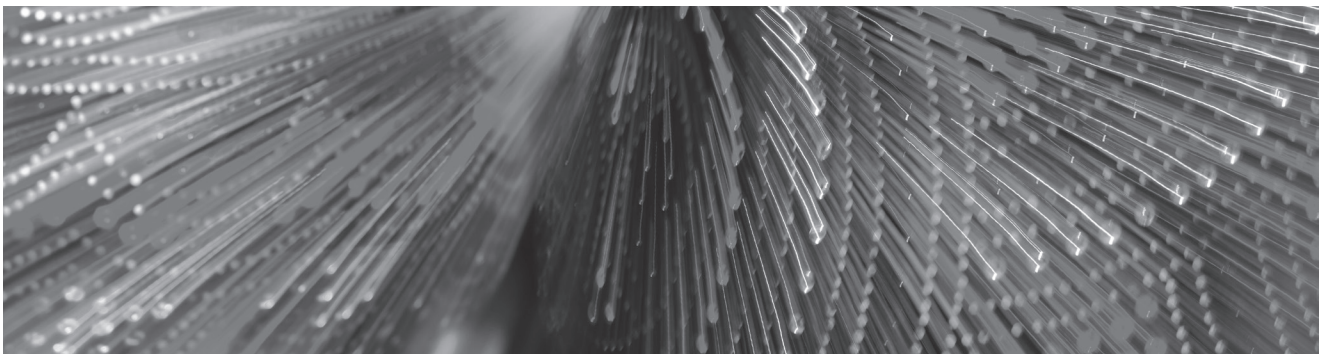
The SAGE Handbook of Social Media



Edited by
Jean Burgess,
Alice Marwick and
Thomas Poell

SAGE reference
Los Angeles | London | New Delhi | Singapore | Washington DC | Melbourne

SAGE

Los Angeles | London | New Delhi
Singapore | Washington DC | Melbourne

SAGE Publications Ltd
1 Oliver's Yard
55 City Road
London EC1Y 1SP

SAGE Publications Inc.
2455 Teller Road
Thousand Oaks, California 91320

SAGE Publications India Pvt Ltd
B 1/I 1 Mohan Cooperative Industrial Area
Mathura Road
New Delhi 110 044

SAGE Publications Asia-Pacific Pte Ltd
3 Church Street
#10-04 Samsung Hub
Singapore 049483

Editor: Michael Ainsley
Editorial Assistant: Colette Wilson
Production Editor: Sushant Nailwal
Copyeditor: Sarah Bury
Proofreader: Dick Davis
Indexer: Caroline Eley
Marketing Manager: Lucia Sweet
Cover Design: Wendy Scott
Typeset by: Cenveo Publisher Services
Printed in the UK

At SAGE we take sustainability seriously. Most of our products are printed in the UK using FSC papers and boards. When we print overseas we ensure sustainable papers are used as measured by the PREPS grading system. We undertake an annual audit to monitor our sustainability.

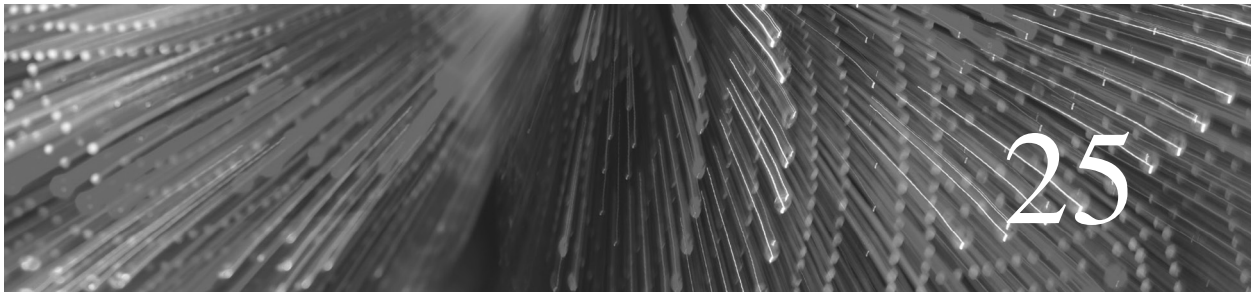
Library of Congress Control Number: 2017937664

British Library Cataloguing in Publication data

A catalogue record for this book is available from the British Library

ISBN 978-1-4129-6229-2

Contents



25

Privacy and Surveillance

Daniel Trottier

We like to think that we have control over our social media presence. Yet the fact that users are typically always connected to these profiles means that a single oversight can lead to drastic consequences. A college student I interviewed on this topic was shocked to discover that her mother was, as it turned out, her Facebook friend. While acknowledging that she must have consciously 'friended' her at some point in time, coming to terms with this connection was a lesson in social media visibility:

> I had no idea she had Facebook first of all … And I was like, 'That is so creepy!' Like, I had no idea I had my mom as a friend and I have no idea how long she has been creeping my Facebook! … And it turned out she'd been like looking at my Facebook almost every day for like five months.

While the fallout of this connection was relatively benign, this young user vowed to be more vigilant about her friendship ties, especially with people she did not know. Social media platforms like Facebook, Twitter, and Instagram allow users to circulate personal information, such as photographs and geolocative details, as well as articulate interpersonal and professional relationships. Individual users and other social actors are perpetually coming to terms with the consequences of accumulating and circulating this information. This chapter presents an overview of contemporary surveillance practices that occur on social media, focusing on how these practices force a reconsideration of privacy as a legal and cultural value.

I introduce surveillance as a social scientific concept to underline how collecting, processing and acting upon information about individuals and groups of individuals is an organizational logic of virtually every social sphere, including policing, marketing, interpersonal relations and the workplace, all of which are also present on social media. Framing social media in terms of surveillance evinces a number of concerns to be addressed. First, the asynchronous and distributed nature of information exchange on

platforms like Facebook results in forms of visibility that are both unverifiable and unanticipated. Indeed, visibility can be knowingly harnessed as a means to harm others. Second, the cross-contextual nature of many platforms results in surveillance creep, whereby personal information provided in one context is repurposed for new practices. Users rely on terms like 'creeping' and 'creepy' to make sense of such unwanted forms of exposure. Recent scholarship in the area of social media and surveillance underscores that contemporary surveillance practices may be participatory (Albrechtslund, 2008), lateral (Andrejevic, 2005), and social (Marwick, 2012). These concepts complicate panoptic understandings of surveillance, since individuals who were traditionally framed as the *object* of surveillance are active agents on social media, who may nevertheless contribute to their own visibility as well as that of other social actors. Institutions also exploit these platforms; individual use may mutually augment institutional surveillance and vice versa (Trottier, 2012).

