Chapter 12

Doxxing: A Scoping Review and Typology

Briony Anderson and Mark A. Wood

Abstract

This chapter examines the phenomenon of doxxing: the practice of publishing private, proprietary, or personally identifying information on the internet, usually with malicious intent. Undertaking a scoping review of research into doxxing, we develop a typology of this form of technology-facilitated violence (TFV) that expands understandings of doxxing, its forms and its harms, beyond a taciturn discussion of privacy and harassment online. Building on David M. Douglas's typology of doxxing, our typology considers two key dimensions of doxxing: the form of loss experienced by the victim and the perpetrator's motivation(s) for undertaking this form of TFV. Through examining the extant literature on doxxing, we identify seven mutually non-exclusive motivations for this form of TFV: extortion, silencing, retribution, controlling, reputation-building, unintentional, and doxxing in the public interest. We conclude by identifying future areas for interdisciplinary research into doxxing that brings criminology into conversation with the insights of media-focused disciplines.

Keywords: Doxxing; Technology-facilitated violence; anonymity; privacy; personally identifying information; informational privacy

Introduction

Doxxing, a neologism derived from the hacker culture slang of "dropping dox [documents]," has been used to describe a range of acts in which private, proprietary, or personally identifying information is published on the internet against a party's wishes, usually with malicious intent. To assist researchers in distinguishing between the different forms doxxing may take, in this chapter, we undertake a scoping review of research into doxxing and develop a typology of this form of technology-facilitated violence (TFV).

The Emerald International Handbook of Technology-Facilitated Violence and Abuse, 205–226

doi:10.1108/978-1-83982-848-520211015

Our scoping review reveals that the majority of studies that have examined doxxing focus on its use either within specific fora, such as cryptomarkets (Bancroft & Scott Reid, 2017) and hacker communities (Serracino-Inglott, 2013), or against specific groups, such as white supremacists (Colton, Holmes, & Walwema, 2017). Furthermore, our review identifies seven mutually non-exclusive motivations for doxxing: *extortion*, *silencing*, *retribution*, *controlling*, *reputation-building*, *unintentional*, and *doxxing in the public interest*. These various motivations represent the first dimension of our doxxing typology. The second dimension we consider is the form of loss faced by victims of doxxing, and here we build upon David M. Douglas's (2016) compelling typological work on the phenomenon. As we hope to demonstrate, the intersections between these motivations for doxxing and the subsequent losses experienced by its victims are paramount in understanding harms associated with this form of TFVA.

Our chapter begins by reviewing Douglas's (2016) typology of doxxing, the most sophisticated typological accounting of the phenomenon to date. After detailing the methodology employed to undertake our review, we discuss our findings in three substantial sections. Drawing on Sayer's (1999) distinction between extensive and intensive research, we have divided our review into (1) extensive studies of doxxing, which examine common patterns and characteristics of doxxing; (2) intensive studies of doxxing, which examine how doxxing works within particular cases, communities, and circumstances; and (3) legal studies of doxxing, which examine legal precedent in responding to doxxing. This division, in part, reflects key methodological differences in the studies reviewed. The extensive studies of doxxing ($n = 5$) reviewed employed quantitative methods, namely large-scale cross-sectional surveys ($n = 2$; 40%), content analysis ($n = 2$; 40%), and software testing ($n = 1$; 20%). Moreover, they attempted to generate generalizable knowledge on different dimensions of doxxing. By contrast, the intensive studies of doxxing ($n = 13$) employed qualitative methods, namely interviews ($n = 3$; 23%), content analysis ($n = 4$; 31%), focus groups ($n = 1$; 8%), participant observation ($n = 2$; 15%) and discourse analysis ($n = 3$; 23%), or they represented purely theoretical treatments of doxxing ($n = 3$; 23%).

Douglas's Typology of Doxxing

Douglas (2016) offers the most sophisticated typological treatment of the nature and forms of doxxing. At its core, Douglas defines doxxing as "the intentional public release onto the internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual" (2016, p. 199). Within this definition, he distinguishes between three forms of doxxing: (1) deanonymizing doxxing; (2) targeting doxxing; and (3) delegitimizing doxxing. In each of the three forms of doxxing, Douglas (2016) identifies the individual targeted as being faced with a loss or damage to different things. In the case of deanonymizing doxxing, the target is faced with the loss of their anonymity, either in a professional or personal capacity. In the case of targeting doxxing, the target faces the loss of their obscurity, for example, through having their home address revealed online. And in the case of delegitimizing doxxing, the target faces a loss of credibility, for example, through a doxxer releasing evidence that they have engaged in willful deception or 'immoral' activity.

In conceptualizing these different forms of doxxing, Douglas (2016) draws upon Gary Marx's (1999) typology of the seven forms of *identity knowledge*: information that, if known, precludes the perfect anonymity of an individual. Marx's concept is particularly useful in conceptualizing doxxing because, as Douglas (2016) notes, it removes "some degree of anonymity from a specific person" (p. 200). For this reason, Douglas (2016) suggests that we understand doxxing as the act of publicly releasing a type of identity knowledge about an individual, which acts to establish a "verifiable connection" between one or more other types of identity knowledge about the individual (p. 201).

One important part of Douglas's definition is that it entails the *intentional* public release of personal information. This intentional release of information need not be undertaken with malicious intent. For example, journalists publicly outing the identities of an individual's pseudonym in stories represents doxxing, even when there is no intent of wrongdoing. But for Douglas, accidentally "outing" an individual on the internet through unintentionally releasing personal information does not represent doxxing. In other words, while doxxing may represent one form of outing individuals online, the two terms are not synonymous. According to Douglas (2016), doxxing is also not synonymous with blackmail, defamation and gossip, though it may represent a technique of blackmail (p. 202). Unlike gossip, doxxing trades in identity knowledge as opposed to "suggestion, hearsay [or] innuendo" (Douglas, 2016, p. 202). As Douglas (2016) cogently observes, the difference between doxxing and gossip is "the difference between communicating information *about* someone and communicating information *of* someone" (p. 202).

Methodology

The articles presented in this scoping review were obtained using two electronic research databases: Web of Science and Google Scholar. Articles and conference papers were primarily located using the search terms: "doxing," "doxxing," "dox," and "doxxed." However, to locate articles that discussed the phenomenon of doxxing without using the term, we also searched for: "publication of personal details," "publish personal details," and "exposing personal information," in combination with the terms "malicious," "threaten," "harass," "abuse," and "intimidate." Finally, a snowballing approach was employed to locate relevant articles by scanning the reference lists of each article identified.

