Mirjam Abigail Twigt

52 Social media

Abstract: This chapter discusses three key developments sparked by social media relevant to criminologists: social media as enablers of harm, surveillance, and manipulation. Concerns that social media for crime and crime control purposes contribute to discrimination relate to the general agreement that social media and social media data tend to reinforce pre-existing structural inequalities and power inequalities. Another concern relates to the pace at which companies develop means to gather and use social media intelligence, further hindering capacities for meaningful regulation and oversight. The connections that social media engender however also provide additional means to collectively respond to data harms and to foster new approaches for anti-surveillance and social justice.

Keywords: platforms, profiles, sociality, datafication, privacy work

Social media have become integral to much of everyday life. Most of us use social media platforms to communicate with family and friends, share content and to interact with events in the world. "Social media are by definition social" (Marwick, 2023: 6). Much like offline interactions, the online connections that social media enable are deeply embedded in material realities and social relations. What is new(er) about social media is the ways in which they enhance interactions across spatial and temporal boundaries.

The term 'social media' comes from popular culture grouping together different interactive Web 2.0 internet-based applications that draw on user-generated content (Fuchs, 2017). The first social media sites gained popularity in the 1990s. Some platforms such as Myspace (2003) have waned, whereas others like YouTube (2005, owned by Google) and Facebook (2004) remain successful. More social media platforms continue to emerge, such as TikTok and its Chinese counterpart Douyin, Twitter/X, Viber, WeChat, and SnapChat, which exist next to other popular platforms owned by Meta (formerly Facebook. Inc.) like Instagram and WhatsApp. As smartphones and access to the internet have become less expensive, social media gained further popularity and an ubiquitous global presence.

Social media platforms can be considered as additional places for people to socialize, with different degrees of privacy and group size. They have engendered more scales for sociality as they offer additional means to sustain connections and to build new networks, to establish romantic and/or sexual encounters and to deal with experiences of isolation and exclusion—just to name a few (Miller et al., 2016). Most social media platforms expect users to create service-specific and highly personalized profiles. This allows for connecting and sharing content with other individuals and groups through one-to-one, one-to-many and/or many-to-many exchanges. Many users combine different social media sites.

 https://doi.org/10.1515/9783111062037-053

The socio-technical properties of social media profoundly reshape social relations and politics (Dencik et al., 2022). Amongst other things, they interact with and alter practices and understandings concerning crime, punishment, and control. Online interactions allow additional ways to engage in harmful or illicit acts, in policing and resisting control, not least because extracted social media data can be used for surveillance and manipulation purposes. Processes of extracting and using social media data tend to be unequally distributed across social relations and the global political economy with much risk of further structural discrimination (Couldry and Mejias, 2019). Terms such as 'data universalism' and other manifestations of technological determinism relating to social media easily gloss over material and cultural specificities. In the Global North and across the many Souths there are manifold ways in which people navigate the respective possibilities and restrictions of different social media platforms (Milan and Treré, 2019).

Social media as enablers for new forms of harm and/or criminal acts

Social media platforms allow for new criminal and hurtful practices and for old(er) practices to take place on them. Much has been written on their potentials for amplifying old and new forms of hate, abuse, and discrimination (Noble and Tynes, 2016). For instance, social media platforms have frequently been used to incite racist hatred, using anonymity or fake identities, and by employing seemingly benign practices like the use of memes, GIFs, and emojis (Matamoros-Fernández and Farkas, 2022). The affordances of different social media allow for new ways to organize crime transnationally: for instance, online drug traders in Scandinavia combine the use of the dark web and encrypted one-to-one communication, with public-facing social media profiles that are used for assessing risks and build trust (Bakken, 2022).

Much of social media's potentials, also for inflicting harm, relate to their design, which encourages sharing. Their design and policies enable practices of sharing and coordinating dissatisfaction with society, libidinal desires, and rage online (Paris, 2021). Social media are also prime channels for sharing and spreading false media content (Venturini, 2019). Many social problems that emerge online—such as harassment or cyberbullying—have roots in offline social dynamics. But social media platforms allow for additional ways to know about someone's past or a person's private information, and to direct hurtful comments. There are specific concerns on the influence of social media on young people's mental health (Angel and boyd, 2024).

An important difference between social media and other interpersonal communication, such as letters and landline phones, is that information shared in a closed online community or in a confidential setting can easily—intentionally or unintentionally—leak into more public channels and to contexts for which it was not intended (Chun, 2017). Whereas this can happen on a personal level, data breaches and hacks also often

occur on a larger scale: Facebook and Twitter/X are among the world's largest social media companies through which personal data of millions of users have become exposed, information that could be misused for reputational damage, fraud, and identity theft (Information is beautiful, 2024; see ID Theft by Langford, Wærstad, and Svensson).

