Ethical issues in large-scale journalistic investigations

Gillian Phillips

Abstract

The advent of large-scale journalistic investigations based on "big data" is a relatively recent phenomenon. The exponential growth in the volume of data being stored and generated by state and private entities and the tendency to centralize that storage, while allowing too many people access to it, has created a structural vulnerability. This has enabled disgruntled employees or contractors to access, copy, and leak vast amounts of such data. Such leaks have resulted in information of huge public importance being published by journalists and media outlets, and have led to government inquiries, political resignations, tax reform, and numerous criminal prosecutions. Standing behind a journalist's activity where use of big data is concerned is the public interest. It justifies a journalist accessing and interrogating that data, it underpins follow-up inquiries and investigations, and, ultimately, it justifies what is published. But the public interest is a singularly ill-defined concept. This chapter aims to examine, from a UK perspective, some of the ethical issues that arise for journalists working on "big data" leaks, including how such "big data" is obtained, stored, shared, searched, interrogated and analyzed, and published, and where the public interest sits in this process.

"[O]*ur job is to receive [information] responsibly and to publish or not by our own unvarying news standards*." (Max Frankel, Former Executive Editor, *The New York Times*, 2011)

Introduction

The advent of large-scale journalistic investigations based on "big data" is a relatively recent phenomenon. It has come about mainly, if not solely, because of the exponential growth in the volume of data now being stored and generated. As the General Counsel at the Center for Investigative Reporting, put it:

> Since about 2008, the explosion of data journalism – defined as journalism that heightens the role numerical information plays in storytelling – is now a driving force in newsrooms around the country. Journalists are quickly learning how to obtain troves of data through electronic leaks, drones, and cutting-edge computer programs that sometimes require little more than the click of a button to access information. In other instances, journalists confronted with processing large swaths of information must employ complicated algorithmic and programming skills. Many larger news organizations have even built internal digital programs and tools to sort through these data swells and leaks – as was done with the Panama Papers. (Baranetsky, 2018, p. 1).

The tendency of state and private entities to centralize and store vast quantities of information and allow too many people access to it has created a structural vulnerability. This has enabled disgruntled employees or contractors, such as Chelsea Manning, Edward Snowden, and HSBC leaker Hervé Falciani, to access, copy, and leak vast amounts of data. Random acts of carelessness, such as documents or laptops left on trains or in cars, have resulted in highly confidential and personal details being circulated. Deliberately illegal acts, such as that by

Football Leaks hacker, Rui Pinto, have resulted, in some instances, in wholesale dumps of unexpurgated, highly personal data (Sony, Ashley Madison, TalkTalk). Huge volumes of leaked data have become available from all sorts of sources, including governments (in 2010, WikiLeaks published 400,000 pages of leaked United States government documents and diplomatic cables; in 2013, Edward Snowden leaked 1.7 million documents from the US's National Security Agency and other friendly government surveillance programmes); politicians (in 2016, the US Democratic National Committee's computers were hacked); and businesses (the Panama and Paradise Papers leaks). Such leaks have seen information of huge public importance published and have led to government inquiries, political resignations, tax reform, and numerous criminal prosecutions.

This chapter aims to examine, from a UK perspective, some of the ethical issues that arise for journalists working on "big data" leaks, including how such "big data" is obtained, stored, shared, searched, interrogated and analysed, and published, and where the public interest sits in this process.

The crucial role of the public interest

Standing behind a journalist's activity where use of big data is concerned, is the public interest. It justifies a journalist accessing and interrogating that data; it underpins follow up inquiries and investigations and, ultimately, it justifies what is published. But the public interest is a singularly ill-defined concept. No single homogenous definition exists (Foster 2007, Elliott 2010). In many jurisdictions a narrow, restrained definition is used. In a UK context, some points of reference can be found in the 2019 Crown Prosecution Service's Legal Guidance on "assessing the public

interest in cases affecting the media." While this notes (p. 2) that "neither journalists nor those who interact with them are afforded special status under the criminal law," it provides that separate consideration must be given to any public interest that may exist in the journalistic endeavour and identifies as a critical question "whether the public interest served by the conduct in question outweighs the overall criminality" (p. 4). It sets out a three-stage approach to this question: assess the public interest served by the conduct in question; assess the overall criminality; and weigh up these two considerations (pp. 7-8).