Both users and researchers believe that social media surveillance endangers privacy. The emergence and domestication of social media has augmented these concerns by pushing personal information into the public eye. However, focusing exclusively on privacy overlooks the social complexities of social media. This chapter considers ways of understanding and resisting contemporary surveillance that fully consider privacy, but go beyond it. It will provide an overview of relevant accounts of and approaches to privacy, including legal and rights-based interpretations, performative and enacted approaches, as well as approaches that consider context and culture as key elements. These perspectives highlight controversies linked to the use of social media platforms, for example when users' expectations of privacy diverge from a platform's technical configuration. In this chapter, I also consider scholarly critiques of privacy. Public discourse typically frames privacy as an individual concern, with a narrow sense of responsibility that precludes caring for others (Lyon, 2001). Attempts to assert privacy on social platforms may also justify surveillance practices against others. Finally, privileging privacy may come at the expense of awareness of other social harms linked to surveillance, including categorical discrimination and a chilling effect on public speech.

INTRODUCING SURVEILLANCE AND VISIBILITY

Surveillance, which implies watching over others, is performed by individuals and organizations. David Lyon defines surveillance as 'processes in which special note is taken of certain human behaviors that go well beyond idle curiosity' (2007: 13). Surveillance processes can be broken into various steps: collecting personal data about individuals, processing that data, profiling those individuals or groups of individuals, and the social consequences stemming from that assessment. This distinction is worth noting due to temporal and contextual gaps between these steps. For example, an individual may write a series of tweets expressing her political views in the context of a controversial election. Years later, they may be used by a potential employer to assess that she is not a good 'fit' (Walker, 2012).

Surveillance is often understood through dystopian literature and movies, such as George Orwell's *1984* and Steven Spielberg's *Minority Report*. A well-known model in surveillance studies is the panopticon, a prison model by the 19th-century English utilitarian philosopher Jeremy Bentham, and made famous by Michel Foucault, a 20th-century French philosopher. In the panopticon, all prisoners can be viewed from a central tower, whose guards cannot be seen. Surveillance becomes both all-encompassing and uncertain, as inmates never know when they are being watched by prison guards. This

uncertainty pushes inmates to watch over themselves (Foucault, 1977: 221). This self-scrutiny is evident in contemporary society, as individuals are broadly expected to watch over their own behavior. While people are aware that their lives are visible to others, notably through socializing on social media, a lack of self-awareness may still lead users to commit a social gaffe by uploading discrediting content into the public realm (Ronson, 2015). Yet high-profile coverage of these gaffes compels everyone else to be vigilant in their self-scrutiny. For example, when a former vice-president at a public relations firm was invited to FedEx's headquarters in Memphis to give a talk about digital media, he issued a disparaging tweet about the city, offending his host (and client) in the process (Andrews, 2009). Unknowingly, this social media expert delivered an important lesson about the consequences of self-expression online.

In addition to Orwell and Foucault, surveillance studies stems from the study of police practices (Marx, 1988), emerging technologies (Norris and Armstrong, 1999; Lyon, 2009), and micro-level interactions to manage one's identity (Goffman, 1959). These studies support the view that surveillance is more than just a strategy for espionage and undercover policing, but rather a broader organizational strategy for knowing and directing a given population. In fact, gathering personal information is a dominant logic for modern governments and organizations (Dandeker, 1990), as evidenced in developments such as the census as well as modern boulevards that rendered citizens and their movements more visible. Surveillance is ubiquitous, not just because of ubiquitous technologies, but because watching and assessing pervades 'virtually every enduring social relationship' (Rule, 2011: 64). Thus, some of the dimensions that render social media 'social', including the digitization of pervasive social relations, are precisely what facilitate surveillance practices on platforms like Facebook. Many scholars contend that the rise in contemporary surveillance is partly explained by large-scale migration to urban centers. As individuals were no longer rooted in a fixed setting, people turned to modes of verification that sought to make up for the fleeting and unverifiable nature of social relations (Lyon, 2001). When reputations become less tangible, social actors may seek additional measures to ensure trust. This is most apparent in login, reputation and verification measures on social media platforms. Some users suggest that Facebook marks a return to a small town dynamic, in the sense that everyone knows everyone else's business (Trottier, 2012). Yet social media are a more enhanced form of surveillance when compared to the rural dwelling, as digital information is retained indefinitely, rendered searchable, and hosted on platforms like Facebook that are unstable and ever-changing. In other words, these social platforms are part of an emerging global techno-commercial infrastructure that greatly augments the capacity and persistence of surveillance practices through these platforms.

Surveillance processes typically target personal information, which is understood as a source of revenue to corporations (CBC, 2015), a strategic asset for security agencies (Brelsford, 2015), and a burden for individuals to manage. Personal information refers to biographical data (date of birth, nationality), but also transactional data (recent online purchases, GPS coordinates). This covers a broad range of behavioral and attitudinal measures that can be aggregated and utilized far beyond the context in which they first emerge. For example, insurance companies use social media to find evidence of fraud (Millan, 2011) or determine nebulous measures such as 'quality of life.' An insurance company asserted that a Canadian woman's presence on Facebook, including photos 'showing her having a good time at a Chippendales bar show, at her birthday party and on a sun holiday' demonstrated that she was not depressed enough to receive compensation (CBC, 2009). Quality of life is

difficult to quantify, and this ruling took place at a time when legal systems were uncertain about how much importance to attribute to Facebook evidence. Although these investigations were controversial, they demonstrate that social media content is increasingly scrutinized, and that courts make rulings based on this content. Sites like Facebook are also a prime source of information for divorce lawyers (Popken, 2011). Here, it is not the individual's profile that is scrutinized, but a combination of that presence and the spouse's access to their network of friends. A broad section of the divorced couple's social life is made visible through their use of social media. Visibility once reserved for trusted peers has crept into public sphere, and into investigative work.

Scholars recognized the pervasive and determinant nature of the profile long before social media users were updating and maintaining theirs (Gandy, 1993). The profile is the principal online interface between users and their social contacts, but also between individuals and corporations, governments and other organizations. Profiles refer to any accumulation of information of an individual by an organization, and are therefore key to online sociality as they enable users to build and maintain a consistent identity. Individual profiles range from online identities on social media, to customer profiles in loyalty card systems, to medical records within a healthcare scheme. Yet they may bear troubling consequences for users who lack control over their data or even the ability to view what an organization has collected about them. Such profiles are not operated by the user, but operate on behalf of the user, who may in turn struggle to fix disparities and cope with assessments made against them on the basis of such profiles. Likewise, vital aspects of social media profiles are beyond the individual's direct control, including tagged photos and posts on Facebook, negative reviews on Airbnb, and peer recommendations on LinkedIn.