Studies were included in the review if they met two eligibility criteria: (1) they discussed the nonconsensual disclosure of personally identifying information on the internet (i.e., doxxing); and (2) they examined the phenomenon at length, as opposed to merely in-passing. These broad inclusion criteria enabled us to include articles that, while not focusing primarily or wholly on doxxing, detailed the phenomenon at length in relation to other issues such as online hacktivism (Heemsbergen, 2016) or intimate partner violence (Fish & Follis, 2016). Articles published in languages other than English were excluded from the review.

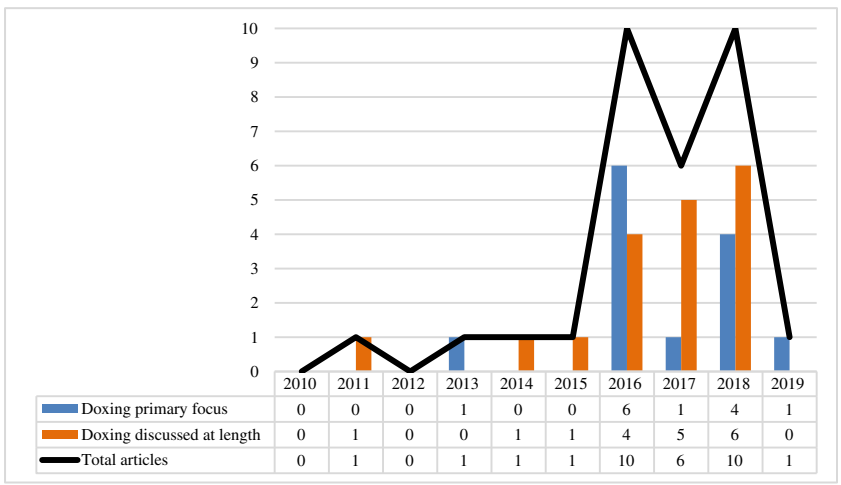
Titles, abstracts, and keywords were screened to identify clear inclusions. In cases where we were unsure of an article's eligibility, we analyzed how the terms

"doxing"/"doxxing," "doxed," or "dox" were used in context. Our initial searches returned 48 results on Google Scholar and 10 results on Web of Science. Three additional articles were located through a snowball technique for an initial total of 61 papers. Following a preliminary analysis, 29 papers were excluded as they mentioned doxxing only in-passing, leaving 32 articles, which are the focus of this chapter.

Results

As we found, the academic literature on doxxing is relatively new. Despite the term dating back to the mid-1990s, we identified no academic articles published before 2010 that employed the term in the sense explored here. Indeed, the earliest reference to the term in academic literature that we identified appears in Phillips's (2011) article on RIP Trolling (the organized practice of targeting social media memorial pages with abusive or harmful content). The overwhelming majority of the articles identified in our scoping review dated from the mid-2010s onwards, with most articles being published between 2017 and 2018. Few articles had doxxing as their primary focus. More frequently, doxxing was discussed alongside other practices, as a technique of politically motivated harassment (Colton et al., 2017; Fish & Follis, 2016; Massanari, 2015, 2018), as a form of intimate partner violence (Freed et al., 2018), or as a contestation of privacy rights (Corbridge, 2018; MacAllister, 2017) (Fig 12.1).

As noted above, we identified seven mutually non-exclusive motivations for doxxing in the literature: *extortion*, *silencing*, *retribution*, *controlling*, *reputation-building*, *unintentional*, and *public interest*. *Extortion doxxing* or "doxtortion" entails



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Doxing primary focus	0	0	0	1	0	0	6	1	4	1
Doxing discussed at length	0	1	0	0	1	1	4	5	6	0
Total articles	0	1	0	1	1	1	10	6	10	1

Fig. 12.1. Combined Line/Bar Graph Showing the Number of Doxxing-Related Studies Published per Year between 2010–2019.

releasing or threatening to release compromising information about an individual online to extort (usually) financial benefits from them. *Silencing doxxing* involves leveraging doxxing, or the threat of doxxing, to remove an individual from an online forum. *Retribution doxxing* is doxxing motivated specifically by a desire to "punish" an individual. As detailed in the studies discussed below, retribution doxxing may represent a technique of targeted harassment employed against individuals holding opposing political views. However, it may also take the form of informal justice-seeking actions (see Salter, 2013; Wood, Rose, & Thompson, 2019), wherein victims of crime seek justice beyond the formal justice system through publishing personally identifiable information online about their perpetrator's actions.

Controlling doxxing is used to control an individual's behavior. As such, it may represent a measure of technology-facilitated coercive control, often employed in concert with other iterations of intimate partner violence (Douglas, Harris, & Dragiewicz, 2019). Often coinciding with one or more of the other motivations we identified, *reputation-building doxxing* serves to grant entry or clout within a group or subculture through, for example, demonstrating skill within a hacker forum. Unlike the forms of doxxing outlined above, *unintentional doxxing* is not undertaken with malicious intent but rather results from carelessness or negligence on the part of the perpetrator. Unintentional doxxing may, for example, result from journalists failing to protect the anonymity or obscurity of their sources. Lastly, *public interest doxxing* is motivated by a belief that the release of personally identifiable or proprietary information will promote the welfare or well-being of the general public (see Cheung, this volume). Public interest doxxing may take numerous forms, including as a mechanism for holding governments, institutions, and public figures accountable, as well as a mechanism for issuing public safety announcements through, for example, releasing personally identifiable information about predatory Tinder dates.

As detailed in Table 12.1, most of these motivations can underpin more than one of the three forms of doxxing identified by Douglas (2016), leading to a variety of subcategories. However, our review of the literature also indicates that the forms of loss that may be faced by doxxing victims are not exhausted by the three forms anonymity, obscurity, and legitimacy identified by Douglas. Specifically, Douglas's original typology faces challenges when we consider the case of corporate or organizational doxxing: doxxing that targets an organization rather than an individual (Khanna, Zavarsky, & Lindskog, 2016). As we detail below, the existence of corporate doxxing necessitates the addition of a fourth form of potential loss faced by doxxing victims, *competitive advantage* over other corporations or organizations. This prompts a fourth variety of doxxing, *disadvantaging doxxing*, which may be underpinned by a variety of motivations.

Extensive Studies of Doxxing

To date, only a few studies have examined the demographic characteristics of doxxing perpetrators and victims (Chen, Chan, & Cheung, 2018; Chen, Cheung, & Chan, 2019). Drawing on a random sample of 2,120 secondary school students

Table 12.1. A Typology of Doxxing.

