Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing

Briony Anderson
The University of Melbourne, Australia
Mark A. Wood
Deakin University, Australia

Abstract

This article develops a framework for analysing the harms of doxxing: the practice of publishing personal identifying information about someone on the internet, usually with malicious intent. Doxxing is not just a breach of privacy, nor are its effects limited to first-order harms to an individual's bodily integrity. Rather, doxxing increases the spectre of second-order harms to an individual's security interests. To better understand these harms—and the relationships between them—we draw together the theories of Bhaskar, Deleuze and Levi to develop two concepts: the virtualisation of violence and harm imbrication. The virtualisation of violence captures how, when concretised into structures, the potential for harm can be virtualised through language, writing and digitisation. We show that doxxed information virtualises violence through constituting harm-generating structures and we analyse how the virtual harm-generating potential of these structures is actualised through first- and second-order harms against a doxxing victim. The concept of harm imbrication, by contrast, helps us to analyse the often-imbricated and supervenient relationship between harms. In doing so, it helps us explain the emergent – and supervenient – relationship between doxxing's first- and second-order harms.

Keywords

Doxxing; virtuality; technology-facilitated violence; harm imbrication; digital criminology; second-order harms.

Please cite this article as:
Anderson B and Wood MA (2022) Harm imbrication and virtualised violence: Reconceptualising the harms of doxxing. *International Journal for Crime, Justice and Social Democracy* 11(1): 196-209. https://doi.org/10.5204/ijcjsd.2140

Introduction

Derived from the hacker culture slang of 'dropping dox [documents]', doxxing is the non-consensual practice of publishing private or *personal identifying information* (PII) about someone else on the internet. Such PII is 'of' you: information that is personal and identifies you in some way, such as your name, phone number, home address or workplace. Consequently, when PII is doxxed, it can become ancillary to a range of further harms, including media-facilitated harassment and other direct threats to the victim's physical security (Faruqi and Mann 2019). Here, considerations of personal security must expand beyond binary distinctions of 'offline/online' security towards a more complex accounting of 'onlife' security (Floridi 2014).

To better understand the harms of doxxing, we bring two perspectives—critical realist theory and Deleuzian theory—into conversation with criminological insights on second-order harms (Gross 1979). By synthesising insights from these perspectives, we propose a new approach to understanding the harms of doxxing that acknowledges the imbrication of empirical experiences of harm, actual harmful events and real harm-generating mechanisms that constitute threats to the future security of individuals. The harms of doxxing, we argue, lie in not only actualising 'virtual' potentialities for harm but in exponentially increasing the future potential for harm—an example of what we term the *virtualisation of violence*.

What precisely do we mean when we speak of the virtual? Criminologists typically use the term 'virtual' to describe practices or spaces generated by digital technologies (see, e.g., Fairbairn and Spencer 2018; Williams 2006). While doxxing *is* facilitated through digital technologies, our conceptualisation of the virtual does not equate it with the 'digital', 'online' or 'cyber'. We instead take Deleuze (1991) as our point of reference for conceptualising the virtual. As explicated in the work of Deleuze (1991, 1994), and, to a lesser extent, Bergson (1991), the virtual can be understood as potentialities that are 'real but not actual' (DeLanda 2016: 122). These potentialities can be actualised in myriad ways, but they can also remain dormant. Moreover, through being concretised into a structure that may generate harmful events, harm can be *virtualised*, kindling new potentials for future harms.

This article proceeds as follows. In the literature review, we examine how researchers have conceptualised the harms and motivations underpinning doxxing. Further, we situate doxxing squarely under the umbrella of technology-facilitated violence and provide a brief review of research into this field. In the next two sections, we detail how, by providing a means for conceptualising the *virtualisation* of harms, a synthesis of Bhaskar and Deleuze's ontologies may provide a useful framework for understanding the harms of doxxing and other forms of technology-facilitated violence. There are, of course, key differences between Deleuze's differential ontology and Bhaskar's critical realist ontology. However, following Rutzou (2017; see Rutzou and Elder-Vass 2019), we argue that the two ontologies might be brought into further conversation.[1] Bringing Bhaskar and Deleuze into dialogue, we argue, can offer an ontology that, among other things, enables us to acknowledge that virtual harm-generating powers are no less real than actual(ised) harms.