Profiles are a quasi-involuntary construction and representation of the self. Yet the term 'profile' refers to a wide range of other 'data doubles' (Haggerty and Ericson, 2000: 606), including racial profiles for policing and geodemographic profiles based on postal codes (Burrows and Gane, 2006). Upon moving to a specific postal code, an individual may be categorized by a market research group as a 'newlywed or nearly dead' or as embracing a 'shotguns and pickup trucks' lifestyle. Again, these profiles serve as stand-ins for – or simulations of (Bogard, 1996) – the actual person, and these simulations have tangible consequences for individuals. Cumulative disadvantage (Gandy, 2009) occurs when an individual is negatively profiled, and the consequences of this profiling impact life chances, further reinforcing the negative profile. The expansion of surveillance schemes is fueled by a 'phenetic fix' (Lyon, 2002): a desire by organizations to classify and govern aspects of social life. Surveillance is a concern not only because people's social lives are visible in ways that are unanticipated, but also because models, profiles, and simulations stand in for individuals, who in turn endure the consequences. What remains unclear for both users and scholars is the extent to which their social media activity, as well as that of their peers, feeds into invisible but determinant categories in any number of social contexts. As a result, seemingly inconsequential forms of self-expression, like semi-serious conversations with friends online, feed in to a kind of permanent – and pervasive – record.

Another theme that cuts across surveillance studies is the balance between care and control. Surveillance practices are assumed to be a branch of social control, but many of these practices are implemented for the sake of ensuring a safe environment. This serves as a reminder that not all surveillance practices are received as repressive. For instance, a cyclist may value aerial cameras that monitor speeding motorists, who in turn may be thankful for the CCTV cameras in their parking garage. Likewise, social media visibility affords innumerable social benefits to

those who engage with these platforms. Yet the semblance of care is also used to justify increasingly invasive procedures, and a greater concern with personal lives. The boundary between care and control is also difficult to pinpoint, for example, when a parent who once used a baby monitor, later monitors their child's mobile phone activity, and eventually installs a tracking device in their first car (Steeves and Jones, 2010).

AN EMERGING TYPOLOGY OF USER-LED SURVEILLANCE PRACTICES

Surveillance on social media primarily concerns users' personal data. Yet these individuals themselves play a crucial role in the production and circulation of this information. Recent scholarship on this topic reveals insights about how user information is being repurposed through new practices and expectations, and how users themselves manage and even initiate these developments. In referring to social surveillance, Marwick suggests that platforms like Facebook and Instagram 'are characterized by both watching and a high awareness of being watched' (2012: 379). Social surveillance thus speaks to relationships where those who watch over others on social media are also rendered visible through these very same platforms. In practice these users balance out seemingly conflicting desires for exposure and privacy. Unlike the relationship between an employer and employee, social surveillance is a product of everyday power differentials, rather than more rigid power asymmetries. These dynamics speak to contemporary visibility on social platforms, and how in particular they inform interpersonal relationships.

Through social media, watching and being watched are bundled together, as are curating a visible and a private self. Scholars may wonder how these practices co-exist – and perhaps are co-constructed – with surveillance practices led by states and other institutional actors. Trottier (2012) refers to *mutual augmentation* to consider how formerly distinct surveillance practices by different actors in separate social contexts manifest online. Noting that many institutional actors drew from interpersonal experiences and skillsets when using social media, Trottier argues that various surveillance practices may now share the same interface, information and even the same tactics. By converging on platforms like Facebook, these different types of surveillance amplify and enhance each other. For example, recognizing that prospective employers may access their profile, job candidates may scan their friends' content with an 'employability' lens, thus internalizing and extending the gaze of the job interview. Likewise, a campus security officer may turn to a university gossip page on Facebook, taking advantage of the interpersonal scrutiny between students. As social media are governed by a logic of connectivity that relies on social media affordances to algorithmically link users to other users, content, advertisers and platforms (Van Dijck and Poell, 2013), information authored with one audience in mind has the tendency to take on an unanticipated afterlife, often to a completely different audience.

Participatory surveillance refers to a process whereby social media users knowingly share information about themselves, and derive some form of empowerment from this sharing (Albrechtslund, 2008). This perspective serves as an important intervention to scholarly and journalistic accounts that assume that users unknowingly violate their own privacy when uploading content to social platforms. Indeed, users often yield specific pleasures and values from online sharing, such as sharing exercise logs or calorie intake with an online fitness community (O'Hara, Tuffield and Shadbolt, 2008). However, it is conceptually and practically important to consider whether a user can fully consent to share personal data, given the ever-changing visibility of platforms, along with other users' unanticipated intentions. As such risks

become embedded in public awareness, we can imagine that these are factored in as a kind of transaction cost associated with participatory surveillance.

Another departure from the typical watcher/watched framework is through Mann's theory of sousveillance (Mann, Nolan and Wellman, 2003). This refers to a reversal of the surveillant gaze, whereupon the relatively powerless social actor watches (and typically records and transmits footage of) the more powerful actor. Such practices are linked to recent political movements, including Edward Snowden and Chelsea Manning's revelations about government surveillance schemes, as well as cop-watching initiatives, the latter of which takes advantage of social media to render police misconduct visible. While mobile devices and social platforms are used in key political interventions, scholars may question whether these uses contest or confirm traditional power differentials over the long term. In the case of cop-watching initiatives, consider police adoption of body-worn cameras that aim to provide a more authoritative account of the same incidents (Brucato, 2015; Sandhu and Haggerty, 2015), as well as the fact that visibility of police abuse does not readily translate into accountability.

Finally, lateral surveillance refers to a broader cultural condition of individuals watching other individuals (Andrejevic, 2005). As this concept is not limited to social media platforms, it underlines a broader media culture characterized by a lack of trust in the other, coupled with a savvy subject position that compels individuals to bypass their peers' self-presentation through a series of techniques and technologies, including nanny cams and home drug test kits. Faced with the ever-present possibility that a peer may misrepresent themselves online or in-person, this media culture privileges interpersonal surveillance (and the knowledge this might yield) over what the peer under scrutiny might claim, for instance, on a blind date. A social dynamic that crosscuts these concepts is that individuals are watching over other individuals, using the same technologies and practices to simultaneously watch over themselves. This implies a heightened preoccupation with information flows in almost any interpersonal setting. It also speaks to a blurring of the boundary that would otherwise distinguish socializing and surveillance, as both now involve the asynchronous overview of aggregated personal data on social platforms.

