# Surveillance of Journalists/Encryption Issues

EINAR THORSEN
*Bournemouth University, UK*

Journalists and their sources across the world are increasingly vulnerable to digital attacks from state and nonstate adversaries, which can threaten source confidentiality and undermine news work. In a fast evolving global digital communications landscape, threats to journalists include digital surveillance and tracking of their activities; hacking and theft of data; disrupting operations through denial of service attacks and account hijacking; public shaming, online harassment, and cyberstalking; and confiscation or destruction of computer hardware as well as physical threats to persons. Lack of knowledge about how to integrate defensive measures and digital security such as encryption into everyday routinized news work is a considerable challenge for journalists and has been highlighted by a number of studies—for example, in UNESCO reports by Henrichsen, Betz, and Lisosky (2015) focusing on an international survey of journalists or Posetti's (2017) report on protecting journalism sources in a digital age; in Kleberg's (2015) report on digital source protection; in Bradshaw's (2015) study of U.K. 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, United Kingdom, and United States). Research has found journalists and their sources do not sufficiently understand data anonymization or digital communication security. They also highlight perceived lack of usability of encryption tools, which hinders their uptake among journalists. Such arguments are widespread in the journalistic community and put at risk the ability of journalists to guarantee the safety of their sources—be they whistleblowers or not—in a complex digital communications landscape.

Cryptography broadly describes principles that transform data to make it illegible to unintended audiences, establishing authenticity of data or communicators, and prevent unauthorized use of information. Encryption meanwhile refers to a specific form of cryptography that ensures confidentiality of information or communication by transforming legible data (plain text) into unintelligible data (ciphertext). These practices are not confined to digital communications, with early forms of cryptography used by ancient civilizations including the Egyptians and Greek, before Arab mathematicians adopted more sophisticated and systematic approaches around AD 800. The electromechanical rotor machine, Enigma, used by the Germans during World War II is one of the most famous examples of early encryption technology in the modern era. Alan Turing who worked for the British codebreaking center responsible for decrypting the Enigma machine, pioneered theoretical computer science and early concepts of

*The International Encyclopedia of Journalism Studies*. Tim P. Vos and Folker Hanusch (General Editors), Dimitra Dimitrakopoulou, Margaretha Geertsema-Sligh and Annika Sehl (Associate Editors).

DOI: 10.1002/9781118841570.iejs0272

artificial intelligence, demonstrating the close relationship between cryptography and the evolution of digital communication.

Cryptography is widely regarded as accepted and essential to protecting global information flows and communication networks, often denoted in less technical terms as just "secure communication" or "secure connection"—for instance, when a person is authenticating on a social network or online bank to establish a trust relationship. Here encryption plays a key role in the secure exchange of information between a client computer and the server and is integral to establishing trust (verifying the authenticity and identity of the communication partner), confidentiality, privacy, and sometimes anonymity of the communication. Cryptography is in other words widespread in our daily use of digital communications and integral to the operational logic of trade, commerce, governance, and so forth.

Public debates about cryptography, journalism, and citizens' right to privacy ignited in recent years following Edward Snowden's global security revelations in 2013. At the center of Snowden's revelations was the coordinated global mass surveillance by the NSA in the United States, GCHQ in the United Kingdom, and allied intelligence services in the Five Eyes Group, indiscriminately targeting *all* citizens' communications—as opposed to merely those citizens under suspicion or investigation. This sparked global outcry and fueled attention on how citizens and journalists might protect themselves from privacy intrusion. The full extent of Edward Snowden's NSA leak remains uncertain, but it is estimated that he has turned over at least 58,000 documents acquired while working at the NSA on behalf of Booz Allen Hamilton, one of the largest U.S. defense and intelligence contractors.

