Chapter 11

From Targeted to Pervasive Surveillance: The Rise of Anti-Surveillance Activism against Twin Big Brothers

Ulaş Başar Gezgin[1]

Abstract

This article consists of 3 sections: The first section offers an introduction to the major notions of surveillance studies such as surveillance society, privacy, transparency etc. It is argued that the so-called 'liberal democracies' are no longer so liberal when it comes to surveillance. Pervasive surveillance by twin big brothers (ie states and corporations) over all the people are justified on the basis of crime prevention, security, terrorism or profit maximization. In the wake of Snowden revelations that magnified and even confirmed the suspicions about surveillance, anti-surveillance movements have been in the making. They are still weak and quite fragmented, as it is rare to see that democracy movements busy with their other priorities are interested in data justice issues. So we have a set of suggestions for anti-surveillance activism. Thirdly, we tried to reflect on alternatives to mass surveillance. As it is considered to be inevitable, we need to think about how to transform it and transform to what. Burgeoning notions such as sousveillance, equiveillance and coveillance are discussed within this context. We propose that anti-surveillance movements in a more socially conscious form should join hands with wider social justice movements via the notion of data justice.

Introduction

It will not be an exaggeration if we would argue that our so-called 'information society' or 'big data era' revolve on the conflicts and contradictions between surveillance and privacy. Governments' and corporations' pervasive surveillance which is often deceptive in which citizens, users or consumers are not even made aware that they are being surveilled (Monahan, 2016) brings about a trade-off between human rights and especially privacy on the one hand, and security and crime prevention on the other (Cvetković, 2017).

1 Professor, Istanbul Galata University, Faculty of Arts and Social Sciences, Department of Psychology, ulas.gezgin@galata.edu.tr, Orcid: 0000-0002-6075-3501

https://doi.org/10.58830/ozgur.pub135.c627

Under state and corporate surveillance, the contours of citizens, users and consumers are blurred; as surveillance is pervasive and continuous: While Person A is tracked down by corporations as existing or potential costumers; she is watched by government agencies in various tasks related to citizenship such as official documentation of personal data. This is also blended with surveillance on the net in which the same person is positioned as a user. Thus, concatenating citizens with users and consumers in the same person is justified.

Surveillance is not new; the historical origins of surveillance can be found in the observational methods of the social sciences which emerged in the colonial era (Bratich, 2017). Although claimed to be based on an objective approach (isn't it just an observation anyway?!), it has often been based on power distance favoring the observer at the expense of the observed. While surveillance is not new, that is not the case for mass surveillance.

Lamer (2017) rightly points out that

> "When it comes to protecting human rights, the use of mass surveillance creates a vicious cycle: Security threats require mass surveillance; mass surveillance undermines human rights, especially those of human rights defenders and journalists, who are vital for civil society. In turn, the erosion of civil society leads to a lack of public debate and, thus, a lack of policies curtailing mass surveillance and securitisation. This gives the government more leeway to introduce even more legislation that undermines human rights in the name of protecting people from security threats" (p.407).

States have already moved from targeted surveillance whereby only suspected criminals were being watched to mass surveillance where every citizen is deemed to be potential suspects (Wright, 2017). This move coupled with corporate surveillance for ultimate profit maximization characterizes the notion of surveillance society. In some of the cases, personal data are shared with consent, while in other cases without consent. As a result, the citizens lose sense of control and experience feelings of lack of privacy and trust (Hofmann, 2017). In a surveillance society "surveillance has become virtually ubiquitous" (Wright et al., 2015, p.282), whereas undue surveillance is defined as "that which does not serve the public interest, but only the interests of corporate aggrandisement and/or the intelligence agencies and their political defenders" (Wright et al., 2015, p.287). However, in practice, usually it is hard to decide which surveillance act is due or undue.

Wright (2017) states that

> "No one can or should doubt the growing ubiquity of surveillance systems in modern societies. Personal data fuels the modern economy, which is another way of saying that we live in a surveillance society. Surveillance undermines fundamental rights such as privacy and dignity. Hence, a surveillance society undermines democracy itself. One could justifiably regard 'information society', as a terminological wolf in sheep's clothing, where the information society is actually a surveillance society" (p.50).

