Social Media Surveillance

IAN BROWN
University of Oxford, UK

Surveillance is a broad term. Human beings are routinely aware of their environment, consciously and less consciously taking note of the appearance and behavior of others nearby. It occurs in every social system – between friends, by colleagues and managers, and by bureaucrats (Marx, 2012). This includes human activity on social media websites such as Twitter, Google+, YouTube, and Facebook, which reached 1.19 billion active monthly users in October 2013. While individuals typically use social media to communicate and share photos, web links, and other types of information with their associates, the main aim of social media providers is to use all of this data to create profiles that can be used to show users targeted adverts.

More deliberate monitoring of individuals often takes place in an adversarial and inquisitorial context, increasingly using technical means to gather and analyze data, and is used for social, environmental, economic, or political governance.

Etymologically, *surveillance* comes from the French word meaning "oversee" or "watch over," carried out by watchers, overseers, and officers – implying social hierarchy (Fuchs, 2011, p. 124). The process is typically distributed across interlinked systems, bureaucracies, and social connections – converging into "surveillant assemblages" – and embedded within everyday life (Lyon, Haggerty, & Ball, 2012). Social media sites increasingly resemble such assemblages, as they draw in data on user activity elsewhere on the internet via "cookies" and other tracking mechanisms, and from other sources of information on users, such as retailer loyalty cards, customer surveys, and smartphone location traces.

Surveillance is an ancient social process, but in the late twentieth century became a central organizing societal practice, affecting power dynamics, institutional practice, and interpersonal relations. Alongside changing technology, this transformation was driven by factors including increasing managerialism, greater public perception of risk, and political expediency (Lyon et al., 2012). The extent and intensity of surveillance practices in some modern polities – both democracies and authoritarian regimes – have led them to be labeled surveillance societies (Marx, 2012).

A number of factors need to be taken into account when considering a particular instance of social media surveillance. Who is carrying it out – a government agency, with a broad or narrow focus? A business dealing with customers, or profiling and marketing to potential customers? A community of individuals? What are the power relations between the surveiller(s) and the surveilled? What kinds of data are being collected, using which means? These might include narrative reports (by journalists or police officers), audiovisual recordings (by webcams), or activity traces, relating to public, personal, private, sensitive, or intimate situations – all of which now take place via social media. Which norms or rules cover data security, access, and use, and how are these enforced? Which cultural factors shape the experience of watching and being watched? Is surveillance culturally linked to modernization or a benevolent welfare state, or used as a weapon against internal or external enemies during a crisis (Marx, 2012)?

Social media users spend a great deal of time curating online "exhibitions" of different aspects of their identities. Identity play and control are especially important to young people as they grow up and develop their own independent identities and peer relationships. The use of social networks is now a key part of this process in advanced economies, critical for friendships, social capital, and popularity (Joinson & Paine, 2007) and experimentation with different roles and types of identities. Children can use private online spaces for "silly, rude or naughty behaviour" and to seek confidential information and advice (Livingstone, 2006, p. 132). This can be vital for children who may feel isolated in their local environment, such

The International Encyclopedia of Digital Communication and Society, First Edition.
Edited by Robin Mansell and Peng Hwa Ang.

DOI: 10.1002/9781118290743.wbiedcs122

as lesbian or gay teenagers, and who can make friends online with geographically remote individuals (Marwick, Murgia-Diaz, & Palfrey, 2010). This "identity work" in social networks, however, has a consequence usually unintended by the user: the development of commercial profiles that can have a significant impact on life chances.

Individuals' close social circle members can respond quite negatively to expressed identities that are contrary to an expected social role. The internet has given individuals greater opportunities to express and develop marginalized identities (e.g., sexuality and fringe ideologies), and to overcome social anxiety. Active participation in online groups related to stigmatized identities and ideologies allows individuals to gain support from group members, leading to increased self-acceptance and reduced feelings of isolation, difference, and shame, as well as significant increased willingness ultimately to share these identities with family and friends.