The exposure to online hatred and other social media-related harms is not equally divided. People of color, women, and LGBTQI+-individuals are more often targeted. The societal repercussions tend also to be greater for them, not least because legal systems are still catching up on how to address social media-facilitated harms and many societal and material barriers for legal recourse exist (Citron, 2016).

Social media as enablers of surveillance and control

Surveillance—the systematic collection of personal information to manage groups—is not new, but the rise of social media adds new dimensions (see Surveillance by Lyon). Firstly, surveillance is deeply embedded in social media infrastructures and business models. Many social media platforms are intricately linked to what Shoshana Zuboff has critically termed *surveillance capitalism* (Zuboff, 2019). Such platforms commodify vast amounts of behavioral data generated through users' engagement. Infrastructures that track user activities and quantify these as data-points create capital, as millions of social media messages a day are analyzed to gain extensive profiles of users. These profiles are subsequently sold, directly or via data brokers, to advertisers, to security officers who want to control a particular target group, or as training data for the development of Artificial Intelligence (AI) (see Artificial Intelligence by Van Brakel). Vice versa, machine learning tools are also used to analyze social media interactions (Amoore, 2020).

The availability of information on social media also changes governmental surveillance. Using social media data for surveillance and policing purposes does not necessarily require advanced techniques. Research shows how UK police officers would manually search the social media presence of targeted persons, inadvertently also collecting detailed information of non-targeted persons (Fussey and Sandhu, 2022). Fake social media profiles can be set up to gather digital evidence, as has been the case in several countries where queerness is criminalized (Rigot, 2022).

Despite their potential for discrimination, data-driven systems have increasingly become integrated into governmental processes. Seemingly mundane data—clicks and likes, time spent on a site, the music preferences—are collected and put together based on shared features and common behavioral patterns the use of which can be of severe consequence: they can influence one's credit score or risk assessments conducted by the police (Redden, 2022: 70 – 71). The widespread experimentation with social media data by public institutions ranging from The Netherlands, the US, the UK, and India on areas such as predictive policing, welfare provision, and fraud prevention have had many harmful effects, such as extended surveillance, stigmatization, wrong-

ful accusation, detention, and deportation. Especially people already marginalized have been adversely affected by such practices (Redden, 2022).

Yet a different aspect are the predictions drawn from data aggregates, which are used for policing activities, as well as military purposes. For example, techniques and tools for facial recognition, sentiment analyses, mappings of suspicious relations or events draw on social media data (Trottier, 2014). Companies offer technologies for intercepting 'real time' communication on social media or for accessing a person's social media information. What is more, digital data extraction devices and tools to restore deleted social media data are not only appropriated by dictatorial regimes, allowing them to take action against dissent (Loewenstein, 2023). Several EU member states also use them to search social media traces of people seeking asylum (Josipovic, 2023). This is but one example of how social media data are used for migration and border control purposes, despite ample questions about the accuracy and the legality of such procedures (Oliveira Martins et al., 2022).

Social media as enablers of polarization and/or manipulation

Surveillance capitalism has close links to the 'attention economy' (Celis Bueno, 2017). The longer one engages with a specific social media platform, the more data can be gathered. What social media users see on their feeds is curated by algorithms (see Algorithm by Leese), for instance through the push of 'viral' content and tailored predictions based on what you and people like you 'liked.' The algorithmic selection of social media contents has thus been criticized for creating echo chambers (Jamieson and Cappella, 2008) or filter bubbles (Pariser, 2011), by making social media encounters with people with opposing views more limited and making news-intake more one-sided. This criticism has also triggered new developments in curating contents. A systematic review of existing research on social media and polarization suggests a more complex picture, with a formative role for self-selection and more vocal elites (Ross Arguedas et al., 2022).

Other sources of manipulation are bots and trolls used to spread and amplify false and/or dangerous content (Woolley and Howard, 2016), but also to set up campaigns for targeting specific user groups. The Cambridge Analytica Scandal of 2018, for example, revealed how the data of more than 80 million Facebook users was used to target particular demographic groups with tailored messages to steer voters' decision making (Redden, 2022: 67). As a response to such issues, governmental pressures and reputational concerns have stimulated social media platforms to curtail media manipulation and other social media-related harms, for instance via content moderation. Here, automated approaches are combined with the labor of content moderators to filter out violent and/or inappropriate social media content and distinguish false accounts.

Social media companies, too, have an interest in addressing manipulation and polarization, but their initiatives, too, create social repercussions. As profit-oriented businesses, social media companies are concerned with not offending the majority of their users and influential nations. When taking actions, social media platforms owners, however, tend to draw on their own normative frameworks. There is power in determining what and who causes harm, as such definitions can easily be experienced as punitive and selective (Myers West, 2018). Social-media platforms, then, also exercise normative power: Loewenstein (2023), for example, has documented how social media platforms censor, suspend, and make content disappear among already marginalized groups.