	Form of Information Published	Personal Identifiable Information			Proprietary Information
	Loss experienced by the victim	**Loss of anonymity (Deanonymizing doxxing)**	**Loss of obscurity (Targeting doxxing)**	**Loss of legitimacy (Delegitimizing doxxing)**	**Loss of competitive advantage (Disadvantaging doxxing)**
Motivation	**Extortion**	**Deanonymizing doxtortion** • Acquisitive doxxing extortion.	**Targeting doxtortion**	**Delegitimizing doxtortion** • Doxware-facilitated doxtortion. • Sexual extortion/ doxtortion.	**Disadvantaging doxtortion** • Corporate doxtortion (Khanna et al., 2016).
	Silencing	**Deanonymizing doxxing to silence** (Massanari, 2018; Jones, 2016). • Doxxing as a political silencing technique (Massanari, 2018).	**Targeting doxxing to silence** (Jones, 2016; Massanari, 2018). • "Swatting" a member of a marginalized community (Binder, 2018).	**Delegitimizing** doxxing **to silence** • Gamergate Zoe Quinn case: rumors of unprofessionalism imbued with sexist and derogatory comment (McIntyre, 2016).	

	Controlling	**Deanonymizing doxxing to control** (Bancroft & Scott Reid, 2017; Fish & Follis, 2016; Heemsbergen, 2016; Marwick, 2013).	**Targeting doxxing to control** (Freed et al., 2018). • Doxxing as a form of intimate partner violence (Freed et al., 2018).	**Delegitimizing doxxing to control** (Freed et al., 2018). • Threats of doxxing as a technique of coercive control (Freed et al., 2018).	
Motivation	**Retribution**	**Retributive deanonymizing doxxing** (Coleman, 2014; Colton et al., 2017; Corbridge, 2018; MacAllister, 2017; Marwick, 2013; McNealy, 2017; Serracino-Inglott, 2013; Snyder et al., 2017) • Stalking and other malicious harassment; see *Wilkinson v Downton* (Corbridge, 2018).	**Retributive targeting doxxing** (Marshak, 2017; Snyder et al., 2017)	**Retributive delegitimizing doxxing** (Chen et al., 2018, 2019; Snyder et al., 2017). • Threat to professional reputation e.g., the case of Dr Quinn (Pittman, 2018). • Nonconsensual sharing of sexual imagery.	**Retributive disadvantaging doxxing**

Table 12.1. *(Continued)*

	Form of Information Published	Personal Identifiable Information			Proprietary Information
	Loss experienced by the victim	**Loss of anonymity (Deanonymizing doxxing)**	**Loss of obscurity (Targeting doxxing)**	**Loss of legitimacy (Delegitimizing doxxing)**	**Loss of competitive advantage (Disadvantaging doxxing)**
		• Online hate campaigns; Brianna Wu case (MacAllister, 2017).			
	Reputation-building	**Deanonymizing doxxing for reputation-building** (Massanari, 2018; Snyder et al., 2017). • Doxxing as a vehicle for obtaining social capital within hacker subculture (Snyder et al., 2017).	**Targeting doxxing for reputation-building** (Massanari, 2018; Snyder et al., 2017).	**Delegitimizing doxxing for reputation-building** (Massanari, 2018; Snyder et al., 2017).	**Disadvantaging doxxing for reputation-building**
Motivation	**Public interest**	**Deanonymizing doxxing in the public interest** (Coleman, 2014; Colton et al., 2017).	**Targeting doxxing in the public interest**	**Delegitimizing doxxing in the public interest** (Oldberg, 2016). • Snowden NSA leaks as a form of	**Disadvantaging doxxing in the public interest**

	• Citizen journalists deploying Twitter and other platforms to identify attendees of a white supremacist rally.		"organisational doxxing" (Oldberg, 2016).	
Unintentional	**Unintended deanonymizing doxxing** (McNealy, 2017). • Journalistic doxxing of anonymous sources (McNealy, 2017).	**Unintended targeting doxxing** (McNealy, 2017). • Journalistic doxxing of individuals (McNealy, 2017).	**Unintended delegitimizing doxxing** (Chen et al., 2018, 2019).	**Unintended disadvantaging doxxing**

in Hong Kong, the first article published by Chan and colleagues reports on a cross-sectional survey of doxxing victimization, as well as the age, gender, and education-level demographics of doxxing victims and perpetrators. Chen et al.'s (2018) regression analysis found positive correlations between depression, anxiety, and stress, and the doxxing of most forms of personal information. Furthermore, they found strong positive correlations between the doxxing of mobile phone numbers and depression and anxiety among victims. The disclosure of phone numbers provides an example of our category of *retributive targeting doxxing*: doxxing underpinned by a perpetrator's motivation to punish a victim through facilitating harassment against them. Furthermore, Chen et al.'s (2018) study indicates that women are more likely to be victims of doxxing than men, with victimization prevalence for all but one type of information (Hong Kong ID number) higher among female students (p. 4). In the same study, 50.7% of respondents indicated that they had been doxxed by a classmate, 30.3% had been targeted by an individual in the same grade, 25.7% by a friend outside of school, and 24.6% by a parent or family member (Chen et al., 2018). Only 4.1% indicated that they had been doxxed by a stranger (Chen et al., 2018). This suggests that the interpersonal relationship between the victim and perpetrator is one of familiarity, which casts doxxing as a technique of social harassment, rather than random harassment of a stranger.

In a second article stemming from this study, Chen et al. (2019) examine adolescents' intentions when doxxing their peers. In doing so, Chen et al. (2019) distinguish between what they term social doxxing defined as "obtain[ing] social information" but not releasing it about a person they liked and hostile doxxing, which is collecting and releasing personal information with malicious intent (p. 1). Here, however, we identify several definitional concerns about the category of "social doxxing." Namely, given that the notion of social doxxing proposed by Chen et al. (2019) does not involve the *releasing* of personal information by perpetrators, does this constitute doxxing at all? We argue that it does not. Rather, what Chen et al. (2019) describe as social doxxing more accurately represents what Andrejevic (2004) has termed "lateral surveillance." There are two reasons for this: first, it involves *public* rather than *private* information which conflicts with Chen et al.'s (2019) acknowledgment that the target information of doxxing "can be any personal, private, or sensitive information" (p. 2) and second, it does not involve the release of this information.

