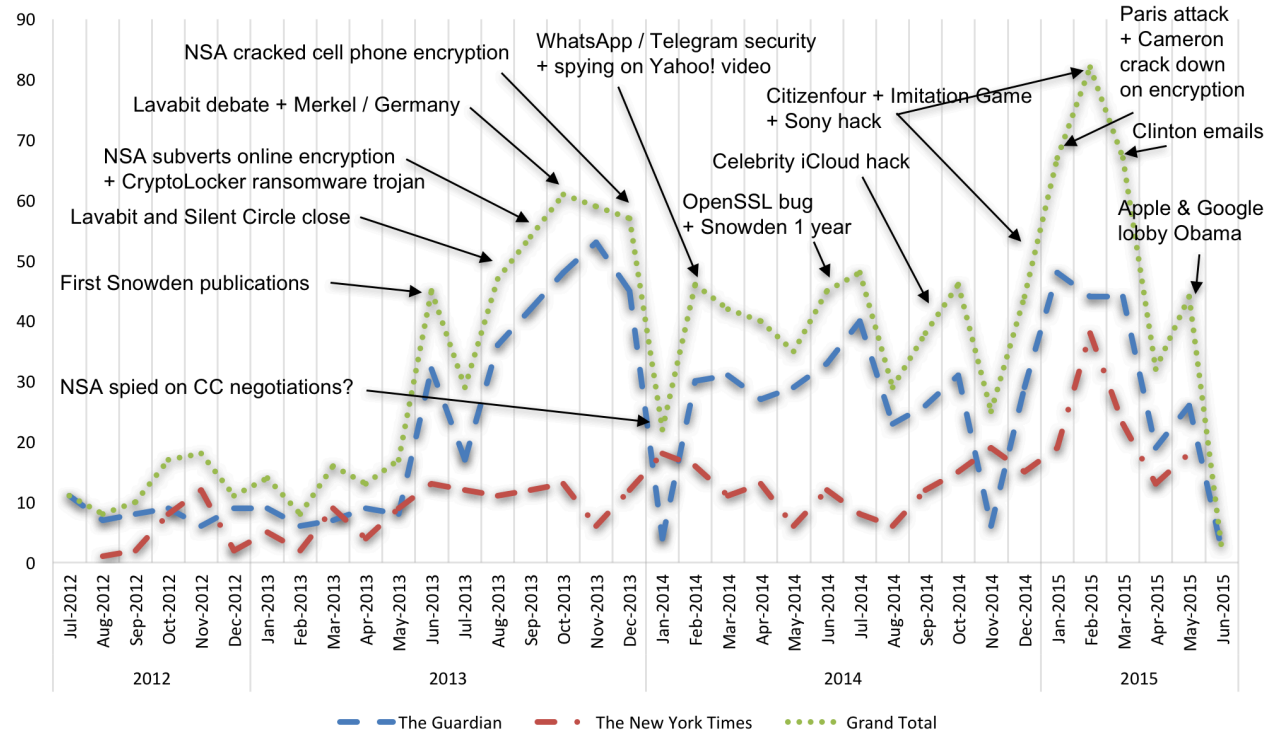


Figure 1 News reporting of encryption from June 2012 to June 2015

	The Guardian				The New York Times				Grand Total	
Primary context of article	2012	2013	2014	2015	2012	2013	2014	2015	Articles	%
Security	9	55	95	37	6	22	45	32	301	24%
Surveillance	5	101	37	31		30	19	12	235	19%
~~Other~~	14	35	49	33	7	14	16	10	179	14%
Privacy	1	22	26	21	3	18	15	3	109	9%
Hacking	5	17	37	14	4	6	13	8	104	8%
Business	6	22	14	4	1	4	10		61	5%
Terrorism		1	6	13		1	2	10	33	3%
Crime gangs	1	10	7	2			4	8	32	3%
Communication		14	4	3		2	3		26	2%
Finance		3	7	4		1	4	4	23	2%
China		1		3	2		3	13	22	2%
International relations	3	5	4	1		1	5	3	22	2%
Censorship	1	3	2	7		7	1		21	2%
Paedophiles / child abuse		10	4	1					15	1%
Cyberwarfare	1		4	1			4	5	15	1%
Activism	1	4	2	2	2		1	1	13	1%
Piracy	2	4	2	1		1			10	1%
Russia		1	1	1			6		9	1%
Economy		3	2	1		1			7	1%
Social media		1	1	3				2	7	1%
Streaming (region lock)			5						5	0%
Grand Total	**50**	**312**	**309**	**183**	**25**	**108**	**151**	**111**	**1249**	**100%**

65%

Figure 2 Primary news context of articles mentioning encryption

The primary news contexts was similar for both publications, with only six categories containing noteworthy differences: *The Guardian* placed greater emphasis on news contexts containing communication, paedophiles/child abuse, and piracy; whilst *the New York Times* placed greater emphasis on news contexts with China, cyberwarfare, and Russia. This implies a somewhat different emphasis on risk factors associated with encryption - the US publication associated it with Cold War adversaries, whilst the UK publication showed a comparatively greater concern about paedophiles and copyright infringement. It is important to note, however, that these primary news contexts represent a fairly low proportion of the coverage overall - each category about 1-2% of the total corpus.