Enacting concrete policymaking and politics

Social media developments occur quickly, whereas data regulation ecologies tend to lag behind. Concerns for surveillance and other social media-related harms have been translated into regulatory frameworks for responsible data handling such as the EU's General Data Protection (GDPR). Questions remain about their scope and enforceability (Hintz, 2022). And with their narrow emphasis on the protection of personal data, these frameworks draw on the ontological premise of 'hyperindividualism' (Bigo et al., 2019: 5). The individual social media-user is required to protect themselves through technological self-defense. Meanwhile participating in an online social life on the most widely used services and platforms already requires agreeing to comprehensive data collection (Hintz, 2022).

Many social media users engage in 'privacy work' via a wide array of practices such as obfuscating personal information, self-censoring, using code language, encryption, and virtual private networks (VPNs) (Marwick, 2023). But approaching a desired level of privacy—clear boundaries between self and others and between what is public and private—is difficult, if not impossible, to sustain. Even if people fully abstain from social media, they cannot control what others share about them online, or if big data technologies make inferences about their behavior in other ways. Much of the value of social media data relates to their relational value. Data policies and legislation that focus solely on the individual data subject fail to address the relational value of social media data, and how this reshapes crime and control within societies.

The pace at which possibilities for social media intelligence gathering develop increasingly outstrips capacities for meaningful regulation and oversight. At the same time, much of the difficulties for meaningful regulation of social media is characterized by inherent contradictions within legal and regulatory frameworks. In addition to the GDPR, other EU legislation such as the Digital Markets Act (DMA) and the Digital Services Act (DSA) are developed to regulate and curtail the power of social media platforms (Meaker, 2024). These, however, coexist with the EU's ongoing emphasis on 'innovation' and specific understandings of national 'security' (Hintz, 2022).

Corporate initiatives to implement data ethics have had varying degrees of success, but these largely rely on the goodwill of the industry with little space for governmental entities to interfere. Rather, their suggestions for technological solutions (more data, algorithmic sophistication) for socio-political problems suggests that much work is ahead for civil society actors, tech workers, and activists. Among other things, this will consist of activities geared to bring forward the harms and violations brought about by social media platforms, to reappropriate decentralized social media interactions for building communities, and to question data extraction practices by social media platforms on a more profound level (Dencik et al., 2022).

Conclusion

This contribution shared a critical account of the ways in which social media interact with and have become an element of crime and crime control. The potentials of social media were initially idealized as democratizing and leveling. By now, there is general agreement that social media reinforce already existing unequal power differentials in gender, class, race, legal status, and sexuality (Chun, 2017). In extension, this raises concerns about the ways in which the use of social media for crime and crime control can further entrench structural inequalities and contribute to discrimination.

The connections that social media engender, however, also provide additional means to collectively respond to these developments and to identify new forms of data justice (see Data Justice by Redden). Social media are also means for sousveillance, the redirection of surveillance toward those traditionally in position of power. They allow to capture, share, and gain attention for injustices, such as police violence (Goldsmith, 2015), for creating counter-narratives, for establishing safe passages for people on the move (Milijovic, 2018) and for strengthening social movements through narrative capacities (Tufekci, 2017). Rather than moving away from social media, there is value in moving toward data justice approaches that further bridge anti-surveillance and social justice activism (Dencik et al., 2022).

Suggested reading

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2022). *Data Justice.* London: SAGE.

Fussey, P., & Sandhu, A. (2022). Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, 26(1), 3 – 22.

Matamoros-Fernández, A., & Farkas, J. (2021). Racism, hate speech and social media: A systematic review and critique. *Television & New Media*, 22(2), 205 – 224.

Marwick, A. (2023). *The Private is Political: Networked Privacy and Social Media.* New Haven, CT: Yale University Press.

References

Angel, M., & boyd, d. (2024). Techno-legal solutionism: Regulating children's online safety in the United States. In *CSLAW'24: 3rd ACM Computer Science and Law Symposium, March 12 – 13, Boston, MA.*

Amoore, L. (2020). *Cloud Ethics: Algorithms and Attributes for Ourselves and Others.* Durham, NC: Duke University Press.

Bakken, S. A. (2021). Drug dealers gone digital: Using signalling theory to analyse criminal online personas and trust. *Global Crime*, 22(1), 51 – 73.

Bigo, D., Isin, E., & Ruppert, E. (2019). *Data Politics. Worlds, Subject, Rights.* Abingdon: Routledge.