Given social doxxing arguably falls outside the definitional boundaries of doxxing, we focus here on Chen et al.'s (2019) findings relating to hostile doxxing. Although Chen et al. (2019) did not find gender a statistically significant predictor of perpetrating hostile doxxing, the young males sampled in their study were more likely than the young women to target "personally identifiable and physical location information" (p. 11). Given the expansive definition of doxxing employed within this research includes "social information" that is publicly self-disclosed by individuals, this finding *indicates* that what is generally understood as doxxing (the public release of personally identifiable and other private information) is a gendered phenomenon in both its perpetration and victimology.

Whereas Chen et al. (2018) and Chen et al.'s (2019) study of doxxing drew upon a cross-sectional survey approach, Snyder, Doerfler, Kanich, and McCoy (2017) adopt a naturalistic approach to examining doxxing rates, employing a specialized web crawler to collect data on doxxing files uploaded to three websites associated with doxxing: Pastebin, 4Chan, and 8Chan. This approach produced several findings contrasting with those of Chen et al. (2018) and Chen et al. (2019). For example, Snyder et al. (2017) found that victims of doxxing were overwhelmingly male and a significant number were active in a gamer community (p. 432). However, we would suggest that this may be a product of Snyder et al.'s (2017) focus on files uploaded to Pastebin, 4Chan, and 8Chan, rather than a generalizable finding. Indeed, Snyder et al.'s (2017) somewhat questionable assertion that there "appears to be few dox files that appear elsewhere that do not also appear on pastebin.com, 4chan.org, and 8ch.net" (p. 434) contrasts with Chan et al.'s (2018) finding that it was instant messenger applications and mainstream social networking sites that were the most prevalent platforms used to perpetrate doxxing. This hypothesis is given further credence by the fact that two of the other main "communities" targeted by doxxing on these sites were hackers (a key community associated with 4Chan and 8Chan) and celebrities; a demographic that has been targeted by hack-facilitated doxxing (Snyder et al., 2017). This discrepancy further indicates that Snyder et al. (2017) focused on a particular subset of doxxing incidents, rather than doxxing more generally, which, as a number of the studies discussed below indicate, is often quotidian in nature and not necessarily classified as doxxing by its perpetrators.

Through their analysis, Snyder et al. (2017) identify four general motivations for doxxing: (1) *competitive*: demonstrating superior abilities within a subculture; (2) *revenge*: doxxing in retribution to a perceived harm committed against the perpetrator; (3) *justice*: doxxing someone in response to them committing an act perceived to be immoral or unfair; and (4) *political*: doxxing in the service of a goal larger than targeting a single individual. As the intensive studies discussed in the next section demonstrate, these four motivations are very much ideal types and are far from exhaustive, with doxxing also being employed for the purpose of coercion and control, among other things (Dragiewicz et al., 2018; Freed et al., 2018). Although we question Synder et al.'s (2017) distinction between revenge and justice, (given that both are underpinned by a retributive conception of justice), three key motivations for doxxing can be extracted from their typology: *reputation building* (analogous with Synder et al.'s competitive motivation), *retribution*, and *public interest* doxxing (analogous with their political motivation category) (p. 1).

Unlike the three papers detailed above, the final two articles broadly reporting on extensive studies of doxxing examine *responses* to doxxing. The first of these, Fiesler et al.'s (2018) study of the community rules governing subreddits within the social media site Reddit, provides an indication of the prevalence of anti-doxxing rules on the site. Analyzing a dataset of 100,000 subreddits, Fiesler et al. (2018) found that, of the 23,752 subreddits that had rules, only 128 (0.54%) had rules specifically prohibiting doxxing. However, it is worth contextualizing this finding by noting that posting "personal and confidential information" (i.e., doxxing) is prohibited in Reddit's (2019) Content Policy. This may explain, in part, why few of the subreddits Fiesler et al. (2018) examined banned the behavior.

The four papers examined so far in this section pertain to personal doxxing, that is, doxxing targeting an individual. Khanna et al.'s (2016) study, however, focuses on responses to *organizational* or *corporate doxxing*: releasing organizational secrets and sensitive proprietary information (see Oldberg, 2016). In their analysis, Khanna et al. (2016) examine tools used to undertake organizational doxxing attacks, most notably Maltego Chlorine CE 3.6.0, a forensics and intelligence program that gathers information from open sources. Identifying key limitations in Maltego Chlorine CE 3.6.0 as a doxxing tool, Khanna et al. (2016) suggest a number of countermeasures that organizations may employ to prevent doxxing attacks. These include employing the very tools of organizational doxxers used against companies and conducting information privacy audits through websites such as Pipl, which can trace the source of information on the internet.

Although Khanna et al. (2016) do not systematically compare and contrast corporate doxxing to doxxing targeting individuals, their analysis demonstrates two key ways in which the former may differ from the latter. Namely, corporate doxxing often differs from doxxing targeting individuals in that it (1) often involves the release of proprietary information rather than personally identifiable information; and (2) the form of loss faced by the victim is often an economic loss of competitive advantage against other corporations, as opposed to a loss of anonymity, obscurity, or legitimacy. When the form of loss is competitive advantage through the release of proprietary information, we might term such doxxing *disadvantaging doxxing*. In proposing this category, it is important to qualify that disadvantaging doxxing is not synonymous with corporate/organizational doxxing, for corporations can be the victim of both disadvantaging and delegitimizing doxxing. Moreover, that this can occur suggests that, contra Douglas, delegitimizing doxxing can be underpinned by a disclosure of either personally identifying information or proprietary information. The release of sensitive confidential information about a corporation's waste (mis)management may, for example, lead to backlash against the corporation, and consequently, economic losses as a result of boycotts. However, this economic loss is rooted in the corporation's loss of legitimacy, rather than in a loss of trade-secrets, and thus should be categorized as delegitimizing doxxing.

Intensive Studies of Doxxing

Doxxing in Forums Characterized by Social Community Anonymity

A considerable portion of the literature examining doxxing concerns its use within populations and communities characterized by strategic internet-facilitated anonymity, namely, hacker collectives and subcultures (Coleman, 2014; Fish & Follis, 2016), webcam models (Jones, 2016), darknet cryptomarkets (Bancroft & Scott Reid, 2017), and internet news story commenters (McNealy, 2017). In internet fora, where anonymity affords users protection, such as hacker subcultures and darknet cryptomarkets, doxxing may be employed as a technique to "out" individuals who break rules or to ensure compliance with a community's norms (Bancroft & Scott Reid, 2017). As Bancroft and Scott Reid's (2017) interviews with cryptomarket

users demonstrated, cryptomarket users may use the threat of doxxing for disciplining vendors who scam buyers (p. 504). In some situations, the motivation for deanonymizing individuals in these fora was retribution, falling within the category of *retributive deanonymizing doxxing*. In other situations reported in the literature, however, the motivation for deanonymizing other users was instead a bid to control behavior–what we term *deanonymizing doxxing to control*. A vendor may, for example, be "partially doxxed" through publicly releasing part of their phone number to demonstrate the doxxer's knowledge of the number, without releasing it in its entirety and opening them up to abuse (Bancroft & Scott Reid, 2017, p. 504). Such threats of doxxing would often, however, elicit a very negative response from other users. Given that in such fora "anonymising [is] both practical and a moral norm" (Bancroft & Scott Reid, 2017, p. 504), doxxing can be viewed as a threat to social community anonymity, evoking a similar response to the practice of "snitching."