UK editorial codes, such as those applied by Ofcom, the BBC and IPSO, employ remarkably similar approaches to their definitions of public interest. Journalists act in the public interest, these codes say, when they

1. expose crime, wrongdoing, serious impropriety or injustice,
2. prevent the public from being misled,
3. protect public health and safety; or
4. reveal information which helps the public make decisions of importance.

What level of public interest is needed to justify any publishing of leaked data, will depend on a number of factors, including but not limited to the level of intrusion, the seriousness of the allegation, and who the subject matter is. It may also involve consideration of how material was obtained. A publisher should normally consider what level of public interest it believes is appropriate to justify publication. While low level public interest justifications, such as exposing hypocrisy, may be sufficient as a balance to/defense for a (civil law) breach of confidence or a

privacy claim, they may not be sufficient where there has been a very high level of criminality involved. But each case will depend on its own facts. Editors will have to make their own determinations, in all the circumstances, as to whether they believe there is a sufficient public interest in publishing any particular story.

How is the public interest ascertained?

Where there has been some sort of prior sift, whether by an intermediary or source – who may not feel constrained by the ethical restraints of a journalist – that person can pass on initial background information to the journalist, and hopefully highlight what the public interest in examining and publishing the information might be. Both Chelsea Manning and Edward Snowden were familiar with their material, knew why they were leaking it, had formed their own belief about the public interest (the harm or damage caused to the public by not knowing), and passed all this knowledge on, either directly or through intermediaries to the journalists. If nothing is passed on about the content of the material, a journalist may be in the dark as to whether there is any public interest to justify examining the material, let alone publishing it. This scenario – the blind data dump – is particularly problematic where a journalist is the passive receiver of leaked information, knows nothing of its content or the motive for the leak. A possible approach here, which fits with normal journalistic inquiry and investigation, is to regard the anonymous sending of material to a journalist in this way as creating an implication that it must be being sent with a public interest motivation, and so it is appropriate and responsible, at the very least, for a journalist to investigate and interrogate that material and come to their own conclusion as to whether there is any public interest in it.

Take, for example, the secure drop systems operated by many news organizations. It may not be obvious how material deposited was obtained or what is in it. The *Guardian's* secure drop system tries to meet this concern via a pulldown selective menu of options:

> You don't have to give us a way to contact you, but it can be useful for us to be able to do so. It can also help us if you are able to provide some background about what is in the documents, and why you think they might be of interest to us. We can correspond with you on SecureDrop, or you can use SecureDrop to confidentially provide us with other contact information (*Guardian*, 2017).

Identifying a possible public interest at the outset of any investigation of such data is not solely an ethical matter; it also has legal ramifications, at least in the UK, as a consequence of laws around breach of confidence, misuse of private information and data protection. As suggested, at the initial stage, when material has been received, to examine it, particularly where it may contain private, personal, or confidential information, a journalist should have and be able to demonstrate they had a reasonable belief in a possible public interest (see for example the journalism exemption for processing personal data in the Data Protection Act, 2018). To evidence a possible public interest, it is advisable to have in place and – at least in more serious instances – to document an editorial approval process assessing and reviewing, on an on-going basis, the public interest.

Obtaining big data

Passive receipt versus active pursuit

Journalists generally get access to big data material because they are given it (whether anonymously or via a known source such as a whistleblower/leaker or because a third-party intermediary is passed the information and facilitates access to it). Journalists rarely directly obtain big data information. Exceptions include documents unearthed from abandoned state ministries in the aftermath of wars, such as those gathered by the Daily Telegraph's foreign correspondent, David Blair, from the ruined foreign ministry in Baghdad in April 2003, and the thousands of files gathered by journalists from *The New York Times* from Islamic State offices in Mosul in 2018.

In many of the recent big-data leaks, journalists were not implicated or involved in the initial obtaining of the material: It was provided to them as passive receivers. Examples where journalists were not implicated in the initial leaks include the Edward Snowden leaks from the US National Security Agency in 2013, the leaks of information on tax evasion schemes from the Swiss subsidiary of the British multinational bank HSBC in 2015, as well as the journalistic investigations known as the Panama and Paradise Papers in 2016 and 2017, and the Football Leaks in 2018. A more recent example is Operation Car Wash, the June 2019 reporting by the online investigative website, The Intercept, on government corruption in Brazil (Allsop, 2019). Where an external third-party gains unauthorised access to information stored on a private computer system or internal network - otherwise known as "hacking" - that will inevitably involve some element of criminality by that third party. Whatever the motive or intent of that party for obtaining access – they usually have no professional or employment relationship or connection to the organizations they hack (see for example Football Leaks hacker Rui Pinto in Allsop, 2019)) and may have only a vague or even no idea what the information they hack will

