Surveillance

Current Debate & Key Players

- In today's world, characterised by big data surveillance, enormous amounts of data are sucked up by systems that store, amalgamate, and analyse that information, in turn suggesting patterns and trends that play a key role in security, marketing and governance.

- In 2013, Edward Snowden, a former security contractor for the US National Security Agency (NSA) approached journalists to reveal mass surveillance of innocent citizens by Western security bodies on a broad scale.

- Reporters, who performing the role of watchdog media rely on confidential communication with each other and with sources to hold governments and other elected officials to account have also been caught up in the vortex of bulk information-gathering1. For e.g. emails from the New York Times, the Guardian, Reuters, the BBC, Le Monde, the Sun, NBC and the Washington Post were stored by Britain's GCHQ spying agency as part of a test exercise, documents revealed by Snowden revealed.

- In addition, one of the restricted documents destined for army intelligence warned that "journalists and reporters representing all types of news media represent a potential threat to security", adding: "Of specific concern are 'investigative journalists' who specialise in defence-related exposés either for profit or what they deem to be of the public interest2" – otherwise referred to by Lyon (2015) as 'bad needles' [from the perspective of the security agencies]. This raises the ominous spectre of journalists being specifically targeted as threats as opposed to being simply, though no less gravely, swept up along with terrorist suspects in a "web of surveillance" (Lyon, 2015, p.24).

- Surveillance and 'sousveillance' by the media in Western democracies (Mann and Ferenbok 2013), tend towards a form of relative equilibrium based on a form of action-reaction 'game' between States and media professionals: journalists and the platforms they use for communication with each other and with confidential sources - such as Google, Skype - counter attempts at surveillance by state entities, in particular intelligence agencies and the police, through both technology and political action.

- Historically, in mature democracies of Western societies, there is an institutional system of checks and balances, including for the most part relatively independent judicial systems that allow for the maintenance of such equilibrium, on the basis that

[1] http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post?CMP=Share_AndroidApp_Gmail
[2] http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post?CMP=Share_AndroidApp_Gmail

journalism's core raison d'être is to hold power accountable. However, in recent years, in a number of Western democracies there is now a growing tendency towards the weakening of democratic oversight, mechanisms and entities, which poses a threat to the state of equilibrium.

- The technological capacity of capturing and processing large amounts of data is being coupled with institutional changes that put forth new legislative actions underway.

- Western democratic states are intensifying efforts to pass more all-encompassing surveillance frameworks, from indirect practices such as assigning ISPs with new roles as surveillors of data traffic to the back-door circumvention of encryption. This could involve special keys that would allow governments to access encrypted data when investigating terrorists and other criminals.

- Such efforts are further accompanied by other restrictive state security legislation like Spain's new Citizens Security Law, also known as the gagging law, which prohibits "the unauthorised use of images of police officers that might jeopardise their or their family's safety or that of protected facilities or police operations3", further reducing the space for watchdog journalism.

- Normatively, Western governments seeking intensified surveillance argue that a lack of transparency is necessary for security reasons. For eg. in the US the Foreign Intelligence Surveillance court meets in secret as part of the surveillance process. And in France a recently-passed surveillance law, compared by some observers to the US Patriot Act, grants state intelligence agencies broader powers to spy on citizens but lacks oversight and transparency, and threatens civil liberties, rights campaigners warn.

- Surveillance tactics, technologies and legislation impact on journalists' priorities in fulfilling their watchdog role, because of among other things a chilling effect on whistle-blowers and other confidential sources.

- The attempts by journalists to retain space in which to do their jobs challenging power and holding public officials to account tends to suffer every time there is a terrorist attack. In the immediate aftermath of attacks like those on September 11 or in the following years in Madrid, London, and more recently Paris and Brussels the balance of public discourse tilts towards security over privacy. Legislation such as the Patriot Act is passed that not only infringe on the liberties of ordinary citizens but make it more difficult for free journalists to do their job. As the years pass, the surveillance capacities that can be coupled with such legislation have grown exponentially, so with each new attack the cumulative threat to journalism is even greater.