While doxxing use within hacker and hacktivist subcultures has primarily been examined in relation to doxxes carried out against out-group members, doxxing also represents a strategy employed against fellow hackers (Fish & Follis, 2016; Serracino-Inglott, 2013). Writing on the hacktivist collective "Anonymous," for example, Serracino-Inglott (2013) states that "Being 'doxxed'… is perhaps the worst form of humiliation that can befall an Anon [member of Anonymous], and the community uses 'doxxing' as a form of internal discipline/punishment" (pp. 219–220). This "outing" of hackers' identities again falls under the category of *deanonymizing doxxing to control*.

Like cryptomarket vendors, hacktivists often seek to maintain anonymity on the internet to avoid law enforcement detection. Effective information management is, therefore, key to maintaining a hacktivist identity (Fish & Follis, 2016). For this reason, Fish and Follis (2016) argue that "outing" hacktivists through doxxing represents a technique for opening them up to forms of subjection: the "broader process of subordination and subject creation that [emerge] in relation to dominating institutions of power" (p. 3282). A similar line of argument is offered in Heemsbergen's (2016) analysis of doxxing as a form of control. Drawing on Brighenti's (2010) visibilities theory, Heemsbergen (2016) discusses the doxxing of hacktivists as one example of *visibilities of control*: techniques that invoke the "purposeful and contextual asymmetrisation and hierarchisation of visibilities" for the purposes of (social) control (Brighenti, 2010, p. 148).

Law-enforcement-related detection or subjection are not, however, the only motivations for doxxing members of anonymous internet communities. Nor is such doxxing employed solely in anonymous forums characterized by illicit activities. As Jones (2016) details in a study of the adult webcam model industry, doxxing is also employed in forums characterized by anonymity to harass members engaging in legal pursuits. Within the adult webcam model industry, as Jones (2016) explains, doxxing represents a key strategy employed to harass models. For this reason, the models Jones (2016) studied took stringent measures to prevent doxxing, such as keeping up-to-date firewall and virus protection to avoid hacking of personal information, turning off smartphone geotagging, using a separate work phone, and manufacturing a cam-girl identity (pp. 243–245).

Such doxxing may fall under a number of our categories. For example, when used to facilitate further harassment of a model, we might categorize the doxxing as *retributive targeting doxxing*. When used with the specific aim to remove a model from a forum, we might instead speak of *targeting doxxing to silence*.

Examining a very different population characterized by social community anonymity, McNealy (2017) describes "media doxxing," in which news media outlets dox either a source or commenter on news articles (p. 283). This may fall into one of two of our categories: *deanonymizing doxxing in the public interest* when a journalist deliberately "outs" a source citing public interest and *unintentional deanonymizing doxxing* when an individual through accident or negligence deanonymizes a person. It is worth qualifying here, however, that where the boundaries lie between journalistic reporting and doxxing is a contested issue (see Garber, 2014), and as Grey Ellis (2017) notes, we should be wary of conflating the two.

Doxxing as Digilantism and Technology-Facilitated Coercive Control

Much of the media attention doxxing has received has concerned its use by activists and other individuals for politically motivated goals. Doxxing, as Bowles (2017) describes, has become "a mainstream tool in the culture wars," while numerous news articles have examined its use by members of the alt-right (Faruqi, 2019; Grey Ellis, 2017) and Antifa (Mohammed, 2017). It is perhaps unsurprising then that a considerable portion of the small academic literature examining doxxing has similarly addressed this issue. Regardless of the politics espoused by its perpetrators, when used for political ends, doxxing represents a form of what scholars have termed "digilantism";

> …politically motivated (or putatively politically motivated) practices outside of the state that are designed to punish or bring others to account, in response to a perceived or actual dearth of institutional remedies. (Jane, 2017, p. 3)

In a socio-technical analysis of the #Gamergate controversy, Massanari (2015) examines doxxing as one technique deployed by what she terms "toxic technocultures." Such toxic technocultures, Massanari (2015) argues, are "unique in their leveraging of sociotechnical platforms as both a channel of coordination and harassment and [in their] seemingly leaderless, amorphous quality" (p. 333). Within such toxic technocultures, doxxing can represent a coordinated technique of harassment employed in response to an issue members have united against. Such doxxing can represent what we term *targeting doxxing to silence* and *delegitimizing doxxing to silence*, for it aims to "silence" or remove individuals from social media through launching coordinated harassment and/or shaming campaigns. Moreover, within such technocultures, successfully obtaining private information about a perceived "opponent" offers a vehicle for members to demonstrate technological prowess; what we term *targeting doxxing for reputation-building*.

Importantly, as Massanari's (2015) analysis demonstrates, toxic technocultures that sanction doxxing can be supported by the very design and polices of social media platforms themselves (336). This is on account of their "platform politics": "the assemblage of design, policies, and norms that encourage certain kinds of cultures and behaviors to coalesce on platforms while implicitly discouraging others" (Massanari, 2015, p. 336). Furthermore, as Massanari (2018) explores in her article on the risks and ethics of researching "alt-right" movements, researchers studying White ethnonationalist, fascist, and misogynistic communities themselves face the risk of being doxxed. Researching the alt-right, in short, can result in academics, as well as their family, friends, and professional networks, becoming targets of the "alt-right gaze" and its attendant techniques of harassment and doxxing (Massanari, 2018, p. 4).