reveal – those obtaining material through putatively criminal means will be vulnerable to criminal prosecution (*Bartnick v Vopper,* 2001). In many jurisdictions, even internal leakers who have not employed criminal means to access information, may still find themselves vulnerable to criminal prosecutions by the state.[1] Blowing the whistle almost inevitably involves personal risk for the individual behind the leak. Journalists, because of their right and duty to receive and impart information (accorded by most international conventions that recognize freedom of expression, including the US Constitution, the International Covenant on Civil and Political Rights and the European Convention on Human Rights, among others) have more protection.

In the US, as long as a journalist is a passive receiver of such material and have not themselves engaged or assisted in its unlawful obtaining, case law and practice has suggested they should not be vulnerable to prosecution (*Bartnick v Vopper,* 2001, *New York Times Co. v. United States*, 1971). However, the announcement in May 2019 by the US Justice Department, that Julian Assange, the founder of WikiLeaks, was being charged under the Espionage Act for his connection to the 2010 leak by Chelsea Manning of confidential military and diplomatic documents, suggests this may not be as clear cut a proposition as has been assumed (*USA v Assange,* 2019). The proposition that Assange violated the Espionage Act, and so committed a criminal offence, by "soliciting, obtaining, and then publishing" classified information, highlights a potential vulnerability for any investigative journalist who gets too close to their source; a journalist who receives a one-off anonymous dump of information may be in a better position than one who maintains any sort of on-going relationship with a source. Similar threats of criminal prosecution of journalists have been issued in the UK[2].

Some reassurance for journalists in the UK who are the passive recipients of big data leaks is, however, provided by the Crown Prosecution Service's Legal Guidance (CPS, 2019, pp. 3-4, 7-8). Even if a journalist is not vulnerable to criminal action, as with any case where a journalist receives a leak of information, big or small, they may still be vulnerable to attempts, through criminal and civil process, to discover the source of the leak (see below) and to pressure to handover or return, or delete or destroy, the data. In a number of jurisdictions since 2018, police have searched journalists' offices and homes, seized computers or have used statutory powers to seize journalists' telephone records from telephone providers, all with a view to locating the source of leaks. Civil processes have also been deployed to try to locate an internal source (*Interbrew v Financial Times*, 2002; see also endnote 2 on the efforts of the UK government in 2019 to find the source of the leaked internal emails from UK Ambassador to the US).

As with any investigation, whether it is based on a big data leaks or not, where a journalist themselves actively engages in criminal activity to obtain information, they put themselves at the mercy of prosecutors and the criminal justice system. In the UK, a journalist may be able to justify employing criminal methods to obtain material, if there is a strong public interest in the subject matter of their investigation; that is not to say that they are not potentially guilty of criminal activity, but it may not be considered to be in the public interest to prosecute them (CPS, 2019, pp. 7-8; See also *Guardian* 2012, Sweney).[3]

Relationship with sources

The standard journalistic ethic that a journalist should avoid getting too close to a source - as this can compromise both their independence and objectivity - applies equally to big data leaks. If a

journalist actively encourages or assists a source to obtain material, the ground is legally and ethically complicated; if they become too directly involved in the source's activities, they may put themselves in the firing line for a criminal prosecution. A considerable part of the US government's indictment of Julian Assange under the Espionage Act, relates to his relationship with his source, Chelsea Manning. One of the many things he is accused of is trying to persuade his source to disclose more secret information (*USA v Assange*, 2019).