WHAT DOES SURVEILLANCE BRING TO OUR ATTENTION?

Approaching social media practices from a surveillance studies perspective reveals a number of features. First, the prevalence of information sharing speaks to a *datafication* of sociality on social media platforms. Surveillance studies is ultimately concerned with the use and appropriation of personal information in a range of social contexts. These concerns are heightened when discussing social media, where every click and 'like', alongside thousands of images, messages and other user inputs, contributes to an ever-growing and semi-public record. Even the absence of an active profile, along with attempts to delete data and remove one's presence, generates digital traces and thus contributes to this record. As these data are largely contained on a limited number of privately owned platforms, we may consider the latter to be a series of digital enclosures where online activity is contained, managed and brokered (Andrejevic, 2009).

Users may accept surveillance practices in some contexts, but not others. Yet the boundary between acceptable and unacceptable use is actively eroded. Consider the notion of 'function creep' and the spread of surveillance practices from one context to another (Winner, 1977; Lyon, 2007). Seemingly intrusive technologies typically emerge in airports, casinos, and other locations that can justify

a heightened scrutiny of individuals. This scrutiny is then normalized, and spreads to other contexts. Likewise, exceptional events can justify the unveiling of surveillance technologies. If a multinational company hires a social media expert, it would seem reasonable for them to scrutinize the social media presence of their short list of candidates. However, they may decide to extend this practice to all future hires. What users accept in one context may provoke unease in slightly different circumstances. Indeed, it comes as no surprise that early Facebook users drew upon this term to describe the ever-shifting landscape of information sharing (Trottier, 2012). The term 'creep' stands as a cogent way of sensing and expressing surveillance concerns.

Surveillance studies is also deeply concerned with the convergence of formerly distinct surveillance regimes. This includes merging databases and individual profiles, whether through technological innovation (Jenkins, 2006) or through post 9-11 legislation (for example, the 2001 USA PATRIOT Act; Bill C-51 in Canada). This suggests a kind of surveillant assemblage (Haggerty and Ericson, 2000) that leads to all-encompassing and seemingly irrefutable profiles, by leaking information from one context to another. The notion of the assemblage draws from postmodern contributions to theories of social control that consider the prevalence of temporary connections between discrete entities, allowing for the strategic information 'flows' and 'leaks'. Although censorship still occurs online, a generalized desire to get individuals to speak and implicate themselves is a more effective strategy for asserting a particular social order. This can be traced back to the role of the 'confession' in the Catholic church (Foucault, 1980), but it extends into contemporary culture through reality television tropes, notions of interactivity as 'empowering', and social media interfaces that solicit personal information. In some contexts, posting inflammatory content could negatively impact someone's life chances, if, for instance, they are denied employment or are unable to cross a border. Despite recent public conversations about information leaks on social media, we may be compelled to have a presence on these sites by our peers, the telecommunication industry and even our employers, and the absence of one could also lead to social harms. For example, in cities such as New York and San Francisco, landlords have refused to provide housing for tenants who don't have a visible social media presence (Morozov, 2013).

Surveillance in the context of social media underscores how all interactions on platforms like Twitter and Instagram are about the strategic and often unanticipated exchange of personal details. Perhaps more importantly, the collection and use of this information maintains a particular social order, including power asymmetries. In fact, asymmetrical visibility feeds into asymmetrical power relations. For example, the company behind a social media platform may have access to data about users that the users themselves cannot access – even if this breaches data protection laws. On the other hand, those same users may possess only minimal knowledge about the platform and its owners' intentions. They might not know how their information is being used, who views their profile, or how future platform redesigns will impact how they engage with the site. If we view the relationship between user and technology companies as adversarial, the latter has a strategic advantage that stems directly from this asymmetrical visibility.

Yet users can also harness social media visibility as a kind of weapon. During the 2011 Vancouver riot, users uploaded images and videos of suspected rioters in real time. They invited others to provide not only names, but any other available personal information, including address, employment, and scholarships. This was done to bring suspects to the attention of the police, but also to shame them and prevent others from committing similar acts (Schneider and Trottier, 2013).

This campaign took advantage of networked and distributed sociality to crowd-source a pervasive form of surveillance. Unlike earlier forms of vigilantism, these actions take advantage of the diffuse, sped-up and far-reaching circuits of visibility on social media platforms. This kind of response is becoming more common when it comes to identifying and shaming suspected child exploiters, terrorists, and those deemed guilty of minor social gaffes such as bad parking and poor public transit etiquette (Trottier, 2014). Along with 'doxxing' practices (Massanari, 2015) and the 'human flesh search engine' in China (Cheung, 2009), these cases suggest that users are harnessing networked sociality and online visibility to gather and broadcast information about targeted individuals as a type of online vigilante justice.

The above developments force a reconsideration of the prevalence and relevance of a so-called big brother in the age of social media. Those who watch over others online are dispersed in their social and political intentions, as well as their access to various forms of capital. We may instead speak of little brothers and sisters (Andrejevic, 2004). Yet little sisters do not displace big brothers. Rather, the relation between them is mutually augmenting. Little sisters may take advantage of the social visibility effected by big brother, such as using tax records to publically shame corporations. Likewise, police following a violent crime may use dozens of mobile video recordings posted by witnesses on YouTube. The uneasy co-existence of big and little siblings will remain a troubling dynamic in the study of social media surveillance.

While the following section addresses privacy, it is already evident that surveillance and data collection are concerning for reasons that extend beyond privacy. Surveillance regimes are indeed ubiquitous, multi-contextual, and increasingly converging. Public exposure is a concern, yet surveillance also contributes to profiling, a foreclosure of life chances, and patterns of discrimination.

PRIVACY AND SOCIAL MEDIA: A PRIMER

Privacy is central to both the study and personal experience of surveillance. It is a legal concern linked to individual and collective rights, but is also performed through everyday social interactions. In practice, individuals have various conceptual models of privacy which are balanced against other priorities. Privacy's relevance in modern law was identified by Warren and Brandeis, who defined it as 'the right to be let alone' (1890), that is, freedom from surveillance and scrutiny. Alan Westin also shaped the contemporary understanding of privacy in his 1967 book *Privacy and Freedom*. Westin describes privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' (1967: 337). This definition implies a degree of control over personal information flows that has been greatly complicated by social media.