In news media discourse, doxxing has been associated with members of the alt-right, fueled, in part by Reddit banning the r/altright subreddit for doxxing (Coldewey, 2017). It would be incorrect, however, to characterize doxxing as a weapon solely wielded by right-leaning groups. Although doxxing has been regarded as one of the alt-right's weapons of choice, the technique has also been employed *against* members of this group, as well as individuals who engage in trolling (Phillips, 2011) or identify as white supremacists (Colton et al., 2017; Mohammed, 2017). Marwick (2013), for example, explores the use of doxxing as a regulatory mechanism, targeting individuals who perpetrate hate speech on the internet anonymously or pseudonymously – a further example of what we term *deanonymizing doxxing to control*. Here, Marwick (2013) considers doxxing narrowly as an act of unmasking anonymous transgressors and considers it closely aligned with the logic of online shaming (p. 15). Yet, as Marwick (2013) notes, the use of doxxing as a regulatory mechanism is extremely vexed, for the technique "is as frequently used to further online sexism as to prevent it" (p. 14). Furthermore, it is important to qualify here that while certain forms of doxxing may follow a similar logic to online shaming, the two are not synonymous, as the aim of shaming victims is not a necessary condition of doxxing. At this point, it should be noted that no scholarship to our knowledge has considered the application of doxxing as a technique of community safety, as commonly deployed on Twitter to warn other users of "dodgy Tinder dates" or sexual assailants in a community. This phenomenon could be an exemplar of *deanonymizing doxxing in the public interest* and warrants further research attention.

As this and the preceding section have detailed, the overwhelming majority of academic research into doxxing have examined its use within the context of political, activist, and transgressive communities. However, doxxing victimization and perpetration is far from limited to political, activist/hacktivist, hacker, and cryptomarket circles. As Freed et al.'s (2018) study of technology-facilitated intimate partner violence reveals, doxxing may be readily employed as a technique of intimate partner abuse in at least three different forms. First, in an example of what we term *delegitimizing doxxing to control*, a perpetrator may threaten to release personal information shared confidentially with them (for example, sexual orientation or HIV status). Alternatively, abusers may release such information to family, friends, and employers of the victim. And finally, in

an example of either *targeting doxxing to control* or *retributive targeting doxxing*, abusers may distribute personal information about a victim to facilitate abuse by others. In the latter instance, perpetrators might, for example, create fake internet profiles that present the victim as a sex worker, leading them to be harassed by individuals seeking sexual services (Freed et al., 2018; see also; MacAllister, 2017). Owing to its use as a technique of intimate partner violence, scholars such as Dragiewicz et al. (2018) have recently proposed labeling it, along with acts such as monitoring a partner's email and stalking their Global Positioning System data, as a form of "technology-facilitated coercive control."

Jurisdictional Interpretations of Privacy and Doxxing

Although scholarly works placing doxxing within legal frameworks are scant, substantial literature about the legal definitions, rulings, and contestations of the right to privacy exists. As a breach of privacy and a technique of harassment, doxxing is aligned with these literatures, while testing the thresholds of meaning held by traditional notions of privacy. Assessing the jurisdictional interpretations of privacy in Australia, the United States and the European Union, this section will reflect on legal remedies for doxxing articulated in existing studies.

While most of the legal articles included some consideration of legal responses and remedies, Corbridge (2018) and McIntyre (2016) offer the most sustained engagement with possible legal reparations for doxxing offenses. Drawing on legislation in the Australian context, Corbridge (2018) argues that there is sufficient legal precedent to address doxxing as a harassment harm, using the South Australian Criminal Code as an exemplar. In South Australia, doxxing can be punished by up to three years in prison as a stalking offense in cases where the victim has been doxxed more than twice by a perpetrator (*Criminal Law Consolidation Act*, 1935, s. 19AA(1) (a) (ivb)). This response has several shortcomings. In the case of viral doxxing campaigns, a victim might receive hundreds of breaches of personally identifiable information, all from different users/perpetrators. This raises the question: how can the legal condition of "two or more" instances of doxxing be satisfied when the victim suffers hundreds of singular breaches of their privacy? To address this, Corbridge (2018) argues for an expansion of powers granted in the Australian Constitution to include a new statutory cause of action: "serious invasion of privacy," taking the form of a tort (p. 1). Corbridge (2018) puts forward that this approach will disregard the US propensity to lean "towards protecting freedom of information," and instead will emulate the EU's robust consideration of privacy and data protection (p. 3).

In contrast, McIntyre's (2016) work is largely critical of current legal understandings of doxxing as a form of harassment. Addressing doxxing in the US context, McIntyre's (2016) work criticizes the response of the criminal law as contingent on the outcomes of doxxing rather than the initial breach of privacy. In the United States, charges can only be laid if the doxxing leads to the facilitation of stalking and only within specific states (McIntyre, 2016, p. 118). McIntyre (2016) also highlights that "legal" doxxing–that is, information that was

published in an open access online forum before the doxxing–cannot be prosecuted as a criminal act. US interpretations of the harm of doxxing are commonly conflated with challenges to free speech rights, resulting in convoluted and circular claims of the right "to" dox. Highlighting that many statutes only apply to abuse that is "communicated directly to the victim," McIntyre (2016) exposes a key oversight in the existing US legal precedent (p. 120). While harassment offenses have historically been "events" that directly affect the victim, doxxing is a harm that both directly and tacitly affects its victim, as it combines the real risk of present-day privacy breaches with the future risk of ongoing breaches. McIntyre (2016) also offers a critique of tort remedies, finding that the tort of public disclosure of private facts is inhibited by dated definitions of "private" information, lacking the specificity of online contexts to be functionally useful as a remedy. Indeed, this is a common critique that contemporary legal responses "lack the vocabulary" to distinguish between harassment in "online" and "offline" spaces (Marshak, 2017, p. 502).

In the US context, this "lack of vocabulary" is underpinned by First Amendment considerations, which significantly impede doxxing cases from being prosecuted. Binder's (2018) article discusses the ruling of *Elonis v United States (2015)*, in which the "true threat" exception to protected speech is tested: if the doxxing resulted in "expression of an intent to commit an act of unlawful violence," then the speech is not protected by the First Amendment and can be actioned under federal anti-threat statutes (p. 63). Bizarrely, the Supreme Court held that the "true threat" exception only exists if the doxxer "subjectively views their actions as threatening," with no regard for victim perspectives (Binder, 2018, p. 63). MacAllister (2017) continues this US-centric critique in her work, examining the "true threat" exception to the First Amendment in doxxing cases. Differentiating between "intent to commit unlawful violence" and the "conditional" threats, MacAllister (2017) couches doxxing as a type of speech that is not protected by the First Amendment and can therefore be feasibly brought before a court as an offense (p. 2565). However, MacAllister (2017) also problematizes the inability to hold US internet service providers liable in cases of doxxing because of the protections afforded by the *Communications Decency Act* (1996).[1] As explored in the legal articles discussed above, legal remedies for doxxing remain unclear and provide limited consideration of victim's experiences compared to the free speech considerations of perpetrators.