Civil law issues

Even if no criminal act is involved, internal leaks of data will inevitably involve some element of breaching private law rights (an employment contract or confidentiality) by the leaker. Separate from criminal law, as mentioned above, there may be civil law consequences for both the source who obtains, and the journalist who receives, leaked material. Journalists receiving or threatening to publish material received in these circumstances can find themselves caught up as third parties in civil law actions, such as applications seeking prior restraint of publication or disclosure of sources or for information to be returned or destroyed. This can arise particularly where, before publishing, a journalist (responsibly and ethically) approaches the person or organization who is to be the subject of their story, and tells them the gist of the story that they are proposing to write; if their information is derived from a leak, such an initial approach may reveal that the journalist has information they should not have, and so creates a risk of them being subjected to a prior restraint or source disclosure application.[4]

The storage, sorting, and sharing of big data

Once material has been received and a decision taken that it is in the public interest to interrogate it, consideration needs to be given to a number of practical matters: How and where is the material to be securely stored, and who is to be able to access it and how? Unlike the 7,000 odd pages of the Pentagon Papers leak in 1971, big data material is rarely manually handed over to newsrooms in cardboard boxes. Documents are often transmitted electronically to newsrooms through special security tools, or via encrypted data storage devices. The material needs to be searched, (normally with dedicated tools), to further determine what of it is in the public interest and worth publishing. In many cases, it will be necessary to carry out all of this initial sifting and interrogating under the strictest conditions of secrecy. Bill Keller, writing in the *NYT Magazine* about the initial contact from the *Guardian* about the Wikileaks documents, described it as a "cloak-and-dagger" adventure that combined the intrigue of "handling a vast secret archive with the more mundane feat of sorting, searching and understanding a mountain of data" (Keller, 2011, p. 1).

Legally and ethically, leaked data must always be kept securely. The *Guardian* kept a downloaded set of Edward Snowden's NSA documents at its London offices, in a room it called "the bunker." The door was kept locked, and a guard was stationed outside. Before entering, basic security measures such as window coverings and those people allowed in being required to leave their phones and any other personal electronic devices on an outside table were used. New laptops, unconnected to the Internet or to any other network, were deployed, and the documents were kept on these computers in encrypted file containers. Accessing each container required three passwords, and no individual knew more than one. On the Paradise Papers, the *Guardian* team worked from a designated project room, which was separate from the main newsroom. This

room was kept locked when not in use and was only accessible to those working on the project. Access to the data was managed using a secure online portal, which allowed journalists to search and interrogate the data remotely. Using an I-Hub platform, *Guardian* journalists were able to liaise with journalists from other members of the consortium and were able to exchange information about significant findings arising from their respective interrogations of the data. All those who were part of the collaboration communicated via encrypted channels. Printing of copy documents and electronic downloads were kept to a minimum, and hard-copy or electronic documents obtained were only kept where relevant to the stories on which the journalists were working at the time. Documents that were no longer needed were physically destroyed or permanently deleted on a rolling basis. In addition, journalists had designated "clear outs" at specific points in the investigation in respect of both physical documents, which were shredded, and electronic documents, which were permanently deleted from internet caches, download folders and any encrypted storage devices that were used by journalists.

The need to keep material safe and secure also plays out on another ethical plane: that of protection of sources. Nowadays, most law enforcement and government agencies know that digital communications leave footprints, allowing the source, recipient, or both to be identified, thus making it easier for authorities to initiate prosecution proceedings. There are various legal surveillance and technological tactics in place that allow the intelligence community and law enforcement to access electronic communication records and ascertain what information has been shared with journalists. Because of this problem, tools like SecureDrop and other open-source systems have been developed and used by media institutions to securely transfer documents without revealing a source's identity. Some newsrooms have sought to counter

tracking and tracing problems by creating new documents altogether before publishing, so that any possible watermarks or signage is completely removed. Additionally, newsrooms employ traditional tactics like redactions, verification, and anonymous sourcing as well as stripping electronic documents of all metadata.

From a purely practical perspective, the size of big data leaks means that without a serious amount of human input it is hard to ensure the full redaction of libellous or private information. Making redactions requires a lot of time and legal input, but getting redactions wrong can have consequences. As a basic tenet of defamation law, anything a newsroom publishes – even if it is contained in third-party documents – can trigger liability; a lack of careful or sufficient redaction may lead to possible liability and expensive litigation.

Searching, interrogation, and analysis

Notwithstanding the development of new technical tools to search and analyse material, standard news gathering checks around verification of documents, names, dates, places, interviewing of sources, and seeking official responses still need to be done. In any investigation based around big data, while the initial interrogation may be strictly managed, limited, and narrowly defined, once information starts to emerge and results are produced, the ambit of the public interest may shift and develop as new lines of inquiry emerge. With this, the parameters of where the public interest lies will evolve and develop over time, and so should be kept under review. Sending right to reply letters and seeking official responses in a timely fashion can be a key part of this process. The public interest in each stage of an ongoing investigation of this nature will need to be continuously considered and monitored.