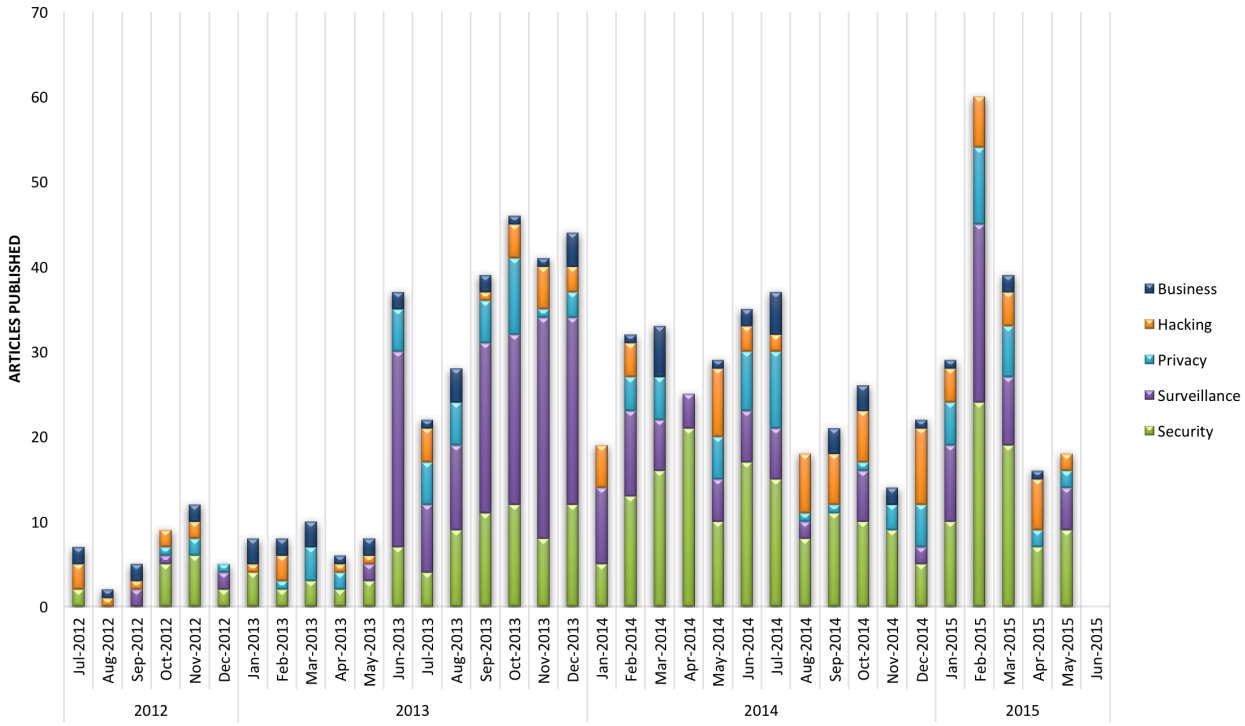


Figure 3 Primary news context of articles mentioning encryption (showing top-5 contexts only)

Global surveillance disclosures contributed to an increase in volume of news mentioning encryption, but also precipitated a shift in news contexts with a new emphasis on surveillance. However, the primary news context changes after about 9 months: moving from predominantly surveillance to predominantly security (see Figure 3). This was in part due to computer companies implicated by the Snowden leaks getting involved in public discussions about cybersecurity. It also signals the ability of powerful elite sources in the UK and US to shift the primary discourse away from surveillance and on to concerns about national security, as discussed below. This is significant since framing the debates in terms of a national security agenda allowed proponents to legitimise both surveillance activities *and* attempts at breaking encryption. The vast majority of terrorism related coverage was in January 2015, concerning the Paris attacks and Cameron's subsequent attack on encryption

technology as an alleged surveillance circumventions resource for ISIS. Post-Snowden revelations there was also an increase in news concerned with encryption and privacy, which remained prominent throughout most of the sample period. There was also a noticeable increase in news about hacking, with spikes in 2014 and early 2015 in relation to the iCloud and Sony leaks. The post-Snowden revelations also appear to have contributed to an increase in news concerned with encryption and privacy, which remained prominent throughout most of the sample period.

Private corporations and experts

In order to further critique how - and, crucially, in whose interest - these primary news contexts are constructed, the study examined primary and secondary news sources. These sources can be understood as the 'primary definers', whose discursive priorities help shape the news context. Analysis of source usage in other words documents which voices are heard in the context of encryption, and of course by extension, which are excluded.

The most striking finding here is that approximately 40% of news articles that mentioned encryption only cited a single source (see Figure 4). This was marginally lower in the case of *the Guardian* (43.3%) than *the New York Times* (30.9%). Some 12.5% of news articles overall did not even attribute a single source within the story. Here *the New York Times* (16.5%) fared slightly worse than *the Guardian (*10.7%).