The first Snowden exposé was published in June 2013 by *The Guardian* and revealed the NSA had collected mobile phone records and metadata from than 120 million Verizon subscribers. Following this came a string of secret programs, each detailing the pervasive data gathering techniques deployed by intelligence services. The PRISM program (revealed in June 2013), allowed the NSA to access user data directly from the servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple (listed in order of entry to the program). GCHQ meanwhile was exposed for tapping into transatlantic fiberoptic cables (June 2013), under an operation codenamed Tempora. This purportedly went beyond metadata to include content of telephone calls, email messages, and other personal online activities. The NSA's Boundless Informant (June 2013) was designed to count, categorize, map, and visualize global communications metadata, which also revealed the extent of surveillance on citizens located within the United States. Another NSA tool, Xkeyscore (July 2013), reportedly covered "nearly everything a typical user does on the Internet"—including again the content of emails, web history, and metadata. Other revelations included the NSA monitoring conversations of 35 world leaders, including German Chancellor Angela Merkel (October 2013); NSA/GCHQ infiltrating online games such as World of Warcraft and Second Life (December 2013); NSA paying security firm RSA to build a flawed encryption system with a "back door" for intelligence analysts (December 2013); and GCHQ's Optic Nerve program that enabled bulk collection of Yahoo! webcam images (February 2014).

Cryptography plays an important part in ensuring secrecy of intelligence services and thus exposures of how they operate are often dependent on leaks from inside informants

or whistleblowers. They in turn, too, rely on cryptography to evade detection when communicating with journalists or other outsiders. Snowden, having saved classified documents to USB drives, initially failed to establish contact with Glenn Greenwald because he did not have the time to work out how to communicate via encrypted email. Snowden therefore decided to contact documentary maker Laura Poitras, who he knew used encryption, but did so via an intermediary Micah Lee of the Electronic Frontier Foundation to obtain her public encryption key. Snowden used the now defunct secure email provider, Lavabit, encrypted his messages using GNU Privacy Guard (GPG), used Off-the-Record Messaging (OTR) for instant messages, and routed all communication via the Tor network—having asked Lee to provide Greenwald with a Tails installation on a USB stick (a specialized version of Linux aimed at preserving privacy and anonymity). Tor is an anonymity network that defends against traffic analysis by sending encrypted information through a distributed network of volunteers, who in turn incrementally decrypts the message until it reaches its destination—in so doing obscuring the origin and final destination of the message by the intermediaries handling it. Tails is an operating system specifically designed to preserve privacy, anonymity, and leave no trace of activities on the computer it is being used.

This might seem like an impenetrable list of acronyms and technical language, but they broadly describe some of the safeguards and countermeasures available *and* necessary for journalists to preserve the privacy of their work and protect identity of sources. While Snowden's approach will have assumed a threat modeling of a highly advanced and persistent adversary (the U.S./U.K. intelligence services), other journalists may adopt less stringent approaches in certain areas to fit with practical demands of everyday news work and their personal risk assessment. However, mass use of encryption is widely regarded as important to aid the effectiveness of surveillance circumvention, a logic referred to by Penney (2013) as the "economics of privacy and mass surveillance." Increasing both the volume and complexity of messages intelligence agencies, spies or criminals have to decipher, makes surveillance more expensive, thus increasing the safeguards regular users have from mass or indiscriminate surveillance. 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. 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.

The popularity of mobile messenger apps like Signal and Telegram is contributing to changing behaviors and normalizing secure communication, since they provide user-friendly end-to-end encryption and privacy controls. Even one of the most popular messenger apps like WhatsApp has adopted end-to-end encryption, using the same protocol as Signal in partnership with Open Whisper Systems. Coupled with the use of VPN to protect data transmission, these solutions offer a simple and user-friendly starting point for journalists and sources to communicate securely. Journalists have also responded by adopting more advanced methods to protect their work and identity of sources, for example, using QubesOS that provides secure

compartmentalization of applications and relays internet traffic anonymously using Tor, or using bespoke hardware such as Blackphone provided by Silent Circle. Various news organizations across the world—including newspapers like *The Guardian* and *The New York Times*, websites such as BuzzFeed and The Intercept, broadcasters like NRK and CBC, and the Associated Press wire service to name a few—have deployed the open-source SecureDrop, which enables whistleblowers to submit information securely and anonymously over the Tor network.