- Journalists have become aware of the need to protect sources for example through the use of encryption tools, but also to also protect the functions of journalism as free from interference, through the use of advocacy platforms, such as press freedom civil

[3] http://www.theguardian.com/world/2015/aug/16/spanish-woman-fined-gagging-law-photographing-police

society organisations to push back with legal challenges. They are developing counter tools to protect and/or construct safe communicative spaces within which they can pursue the coverage of, especially, sensitive stories to counter any slide into subdued, ephemeral democracy.

Key players:

US & UK governments and their respective intelligence agencies, in particular NSA and GCHQ (both responsible for data surveillance).

Mass surveillance of innocent citizens by these two states lay at the heart of the Snowden revelations. The US reformed the mass surveillance system ushered in through the post 9/11 Patriot Act, through the Freedom Act, but surveillance of US citizens is still intense and pervasive. The UK meanwhile, despite the Snowden revelations is attempting to pass the IP Bill, which would expand surveillance powers.

Other Western democratic states

From France, the Netherlands and Spain, to Austria, Hungary and Poland, are all seeking to – or have already passed – surveillance laws that result in decreased democratic transparency and oversight and increased surveillance capacities.

The Council of Europe

In a post-Snowden report on mass surveillance it said: "The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 European Convention on Human Rights (ECHR)), freedom of information and expression (Article 10, ECHR), and the rights to a fair trial (Article 6, ECHR) and freedom of religion (Article 9) - especially when privileged communications of lawyers and religious ministers are intercepted and when digital evidence is manipulated). These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardizes the rule of law." Its human rights commissioner Nils Muiznieks has warned that a series of Western European countries are threatening democratic rights, in particular the right to privacy and free expression, through increased surveillance laws.

The United Nations Office of the High Commissioner for Human Rights

UN Special Rapporteur on the protection and promotion of human rights while countering terrorism Ben Emmerson has urged Governments involved in mass surveillance of the internet for counter-terrorism purposes to update their national legislations in line with international human rights law for new technology surveillance measures:

"States need to squarely confront the fact that mass surveillance programmes effectively do away with the right to online privacy altogether," he said the, during the presentation of a report to the UN General Assembly on the use of mass digital surveillance for counter-terrorism purposes, and the implications of bulk access technology for the right to privacy. "I don't accept the analogy that sending an email is like sending a post-card. States' obligations under the International Covenant on Civil and Political Rights include respecting the privacy and security of digital communications … Measures that interfere with the right to privacy must be authorised by accessible and precise domestic law that pursues a legitimate aim, is proportionate and necessary … Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right to privacy … States should be transparent about the nature and extent of their internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use."

He also urged states to provide a detailed and evidence-based public justification for the systematic interference with the privacy rights of the online community by reference to the requirements of article 17 of the Covenant: "We need strong and independent oversight bodies that are adequate for a review before these programmes are applied … Individuals must have the right to seek an effective remedy for any alleged violation of their online privacy rights."

Journalists

Disproportionately threatened by increased, less accountable surveillance because it makes it much more difficult for them to enjoy the secrecy among themselves and with sources that is vital if the media is to continue to play a watchdog role in democratic society.

Whistleblowers

Core to exposing wrongdoing, whistle-blowers are more reluctant to come forward and contact journalists for fear that they are more easily identifiable through expanded surveillance. A key element of democratic oversight and accountability is thus threatened.

Civil society (including NGOs, hacktivists etc)

Civil society NGOs such as the Committee to protect Journalists, the Electronic Frontier Foundation, the American Civil Liberties Union, as well as activists (including hacktivists), advocate for the protection of privacy on the Internet and seek to counter through campaigns as well as legal challenges policy moves towards greater surveillance.