Primary source	The Guardian	The New York Times	Total
Private corporation	26.0%	13.2%	21.9%
Expert	14.4%	14.9%	14.6%
Other	13.3%	13.2%	13.3%
None	10.7%	16.5%	12.5%
NGO	3.7%	5.8%	4.4%
Media	4.3%	3.5%	4.1%
Government (other)	3.2%	4.1%	3.4%
Citizen	2.6%	4.8%	3.3%
Government (US)	2.0%	6.1%	3.3%
Leaked document	3.4%	3.0%	3.3%
Government (UK)	3.9%	0.5%	2.8%
Activist	2.6%	2.3%	2.5%
Whistleblower	2.8%	1.3%	2.3%
Politician (US)	1.5%	2.8%	1.9%
FBI	0.6%	3.0%	1.4%
Politician (Other)	1.1%	1.3%	1.1%
Politician (UK)	1.4%	0.0%	1.0%
NSA	0.7%	1.3%	0.9%
Hacker	1.1%	0.5%	0.9%
GCHQ	0.5%	1.3%	0.7%
Criminals	0.4%	0.3%	0.3%
CIA	0.0%	0.5%	0.2%
Grand Total	**100.0%**	**100.0%**	**100.0%**

Secondary source	The Guardian	The New York Times	Total
None	43.3%	30.9%	39.4%
Expert	12.2%	12.9%	12.4%
Private corporation	10.8%	15.2%	12.2%
Other	5.9%	13.2%	8.2%
NGO	7.3%	3.8%	6.2%
Government (US)	2.1%	3.8%	2.6%
Media	2.7%	2.3%	2.6%
Citizen	2.2%	2.3%	2.2%
Government (UK)	2.6%	0.8%	2.0%
Government (other)	1.8%	2.5%	2.0%
Activist	1.3%	2.0%	1.5%
Politician (Other)	1.2%	2.0%	1.4%
Politician (US)	0.9%	2.0%	1.3%
NSA	0.9%	2.0%	1.3%
Politician (UK)	1.4%	0.3%	1.0%
Leaked document	1.2%	0.8%	1.0%
Whistleblower	1.2%	0.3%	0.9%
FBI	0.4%	1.5%	0.7%
Hacker	0.5%	0.3%	0.4%
GCHQ	0.2%	0.5%	0.3%
Criminals	0.1%	0.5%	0.2%
CIA	0.0%	0.3%	0.1%
Grand Total	**100.0%**	**100.0%**	**100.0%**

Figure 4 Primary and secondary source usage in news articles mentioning encryption

Overall private corporations dominated both primary and secondary source usage in both publications. *The Guardian* used private corporations 26% as a primary and 10.8% as a secondary source, whilst *the New York Times* usage was slightly less at 13.2% as a primary and 15.2% as a secondary source. Emphasis on private corporations here is problematic since many of the organisations concerned were those who were accused of colluding with the NSA and GCHQ to aid covert mass surveillance - Google, Facebook,

Apple, and Microsoft, featuring prominently. Indeed, collusion was even noted in some of the news articles analysed: *the Guardian*, for example, reported how "it emerged Microsoft had worked to circumvent its own encryption to enable NSA access to customer records" (21 August 2013), while *the New York* Times highlighted how the global surveillance disclosures showed how the NSA "has encouraged or coerced companies to install back doors in encryption software and hardware, worked to weaken international standards for encryption and employed custom-built supercomputers to break codes or find mathematical vulnerabilities to exploit" (6 September 2013). But more often than not news reports allowed private corporations to a) proclaim their innocence in connection with NSA/GCHQ surveillance ("Apple follows Facebook's lead and reveals US surveillance requests", *the Guardian*, 17 June 2013); b) extolling the virtues of their own efforts to enhance encryption (e.g. "Google moves to boost email privacy by releasing end-to-end encryption tool", *the Guardian*, 4 June 2014, and "Tech Giants Urge Obama to Reject Policies That Weaken Encryption", *the New York Times*, 19 May 2015); or c) play down the severity of own security breaches and to defend their mitigation strategies (e.g. "Adobe Announces Security Breach", *the New York Times*, 3 October 2013). Thus news articles were effectively providing these private corporations with a platform to exonerate themselves from the accusations, and frequently doing so without being challenged. Cross-tabulating the results we find that when private corporations were cited, they did so primarily as a lone source (41% of instances) or where both the primary *and* secondary source was a private corporation (19% of instances).

The second highest primary source was of individuals positioned as subject 'experts'. This included independent analysts, for example on politics or national security matters, and computer technicians who were cited to help explain technical aspects of the global surveillance disclosures. Their contributions were not solely to explain technical workings of encryption, but also to illuminate the severity of risk associated with various computer failures or even attack the NSA/GCHQ practices.

Both publications made similar use of expert sources, with overall 14.6% as a primary source and 12.4% as a secondary source. As with private corporations, expert sources were either positioned alongside other expert sources (23% of instances) or as the sole source of the news article (20% of instances). No other source pairing was afforded a similar dominance to that of private corporations or experts. Indeed alternative sources that might have acted as a counterbalance to private corporations - such as NGOs (4.4%), citizens (3.3%), activists (2.5%), or whistleblowers (2.3%) - were given comparatively little attention as primary sources.

Both *the Guardian* and *the New York Times* also cited a range of official government and security services sources, who typically defended the reported activities as 'bulk collection' of metadata necessary for intelligence operations. Here there was an emphasis on the domestic government or agencies - *the Guardian* as expected drawing on UK sources, whilst *the New York Times* relied more on US sources. Aside from each publication's preference for domestic sources, *the New York Times'* greater use of official

Government and military sources was also evident in previous studies into news framing of Manning (Thorsen et al. 2013) and Snowden (Di Salvo and Negro 2015).