While privacy is an abstract concept, it is also a cause that is championed by activists and policy makers (Bennett, 2008), as well as managed in everyday contexts by individuals (Nippert-Eng, 2010). Macro-level advocacy shapes laws, policies, and best practices through an international network of governmental and non-governmental actors. A micro-level understanding of privacy is informed by Erving Goffman's work on self-presentation (1959). His dramaturgical approach underscores the performative nature of social interactions by framing social life in terms of roles, stages and audiences. Goffman argues that individuals are deliberate and strategic in their social interactions. This is partly for the sake of cooperating with others to maintain a cohesive understanding of the world, but also to remain in good standing with others. He distinguishes between front stages, locations and contexts where social performances occur, and back stages where performances are managed. These regions map very well

with a cursory understanding of 'the public' and 'the private,' and are embedded in architectural designs (for example, most service sector workplaces have a clear barrier separating front and back stages), as well as social media interfaces, where the distinction may be more fluid.

The construction and performance of identity gains salience when considering another one of Goffman's sociological contributions: stigma (Goffman, 1963). Stigma refers to personal attributes that an individual wishes to hide from others, ranging from biographical details (a criminal record), a physical trait (a skin condition), or a social quality (an inability to understand the rules of football). Goffman contends that individuals go to great measures to hide stigmatizing information from public scrutiny, and that the privacy of the back stage is paramount for concealing these stigmas. Moreover, stigmas are as ubiquitous as the technologies and processes that risk uncovering them:

> …There is only one complete unblushing male in America: a young, married, white, urban, northern, heterosexual Protestant father of college education, fully employed, of good complexion, weight and height, and a recent record in sports. (Goffman, 1963: 128)

An oft-repeated critique of privacy concerns is that if you have nothing to hide, you have nothing to fear. Based on the pervasive nature of categorical discrimination, Goffman stresses that social interactions are typically a high-stakes affair.

Privacy is a relevant social concern. It is a legal right, and it is also a requisite for maintaining one's dignity. Yet there is more to information technologies and accountability than simply ensuring privacy rights. As a starting point, consider the many ways that individuals understand privacy. Though some of these perspectives are more nuanced than others, they all hold some degree of conceptual and empirical purchase. An initial approach to privacy is based on a private/public distinction. Such binaries are tangible, conceptually elegant ways of making sense of the social world. We can return to Goffman's front and back stages in order to understand how individuals divide the social world into 'private' and 'public'. For instance, Facebook users readily make distinctions between private regions like their inbox and public regions like an event wall. Likewise, users experience privacy violations when information in a private space leaks to a public one. While this distinction is helpful for comparative purposes, not all private spaces are identical. An initial corrective would move away from absolutes like private and public, and instead situate privacy on a continuum. Users do make these distinctions in a comparative sense: an inbox message on Facebook is private compared to a wall post, but it is still public in the sense that it has been shared with an audience of one or more. Likewise, a photo on an event page may be considered public, but could be subject to further public exposure if it were published in a newspaper.

Some scholars believe that a private/public continuum fails to fully address social complexity, and instead advocate for a contextual understanding of privacy (Nissenbaum, 2009). Users may be comfortable sharing some information with a marriage counselor, and other information with close friends. Yet having either type of information cross over to the other context might cause embarrassment and harm. Users on contextually broad platforms like Facebook or Twitter encounter this challenge as they struggle to find information they are comfortable sharing with friends, co-workers, family, and others simultaneously. Multi-contextual services need to develop privacy settings that are robust enough to maintain contextual boundaries. Perhaps the most important contextual violation is the transition from online to offline. Individuals may still expect a boundary that separates the two, yet this boundary is more permeable and requires greater effort to maintain. The now-iconic 'on the internet, nobody knows you're a dog' cartoon published in 1993 by *The New Yorker* is indicative of an antiquated understanding of privacy.

Another perspective considers how people may value privacy, yet compromise their own due to competing or conflicting values. In other words, people may choose to expose private information for the sake of achieving publicity. In a set of interviews on how users come to terms with online visibility, a college freshman likened social media to reality television and describes Facebook as: 'our own little form of entertainment where we can get a glimpse of everyone's life. … It's like our own little video camera following us around and taking snapshots of our life, for everyone to see.' Not only is the public exposure of otherwise private information seen as desirable, but it is also a reciprocal activity among peers. Users describe watching others in the same breath as being watched by others, to the extent that one practice informs and justifies the other. They acknowledge that they may regret this visibility later on – if not immediately – but that this regret is offset against other values and priorities. They do not necessarily want their personal information to be public, but they want social ties and validation, and exposure via social media is the most tangible way to obtain these things. Other users may go public for the sake of feeling secure. As one student user reports:

> By having a Facebook profile – I mean, you're agreeing to have this information posted. Like, all this information available to people. Obviously if you're posting it, you want people to see it. Because why else would you put it up there? … It's almost like an insecurity thing. And it's kind of like a way of saying, 'Oh, look at me. Look at my life. Look at all the friends that I have and look at all of the people that want to talk to me' and I don't know. I guess in that way it made me really self-conscious about Facebook.

Interpersonal security is a positive value that pushes users to compromise their online privacy. In other instances, they feel social pressure from their peers to have a public presence on social media. Among the 30 young users interviewed, there was consensus that they joined Facebook at the behest of their friends, and now maintain an active presence because of this social pressure (Trottier, 2016).

Privacy is an elusive concept, for scholars as well as social media users. Users invoke different kinds of imagery to make sense of their experiences and values on social media. These often represent some blend of compliance and discomfort with social media visibility. One set of users we interviewed initially likened their Facebook photo albums to real-life photo albums, and described privacy concerns as though strangers were breaking into their homes to browse through their photos. Others objected to this imagery, treating Facebook instead as a whiteboard on a residence door. The profile is public, fundamentally social, and meant to be shared. This imagery still links the profile to the individual's integrity, as it is still subject to abuse. Still other participants drew links between being on Facebook and being outdoors. This suggests that users should have limited expectations of secrecy, but still not be subject to invasive or humiliating encounters. Social media research often rests on the assumption that users' motivations to harness social media are tempered by privacy concerns (Ellison et al., 2011). It assumes people deliberately seek a safe space to be sociable. Yet the range of contexts and practices that we observed on social media instead suggest that other social values conflict with or compromise users' desires for privacy. Many users are not concerned with privacy when building a presence on social media; some will develop an awareness of these concerns only if they experience privacy violations. Yet many will be oblivious to privacy, regardless of how private or public they regard their information. Users often recognize that this may be contextual: while university students feel privacy invasions are not an immediate concern, they acknowledge that privacy will likely be more important when they move on to the next stage in their lives. Conversely, users who value privacy may not be concerned with it on a per-use basis. These findings speak to the risk of ubiquitous, everyday

technology. On social media, even vigilant users may compromise their privacy simply through continuous engagement.