In contrast to the US's prohibitive treatment of privacy as a secondary right to freedom of speech, more affirmative conceptions of individuals' right to privacy can be found in England, as well as in the *European Convention of Human Rights*. Nicole Moreham (2014), for example, shifts away from the proprietary framings of privacy by distinguishing "informational privacy" as the "misuse of private information," from "physical privacy" as "unwanted sensory access" (p. 353). In this framing of privacy, the subject can choose "the extent to which he or she is accessed by others" (2014, p. 352), echoing Corbridge's (2018) call for law to protect informational self-determination. While traditional English legal approaches treat breaches of privacy as the exchange of information, Article 8 of the *European Convention of Human Rights* broadens legal considerations of "private life" (Moreham, 2014, p. 356). Namely, Article 8 adds nuance to

considerations of privacy breaches being an imposition on the right to not be surveilled, peeped at, or infiltrated in the private domain. Importantly, Article 8 must be balanced against the perpetrator's Article 10 right to freedom of expression (Moreham, 2014, p. 359), – a key departure from the US approach, as it brings freedom of speech and privacy into *conversation with each other*. Moreham (2014) notes that an expansion of legal language to include the "right to be free from unjustified surveillance, search and recording" would clarify modern privacy problems by treating online profiles as defensibly private, or at least a sphere of limited access (p. 358). This would bring a cause of action against users who abuse this access and use online space to mediate breaches of privacy. Although this expansion of legal language is yet to occur, the UK jurisdiction is poised to be a world leader in the modernization of privacy as a legal right. Such an approach might have considerable implications for the prosecution of doxxing as a breach of individual privacy rights.

Conclusions

The phenomenon of doxxing has gradually been addressed in research examining TFV, where it has often been attached to more generic discussions of online harassment and blackmailing practices. With the notable exception of the reviewed legal studies of doxxing, few studies of doxxing have taken an applied research approach in offering recommendations for reducing harm to victims or developing prevention programs. There is, therefore, a need for policy-geared research into doxxing that extends beyond juridical responses to the phenomenon, for example, research examining doxxing victims' specific reporting needs.

Relatedly, as our review demonstrates, much of the literature on doxxing emanates not from criminology, but rather from ethics, and media and communications studies. This comparative lack of criminological research into doxxing has several consequences. For one, little research to date has examined doxxing with a specific view to its causes. To our knowledge, no study to date has focused on non-demographic predictors of individuals perpetrating doxxing, nor sought to apply or develop crime causation theories that explain different forms of this comparatively under-researched form of TFV. Of course, this is not to make a case for criminological parochialism in examining the causes of doxxing; given its mediated nature, there is much to be gained by taking an interdisciplinary approach drawing on the insights of a range of technology-focused disciplines. We therefore suggest that future research into the causes of doxxing brings criminological theory into conversation with media studies and other disciplines that engage extensively with digital technologies. Furthermore, in noting the need for further research into the causes of doxxing, it is important to issue a caveat: doxxing, like any other crime or social harm is polygenetic–it may be caused by a number of mechanisms. There can be no general theory explaining the causes of doxxing, however, criminological theory can offer transferable accounts on the mechanisms that underpin doxxing events.

In scoping out the current legal interpretations of doxxing, key gaps in the literature have emerged. Presently, legal critiques of doxxing are approached through traditional definitions and conceptualizations of privacy and harassment. As it stands, doxxing is ambiguous in the eyes of the law: it is neither a breach of privacy nor a technique of harassment, but an assemblage of both. By treating harassment and the loss of privacy as discrete outcomes of doxxing, rather than synonymous and intertwined experiences, the legal literature may miss an opportunity to robustly engage with doxxing as a unique form of TFV.

In developing our typology, we stress that it is one of ideal types. Acts of doxxing may be underpinned by multiple motivations, meaning that we must be mindful in applying the types we propose here. Moreover, while our typology considers two of the central dimensions of doxxing the (loss or form of damage faced by the victim, and the perpetrator's motivations) there are other key dimensions worth considering. Future typographical work may, for example, consider the personal information acquisition techniques employed by doxxing perpetrators, such as whether the personal information is obtained consensually or through coercion, hacking, or malware. One such example is doxxing extortion, or "doxtortion," which involves blackmailing or coercing a victim under the threat of releasing personally identifiable information. Doxtortion highlights the need to expand investigations of doxxing beyond the release of documents to encompass the threat of releasing private documents about another person. When undertaken by "doxware" or "leakware" that enables the doxtortion to be carried out by a malware program, doxtortion further complicates the notion of agent responsibility, replacing the "doxxer" with a software that threatens to publish a user's private data (Nadir & Bakhshi, 2018). This illustrates the complexity of this harm, which cannot be reduced to its human actors (see Powell, Stratton, & Cameron, 2018; Wood, 2020). By conceptualizing doxxing using a typology that interconnects motivations, expressions, and experiences of harm, it is our hope that future research will make complex and nuanced connections between the direct and tacit harms of doxxing.

Note

1. The *Communications Decency Act* (1996) outlines the rights and responsibilities of internet service providers in the United States. It primarily outlines anti-obscenity and child pornography provisions, while also detailing that internet service providers cannot be deemed "publishers" of material and are therefore exempt from liability for hate speech and harassment on their platforms.

References

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance and Society*, *2*(4), 479–497. doi:10.24908/ss.v2i4.3359

Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: The case of cryptomarket users. *Information, Communication & Society*, *20*(4), 497–512. doi:10.1080/1369118X.2016.1187643

Binder, N. (2018). From the message board to the front door: Addressing the offline consequences of race- and gender-based doxxing and swatting. *Suffolk University Law Review*, *51*(1), 55–76. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/sufflr51&div=7&id=&page=

Bowles, N. (2017). How 'doxxing' became a mainstream tool in the culture wars. *The New York Times*. Retrieved from https://www.nytimes.com/

Brighenti, A. M. (2010). *Visibility in social theory and social research*. London: Palgrave.

Chen, Q., Chan, K., & Cheung, A. (2018). Doxing victimization and emotional problems among secondary school students in Hong Kong. *International Journal of Environmental Research and Public Health*, *15*(12), 2665–2673. doi:10.3390/ijerph15122665

Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What adolescents look for and their intentions. *International Journal of Environmental Research and Public Health*, *16*(2), 1–14. doi:10.3390/ijerph16020218

Coldewey, D. (2017). Reddit bans r/altright over doxing. *Tech Crunch*. Retrieved from https://techcrunch.com/2017/02/01/reddit-bans-raltright-over-doxing/

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso.