Thus, all sorts of data are being surveilled or can potentially be surveilled. At first blush, it may be thought that pervasive surveillance is just a characteristic of authoritarian regimes. However, various counter-facts such as Snowden revelations are telling us a completely different story. Unlike the clear-cut distinction made by Lokot (2018) between democratic states such as Western European ones and authoritarian states such as Russia, both forms of governments are getting closer to each other everyday especially after declarations of state of emergency or equivalent measures proposed to target terrorism through pervasive state surveillance practices that are often illegal or alegal which refers to the gray zones for which whether laws would be applicable or which laws would be applicable are mooted such as voluntarily self-produced data via social media. Even worse than that, the scope and coverage of the pervasive surveillance are not targeting terror suspects only; Snowden revelations "showed that governments were not only using surveillance technologies for the purposes of countering terrorism. They also spied on allied politicians, journalists and human rights defenders" (Lamer, 2017, p.395).

Based on the accounts provided by Tréguer (2017) concerning the securitization of the French internet, it is hard not to say that France is not an authoritarian state with regard to pervasive state surveillance. Snowden revelations confirmed the nature and extent of state voyerism in the so-called 'Western democracies'. Furthermore, Tréguer (2017) notes the notion of Snowden paradox: While Snowden revelations were expected to support the efforts to restrict pervasive state surveillance, they led to expansion and legalization of that surveillance model (Hintz, & Dencik, 2016; Tréguer, 2016). Surveillance in the 'West' is normalized through the state-industry collaboration (Hintz & Milan, 2018). Lamer (2017) states that "looking at the implementation of mass surveillance measures in Europe illustrates that the continent is drifting into a permanent state of securitisation that threatens

not only certain human rights, but the very foundation of democratic societies by permanently altering state-society relations" (p.393).

Before moving to the next section, we need to briefly talk about related notions of privacy and transparency. In the most general terms, privacy can be defined as "the right of individuals to decide for themselves if, when, and how intimate information about them should be made available to others" (Franks, 2016, p.426). Additionally, "Privacy is not secrecy; it is the right of the individual to choose who can access private information and who cannot" (Franks, 2016, p.432). Wright (2017) defines transparency with regard to surveillance as "governments and companies informing citizens in a way that they can easily understand about surveillance practices, about the presence of surveillance technologies, who is responsible for the surveillance systems and why those systems have been deployed. (...) 'Secrecy' is the opposite of transparency" (p.50).

The notions of privacy and transparency are always under the spotlight due to the widespread use of social media which encourages and non-materially rewards self-tracking, self-monitoring and self-surveillance. In this context, Gehl (2015) elaborately explains the main contradiction in the discussions on social media and alternative media:

> "those working in the alternative media tradition have an ambivalent relationship to social media. On one hand, they are eager to see social media as the answer to their long-standing calls for broader participation in media production and distribution. On the other hand, there is no denying that the dominant sites— Facebook, Google, and Twitter—have retained or even intensified some of the problems of mass media power and anti-democratic communication that traditional alternative media theorists have described. This leaves alternative media theory in a double-bind: social media allow for people to be producers, certainly more so than traditional media, but they are owned by for-profit firms who can be hostile to alternative ideas, discourses, and organizing—especially when those practices challenge corporate hegemony. Indeed, I suggest we call these sites corporate social media (CSM)" (p.1).

In most of the cases, it is hard to distinguish state and corporate surveillance (Lamer, 2017), as the governments often outsource surveillance. IT companies are tasked to collect data secretly for the governments. In the mainstream anti-surveillance discussions, state is considered to be evil as also reflected in various dystopic films. However the other twin big brother,

which is the corporation is often ignored. Although it is hard to distinguish them with regard to surveillance, they do differ in terms of accountability:

> "The state, at least in Western democratic societies, is at least theoretically accountable to the people. While one can dispute the extent and effectiveness of that accountability, it is arguably far greater than that of private entities. If government officials engage in surveillance, there is a possibility that these officials can be reprimanded or voted out. When a powerful company, offering products that no one pays for but everyone wants, engages in surveillance, it is more difficult to detect and much more difficult to address. Google, for example, has no particular incentive to care what the public thinks of its policies except to the extent that it affects the company's profitability. It is not bound, even theoretically, to the will of the people" (Franks, 2016, p.459).