Clearly challenging intelligence services or military about national security issues carried a significant risk—not just to digital integrity, but personal safety. Manning, Snowden, and some of the journalists they worked with have been subject to ferociously hostile attacks and death threats—particularly by those whose interests are served by preserving the operational secrecy of state governance. The degrading and inhumane treatment of Manning in solitary confinement during her pretrial detention in 2010–2011 and Snowden's exile in Russia since June 2013, demonstrate that these threats are far from empty rhetoric. In July 2013, meanwhile, *The Guardian* was forced by GCHQ to physically destroy computer equipment storing files provided to them by Snowden, using angle grinders and drills. Two months later David Miranda, partner of then *Guardian* journalist Greenwald, was detained under the U.K. Terrorism Act. This was subsequently deemed lawful by the high court, even though the judges acknowledged the detention had been "an indirect interference with press freedom." These are just some high profile cases in relation to national security specifically. Reporters Without Borders (RSF) and the Committee to Protect Journalists (CPJ) track violence and intimidation of journalists worldwide, revealing a stark problem for press freedom and impunity for crimes committed against media workers. According to the CPJ more than 1,000 journalists have been killed in the last 10 years alone, while RSF estimate that more than 180 journalists and more than 120 citizen journalists remain imprisoned. In response to these pressures, changes to how journalists communicate with their sources are precipitated both by the digital communication flows of the network society *and* the illusive nature of the various legal frameworks designed to protect them.

There are various legal assurances in more than 100 countries that allow journalists to protect their sources from identification. Several countries also have legislation to protect whistleblowers specifically from dismissal or lawsuits—typically imbued in statutes covering labor standards, employment rights, trading regulations, or protection against discrimination. Such laws afford protection for employees or agency workers who speak out against: health and safety violations, environmental damage, criminal offenses, or wrongdoing being covered up. Regardless of protective legislation, whistleblowers, and journalists working with them are frequently persecuted and sanctioned. The status of a source as a whistleblower is often contested, and the organizations they leaked information from call for punitive actions for breaking the law or failing to follow prescribed procedures. In this sense, it has been argued whistleblower legislation provides a symbolic or illusory form of protection, with laws containing loopholes, exemptions, and built-in weaknesses. Such threats are particularly pronounced when the wrongdoing involves government, military, diplomatic, or intelligence material. Indeed, several countries also have specific laws that prohibit the dissemination of information

classified as vital to protect national security interests, including: the U.S. Espionage Act; the Security of Information Act in Canada; and different Official Secrets Acts in India, Malaysia, New Zealand, Ireland, and the United Kingdom. Here "national security interests" supersede those of "public interest."

In recent years there has been a move toward strengthening surveillance powers across the world, often to the detriment of journalists' safety who are covered by draconian legislation either unintentionally or by design. The United Kingdom's Investigative Powers Act (also called the "Snoopers' Charter"), for example, came into effect in November 2016, granting comprehensive and far-reaching digital surveillance powers to police and intelligence services. While the Act offers a safeguarding measure for sensitive professions (including members of parliament, journalists, lawyers, doctors), these are widely regarded by privacy groups and free speech advocates as inadequate to protect journalists and would-be whistleblowers. Further provisions include legal obligations on communication service providers to assist with targeted interception of data, the removal of transmission encryption, and making it a criminal offense to reveal when data requests have been made. Similar legal powers are being debated in Australia, with protracted debates about how safeguards for journalists and news work should be worded to ensure they are effective protections. Other countries already have severe restrictions on encryption—either banning it outright or requiring a license for its use—including in China, Cuba, India, Iran, Libya, Malaysia, North Korea, Singapore, Sudan, and Syria. Even in the United States, encryption is classified as being a "dual use technology," ostensibly a tool that could be used as a weapon and therefore its export is regulated as a munition.

The Telegram app shot to prominence in the aftermath of the Snowden NSA/GCHQ revelations due to its user-friendly end-to-end encryption. Yet this app has also purportedly been used by ISIS as a group messaging tool to spread propaganda and was after the Paris attack in November 2015 reported as a possible communication channel terrorists use to plan logistics of attacks. While Telegram is just one example of "dual use technology" and how polarizing the discourse on cybersecurity can be, similar patterns exist in relation to most encryption technologies. Despite encryption being an accepted necessity for trade and commerce to function, use of encryption for privacy or surveillance circumvention is typically delegitimized by its association with criminal activity. This delegitimizing discourse posits that encryption is used by terrorists and criminals to evade detection and hinders effective intelligence gathering, and law abiding citizens and journalists should have nothing to fear. This ignores the widely accepted view in cyber security and cryptography fields that providing backdoors for intelligence agencies to bypass encryption is a fundamentally flawed logic, since it is impossible to control the access to or abuse of these weaknesses.