Social media surveillance reduces individuals' control over the information they disclose about their attributes in different social contexts, often to powerful actors such as the state or multinational corporations. Social networking tools make it much easier for individuals to share information about their friends and acquaintances, with or without their consent. Any of these actors in turn may treat individuals differently based on that information, and share it without their explicit consent – including using identification technologies to link surveillance data back to individuals.

Such a reduction in disclosure control limits people's ability to regulate their social interactions (Joinson & Paine, 2007) and to position themselves in relation to available social identities. This violates the "contextual integrity" that individuals rely on to play various roles (worker, best friend, social club member, parent, child) in different social situations. It also facilitates economic and governance aims, classifying and controlling individuals in more or less subtle ways, such as by using "risk profiles" to allocate credit or make decisions on individual passage through a border (Lianos, 2003).

Individuals may feel that such classifications are blunt or miss important data relevant to the making of a fair decision. They may also have a "chilling effect" on the possibilities for whistle-blowing and democratic activism.

The Impact of New Technologies and Practices

The rapid development of computing technologies, and the social, political, and economic practices that have shaped and been shaped by this development, is one of the most significant enablers of social media surveillance.

Computer processing power continues to grow, following Moore's Law, doubling roughly every 18–24 months, although at some point the fundamental limits of engineering will limit this growth. Computer storage capacity and communications bandwidth are increasing at least as quickly. These exponential increases will significantly enhance the capability of organizations to collect, store, and process personal data.

Digital technologies generally can be configured to generate voluminous records of personal activity. In the online environment almost every communication and webpage access leaves behind a detailed footprint, linked to individuals through the IP (internet protocol) address of their computer or smartphone, and through digital "cookies" left on their browser by websites. Social media firms encourage individuals to share information about themselves with their "friends," along with the operators of those sites. Mobile phones send location information to network providers to enable calls to be forwarded, and to enable location based services such as mapping and advertising. Social media apps running on these smartphones allow users to both explicitly and implicitly share information about themselves and those around them.

Social networking sites provide detailed options for controlling who gets access to individual profiles and shared content – although these controls are often difficult to use and not prominent. Users rarely alter default settings which, therefore, have a strong impact. The providers' economic interests are generally in encouraging greater disclosure, while providing some less prominent options for the roughly one quarter of the population identified as "privacy fundamentalists" (Harris Interactive & Westin, 1999).

Behavioral advertising companies track individuals across sites to show advertisements targeted to their profiles. Advertising agency WPP, for example, has built such profiles on 500 million individuals in North America, Europe, and Australia, while social media site users explicitly and implicitly provide profile data to enable advertising targeting. Facial recognition software is being used to match photographs and video footage of individuals against databases of criminal suspects and, more recently, by social networking sites to enable the identification of individuals in uploaded photos.

Very low-cost remotely readable radio frequency identification (RFID) tags are increasingly attached to consumer goods and access control cards, the first wave of the "internet of things" that could make some aspects of the physical world as trackable as internet activity. More sophisticated tags are included in many nations' passports, and are also being used for road toll payment systems, public transport ticketing, and in contactless payment cards such as MasterCard's PayPass and Visa's Paywave. Gadgets such as heart rate monitors already allow individuals to share sensor information about themselves and their environment through social media.

This "ubiquitous computing" will become a pervasive phenomenon with some individuals recording detailed information about every aspect of their lives (Askoxylakis et al., 2011). Privacy-sensitive individuals will have a limited ability to opt out of such environmental sensing by others. In the next decade, these sensors and tags are likely to become ubiquitous, dramatically smaller, and much more capable. They will fade further into the background of everyday life, with little to remind people of the data trails they are generating.