Anti-Surveillance Movement: Directions and Misdirections

As a response to Snowden revelations and some other leaks, anti-surveillance activism becomes the agenda. There are various forms to resist or at least try to resist the surveillance society. Tanczer, McConville, & Maynard (2016) recommend the use of Tor Browser and VPN (Virtual Private Network) as anti-surveillance measures, while Gehl (2015) lists "Diaspora, rstat.us, Twister, GNU social, and the Dark Web Social Network" (p.1) as alternative social medias with lower levels of privacy intrusion. On the other hand, some other recommendations such as the use of FireChat in Hong Kong and Zello in Latin America were later on found to be virtual traps. While the demonstrators have the illusion of virtual freedom, they are under the control and constant monitoring of the governments through their use of these apps (Sigal & Biddle, 2015). At a more complex level, Van der Velden (2015) described a privacy-friendly mobile app which allows pixelation of the faces in videos so that the people would not be identified by authoritarian regimes. The app which is called as 'InformaCam' can clear metadata which makes state surveillance more difficult. Converging with these, in her research on online practices of Russian activists, noting a trade-off between online visibility and security under conditions of pervasive state surveillance, Lokot (2018) concludes that "navigating the internet using security tools and protocols such as VPN, two-phase authentication, and encrypted messaging is increasingly seen as the default modus operandi for those participating in organised dissent in Russia to mitigate growing state surveillance" (p.332).

Likewise, for French internet, Tréguer (2016) concludes that

> "Judges now appear as the last institutional resort against large-scale, suspicionless surveillance. If litigation fails, the only possibility left for resisting it will lie in what would by then represent a most transgressive form of political action: upholding the right to encryption and anonymity, and more generally subverting the centralized and commodified technical architecture that made such surveillance possible in the first place" (p.63).

These are nevertheless more or less individual-level measures. Wright et al. (2015) also present and discuss collective actions against surveillance such as endorsing more privacy-friendly services and practices, and boycotting those with higher levels of surveillance, as well as demonstrations. In this context, hacktivism techniques which also cover DDoS attacks that "consist of website requests in such high numbers that servers cannot respond and websites become unavailable" and which are considered to be analogous to the "sit-ins and occupations" in offline spaces (Asenbaum, 2017, p.9) are also on the table.

Klein (2015) notes and explores the ambivalent public status of the notion of hacktivism in the case of Anonymous. As hackers, they are viewed negatively, whereas as anti-corporate and anti-dictatorial activists in pursuit of democracy and freedom of expression, they are treated as social activists. From the former perspective, they are considered to be criminals and even terrorists, while from the latter perspective, they are a sort of whistle blowers or investigative data journalists. Klein (2015) identifies 4 public images associated with hacktivists in general and Anonymous in particular: "legitimate activists, vigilante heroes, global threats, and malicious pranksters" (p.388). The negative views are found to be more common which is not surprising considering the close connections between the media, corporate world and governments. Klein (2015) argues that almost all hacking activities by Anonymous are proposed to be for free speech/open internet, political cause/social justice and anti-surveillance. Nevertheless, their secrecy casts doubt on their viability as a resistance model for prospective mass movements.

As stated earlier, one of the turning points in anti-surveillance activism was Snowden revelations. According to Bakir (2017), what Snowden revelations showed was forced transparency over citizens:

> "(a) Citizens had no control over their own personal visibility, because the state had secretly imposed mass surveillance on people. Because

> of the secret imposition, citizens cannot be said to have consented to this surveillance.
>
> (b) The level of oversight of the state and corporations was insufficient to built social trust – as evident by the huge social outcry over mass surveillance in states like the USA following Snowden's leaks" (p.5-6).

For many citizens and even for some of the activists, Snowden revelations have brought out some kind of learned helplessness whereby pervasive state surveillance has been concluded to be inescapable. This is called as 'surveillance realism' (Dencik & Cable, 2017). In fact, the activists had known or believed to know the pervasiveness of state surveillance long before Snowden leaks; thus, Snowden revelations, rather than providing new information, confirmed what they knew or believed to know about the subject (Dencik & Cable, 2017). Thus, some of the activists did not even bother to change their digital habits and behaviors as a response to Snowden leaks.