Celis Bueno, C. (2017). *The Attention Economy: Labour, Time and Power in Cognitive Capitalism.* London and New York: Rowman & Littlefield.

Chun, W. H. K. (2017). *Updating to Remain the Same Habitual New Media.* Cambridge, MA: the MIT Press.

Citron, D. K. (2016). *Hate Crimes in Cyberspace* (Reprint ed.). Cambridge, MA: Harvard University Press.

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4), 336 – 349.

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2022). *Data Justice.* London: SAGE.

Fuchs, C. (2017). *Social Media: A Critical Introduction.* London: SAGE.

Fussey, P., & Sandhu, A. (2022). Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, 26(1), 3 – 22.

Goldsmith, A. J. (2015). Disgracebook policing: Social media and the rise of police indiscretion. *Policing and Society*, 25(3), 249 – 267.

Hintz, A. (2022). Data and citizenship. In L. Dencik, A. Hintz, J. Redden, & E. Treré (eds.), *Data Justice* (pp. 73 – 88). London: Sage.

Information is beautiful. (2024). *World's Biggest Data Breaches & Hack.* Updated January 2024. Retrieved from: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Jamieson, K. H., & Capella, J. N. (2008). *Echo Chamber: Rush Limbough and the Conservative Media Establishment.* Oxford and New York: Oxford University Press.

Josipovic, I. (2023). What can data justice mean for asylum governance? The case of smartphone data extraction in Germany. *Journal of Refugee Studies*, 36(3), 534 – 551.

Loewenstein, A. (2023). *The Palestine Laboratory. How Israel Exports the Technology of Occupation around the world.* London: Verso.

Marwick, A. (2023) *The Private is Political: Networked Privacy and Social Media.* New Haven, CT: Yale University Press.

Matamoros-Fernández, A., & Farkas, J. (2021). Racism, hate speech and social media: A systematic review and critique. *Television & New Media*, 22(2), 205 – 224.

Meaker, M. (2024). Europe is breaking open the empires of big tech. *Wired.* 6 March, Retrieved from: https://www.wired.com/story/europe-dma-breaking-open-big-tech/.

Milan, S., & Treré, E. (2020). Big data from the South(s): Beyond data universalism. *Television & New Media*, 20(4), 319 – 335.

Milivojevic, S. (2019). 'Stealing the fire', 2.0 style? Technology, the pursuit of mobility, social memory and de-securitization of migration. *Theoretical Criminology*, 23(2), 211 – 227.

Miller, D., Costa, E., Haynes, N., McDonald, T., Nicolescu, R., Sinanan, J., Spyer, J., Venkatraman, S., & Wang, X. (2016). *How the World Changes Social Media.* London: UCL Press.

Myers West, S. (2018). Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms. *New Media & Society,* 20(11), 4366 – 4383.

Noble, S., & Tynes, B. (2016). *The Intersectional Internet: Race, Sex, Class, and Culture Online.* New York: Peter Lang Inc.

Oliveira Martins, B., Lidén, K., & Gabrielsen Jumbert, M. (2022). Border security and the digitalisation of sovereignty: Insights from EU borderwork. *European Security*, 31(3), 475 – 494.

Paris, B. (2021). Configuring fakes: Digitized bodies, the politics of evidence and agency. *Social Media & Society*, 7(4), 1 – 13.

Pariser, E. (2011). *The Filter Bubble: What the Internet is Hiding from You.* London: Viking.

Redden, J. (2022). Data harms. In L. Dencik, A. Hintz, J. Redden, & E. Treré (eds.), *Data Justice* (pp. 59 – 72). London: Sage.

Rigot, A. (2022). *Digital Crime Scenes: The role of digital evidence in the persecution of LGBTQ people in Egypt, Lebanon and Tunisia.* Berkman Klein Center for Internet & Society at Harvard University.

Ross Arguedas, A., Robertson, C., Fletcher, R., & Nielsen, R. (2022). *Echo Chambers, Filter Bubbles and Polarisation: A Literature Review.* Oxford: Oxford University.

Trottier, D. (2014). Vigilantism and power users. Police and user-led investigations on social media. In D. Trottier & C. Fuchs (eds.), *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube* (pp. 209 – 222). Abingdon: Routledge.

Tukefci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest.* New Haven, CT: Yale University Press.

Venturini, T. (2019). From fake to junk news: The data politics of online virality. In D. Bigo, E. Isin, & E. Ruppert (eds.), *Data Politics. Worlds, Subjects, Rights* (pp. 123 – 144). London: Routledge.

Woolley, S., & Howard, P. (2016). Automation, algorithms and politics|political communication, computational propaganda, and autonomous agents – Introduction. *International Journal of Communication*, 10(9), 4882 – 4890.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* London: Profile Books.