The accessibility of technology mediated activities to surveillance, not present in face-to-face interactions, can make individual control more difficult. Digital data is usually persistent (saved by default, perhaps indefinitely), searchable (much easier to find), replicable (easily shareable in convincing form), and, as a result, lacks a specific audience (boyd, 2008, p. 126). None of these qualities is obvious to less experienced users. Real-world gossip is deniable, usually geographically limited, and fades over time. Digital information about an individual – however partial and unrepresentative – can persist as a digital scarlet letter.

Underlying developments in computing technology will enable sophisticated analysis of this flood of personal data. Profiling and data analysis algorithms are increasingly used on very large databases to spot patterns and identify individuals and behaviors "of interest." E-commerce stores can see not just their customers' purchasing behavior, but every product customers consider and for how long before deciding whether or not to buy. Service providers can store all information provided by a user, such as search terms. Companies use this transactional data to target special offers at customers and to find ways to provide slightly different products at different prices so as to maximize revenue. Using customer relationship management software, firms also focus on identifying and retaining high-value customers while reducing service levels to less profitable individuals. All of these types of data can be linked via social media profiles, now often automatically linked as they are used to log into cooperating sites elsewhere on the internet.

State Surveillance

Governments are conducting surveillance by analyzing and exchanging ever greater quantities of information on their citizens, using data mining tools to identify individuals "of interest." A "digital tsunami" of data about individuals is produced by modern technologies. Companies are required in many jurisdictions to provide law enforcement and intelligence agencies with access to this data – and in some cases explicitly to retain data for longer than necessary for business purposes. For example, all European Union (EU) member states require telephone companies and internet service providers to store data about their customers' communications and location, for later police access. There have been legislative initiatives, such as the United Kingdom's draft Communications Data Bill, to extend these requirements to social media services.

American and European intelligence agencies are carrying out surveillance of internet mediated activities on a massive scale. Whistle-blower Edward Snowden revealed in 2013 that the US National Security Agency (NSA) is gaining "bulk

access" to records of all telephone calls, using legal orders applied to telephony providers, and, at various points, has attempted to gain access to bulk records of internet communications. Through its PRISM program, the NSA is also able to compel the provision of large volumes of personal data held by US based communications services, including Facebook and Google.

Global submarine cables are the main arteries of the internet worldwide. If they can be successfully tapped, then they provide a "fast track" to total internet surveillance, without the need to target an individual user with more specialized surveillance methods. Much of the rest of Europe's external internet traffic is routed through the United Kingdom, as this is the landing point for the majority of transatlantic fiber-optic cables. The UK's Government Communications Headquarters (GCHQ) has reportedly placed data interceptors on fiber-optic cables conveying internet data in and out of the United Kingdom, and is able to store 25% of global internet traffic for three days on a rolling basis while carrying out further automated analysis.

Much internet traffic is encrypted to protect it from interception, especially since large companies such as Google and Facebook enabled encryption for their services. However, GCHQ and the NSA also reportedly have succeeded in decrypting data protected using many of the commonly used encryption standards. They did this by covertly influencing encryption standards, liaising with technology companies selling products to government, by compromising personnel at selected companies, and through massive investment in computing capacity. Snowden revealed that funding for this program – US$254.9m for 2013 – dwarfed that for the PRISM program ($20m per year).

Before the Snowden revelations, many experts thought that the continued dramatic growth in levels of internet traffic would outstrip the capacity of signals intelligence agencies to monitor this data flood. We now know that NSA and GCHQ have developed technology that is able to record and filter through very large volumes of traffic; there is no technological reason why they should not be able to continue to do this.

In the near future, it will be so easy to put everyone under digital surveillance that it could easily become the default position. This includes international cooperation between public authorities aimed at identifying suspected football hooligans, illegal or trafficked migrants, political activists, terrorists, and pedophiles. Being given any of these labels by any authority, in any country, can quickly lead to such a stigma becoming all-pervasive, without it being possible to challenge the body that initially made the mark.