Encryption purpose

As highlighted in the previous sections, encryption was rarely the *primary* focus of any news articles where it was mentioned. Instead, the majority of articles made references to encryption (or associated terms), without fully explaining what this meant or how it could be utilised. Every mention does, however, contribute to the overarching discourse about encryption and its perceived societal role. In order to critique this further, the study coded for "encryption purpose", cross-tabulated against "encryption of what" and "who was said to benefit from encryption". The first cross-tabulation shown in Figure 5 reinforces how encryption was described primarily in generic terms in the news articles analysed: either as encryption of "communication" (46.3%) or "information" (30.1%). More specific methods such as e-mail encryption (8.1%) and instant message encryption (7.6%) feature too, but much more intermittently.

Cross-tabulating what is being encrypted against the purpose of that encryption, we find that "data protection" (48%) and "privacy" (17%) were the most dominant reasons for using encryption. *The Guardian* reported, for example, that "Facebook is also attempting to protect user privacy from government and third-party surveillance by making all of its communications secure and encrypted." (4 June 2014), in an article highlighting concerns about the social network's audio-recognition feature. This initially appears promising, as it connotes a positive interpretation of people's motivations to adopt encryption to aid communication security. However, the majority of privacy concerns were connected with third-party behaviour tracking for advertising and personalisation purposes. Controlling what data these trackers can harvest even "seems to be buoying a cottage industry of privacy start-ups", according to *the New York Times* (3 March 2013). Meanwhile, only 6.5% of encryption is for the explicit purpose of "surveillance circumvention". Here we find a disconnect between notions of personal privacy, for example, and the intrusive nature of mass surveillance. In other words, need for encryption to protect personal privacy was *not* associated directly with the invasive threat from state surveillance. Moreover, encryption was virtually never associated with military or surveillance activities either. Consequently, encryption is largely detached from both surveillance *and* surveillance circumvention, despite the key role it plays in both.

This notion that encryption aids citizens is further evidenced by cross-tabulating the encryption purpose against who benefits from it (see Figure 5). Citizens were said to benefit in approximately 53% of news articles, and their purpose for using was mainly articulated as data-protection (30.3%) and privacy (21.4%). Again this is promising in terms of aiding a positive discourse about encryption which might aid adoption of different forms of communication security to - among other things - circumvent state sponsored mass surveillance. However, as highlighted in the preceding section on news sources, we know private corporations are primarily those who are afforded a voice in relation to encryption.

These sources are the very same companies that were implicated in the global surveillance disclosures as collaborating with the NSA and GCHQ to facilitate the indiscriminate mass surveillance, which necessarily undermines confidence in their proclaimed concern for enhancing communication security.

	Encryption purpose					
Encryption of	Circumvention	Data-protection	Military	Privacy	Surveillance	Total
Communication	5.2%	21.6%	1.8%	17.3%	0.3%	46.3%
Information	0.9%	26.3%	0.6%	2.1%	0.2%	30.1%
Email	0.0%	1.8%	0.0%	6.3%	0.0%	8.1%
Message	0.3%	1.0%	0.7%	5.6%	0.0%	7.6%
Storage (local)	0.1%	3.0%	0.0%	0.0%	0.0%	3.0%
Storage (cloud)	0.0%	2.1%	0.0%	0.7%	0.0%	2.8%
Currency	0.0%	2.0%	0.0%	0.0%	0.0%	2.0%
Grand Total	**6.5%**	**57.8%**	**3.2%**	**32.0%**	**0.6%**	**100.0%**

Figure 5 "Encryption purpose" cross-tabulated against “encryption of what"

Criminals was the second largest group said to be benefitting from encryption, attributed in approximately 11% of the news articles analysed. Unlike citizens, however, criminals *do* purportedly use it for "surveillance circumvention”. Reinforcing the idea that citizens can protect their privacy against other citizens or private corporations, but only criminals would seek to circumvent state surveillance. Again the myth being that seeking to utilise encryption to circumvent state surveillance is somehow an illicit act, since it is conducted by criminals. *The Guardian* makes this connection in an article shedding light on how "Organised wildlife criminals are using online tools more commonly associated with serious financial crime, drug trafficking and child pornography” (*the Guardian*, 4 September 2012). The article does not specifically name the alleged tools, but mentions “deep web” twice and lists "use of tools such as mailing list servers, password-protected sites and encryption” as a concern in relation to the illicit ivory trade within the EU. Even when articles *did* provide more detail about the underlying technology and its broad applications, the association with illicit sites such as Silk Road tainted those use scenarios:

> "It [Silk Road] operated as a "hidden" site, which was only accessible to people using the sophisticated anonymous browsing service known as Tor. […] Operated by a network of volunteers, Tor provides encryption and identity protection, allowing users to avoid surveillance and traffic interception as well as circumvent internet censorship.” (*the New York Times*, 3 September 2013)

When private corporations, the NSA or US Government were seen as benefactors of encryption, however, it was almost exclusively for the seemingly benign purpose of data-protection. When it was used by Government agencies for sinister purposes, encryption too was depicted as a vice. For example, it was reportedly used in an "Obama administration programme [that] secretly dispatched young Latin Americans to Cuba using the cover of health and civic programs to provoke political change” (*the Guardian*, 4 August 2014). Here encryption is both associated with clandestine US overseas operations, and a presumption that use of encryption is worthy of attracting suspicion in itself. In so doing,

the text maintains a mythical depiction of encryption as a sinister practice best avoided by those with nothing to hide. Military use of encryption was given similarly minacious tropes, with its usage by *other* governments or agencies (typically the traditional Cold War adversaries, China and Russia) positioned as cause for concern against the US and UK's purportedly acceptable usage.