Publication

Consideration will need to be given, one final time, to the selection of the stories that are to be written and to what, if any, of the original underlying material – as opposed to commentary based on it – will be published. This again will involve an editorial assessment of the public interest. Anything published needs to be done within the existing legal framework: defamation, privacy, confidentiality and data protection, but also contempt and copyright. There are other more nuanced concerns. If material is to be published, does it put individuals or their families at risk? Are identities of intelligence operatives revealed or compromised? Are sources protected? Where leaked documents are classified, difficult decisions have to made. Editors have to balance the value of the material to public understanding against the potential dangers to the national interest.

In a November 2010 editorial coinciding with the publication of the first stories based on the US embassy cables, *The New York Times* described what it had done to exclude information that could endanger confidential informants or compromise national security; it shared its redactions with the other news organizations it worked with, as well as with WikiLeaks "in the hope that they would similarly edit the documents they planned to post online." The *Times* also sent the Obama administration the cables it planned to post and invited them to "challenge publication of any information that, in the official view, would harm the national interest." Suggested government redactions were considered and some, but not all, agreed to. These too were shared with the other news organizations and Wikileaks (New York Times, 2010).

Conclusion

While the public interest is important in any journalistic investigation, where large-scale investigations based on leaks of data are concerned, it is absolutely key at every stage of the process that journalists believe they are acting in the public interest and can demonstrate that. Glenn Greenwald, in court testimony, explained of the NSA leaks: *"*We began to publish stories after carefully assessing the risk of publication, and the importance of the public interest involved. Those editorial decisions involved... input from very experienced professionals...That was the case from the very beginning and continues to be the approach to this day" (Greenwald quoted in Millar, 2013, slide 3). What is becoming increasingly apparent is that it is important that this process of identifying and refining the public interest is documented and recorded. Care must be taken, generally through painstaking redaction processes and pre-publication dialogue, to ensure that nothing is published that could imperil sources, compromise operations, or put individuals at risk. And all of this is underpinned at every stage by a public-interest imperative.

Further reading

Bartlett, G. & Everett, M. (2017, May 2). The Official Secrets Acts and Official Secrecy. House of Commons Library Briefing Paper, No CBP07422. Retrieved from https://researchbriefings.files.parliament.uk/documents/CBP-7422/CBP-7422.pdf

IPSO Editor's Code and Codebook (2019, July 1). Retrieved from https://www.ipso.co.uk/editors-code-of-practice/editors-code-resources/

Leigh, D. (2019). Investigative Journalism. A Survival Guide. *Palgrave Macmillan.*

Silver, D.A. (2008). National Security and the Press: The Government's ability to prosecute journalists for the possession or publication of national security information. *Communication Law and Policy* 13(4): 447–48.

References

Allsop, J, (2019, August 2). The complex case of Rui Pinto. *Columbia Journalism Review.* Retrieved from https://www.cjr.org/watchdog/rui-pinto-football-leaks.php

Baranetsky, D. Victoria, (2018, September 19). Data Journalism and the Law. *Columbia Journalism Review.* Retrieved from *https://www.cjr.org/tow_center_reports/data-journalism-and-the-law.php*

Bartnicki v. Vopper, 532 U.S. 514 (2001) Retrieved from https://supreme.justia.com/cases/federal/us/532/514/

Carranca, A. (2019, August 2). Can the president of Brazil jail the Intercept's Glenn Greenwald for publishing leaks? *Columbia Journalism Review.* Retrieved from https://www.cjr.org/analysis/the-intercept-greenwald-brazil-soccer.php

CPS, 2019 Crown Prosecution Service. (2019, November 11). Legal Guidance: Media: Assessing the Public Interest in Cases Affecting the Media. Retrieved from https://www.cps.gov.uk/legal-guidance/media-assessing-public-interest-cases-affecting-media

DPA, 2018 Data Protection Act 2018, Schedule 2, Part 5 para.26. Retrieved from http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/enacted

Elliott, C. (2012, May 20). The readers' editor on …. How should we define 'in the public interest' *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2012/may/20/open-door-definition-public-interest

Foster, S (2007, August 28). Interesting or in public interest? *UK Press Gazette*. Retrieved from https://www.pressgazette.co.uk/interesting-or-in-public-interest/

Frankel, M (2011) former executive editor NYT, in a memo sent to the NYT public editor at the time of the Pentagon papers; quoted by Alan Rusbridger in the Introduction to Leigh, D. & Harding L., WikiLeaks. Inside Julian Assange`s War on Secrecy (2011), p 20.