Colton, J. S., Holmes, S., & Walwema, J. (2017). From noobguides to# OpKKK: Ethics of anonymous' tactical technical communication. *Technical Communication Quarterly*, *26*(1), 59–75. doi:10.1080/10572252.2016.1257743

Corbridge, Å. (2018). Responding to doxing in Australia: Towards a right to informational self-determination. *UniSA Student Law Review*, *3*, 1–28. Retrieved from https://ojs.unisa.edu.au/index.php/uslr/article/view/1489

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, *18*(3), 199–210. Retrieved from https://link.springer.com/article/10.1007/s10676-016-9406-0

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *The British Journal of Criminology*, *59*(3), 551–570. doi:10.1093/bjc/azy068

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, *18*(4), 609–625. doi:10.1080/14680777.2018.1447341

Faruqi, O. (2019). 'We're watching you': Why doxxing is the new weapon of choice for cyber bullies and trolls. *ABC News*. Retrieved from: https://www.abc.net.au

Fiesler, C., Jiang, J., McCann, J., Frye, K., & Brubaker, J. R. (2018). Reddit rules! Characterizing an ecosystem of governance. Twelfth International AAAI Conference on Web and Social Media. Retrieved from https://aaai.org/ocs/index.php/ICWSM/ICWSM18/paper/view/17898/16998

Fish, A., & Follis, L. (2016). Gagged and doxed: Hacktivism's self-incrimination complex. *International Journal of Communication*, *10*, 3281–3300. Retrieved from https://ijoc.org/index.php/ijoc/article/view/5386

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018, April). "A stalker's paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems* (p. 1–13). Montreal: ACM. doi:10.1145/3173574.3174241

Garber, M. (2014, March 6). Doxing: An etymology. *The Atlantic*. Retrieved from www.theatlantic.com

Grey Ellis, E. (2017). Whatever your side, doxing is a perilous form of justice. *Wired*. Retrieved from https://www.wired.com/

Heemsbergen, L. (2016). From radical transparency to radical disclosure: Reconfiguring (in) voluntary transparency through the management of visibilities. *International Journal of Communication*, *10*, 138–151. Retrieved from https://ijoc.org/index.php/ijoc/article/view/4413

Jane, E. A. (2017). Feminist digilante responses to a slut-shaming on Facebook. *Social Media+ Society*, *3*(2), 1–10. doi:10.1177/2056305117705996

Jones, A. (2016). "I get paid to have orgasms": Adult webcam models' negotiation of pleasure and danger. *Signs: Journal of Women in Culture and Society*, *42*(1), 227–256. Retrieved from https://www.journals.uchicago.edu/doi/10.1086/686758?mobileUi=0&

Khanna, P., Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks. *Procedia Computer Science*, *94*, 459–464. doi:10.1016/j.procs.2016.08.071

MacAllister, J. M. (2017). The doxing dilemma: Seeking a remedy for the malicious publication of personal information. *Fordham Law Review*, *85*(5), 2451. Retrieved from https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5370&context=flr

Marshak, E. (2017). Online harassment: A legislative solution. *Harvard Journal on Legislation*, *54*, 503. Retrieved from https://harvardjol.com/wp-content/uploads/sites/17/2017/05/HLL205.pdf

Marwick, A. (2013, October). There's no justice like angry mob justice: Regulating hate speech through internet vigilantism. In *Selected Papers of Internet Research* (Vol. 14). Denver, CO: AoIR.

Marx, G. T. (1999). What's in a name? Some reflections on the sociology of anonymity. *The Information Society*, *15*(2), 99–112. doi:10.1080/019722499128565

Massanari, A. (2015). #Gamergate and the Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society*, *19*(3), 329–346. doi:10.1177/1461444815608807

Massanari, A. L. (2018). Rethinking research ethics, power, and the risk of visibility in the era of the "alt-right" gaze. *Social Media+ Society*, *4*(2). doi:10.1177/2056305118768302

McIntyre, V. (2016). Do (x) you really want to hurt me: Adapting IIED as a solution to doxing by reshaping intent. *Tulane Journal of Technology & Intellectual Property*, *19*, 111–134. Retrieved from https://journals.tulane.edu/TIP/article/view/2667

McNealy, J. (2017). Readers react negatively to disclosure of poster's identity. *Newspaper Research Journal*, *38*(3), 282–292. doi:10.1177/0739532917722977

Mohammed, F. (2017) Is doxxing the right way to fight the "alt-right?" *JSTOR Daily*. Retrieved from https://daily.jstor.org/is-doxxing-the-right-way-to-fight-the-alt-right/

Moreham, N. A. (2014). Beyond information: Physical privacy in English law. *The Cambridge Law Journal*, *73*(2), 350–377. doi:10.1017/S0008197314000427

Nadir, I., & Bakhshi, T. (2018, March). Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1–7). Pakistan: IEEE.

Oldberg, C. J. (2016). Organizational doxing: Disaster on the doorstep. *Colorado Technology Law Journal*, *15*, 181–206. Retrieved from https://ctlj.colorado.edu/wp-content/uploads/2017/01/8-Oldberg-12.25.16_FINAL_PDF-A.pdf

Phillips, W. (2011). LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online. *First Monday*, *16*(12), 1. Retrieved from https://firstmonday.org/article/view/3168/3115

Pittman, J. (2018). Privacy in the age of doxxing. *Southern Journal of Business and Ethics*, *10*, 53–58.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. London: Routledge.

Reddit. (2019). Reddit content policy, *Reddit*. Retrieved from https://www.redditinc.com/policies/content-policy

Salter, M. (2013). Justice and revenge in online counter-publics: Emerging responses to sexual violence in the age of social media. *Crime, Media, Culture*, *9*(3), 225–242. doi:10.1177/1741659013493918

Sayer, A. (1999). *Realism and social science*. London: Sage.

Serracino-Inglott, P. (2013). Is it OK to be an anonymous? *Ethics & Global Politics*, *6*(4), 217–244. doi:10.3402/egp.v6i4.22527

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 internet measurement conference* (pp. 432–444), London: ACM.

Wood, M. A. (2020). Rethinking how technologies harm. *The British Journal of Criminology*. doi:10.1093/bjc/azaa098

Wood, M. A., Rose, E., & Thompson, C. (2019). Viral justice? Online justice-seeking, intimate partner violence and affective contagion. *Theoretical Criminology*, *23*(3), 375–393. doi:10.1177/1362480617750507