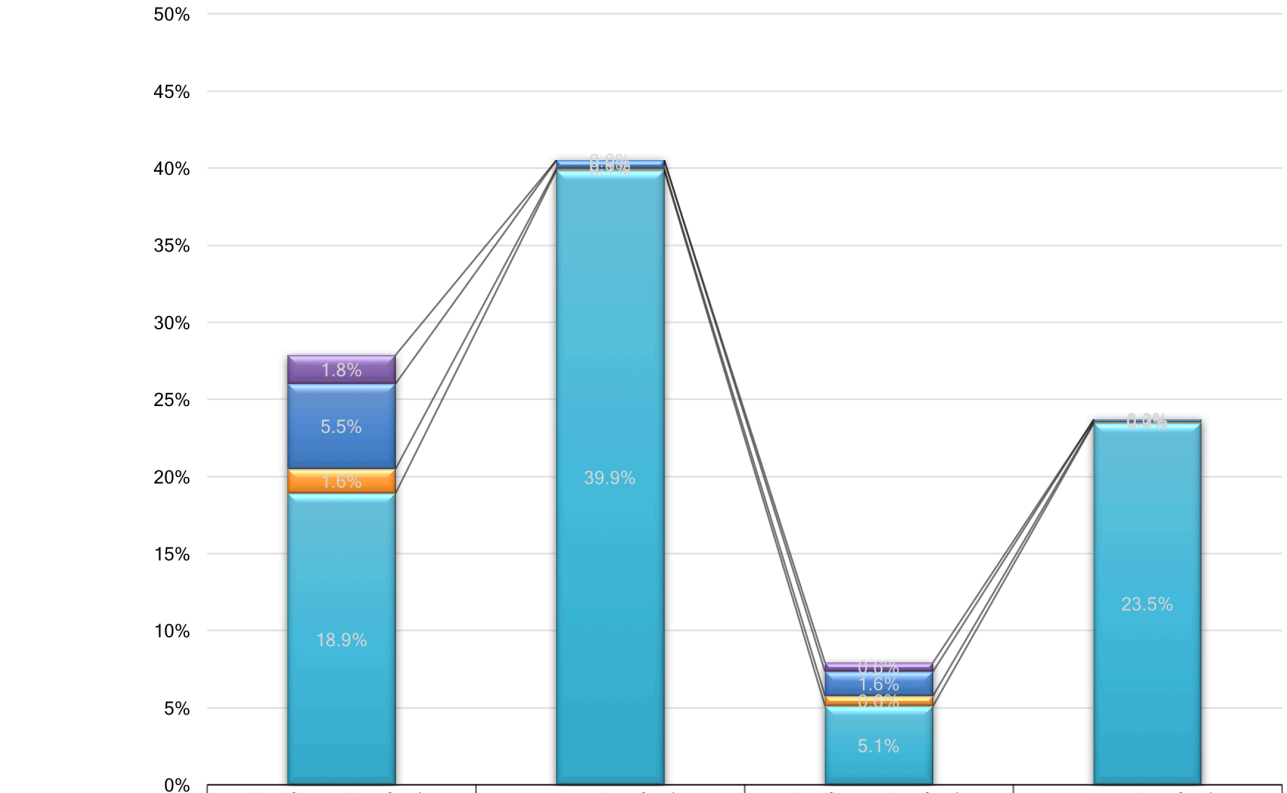
	Encryption purpose					
Benefitting from *crypt*	Circumvention	Data-protection	Military	Privacy	Surveillance	Total
Citizen	1.0%	30.3%	0.1%	21.4%	0.0%	52.7%
Criminals	3.3%	4.0%	0.1%	3.1%	0.1%	10.6%
Private corporation	0.3%	7.2%	0.0%	0.6%	0.0%	8.2%
Government (other)	0.8%	2.7%	2.0%	0.4%	0.2%	6.2%
NSA	0.0%	2.9%	0.1%	0.6%	0.1%	3.6%
Media	0.1%	2.4%	0.0%	1.0%	0.0%	3.4%
Government (US)	0.0%	2.4%	0.6%	0.2%	0.2%	3.4%
Whistleblower	0.2%	0.7%	0.0%	2.3%	0.0%	3.3%
Hacker	0.0%	1.7%	0.0%	1.1%	0.0%	2.8%
Other	0.0%	1.2%	0.0%	0.4%	0.0%	1.6%
Activist	0.6%	0.3%	0.0%	0.5%	0.0%	1.4%
Government (UK)	0.1%	0.7%	0.4%	0.1%	0.0%	1.3%
GCHQ	0.0%	0.4%	0.0%	0.1%	0.0%	0.5%
Expert	0.0%	0.4%	0.0%	0.0%	0.0%	0.4%
NGO	0.1%	0.3%	0.0%	0.0%	0.0%	0.4%
Politician (Other)	0.0%	0.0%	0.0%	0.2%	0.0%	0.2%
CIA	0.0%	0.1%	0.0%	0.0%	0.0%	0.1%
Grand Total	**6.5%**	**57.8%**	**3.2%**	**32.0%**	**0.6%**	**100.0%**