Human Rights Protections

Human rights laws provide one key protection for social media users from government abuse of surveillance powers. A range of potential transatlantic human rights standards for surveillance has been developed by civil society groups, courts, and watchdogs, such as the EU Data Protection Supervisor. Civil society groups have identified some key features for law reform that would strengthen these protections, including:

- Intelligence agencies should only have targeted, limited access to data, such as a specific person or a specific identifier (like a Facebook username) or a small category (like a group on a terrorist organization list or member of a foreign intelligence agency). Data collection should only occur based on concrete suspicions.
- Agency access should be to specific records and communications. They should not be authorized to undertake bulk monitoring, such as the submarine cable taps that give NSA and GCHQ access to vast quantities of data which they then winnow down in secret. Any data access should trigger legal protections – this should not come only when data is picked out of a large data stream already collected by an agency.
- Data collected using special national security powers should be completely blocked from use for other government purposes, including law enforcement. It should be retained for limited periods and deleted once no longer required.
- "Metadata" revealing information accessed, and who people communicate with, where, and when, can be extremely revealing about individuals' lives, and currently receives very

low levels of legal protection. This should change.
- There should be strict limits on intrusion into freedom of association by network analysis (the creation of very large datasets linking people through several communication hops – three in the NSA's case, which can intrude on the privacy of millions of people).
- Privacy protective technologies and limitations should be incorporated within surveillance systems. US groups have campaigned against the extension of interception capability requirements to social networking sites, and against requirements for service providers to build surveillance or monitoring capability into their systems, or to collect or retain particular information solely for state surveillance purposes. They also argue that governments should not require the identification of users as a precondition for service provision.
- Illegal surveillance should be criminalized with effective remedies when individuals' rights are breached. Illegally gathered material should be inadmissible as evidence, while whistle-blowers should be protected for revealing illegal behavior.

Civil society groups are also campaigning for greater transparency of surveillance activities, with publication of details of all surveillance programs, allowing the media, civil society, and individuals to understand and, if necessary, criticize agency activity. Industry groups are also attempting to persuade the US government to allow them to publish more detailed statistics on access to their customer data, with Facebook and Google taking legal action to claim First Amendment rights to share more information with the public about levels of access to user accounts.

Sousveillance, Equiveillance, and Resistance

There is significant resistance to state surveillance by civil liberties and environmental activists, including through the practice of what has become known as *sousveillance* – watching from below. Activists use technologies such as video recording against the surveillance authority, holding a mirror to surveillers and asking: "Do you like what you see?," thereby reducing power disparities. Social media provide a powerful platform for publishing and sharing the resulting recordings.

Surveillance practices used by less powerful groups to equalize power relations with the powerful are known as *equiveillance*. Systems like Google's "glass" could provide some of this functionality while, at the same time, gathering more data about the user for the company (and those law enforcement and intelligence agencies that have access to Google's databases).

Sousveillance can be a powerful tool for holding authority to account, as seen in the 1991 footage of police officers beating Rodney King in Los Angeles that sparked days of rioting, and in the 2012 trial of a London police officer recorded pushing a protest bystander, who fell to the ground and died shortly afterwards. Other examples include "customers photographing shopkeepers; taxi passengers photographing cab drivers; citizens photographing police officers who come to their doors; civilians photographing government officials; residents beaming satellite shots of occupying troops onto the Internet" (Mann, Nolan, & Wellman 2003, pp. 333–334).

Social Sorting

A broader concern about the development of new surveillance technologies is that they can lead to "social sorting," where discrimination and privilege are entrenched through the unplanned consequences of data gathering and analysis (Lyon, 2001). The process of identity construction itself will be increasingly shaped by targeted advertising, search results, and other types of online information presented to users based on surveillance of their previous browsing behavior.

Many public and private sector organizations use profiling to determine service levels for different customers. Employers and universities use information from internal information systems and external social networking sites for selection and disciplinary purposes. Insurers and private health care providers use biographical and transactional data for checking claims and

setting premiums. Law enforcement and intelligence agencies gather a wide range of data for prosecutions and counterterrorism investigations. In the United States, United Kingdom, and Italy, even well educated "digital native" university students have been found to have little idea about the potential consequences of sharing personal information on social networking sites.