SOCIAL MEDIA PRIVACY IN PRACTICE

Popular discourse often suggests that social media and privacy are incompatible, or at least that continued use of these platforms is linked to a general disavowal of such concerns. We may also consider a paradoxical distinction between a concern for privacy in principle and a willingness in practice to routinely disclose personal information online (Barnes, 2006). Yet recent scholarship not only considers how users articulate and perform privacy in the wake of significant legal, technical and market-based pressures (boyd and Marwick, 2011), but also how privacy – or lack thereof – on social media is further shaped by seemingly contradictory enactments on these platforms.

Users may first consider their privacy on social media when configuring their so-called privacy settings. These settings enable the user to choose with whom they consent to share specific types of personal information. On platforms like Facebook, these settings have expanded in response to user outrage, as well as government criticisms following an unanticipated and prolonged contextual expansion of the site (FBNewsroom, 2006, 2009). To be sure, Facebook's privacy settings in 2017 are more granular than they were in 2007, and users may feel overwhelmed by these changes. Yet by navigating through these settings, many users are compelled to think about their privacy in practice (boyd and Marwick, 2011). In addition, some platforms, like Snapchat, are expressly designed for ephemeral communications (Poltash, 2013), while others, like Twitter and Instagram, are primarily framed as tools for public expression. Yet even Snapchat's claims of ephemerality have been compromised by users intentionally leaking private data to the public, alongside the discovery that the platform itself retained photos that were meant to be deleted (FTC, 2014). Note that individuals are not typically bound a single platform, and may choose one over the other at a particular moment on the basis of perceived privacy affordances.

User understandings of privacy are partially shaped through platform engagement, particularly the default privacy settings (boyd and Hargittai, 2010). However, users adopt a variety of privacy-protective behaviors that are independent of privacy settings. For example, boyd and Marwick (2011) document how youngsters may conceal their thoughts and feelings in plain sight by posting song lyrics. If such lyrics are familiar to their peers, these peers will understand what the user is expressing, while parents and other unintended audiences will not access the meaning of that coded message. Other tactics include relying on pseudonyms, as well as maintaining multiple accounts that may distinguish professional roles from personal ones (Trottier, 2012). Several platforms and service providers, such as Facebook and Google, have explicitly targeted these practices through adopting 'real name' policies. These efforts have in turn been met by protest from communities such as transgender people and drag performers (Lingel and Golub, 2015). User tactics also include norms and expectations in embodied contexts; for example, the expectation that house-party attendees will not be photographed and tagged online.

When mapping the myriad ways social media privacy is understood and enacted, it bears noting that these platforms are almost entirely privately owned, which in turn confers a distinct set of rights and entitlements to the platform owners. 'Private' in this context pits platform owners' accumulation of personal data against users' expectations of self-determination in the outcomes of that data. While platforms may retain users' personal information as per their terms of service, this

entitlement may conflict with users' cultural and even legal articulations of privacy rights. To further complicate privacy concerns, social media platforms are frequently conceived of as a public sphere, even if this ideal is not actualized in practice (Fuchs, 2014). This evokes dilemmas for users as well as other concerned actors: social recognition and self-expression are desirable values, and are key motivations for social media users to upload personal information (Shao, 2009). Indeed, even those who have significant privacy concerns may still seek out a public presence on social media. Surveillance and privacy studies must therefore avoid reductionist accounts of private–public 'tradeoffs', instead focusing on the complex arrangement of motivations (which typically map on to fundamental rights) that govern use and exposure online.

CRITICAL ENGAGEMENTS WITH PRIVACY

Privacy holds purchase as a scholarly concept as well as in public discourse. Users' experiences and concerns on social media are relatively novel, and blend familiarity and unease in a manner that is typical of domesticated technologies (Silverstone and Haddon, 1996). Privacy has become a salient term to describe these experiences. Yet approaching social media visibility exclusively in terms of privacy limits the scope of a social scientific analysis and raises a number of concerns. To begin, privacy is typically conceived as an individual matter, typically overlooking precisely how the social dimensions of social media may put other social actors in harm's way. User privacy often framed as an individual responsibility, and privacy settings for social media as well as public recommendations by advocacy groups support the assumption that it is the user's responsiblity to govern their own data. Yet control over what personal information is knowable to what social actors is a form of autonomy that is largely beyond individual control. Scholars should consider interpersonal dynamics that are crucial to its functioning. In particular, the idea of collaborative identity construction (Trottier and Lyon, 2011) underscores how social media interfaces encourage users to speak on behalf of other users. Through wall posts, tags, and comments, users routinely disclose information about their peers, exposing others to public scrutiny. Concern for the self should extend to a concern for how others are subject to exposure through our own actions.

Related to this individualistic bias in privacy discourse, managing one's own privacy often results in the increased scrutiny of others. Individuals will understandably take measures to safeguard their privacy, notably in the maintenance of private spaces which necessitate securing boundaries, carefully monitoring those who enter and exit that space. Consider the gated community equipped with security cameras and facial recognition software, or the private social media platform that requires visitors to identify themselves and make their actions visible while interacting with others. Likewise, upon finding out that their privacy could be compromised on social media, young users I interviewed reported that they began watching over content their friends would post, taking active steps to manage or sanction them (Trottier, 2012). These measures exemplify the internalization of the surveillant gaze (Foucault, 1977) applied outwards to peers, in the name of self-preservation.

A further limitation of privacy is that it is too easily conceived of as a resource or commodity, which means that those with greater capital or purchasing power will be able to make use of privacy, while others will simply have to cope with unwanted and unanticipated exposure. Privacy thus becomes a luxury good instead of a fundamental right. In defining privacy as the absence of embarrassing and harmful forms of exposure, it is evident that detached houses afford residents more

privacy than apartments, and first-class airport lounges are a comparatively safer space than a crowded concourse in which to commit a jetlag-fueled gaffe. On social media, navigating interfaces and combing through content requires particular sets of media literacy, and also costs time, to say nothing of hardware and services. Many users simply do not have enough of either, and will be disproportionately subject to invasive scrutiny. Public relations efforts on social media are informed by high-profile cases involving politicians, celebrities and other public figures. This arguably constitutes a normalization of strategic identity management, along with a proliferation of online reputation management services and consultancies. While legal debates and political advocacy focus on establishing fundamental privacy and data protection rights and legislation, commoditizing privacy can circumvent a collective and rights-based preservation of privacy.