Figure 6 "Encryption purpose" cross-tabulated against "who benefits from encryption"

Against this backdrop of connoting encryption as something sinister, it is also worth drawing attention to how infrequently media and whistleblowers were seen as benefactors of encryption usage. Fewer than 7% of the news articles overall were concerned with how these two categories used encryption. Again there was virtually no mention of how these groups might use encryption for "surveillance circumvention", even though this has clear ramifications for source protection and journalist / whistleblower relationships. The subject of these news articles were almost exclusively about Snowden or Manning / WikiLeaks, and either how they had communicated with journalists or how media organisations could facilitate future leaks from whistleblowers. Activists (1.4%) and NGOs (0.4%) were similarly absent in terms of possible benefactors of encryption. Whilst this was again frequently associated with Snowden and Manning, the categories were more diverse with activists in Turkey, Syria, China and Ethiopia all mentioned. This dearth in the reporting is nevertheless disconcerting since it engenders a discourse that positions communication security as separate from important usage scenarios for non-elite stakeholders.

These challenges are aggravated by the lack of specificity and detail about encryption software and how this is operationalised in everyday usage. Even with the most generous interpretation of what constituted "encryption technology or software", only just over 40% of news articles in *the Guardian* and approximately 25% in *the New York Times* made specific reference to a technology or piece of software beyond simply using an "encryption" related word - equivalent to 35.8% of the overall sample (see Figure 7). Even fewer articles

made reference to more than one method, with only 10% in *the Guardian* and 6% in *the New York Times*. This is indicative of the *depth* of news reporting that specifically mentions encryption. Without specificity about encryption, myths surrounding the technology and its 'forms of use' remain cloaked in mystery. In effect this perpetuates its inaccessibility for anyone who is not already versed in computer security.



	The Guardian		The New York Times	
	Specific mention of tech	No mention of tech	Specific mention of tech	No mention of tech
Link and instructions	1.8%	0.0%	0.6%	0.0%
Link, but no instructions	5.5%	0.6%	1.6%	0.2%
No link, but instructions	1.6%	0.1%	0.6%	0.1%
No link, no instruction	18.9%	39.9%	5.1%	23.5%

Figure 7 Specific mentions of encryption technology or software, cross-tabulated against presence of links and usage instructions (n=1249)

Overall 63.3% of news articles mentioning encryption failed to name, link to or offer instruction about specific encryption technologies. Another 24% mentioned technology, but without link or instruction. Some 2.4% of the news articles overall *did* offer some form of instruction about how to use encryption, but then failed to link to relevant websites. Only 7.8% of articles linked to websites with encryption software, with the majority coming from *the Guardian* (5.5% of overall sample). Combining links with instructions on how to use the software was only found in 2.4% of the news articles overall. The majority of these news articles were features devoted solely to explaining use of encryption technology or methods, rather than reports about related events or developments. Such news articles were present prior to the Snowden revelations too, emphasising personal privacy (e.g. "How can I protect my privacy online?", *the Guardian*, 13 December 2012; "Trying to keep your e-mails secret when the C.I.A. chief couldn't", *the New York Times*, 16 November

2012). Post-Snowden revelations these continued to emphasise personal privacy (e.g. “How internet encryption works”, *the Guardian*, 5 September 2013; “How not to pay the price for free Wi-Fi”, *the New York Times*, 4 June 2014), and also small businesses (e.g. “The experts’ step-by-step guide to cybersecurity", *the Guardian*, 2 April 2015). Whilst these articles wholly devoted to encryption or related software are laudable, it signals how the operationalisation of communication security is largely siloed and presented as distinct from other news reporting that mentions encryption.

Across the whole sample, specific encryption technology or software was rarely named more than once or twice. In fact, Tor (mentioned in 35 news articles across the sample), VPN (30), PGP (25), Bitcoin (25), Cryptolocker (19), OpenSSL (19), and Lavabit (19) were the only encryption related technologies or software that recurred with any significance. This sporadic pattern is echoed when examining which technologies or software were actually linked to, though with slightly different composition. The only ones linked to more than twice were: VPN (13), Tor (6), LastPass (6), PGP (5), Wickr (4), Silent Text (4), OpenSSL (3), and Telegram (3). Again this is problematic since audiences are unlikely to develop familiarity with the technologies or applications mentioned, and thus - apart from early adopters - remain unlikely to try them out. The constant referencing of new and different technology also reinforces the sense of uncertainty and complexity often associated with many of these. Core communication security technologies such as VPN and PGP were only linked to alongside instructions for how to use them on 4 and 3 occasions respectively across the whole sample of news articles.