However well intended, any backdoor to bypass encryption will paradoxically undermine not only the ability of your adversary to communicate securely, but also enable them to strategically target weaknesses in our own communication systems. The WannaCry ransomware that nearly brought the NHS to a halt at the start of the 2017 U.K. election campaign, for example, was spreading via a Windows exploit stolen from the NSA. That is, the NSA identified the vulnerability and used it to create a backdoor for its own offensive surveillance work rather than reporting it to Microsoft to be

patched—exposing weaknesses in the very same principles and methods advocated by the U.K. government as part of its Investigative Powers Act.

Corporations named in Snowden's global surveillance disclosures have now begun to seek "commercial opportunities in privacy" (Bakir & McStay, 2015). Here corporations are simultaneously seeking to protect the privacy of customers against state surveillance (e.g., Apple's refusal to comply with an FBI request and court order to develop software to bypass its iOS encryption following the San Barnardino terrorist attack in December 2015), while also building business models on the surreptitious exploitation of personal data and behavior modeling (e.g., Google and Facebook). This interoperability of state and private interests, and indeed use of secrecy for their preferment, dramatically complicates efforts to hold these powers to account.

Encryption is important for the protection of civil liberties, as highlighted by UNESCO's 2016 report on encryption and human rights, and essential for ensuring confidentiality and trust in journalism–source relationships. Further research is needed to find ways of countering the delegitimizing discourse concerning encryption and further our knowledge about the rapidly evolving dynamics of digital threats against journalists and their sources. This concerns not just the technologies of surveillance, but international and national policies that enable and legitimize erosion of journalistic freedom.

SEE ALSO: Anonymous Sources and Source Confidentiality; Leaks; Privacy Laws; Source Protection and Shield Laws; Violence against Journalists; Whistleblowers

## References

Bakir, V., & McStay, A. (2015). 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.

Bradshaw, P. (2015). Chilling effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations [Special issue]. *Digital Journalism, 5*(3), 334–352.

Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). *Building digital safety for journalism: A survey of selected issues*. Paris, France: UNESCO.

Kleberg, C. F. (2015). *The death of source protection? Protecting journalists' source in a post-Snowden age*. London, UK: LSE Polis.

Lashmar, P. (2016). No more sources? The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice, 11*(6), 665–688. doi:10.1080/17512786.2016.1179587

Penney, J. W. (2013). The cycles of global telecommunication censorship and surveillance. *SSRN Electronic Journal, 36*(3), 693–753.

Posetti, J. (2017). *Protecting journalism sources in the digital age*. Paris, France: UNESCO.

## Further reading

Schulz, W., & Van Hoboken, J. (2016). *Human rights and encryption*. Paris, France: UNESCO.

Thorsen, E. (2017). Cryptic journalism: News reporting of encryption. *Digital Journalism, 5*(3), 299–317. doi:10.1080/21670811.2016.1243452

Thorsen, E. (2017). Whistleblowing in a digital age: Journalism after Manning and Snowden. In B. Franklin & S. A. Eldridge (Eds.), *The Routledge companion to digital journalism studies*. New York, NY: Routledge.

**Einar Thorsen**, PhD, is associate professor of journalism and communication and head of research for the School of Journalism, English and Communication at Bournemouth University. His research covers online journalism, citizens' voices, and news reporting of crisis and political change—inextricably linked with protecting freedom of speech, human rights, and civil liberties—especially for journalists, vulnerable people, marginalized groups, and in contexts or countries where such liberties are being curtailed. He has also published articles on online communication security, whistleblowers in the digital age, public service media online, Wikinews, and WikiLeaks. Dr. Thorsen is currently co-directing Media Action Against Rape (MAAR) with Dr. Chindu Sreedharan, a GCRF funded research and capacity building project by Bournemouth University and UNESCO in New Delhi.