Guardian, 2012, (2012, May 29). CPS statement on decision not to charge police officer or Amelia Hill. Retrieved from https://www.theguardian.com/media/2012/may/29/cps-statement-police-amelia-hill

Guardian, (2017, March 17). How to contact the Guardian securely. Retrieved from https://www.theguardian.com/help/ng-interactive/2017/mar/17/contact-the-guardian-securely

Interbrew SA v Financial Times Ltd & Others [2002] EWCA Civ 274; [2002] EMLR 446 Retrieved from https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWCA/Civ/2002/274.html&query=(Interbrew)+AND+(SA)

Keller, B. (2011, Jan 26). Dealing With Assange and the WikiLeaks Secrets. *New York Times Magazine*. Retrieved from https://www.nytimes.com/2011/01/30/magazine/30Wikileaks-t.html?mtrref=www.google.com&gwh=25D9738F7C5A2313ED8CC9300B45B40B&gwt=pay&assetType=REGIWALL

Mason, R. (2019, July 15). Theresa May refuses to defend journalists' right to publish leaks. *The Guardian.* Retrieved from https://www.theguardian.com/media/2019/jul/15/theresa-may-refuses-to-defend-journalists-right-to-publish-leaks

Millar, G. (November 2013). Publishing the Snowden Secrets: The Guardian, the government and the people. (Slide Presentation). Retrieved from https://slideplayer.com/slide/3874483/

New York Times editorial, (2010, Nov 29). Retrieved from https://www.nytimes.com/2010/11/29/world/29editornote.html

New York Times Co. v. United States, 403 U.S. 713 (1971). Retrieved from https://supreme.justia.com/cases/federal/us/403/713/

Sweney, M. (2012, June 14). Police advised not to pursue prosecution of Guardian journalist *The Guardian.* Retrieved from https://www.theguardian.com/media/2012/jun/14/police-guardian-journalist-phone-hacking

USA v Assange: Superseding Indictment. (2019, May 23). Retrieved from https://int.nyt.com/data/documenthelper/1037-julian-assange-espionage-act-indictment/426b4e534ab60553ba6c/optimized/full.pdf#page=1

Endnotes

[1] See, e.g. in the US, the cases of Chelsea Manning and Reality Winner, and threats against James Risen and Edward Snowden; in the UK, cases against Sarah Tisdall, Clive Ponting, Richard Tomlinson, David Shayler and Katharine Gun, to name but a few.

[2] In 2019, following publication by the *Daily Mail* newspaper of leaked diplomatic cables from the British ambassador to the US, Sir Kim Darroch, police issued a statement warning editors not to publish such leaks because it could be a breach of the Official Secrets Act (OSA). Later, the police partially retreated from that position, saying it "respects the rights of the media and has no intention of seeking to prevent editors from publishing stories in the public interest in a liberal democracy." However, it added: "We have also been told the publication of these specific

documents, now knowing they may be a breach of the OSA, could also constitute a criminal offense and one that carries no public interest defense" (Mason, 2019).

[3] The Metropolitan Police has used powers under the Regulation of Investigatory Powers Act 1998 to seize journalists' telephone records; in August 2018, police in Northern Ireland arrested two journalists and searched their homes and offices over a suspected leak; in September 2018, Italian police searched the home of an investigative journalist, in Palermo (Sicily), on the orders of prosecutors as part of an investigation into a suspected leak from a judicial investigation; in February 2019, police in San Francisco obtained and implemented a "without notice" warrant to conduct remote monitoring on a journalist's telephone number, and later raided his home and offices and seized computers and other electronic devices; in May 2019, in France, prosecutors subpoenaed journalists from an investigative website and pressed them to reveal the source of a story about the use of French made weapons in the conflict in Yemen; in June 2019, Australian Federal Police obtained and implemented search warrants against two media organizations and their reporters; in July 2019, in the aftermath of Operation Car Wash, the Brazilian President told journalists in Rio de Janeiro that Glenn Greenwald could "do time" in Brazil.

[4] While this is unlikely to occur in the US following *The New York Times* case, it is a more realistic proposition in the UK and other countries with a similar system of law, such as Australia and Canada.