Even when news articles *did* link out or provide instructional information about encryption, it was typically accompanied by explicit warning about the complexities of its usage. Such unequivocal language from both journalists *and* expert sources about encryption constructs and sustains a perception that not only is this too complicated for most people, but it is also not relevant to their everyday lives. Not only does this feed into the mythical discourse about encryption, but it also deters widespread adoption.

Conclusion

This study analysed three years of news reporting on surveillance circumvention technologies and practices, specifically focussing on encryption, on *The Guardian* and *The New York Times* websites spanning 1st June 2012 to 1st June 2015. It sought to identify thematic shifts in news articles mentioning encryption both before and after Snowden’s global surveillance disclosures, by analysing the news contexts in which the subject appears. In so doing it was possible to analyse passing references, without implying that the utterance about encryption itself bore the characteristics of the overall news article (since, indeed, it often barely got a passing mention).

Evidently there was a marked increase in coverage of encryption post-Snowden in terms of volume. There was also a significant shift in the type of coverage post-Snowden, from an initial emphasis on "surveillance" towards "security" issues. Whilst this trend was

clear in both publications, they also exhibited some noteworthy differences in the primary news contexts where references to encryption surfaced. This indicated a somewhat different emphasis on risk factors associated with encryption - whereby *the New York Times* associated it with Cold War adversaries and cyberwarfare, *the Guardian* showing a comparatively greater concern about paedophiles and copyright infringement. Whilst these variances are found in the 'long tail' of the coverage, they are nevertheless cognisant of the domestic news agendas.

Echoing previous media research, we find that news articles relied primarily on elite sources. However, in contrast to Barnard-Wills (2011) and Lischka (2015) who found a dominance of government sources in news reporting of surveillance, those afforded a voice in relation to encryption were primarily private corporations and experts. Despite this, the discourse concerning encryption exhibited the same legitimisation versus delegitimisation dichotomy found in news about surveillance or intelligence services. Indeed the computer companies implicated by the Snowden leaks were getting involved in public discussion about cybersecurity - to delegitimise mass surveillance and legitimise their own intelligence gathering about its users, usually expressed as highlighting their commitment to privacy. And whilst there were some positives to take from the attention placed on "data-protection" and "privacy" for citizens, we need to remember that they are expressed in the context of revelations about how those very companies had colluded with Governments to undermine their own encryption and security features.

When they did refer to officials, each publication relied primarily on domestic sources, reflecting the complexion of the debate in the UK and US respectively. *The New York Times* made greater use of official Government and military sources than *the Guardian*, which echoes previous studies into news framing of Manning (Thorsen et al. 2013) and Snowden (Di Salvo and Negro 2015). As a consequence, the delegitimising discourse (for example that encryption is used by terrorists and prevents effective intelligence gathering) was more prevalent in *the New York Times* than *the Guardian*. In contrast, *the Guardian* would more often reflect negatively on encryption as a consequence of its penetrability - that it would be insufficient to protect citizens against either surveillance or malicious hacking.

The shift *away* from surveillance and on to security issues, meant that the terms of reference when encryption was mentioned also changed. Framing debates in terms of a national security agenda, for example, allowed proponents to ‘reterritorialise' (Munro 2015) debates by legitimating both surveillance activities *and* attempts at breaking encryption. The purpose of encryption was similarly fraught in both positive and negative *purposes*, but readers were always reminded about the *risks*: on the one hand encryption was associated with illicit or criminal behaviour; and on the other hand it was deemed too complicated or not relevant to everyday lifeworlds of law abiding citizens. While these risks are embedded in the de-localised logic of what Beck (2006) terms the “world risk society”, their risk discourse nevertheless serves to legitimise surveillance *over* surveillance circumvention.

"Activists and counter-surveillance practitioners should", according to Monahan, "diligently avoid reproducing the exclusionary logics and reactionary stances of those whom they critique". Indeed, he argues that "high-tech interventions may attract public attention because of their innovative use of technologies, but they can defy replication by others without comparable technical capabilities or resources" (Monahan 2006, 531). Despite this, even Edward Snowden has expressed concern about the usability of encryption tools. At the 2014 Hope conference he reportedly "reserved much of his criticism for software which, while technically strong, offers a poor user experience" (*The Guardian*, 21 July 2014). Snowden was damning about the public key encryption tool, GPG, as "robust and pretty reliable encryption", but claiming "Unfortunately it's damn near unusable" (cited in *The Guardian*, 21 July 2014).

Surveillance *circumvention* is important for civil liberties as highlighted at the outset. But such practices must be part of a broader movement to counter not just the technologies of surveillance, but also the public and private institutions that operationalise it; policies that enable and legitimise it; and of course, as highlighted by Manning, Snowden and others, the conspiratorial operational logic of state and military governance that allows them to exceed their mandate in secret (Thorsen, 2017). Paradoxically one of the most effective ways of disrupting this operational logic is itself a form of secrecy: mass encryption of digital communications. Yet unless the language around encryption is demystified and normalised, we will merely perpetuate its mythical illusion.

Acknowledgements

This research would not have been possible without the determination and diligence of my research assistant, Stefani Tasheva.

Notes

1 *The Washington Post* was Snowden's other initial partner alongside *The Guardian*. Snowden had originally decided against involving *The New York Times* since he was concerned they would delay or spike the story in the interest of national security.