Referring to the notion of fragmentation of Internet after and as a response to Snowden revelations, Hofmann (2017) observes that

> "Another widespread response to the Snowden revelations consists in a decline of trust in and support for the concept of a global, cross-border communication space. Instead of strengthening the normative basis for transnational information flows and instead of improving the security of transmitting, processing and storing data across the globe, relevant actors increasingly consider national or regional data services and suggest keeping data as much as possible in the respective country" (p.94).

We need to talk about a very significant missing point in the relevant discussions: The blossoming anti-surveillance activism has to be situated in its historical context. Sidhu (2015) reminds us that historically speaking, constant monitoring and state surveillance of Black Americans has been a regular practice in the U.S., taking even more complicated and yet more direct forms during Black Lives Matter protests. Although slavery is long gone, racism and discrimination are inherited to the big brother. Such cases show us why the notion of data justice is necessary and relevant. However we should also keep in mind that data (in)justice is not independent of social (in)justice. Thus, data justice and social justice movements need to be integrated. On the other hand, usually tech activism issues are considered to be difficult for 'ordinary' activists. As a result, they are often considered to be

activities that require expertise (Dencik & Cable, 2017). This has to change. In our times, activists have to be tech-savvy and data literate.

Franks (2016) perceptively and elaborately explains the reason for the rising interest in anti-surveillance which is the clash of mass (undifferentiated) surveillance with the interest of the socially privileged. That is also the weakest point of the current interpretations:

> "The contemporary pro-privacy, anti-surveillance movement is similarly limited by interest convergence. The movement is not primarily concerned with the harms imposed on the most vulnerable members of society, but rather with threats to mainstream and elite interests. Surveillance and other privacy violations that were largely tolerated so long as they burdened marginalized groups are challenged now that they affect privileged interests. This kind of interest convergence in privacy will result not in privacy reform across the board, but primarily in privacy reform that will protect, or at least not harm, the most powerful groups" (p.427).
>
> (...)
>
> "Mass resistance to surveillance emerged only when average and elite individuals became the targets of surveillance, and their interests and viewpoints now dominate the contemporary narrative about privacy. The contemporary anti-surveillance movement has done too little to acknowledge the longstanding surveillance of marginalized populations and has given too little thought to what that history means for the future of privacy. By largely ignoring the history of surveillance, focusing on data privacy to the exclusion of other privacy concerns, and failing to adequately recognize the threat to privacy posed by non-state actors, the popular privacy movement undermines its own revolutionary possibilities" (p.428).
>
> (...)
>
> "The practices of slavery and its enduring after-effects, from racial classification laws to mass incarceration, require extensive and intimate state invasions of privacy of black bodies. The poor, often quite literally unable to shield themselves from the gaze of the state, have been subjected to ruthless investigation and regulation in matters ranging from childrearing to housing arrangements. Women's second-class status as citizens - imposed through centuries of legal and social inequality in marriage, education, employment, and reproduction- entailed state scrutiny and control of their most

> private decisions. For those whose lives are intersected by multiple forms of subordination, for example, poor black women, surveillance is a particularly complex and oppressive reality. The extensive and disruptive reach of surveillance into the lives of marginalized populations has largely gone unremarked in the current popular privacy narrative" (p.428-429).

Thus, an anti-surveillance movement that has no theoretical and practical ties with the notions of social justice and data justice would serve only dominant class interests. That is why we need to have at least some idea about what is meant by data justice to further our discussion. Taylor (2017) defines data justice as "fairness in the way people are made visible, represented and treated as a result of their production of digital data" (p.1). In this account, 3 pillars of data justices are proposed to be 'visibility' (referring to 'access to representation' and 'informational privacy'), 'engagement with technology' (covering 'sharing in data' and 'autonomy in technology choices') and 'non-discrimination' (including 'ability to challenge bias' and 'preventing discrimination') (Taylor, 2017, p.9).

In an ideal social democracy, it should be possible for citizens to monitor or watch over the state and corporations. Thus transparency should bidirectional. This is what is meant by the notion of 'equiveillance' which involves mutual watching of parties of equal position in the hierarchy. But this requires a major change in the way the relations between the state and citizens are configured. For instance, in the case of environmental activism, there should be ways to monitor the state and corporate activities that have harmed or have the potential to harm the environment. This ideal social democracy also includes collection of certain types of data for public benefit such as data concerning global warming (see Vera et al., 2018). Furthermore, one way to fight with corruption in various countries would be the financial disclosure of politicians and appointed authorities. But these attempts at financial transparency are usually blocked either by state itself or offshore institutions including Swiss banks and tax havens. This is another case whereby states and corporations collaborate with each other when the matter is plundering the public resources that are supposed to be equitably distributed over the society. In other words, the twin big brothers want to see the consumers/citizens/users to be as transparent as water, but when it comes to their own transparency they sing a different tune.