In each of these cases there can be significant consequences for individuals, but also a potentially discriminatory broader effect if information about gender, ethnicity, religion, sexuality, social class, and other categorical data becomes a factor in employment, insurance, and criminal case decisions. Surveillance can result in further privilege for the powerful, and increasing inequality for marginal groups (Lyon et al., 2012).

While the designers of such decision-making systems have an opportunity to reduce overt discrimination by biased individuals, they may inadvertently perpetuate "the far more massive impacts of system-level biases and blind spots with regard to structural impediments that magnify the impact that disparities in starting position will have on subsequent opportunities" (Gandy, 2010, p. 34). Automated surveillance can lead to automation of social representation, and the removal of the possibility for negotiation and contention – and for rehabilitation, redemption, or change. Predictive data mining, popular as a counterterrorism tactic in the United Kingdom and the United States, may be seen as an extension of "future oriented power" that "discriminates by design, designating certain groups as threats relative to others" (Guzik, 2009, p. 1). This is an area that undoubtedly will become a major focus in future research.

SEE ALSO: Living Labs; Netnography; Network Neutrality; Privacy Law and Policy; Privacy and Social Media; Social Media; Social Media and Data Aggregation; Social Media, Mining and Profiling in; Social Search

References

Askoxylakis, I., Brown, I., Dickman, P., Friedewald, M., Irion, K., Kosta, E., … Wright, D. (2011). *To log or not to log? Risks and benefits of emerging life-logging applications*. Heraklion, Greece: European Network and Information Security Agency.

boyd, d. (2008). Why youth ♥ social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 119–142). Cambridge, MA: MIT Press.

Fuchs, C. (2011). How can surveillance be defined? *MATRIZes, 5*(1), 109–133.

Gandy, O. (2010). Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems. *Ethics and Information Technology, 12*(1), 29–42.

Guzik, K. (2009). Discrimination by design: Data mining in the United States's "war on terrorism." *Surveillance & Society, 7*(1), 1–17.

Harris Interactive & Westin, A. (1999). *IBM-Harris multi-national consumer privacy survey*. Aramonk, NY: IBM.

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In A. Joinson, K. McKenna, T. Postmes, & U.-D. Reips (Eds.), *The Oxford handbook of applied psychology* (pp. 237–252). Oxford, UK: Oxford University Press.

Lianos, M. (2003). Social control after Foucault. *Surveillance and Society, 1*(3), 412–430.

Livingstone, S. (2006). Children's privacy online: Experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, phones, and the internet: Domesticating information technology* (pp. 128–144). Oxford, UK: Oxford University Press.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham, UK: Open University Press.

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introducing surveillance studies. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 1–11). Abingdon, UK: Routledge.

Mann, S., Nolan, J., &Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society, 1*(3), 331–355.

Marwick, A., Murgia-Diaz, D., & Palfrey, J. (2010). *Youth, privacy, and reputation*. Harvard Public Law Working Paper No. 10–29.

Marx, G. T. (2012). "Your papers please": Personal and professional encounters with surveillance. In K. Ball, K. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. xx–xxx). Abingdon, UK: Routledge.

Ian Brown is Associate Director of Oxford University's Cyber Security Centre, and Senior Research Fellow at the Oxford Internet Institute.

His research focuses on information security, privacy enhancing technologies, and internet regulation. He has edited *Research Handbook on Governance of the Internet* (2013) and co-authored *Regulating Code: Good Governance and Better Regulation in the Information Age* (2013) and *Online Privacy and the Law: A European Perspective* (2014), and has contributed to many edited volumes and journals. He has consulted for organizations including the UN, Council of Europe, OECD, US Department of Homeland Security, the EC, and the Cabinet Office.