Bibliography

Bakir, Vian, and Andrew McStay. 2016. "Assessing interdisciplinary academic and multi-stakeholder positions on transparency in the post-Snowden leak era." *Ethical Space: The International Journal of Communication Ethics* 12(3): 25–38.

Barnard-Wills, David. 2011. "UK News Media Discourses of Surveillance." *The Sociological Quarterly*, 52(4): 548–567.

Beck, Ulrich. 2006. "Living in the world risk society". *Economy and Society*. 35(3): 329-345. doi: 10.1080/03085140600844902

Bradshaw, Paul. 2015. "Chilling effect: regional journalists' source protection and information security practice in the wake of the Snowden and RIPA revelations." *Surveillance and Citizenship: State-Media-Citizen Relations after the Snowden Leaks* Cardiff University, 1–32.

Brevini, Benedetta, Arne Hintz and Patrick McCurdy, eds. 2013. *Beyond WikiLeaks: Implications for the future of communications, journalism and society*. New York: Palgrave Macmillan.

Christensen, Lars Thøger, and George Cheney. 2015. "Peering into Transparency: Challenging Ideals, Proxies, and Organizational Practices". *Communication Theory*, 25(1): 70–90. doi: 10.1111/comt.12052

Couldry, Nick. 2015. "The myth of 'us': digital networks, political change and the production of collectivity". *Information, Communication & Society*. 18(6): 608-626. doi: 10.1080/1369118X.2014.979216

Entman, Robert M., 1993. "Framing: Toward clarification of a fractured paradigm". *Journal of Communication*. 43(4). pp. 51-58.

Hall, Stuart. 1973. *Encoding and Decoding in the Television Discourse*. Birmingham: University of Birmingham.

Henrichsen, Jennifer R., Michelle Betz and Joanne M. Lisosky. 2015. *Building digital safety for journalism: a survey of selected issues*. Paris: UNESCO.

Hillebrand, Claudia. 2012. "The Role of News Media in Intelligence Oversight". *Intelligence and National Security*, 27(5): 689–706. doi: 10.1080/02684527.2012.708521

Hintz, Arne, Lina Dencik and Karin Wahl-Jorgensen. 2017, forthcoming. "Surveillance in a Digital Age". In *The Routledge Companion to Digital Journalism Studies*, edited by Bob Franklin and Scott Eldridge II. London: Routledge.

Kleberg, Carl Fridh. 2015. *The death of source protection? Protecting journalists' source in a post-Snowden age*. London: LSE Polis.

Lashmar, Paul. 2016. "No More Sources?" *Journalism Practice*: 1–24. doi: 10.1080/17512786.2016.1179587

Lischka, Juliane A. 2015. “Surveillance discourse in UK broadcasting since the Snowden revelations.” *dcssproject.net*. http://www.dcssproject.net/files/2015/12/DCSS_Broadcasting-report.pdf

Lyon, David. 2014. “Surveillance, Snowden, and Big Data: Capacities, consequences, critique.” *Big Data & Society*, 1(2): 1–13. doi: 10.1177/2053951714541861

Monahan, Torin. 2006. “Counter-surveillance as Political Intervention?” *Social Semiotics*. 16(4): 515-534. doi: 10.1080/10350330601019769

Munro, Iain. 2015. “Organizational resistance as a vector of deterritorialization: The case of WikiLeaks and secrecy havens.” *Organization*: 1–21. doi: 10.1177/1350508415591362

Penney, Jonathon W. 2013. “The Cycles of Global Telecommunication Censorship and Surveillance.” *SSRN Electronic Journal*. 36(3): 693-753.

de Vreese, Claes H., 2012. “New Avenues for Framing Research.” *American Behavioral Scientist*, 56(3): 365–375. doi: 10.1177/0002764211426331

Di Salvo, Philip, and Gianluigi Negro. 2015. “Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States.” *Journalism*: 1–18. doi: 10.1177/1464884915595472

Snowden, Edward. 2016. “Foreword: Elected by circumstance.” *The Assassination Complex*. London: Serpent's Tail: xi-xviii.

Tankard Jr, James W., 2001. “The empirical approach to the study of media framing.” In *Framing public life: Perspectives on media and our understanding of the social world*, edited by Stephen D. Reese, Oscar H. Gandy, and August E. Grant, 95-106. Mahwah: Lawrence Erlbaum Associates

Taylor, Roland. 2015. “The Need for a Paradigm Shift Toward Cybersecurity in Journalism.” *National Cybersecurity Institute Journal*. 1(3): 45–47.

Thorsen, Einar. 2017, forthcoming. “Whistleblowing in a Digital Age: journalism after Manning and Snowden.” In *The Routledge Companion to Digital Journalism Studies*, edited by Bob Franklin and Scott Eldridge II, 569-578. London: Routledge.

Thorsen, Einar, Chindu Sreedharan and Stuart Allan. 2013. “Wikileaks and whistle-blowing: The framing of Bradley Manning.” In *Beyond WikiLeaks: Implications for the future of communications, journalism and society*, edited by Benedetta Brevini, Arne Hintz and Patrick McCurdy, 101-122. New York: Palgrave Macmillan.

Wahl-Jorgensen, Karin, Lucy Bennett and Taylor. forthcoming. “The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations.” *International Journal of Communication*.