Similar to the case of environmental activism, documentation and later on datafication of certain mass activities are needed for both digital and non-digital activism. For instance, Gray (2019) in his case study on

digital activism of Amnesty International points out the significance of data collection and follow-up for "(i) witnessing historical abuses with structured data from digitised documents; (ii) witnessing the destruction of villages with satellite imagery and machine learning; (iii) witnessing environmental injustice with company reports and photographs; and (iv) witnessing online abuse through the classification of Twitter data" (p.1).

Converging with these, in the case of social and ethnic discrimination, both digital and non-digital strands of activism would need scanning of media contents for discriminatory rhetoric and hate speeches. To exemplify, Hrant Dink Foundation which has been named after the assassinated Armenian journalist keeps record of hate speeches against any ethnic groups in Turkey and publish a weekly report (Hrant Dink Foundation, 2019). Likewise, human rights violations need to be recorded as a part of social justice activism (Bratich, 2017).

According to the Gray (2019)'s account of Amnesty International, the activists classify, trace/outline, identify features, compare, count, transcribe and digitise action areas such as "illegal demolitions", "displacements of people", "death penalty", "protest monitoring", "hate speech", "illegal use of weapons" and "extractive industries" with the help of pictures, documents, videos, satellite images, social media, SMS etc. (Gray, 2019, p.5). Here "protest monitoring" can be extended and updated to cover various areas of anti-surveillance activism. All the verbs and tools would be applicable accordingly.

Alternatives to Surveillance Society and Mass Surveillance

As linguistically obvious, the term anti-surveillance is a negative term, but then what is its alternative or what are alternative forms of surveillance? A discussion on anti-surveillance activism would be deficient without working on these questions. Wright et al. (2015) help us clear the way for viable answers:

> "Questioning surveillance is, by definition, not accepting surveillance as inevitable, but rather asking whether a given surveillance system is really necessary and, if it is so determined (...) then asking what sort of controls, oversight and/or counter-measures should be put in place to ensure that the surveillance system does not abuse the public interest" (p.282).

In that sense, Wright (2017) suggests the use of SIAs (Surveillance Impact Assessment) to evaluate the detrimental impacts of mass surveillance before

the implementation of such a program. Alternatives to surveillance in its current form require data transparency which, according to Bakir (2017), "has two important dimensions: "degree of citizen control over how visible they are; and degree of oversight of the surveillant entity" (p.2).

Hong (2017) finds critical discussions on surveillance fundamentally wrong, as they mostly rely on having or not having surveillance at all. For Hong (2017) the discussion should be about the alternatives to surveillance or alternative, benevolent forms of surveillance. In that sense, it would be appropriate to refer to Georgiadou, de By, & Kounadi (2019) who identify 4 approaches to data and privacy which have implications for surveillance:

> "1. [privacy] as a tradeable private good in return for another private good,
>
> 2. [privacy] as something that constitutes who we are, and therefore is unalienable,
>
> 3. [privacy] as something to be delegated to a trusted father-state and traded with a public good, and
>
> 4. [privacy] as something that does not exist anymore and we should get over with" (p.12).

These different views are respectively called as data individualism, data egalitarianism, data hierarchy and data extractivism (fatalism). While the first two are common among the anti-surveillance movements, the third and fourth are more widespread among government and corporate circles. The fourth approach especially normalizes the current status quo in terms of surveillance, while the the first and second approaches are in favor of alternative forms of privacy and surveillance.