Finally, focusing on privacy in public discourse often comes at the expense of other pressing social concerns linked to surveillance and exposure on social media, including discrimination and social sorting. Privacy concerns may reduce our focus to visible and tangible artifacts, such as a user's most recent tweets. Such a focus overlooks the aggregate effect that this body of information has over 10 or 20 years, as well as the myriad of ways in which such aggregated data can be repurposed. If a user's social media presence – including their social graph of connections with others – can be used to determine their employability (Walker, 2012), or their eligibility for a bank loan (Kestler D'Amours, 2015), then it bears focusing on how these personal data feed into pervasive and opaque social categories that govern individuals. Another concern is self-censorship and the broader chilling effect that social media exposure may have on self-expression. As users come to terms with the fact that public and private speech on social media is under watch, they will adjust their behavior accordingly (Trottier, 2012). One aspect of internalizing this gaze is that they may withhold content they would otherwise wish to share with their colleagues, out of fear of unverifiable and undesirable outcomes. At an aggregate level, the increased unwillingness of users to express themselves online means that their potential for service in the public sphere is further compromised. Finally, the above concerns point to fundamental inequities when it comes to our understanding of social media platforms, and in particular user understanding of how their information is repurposed. The actions users may take to mitigate visibility and privacy, such as deleting content or closing an account, may fail to prevent these harms, especially when information remains on the platform's servers, and therefore remains vulnerable to hacks and leaks (Thomsen, 2015). As stated above, asymmetry of control and of knowledge is a primary condition that informs user experiences of privacy, of visibility and of everyday and exceptional moments of surveillance.

CONCLUSION

This chapter considers surveillance and privacy as they relate to social media and a broader digital media landscape. A surveillance studies approach locates privacy as a primary societal concern, one that is both nuanced and paradoxical. Addressing this complexity necessitates cross-disciplinary and multi-perspective research that interrogates how individuals are exposed through social media, and the risks and harms associated with this exposure. Privacy matters, as does publicity, autonomy, and the broader mix of priorities and values that motivate users to build a presence (or not) on social media platforms. It is equally important to consider the design and redesign of these platforms. The continued expansion, transformation and acquisition of sites like Twitter and Instagram shape engagements by scholars, users and policy makers. These changes challenge any definitional or functional understanding of

social media, and in particular suggest that user consent at one moment in time should not extend automatically if, for instance, the platform's user base expands tenfold, or if it is repurposed as a marketing resource.

Along with scholarly engagement, public education and outreach efforts may be effective to promote relevant forms of media literacy. Technologies and their surrounding practices are dynamic, and users are not always aware of the consequences of these changes. A lot of data schemes work by opt-out rather than opt-in, and many users only have a partial understanding of these agreements. This speaks to the weakness of individual consent (Rule, 2011), and awareness campaigns are a potential remedy for dense and largely overlooked privacy statements. Students who share these concerns may wish to examine how social media users of varying backgrounds envision and utilize privacy settings in practice, as well as how they discover and respond to violations of their privacy and informational autonomy. Likewise, the fact that many users remain active on these platforms for extended periods means that the conditions of visibility that they embraced at an earlier stage of their lives may provoke discomfort or social harms at a latter stage. Students of social media and surveillance may also wish to develop an empirically based understanding of how these users respond to such discomfort. Finally, scholarly research should not only focus on how users are coping with these developments, but also re-direct the outputs of these efforts back to users, for example by addressing the consequences of technologically-mediated transparency to a broader public (see Bennett et al., 2014).

REFERENCES

Albrechtslund, Anders. 2008. Online social networking as participatory surveillance. *First Monday*, 13(3): http://firstmonday.org/article/view/2142/1949.

Andrejevic, Mark. 2004. Little Brother is watching: The webcam subculture and the digital enclosure. In A. McCarthy and N. Couldry (Eds.), *Mediaspace: Place, scale, and culture in a media age* (pp. 109–124). New York: Routledge.

Andrejevic, Mark. 2005. The work of watching one another: lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4): 479–497.

Andrejevic, Mark. 2009. Privacy, exploitation and the digital enclosure. *Amsterdam Law Forum*, 1(4): http://amsterdamlawforum.org/article/view/94/168.

Andrews, James. 2009. True confession but I'm in one of those towns where I scratch my head and say 'I would die if I had to live here!' 14 January. https://twitter.com/keyinfluencer/statuses/1119553072.

Barnes, Susan B. 2006. A privacy paradox: Social networking in the United States. *First Monday*, 11(9): http://firstmonday.org/article/view/1394/1312.

Bennett, Colin J. 2008. *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: MIT Press.

Bennett, Colin J., Kevin D. Haggerty, David Lyon and Valerie Steeves. 2014. *Transparent lives: Surveillance in Canada*. Edmonton: Athabasca University Press.

Bogard, William. 1996. *The simulation of surveillance: Hypercontrol in telematic societies*. Cambridge, UK: Cambridge University Press.

boyd, danah and Eszter Hargittai. 2010. Facebook privacy settings: Who cares? *First Monday*, 15(8): http://journals.uic.edu/ojs/index.php/fm/article/view/3086/2589.

boyd, danah and Alice Marwick. 2011. Social privacy in networked publics: Teens' attitudes, practices, and strategies. *A decade in internet time: Symposium on the dynamics of the internet and society*. September. http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1925128.

Brelsford, Paul. 2015. *White Paper: Employing a social media monitoring tool as an OSINT platform for Intelligence, Defence & Security*. www.eurosint.eu/system/files/employing_social_media_monitoring_tools_as_an_osint_platform_for_intelligence_defence_security.pdf.

Brucato, Ben. 2015. Policing made visible: Mobile technologies and the importance of point of view. *Surveillance & Society*, 13(3/4): 455–473.

Burrows, Roger and Nicholas Gane. 2006. Geodemographics, software and class. *Sociology*, 40: 793–812.

CBC. 2009. Depressed woman loses benefits over Facebook photos. *CBC.ca*, November 21. www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html.

CBC. 2015. Windows 10 raises privacy concerns. *CBC.ca*, September 10. www.cbc.ca/news/technology/windows-10-1.3223168.

Cheung, Anne S. Y. 2009. China Internet going wild: Cyber-hunting versus privacy protection. *Computer Law & Security Review*, 25(3): 275–279.

Dandeker, Christopher. 1990. *Surveillance, power and modernity: Bureaucracy and discipline from 1700 to the present day*. New York: St Martin's Press.

Ellison, Nicole B., Jesica Vitak, Charles Steinfeld, Rebecca, Gray and Cliff Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte and L. Reinecke (Eds.), *Negotiating privacy concerns and social capital needs in a social media environment* (pp. 19–32). Berlin: Springer.

FBNewsroom. 2006. Facebook launches additional privacy controls for news feed and mini-feed. *Facebook Newsroom*. September 8. http://newsroom.fb.com/news/2006/09/facebook-launches-additional-privacy-controls-for-news-feed-and-mini-feed/.