Of course, surveillance is not always negative. Home protection systems use surveillance cameras for a positive reason, to control private areas from intruders, which is called as control function of surveillance (Mäkinen, 2016). However, similar to justification for the pervasive state surveillance, the customers are usually scared off unrealistically for sales. Often the buyers psychologically feel secure at home, while the system is never used for its intended purpose in low-crime areas (see Mäkinen, 2016). This unrealistic fear mongering can be a target area of anti-surveillance activism. Nevertheless, even in such a case we can't deny potentially positive uses of surveillance such as baby, elderly or pet monitoring. These are examples of surveillance for monitoring for care (Mäkinen, 2016). Likewise, the surveillance systems can be used to watch nature or wild life (Mäkinen, 2016). On the other

hand, home-based surveillance systems are open to future abuse by states and governments through the introduction of Internet of Things which will make protection of privacy at home life nearly impossible.

Considering the possibility that home-based surveillance systems can be hacked by unknown third parties, Mäkinen (2016) points out what we can call as 'home-based surveillance paradox'. The need to watch others brings the risk to be watched by others:

> "(...) home surveillance systems create a paradoxical situation in relation to exposure. The systems claim to protect the resident from exposure to the outside world (in that they claim to prevent outsiders from entering the premises) but at the same time the systems expose the resident to an unwanted gaze (by including a WiFi-linked camera in the system). This in part created an ambivalent feeling towards surveillance among the residents" (p.72).

Granting the possibility that certain forms of surveillance (but not the mass forms by twin big brothers) can be positive, we need to reflect on the notions of sousveillance, equiveillance and coveillance. In the contexts of protests and demonstrations, sousveillance is defined as "surveillance 'from below' intended to document events, including police conduct, from the protesters' perspective with the possible use of the data to scandalise police misbehaviour or file charges" (Ullrich & Knopp, 2018, p.190).

To characterize friendly watch over social media, a distinction between personal and hiearchical sousveillance is necessary:

> "Personal sousveillance is a form of watching without political or legal intent (such as ubiquitous social media usage, tweeting what we've had for dinner, selfies, life-logging, wearables, and transparency of everyday life). Hierarchical sousveillance has political or legal intent (such as when protesters use their mobile phone cameras to monitor police at demonstrations, or when whistle-blowers leak incriminating documents)" (Bakir, 2017, p.5).

In addition to sousveillance as an alternative form of surveillance, we can mention equiveillance which refers to watching of and by equals as mentioned earlier, and coveillance which refers to watching together: Although the notion of coveillance appears to be democratic at first blush, as it involves watching each other on equal grounds, Samatas (2015) shows that it is not necessarily the case. The notion of coveillance brings the model of citizen-informant who asymmetrically sides with the government to watch other citizens. In other words, through this notion, pro-government

citizens collaborate with the surveilling government on watching other citizens. In contrast to building democracy, such an understanding bolsters authoritarian governments. Thus, a non-authoritarian alternative to mass surveillance is not coveillance, but equiveillance where citizens and their organizations are made legally equal to the twin big brothers.

Conclusion

In this article we discussed various views on anti-surveillance activism as a response to pervasive surveillance. We also reflected on alternatives to mass surveillance. We argue that the most viable way to proceed with anti-surveillance activism would be through social justice movements. But this requires revamping of the current forms of activism, as in some cases they are characterized by middle class agenda only and elitism. The notion of data activism needs to be developed accordingly. This will open up new avenues towards data democracy.

Since the contours of citizens, consumers and users are blurred, we need more interdisciplinary research and social interventions, not only covering social media studies, but also citizenship and consumer research. How to protect privacy and digital rights in general is quite relevant for social media research as it has the potential to change users' communicative behaviors on the net. Digital rights for communicative purposes need to be integrated with consumer rights and citizenship rights.

References

Asenbaum, H. (2018). Cyborg Activism: Exploring the reconfigurations of democratic subjectivity in Anonymous. New Media & Society, 20(4), 1543-1563.

Bakir, V. (2017). Final Report for DATA-PSST ESRC Seminar Series.

http://data-psst.bangor.ac.uk/documents/DATA-PSST-final-report-june-2017.pdf

Bratich, J. (2017). Observation in a surveilled world. In N. Denzin & N. Lincoln (eds.). The SAGE handbook of qualitative research (pp.526-545). Thousand Oaks, CA: Sage.

Cvetković, N. (2017). Secret monitoring: A method of fighting against terrorism. Facta Universitatis, Series: Law and Politics, 15(4), 325-334.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. International Journal of Communication, 11, 763-781.