FBNewsroom. 2009. Facebook announces privacy improvements in response to recommendations by Canadian Privacy Commissioner. *Facebook Newsoom*. August 27. http://newsroom.fb.com/news/2009/08/facebook-announces-privacy-improvements-in-response-to-recommendations-by-canadian-privacy-commissioner/.

Foucault, Michel. 1977. *Discipline and punish: The birth of the prison*. London: Allen Lane.

Foucault, Michel. 1980. *The history of sexuality*. New York: Vintage Books.

FTC. 2014. Snapchat settles FTC charges that promises of disappearing messages were false. *Federal Trade Commission Press Releases*. May 8. www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

Fuchs, Christian. 2014. Social media and the Public Sphere. *triple*, 12(1): 57–101.

Gandy, Oscar H. 1993. *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview Press.

Gandy, Oscar H. 2009. *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Farnham, UK: Ashgate.

Goffman, Erving. 1959. *The presentation of self in everyday life*. New York: Anchor Books.

Goffman, Erving. 1963. *Stigma: Notes on the management of spoiled identity*. New York: Simon & Schuster.

Haggerty, Kevin D. and Richard V. Ericson. 2000. The surveillant assemblage. *British Journal of Sociology*, 51: 605–622.

Jenkins, Henry. 2006. *Convergence culture: Where old and new media collide*. New York: New York University Press.

Kestler D'Amours, Jillian. 2015. How Facebook could affect your chances of getting a loan. *The Toronto Star*, August 10.

Lingel, Jessa and Adam Golub. 2015. In face on Facebook: Brooklyn's drag community and sociotechnical practices of online communication. *Journal of Computer-Mediated Communication*, 20(5): 536–553.

Lyon, David. 2001. *Surveillance society: Monitoring everyday life*. Milton Keynes, UK: Open University Press.

Lyon, David. 2002. Editorial. Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society*, 1(1): 1–7.

Lyon, David. 2007. *Surveillance studies: An overview*. Cambridge, UK: Polity Press.

Lyon, David. 2009. *Identifying citizens: ID cards as surveillance*. Cambridge, UK: Polity Press.

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

Marwick, Alice. 2012. The public domain: Surveillance in everyday life. *Surveillance & Society*, 9(4): 378–393.

Marx, Gary T. 1988. *Undercover: Police surveillance in America*. Berkeley, CA: University of California Press.

Massanari, Adrienne. 2015. #Gamergate and the Fappening: How Reddit's algorithm, governance, and culture support toxic

technocultures. *New Media & Society*. Published online before print (October 9). doi:10.1177/1461444815608807.

Millan, L. 2011. Insurers and social media: Insurers' use of social networks impinges on privacy rights. *The Lawyers Weekly*, March 25. www.lawyersweekly.ca/index.php?section=article&volume=30&number=43&article=2.

Morozov, Evgeny. 2013. The folly of technological solutionism. LSE Public Lecture, March 21. London.

Nippert-Eng, Christena. 2010. *Islands of privacy*. Chicago, IL: University of Chicago Press.

Nissenbaum, Helen. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

Norris, Clive and Gary Armstrong. 1999. *The maximum surveillance society: The rise of CCTV*. Oxford: Berg.

O'Hara, Kieron, Mischa M. Tuffield and Nigel Shadbolt. 2008. Lifelogging: Privacy and empowerment with memories for life. *Identity in the Information Society*, 1(1): 155–172.

Poltash, Nicole A. 2013. Snapchat and sexting: A snapshot of baring your bare essentials. *Richmond Journal of Law & Technology*, 29(4): 1–24.

Popken, B. 2011. Facebook is number one tool for divorce lawyers. *The Consumerist*, May 18. http://consumerist.com/2011/05/facebook-is-number-one-tool-for-divorce-lawyers.html.

Ronson, Jon. 2015. How one stupid tweet blew up Justine Sacco's life. *New York Times Magazine*, February 12. www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=0

Rule, James. 2011. 'Needs' for surveillance and the movement to protect privacy. In Lyon David, Kirstie Ball and Kevin D. Haggerty (Eds.), *Routledge handbook of surveillance studies* (pp. 64–71). New York: Routledge.

Sandhu, Ajay and Kevin D. Haggerty. 2015. Policing on camera. *Theoretical Criminology, Theoretical Criminology* 21(1): 78–95.

Schneider, Christopher and Daniel Trottier. 2013. Social media and the 2011 Vancouver riot. *Studies in Symbolic Interaction*, 40: 335–362.

Shao, Guosong. 2009. Understanding the appeal of user-generated media: A uses and gratification perspective. *Internet Research*, 19(1): 7–25.

Silverstone, Roger and Leslie Haddon. 1996. Design and the domestication of information and communication technologies: Technical change and everyday life. In R. Mansell and R. Silverstone (Eds.), *Communication by design: The politics of information and communication technologies* (pp. 44–74). Oxford: Oxford University Press.

Steeves, Valerie and Owain Jones. 2010. Surveillance, children and childhood. *Surveillance & Society*, 7(3/4): 187–191.

Thomsen, Simon. 2015. Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online. *Business Insider UK*, July 20. http://uk.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7?r=US&IR=T.

Trottier, Daniel. 2012. *Social media as surveillance: Rethinking visibility in a converging world*. Farnham, UK: Ashgate.

Trottier, Daniel. 2014. Vigilantism and power-users: Police and user-led investigations on social media. In D. Trottier and C. Fuchs (Eds.), *Social media, politics and the state: Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube* (pp. 209–236). New York: Routledge.

Trottier, Daniel. 2016. Caring for the virtual self on social media: Managing visibility on Facebook. In I. van der Ploeg and J. Pridmore (Eds.), *Digitizing identities*. London: Routledge.

Trottier, Daniel and David Lyon. 2011. Key features of a social media surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund and M. Sandoval (Eds.), *The internet and surveillance: The challenge of Web 2.0 and social media* (pp. 89–109). New York: Routledge.

Van Dijck, José and Thomas Poell. 2013. Understanding social media logic. *Media and Communication*, 1(1): 2–14.

Walker, Joseph. 2012. Meet the new boss: Big data. *The Wall Street Journal*. Retrieved September 20. http://online.wsj.com/article/SB10000872396390443890304578006252019616768.html.

Warren, Samuel and Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review*, 15(5).

Westin, Alan. 1967. *Privacy and freedom*. London: Atheneum.

Winner, Langdon. 1977. *Autonomous technology: Technics out of control as a theme in human thought*. Cambridge, MA: MIT Press.