Dencik, L., Jansen, F., & Metcalfe, P. (2018). A conceptual framework for approaching social justice in an age of datafication.

https://datajusticeproject.net/wp-content/uploads/sites/30/2018/11/wp-conceptual-framework-datajustice.pdf

Franks, M. A. (2016). Democratic Surveillance. Harvard Journal of Law & Technology, 30, 425-489.

Gehl, R. W. (2015). The case for alternative social media. Social Media+ Society, 1(2), 2056305115604338.

Georgiadou, Y., de By, R., & Kounadi, O. (2019). Location Privacy in the Wake of the GDPR. International Journal of Geo-Information, 8(3). doi: https://doi.org/10.3390/ijgi8030157

Gray, J. (2019). Data witnessing: attending to injustice with data in Amnesty International's Decoders project. Information, Communication & Society, 1-21.

doi: 10.1080/1369118X.2019.1573915

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. Internet Policy Review.

Hintz, A., & Milan, S. (2018). "Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West. International Journal of Communication, 12, 21, 3939–3959.

Hofmann, J. (2017). Constellations of trust and distrust in internet governance. Trust at Risk: Implications for EU, Brussles: European Commission (pp.85-98).

Hong, S. H. (2017). Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient. Surveillance & Society, 15(2), 187-203.

Hrant Dink Foundation (2019). Media Watch on Hate Speech.

https://hrantdink.org/en/asulis-en/activities/projects/media-watch-on-hate-speech

Klein, A. G. (2015). Vigilante media: Unveiling Anonymous and the hacktivist persona in the global press. Communication Monographs, 82(3), 379-401.

Lamer, W. (2017). From sleepwalking into surveillance societies to drifting into permanent securitisation: Mass surveillance, security and human rights in Europe. Global Campus Human Rights Journal, 1(2), 393-413.

Lokot, T. (2018). Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices. Surveillance & Society, 16(3), 332-346.

Mäkinen, L. A. (2016). Surveillance ON/OFF. Examining home surveillance systems from the user's perspective. Surveillance and Society, 14(1), 59-77.

Samatas, M. (2015). "Austerity Surveillance" in Greece under the Austerity Regime (2010– 2014). Media and Communication, 3(3), 68-80.

Sidhu, K. (2016). A Call for Minority Involvement in Cybersecurity Legislation Reform and Civil Rights Protests: Lessons from the Anti-SOPA/PIPA Demonstrations. Hastings Comm. & Ent. LJ, 38, 117-144.

Sigal, I., & Biddle, E. (2015). Our Enduring Confusion About the Power of Digital Tools in Protest. The Fibreculture Journal, 287-293. doi: 10.15307/fcj.mesh.007.2015.

Tanczer, L. M., McConville, R., & Maynard, P. (2016). Censorship and surveillance in the digital age: The technological challenges for academics. Journal of Global Security Studies, 1(4), 346-355.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society, 4(2), 2053951717736335.

Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. Media and Communication, 5(1), 1-12.

Tréguer, F. (2016, April). From deep state illegality to law of the land: The case of internet surveillance in France. In 7th Biennial Surveillance & Society Conference (SSN 2016):" Power, performance and trust".https://halshs.archives-ouvertes.fr/halshs-01306332/document

Ullrich, P., & Knopp, P. (2018). Protesters' Reactions to Video Surveillance of Demonstrations: Counter-Moves, Security Cultures, and the Spiral

of Surveillance and Counter-Surveillance. Surveillance & Society 16(2), 183-202.

Wright, D. (2017). Privacy and trust at risk in surveillance societies. Trust at Risk: Implications for EU, Brussles: European Commission (pp.48-68).

Wright, D., Rodrigues, R., Raab, C., Jones, R., Székely, I., Ball, K., Bellanova, R. & Bergersen, S. (2015). Questioning surveillance. Computer Law & Security Review, 31(2), 280-292.

Van der Velden, L. (2015). Forensic devices for activism: Metadata tracking and public proof. Big Data & Society, 2(2), 2053951715612823.

Vera, L. A., Dillon, L., Wylie, S., Ohayon, J. L., Lemelin, A., Brown, P., ... & Environmental Data and Governance Initiative. (2018). Data resistance: A social movement organizational autoethnography of the environmental data and governance initiative. Mobilization: An International Quarterly, 23(4), 511-529.