In the next section, we examine how harms can be further virtualized through the generativity of digital media. As we detail, this generativity is central to doxxing's second-order harms to victims' security interests. Such second-order harms can be distinguished from the first-order harms of doxxing, which entail direct setbacks to an individual's interests and bodily integrity. However, as we detail in the final discussion section, these harms are very much imbricated, and to understand them, we develop a model of harm imbrication that helps us excavate the relationships between different harm-generating structures. To imbricate is to produce an overlapping of edges, like the scales of a fish or the tiling on a roof. As we will outline, the first- and second-order harms of doxxing are discrete yet also tethered: they are identifiable as distinct events but together produce a compounding harm phenomenon that continues and escalates the disclosure of PII. This concept helps us grasp the layered, interacting and compounding elements that constitute the harms of doxxing, which are not confined to a singular breach of PII or moment of harassment. If we take each breach, dissemination or use of PII as an individual 'tile' or 'scale', we can visualise the compounding effects of doxxing as a layered, enduring and ongoing structure of harm.

Doxxing: A Brief Review

Doxxing is an umbrella term that captures several harms resulting from the non-consensual disclosure of PII on the internet. As Douglas (2016) detailed, we can identify three forms of doxxing, each characterised by a different loss faced by the victim: (1) de-anonymising doxxing; (2) targeting doxxing; and (3) delegitimising doxxing. In de-anonymising doxxing, the victim faces a loss of anonymity through the release of PII that reveals their previously unknown identity (see Serracino-Inglott 2013). To use Marx's (1999) term, de-anonymising doxxing represents a disclosure of someone else's identity knowledge: information that, if known, precludes the perfect anonymity of an individual. In targeting doxxing, by contrast, the victim faces a loss of obscurity through the release of information that allows them to be physically located (see Jones 2016; Massanari 2017). Finally, in delegitimising doxxing, the victim faces a loss of credibility or legitimacy due to doxxed PII undermining their reputation (see Freed et al. 2018).

Much of the academic literature on doxxing has examined the practice as a form of digilantism: that is, as one of many vigilante-style activities carried out using the internet (see Colton, Holmes and Walwema 2017; Marwick 2013; Phillips 2011; Trottier 2020). However, while doxxing is sometimes associated with the digilantism of activists revealing the identity or physical location of political opponents (Mohammed 2017), it can also be underpinned by a variety of other motivations (see Anderson and Wood 2021). These include extortion (Khanna, Zavarsky and Lindskog 2016), silencing individuals on internet forms (Jones 2016), controlling another's behaviour (Freed et al. 2018; see also Dragiewicz et al. 2018), retribution (Snyder et al. 2017), reputation-building (Massanari 2017; Trottier 2020), releasing information in the public interest (Colton, Holmes and Walwema 2017) and unintentionally releasing information about another (McNealy 2017).

To date, the majority of research on doxxing has come not from criminology but from media studies (see Anderson and Wood 2021), where researchers have generated important insights on the veillance cultures informing contemporary doxxing (Eckert and Metzger-Riftkin 2020b) and the emergence of dox-for-hire services (Snyder et al. 2017: 433). The small number of criminological studies that have examined doxxing have tended to frame it as a form of technology-facilitated violence (see Anderson and Wood 2021; Dragiewicz et al. 2018). Technology-facilitated violence is an umbrella term that refers to instances where (digital) technologies are employed to enact physical, psychological or financial harm against another. The term captures technology-facilitated sexual violence such as image-based sexual abuse (Henry and Powell 2018), technology-facilitated domestic abuse (Dragiewicz et al. 2018) and other forms of what Wall (2001) has termed 'cyberviolence', such as hate speech and abuse perpetrated using social media (Matamoros-Fernández 2017). Often imbued with gendered and racial slurs, such cyberviolence is disproportionately levelled against women of colour (Calabro 2018: 61), and, as we will argue, it is imperative that accounts of doxxing consider the intersecting identity categories that shape victims' experiences of the practice.

The Virtual and The Actual

For doxxing victims, the release of de-anonymising, de-obscuring or delegitimising information creates a spectre of future harm—a spectre doxxing shares with other information-transmitted harms, including the non-consensual sharing of sexual images (Dodge 2019; McGlynn, Rackley and Houghton 2017). In this respect, doxxing may follow the following 'life cycle': (1) the *impetus* of initiating harm where previously private PII is publicly disclosed; (2) the *reception* of this publicly disclosed PII by other actors, who may use the newly disclosed information to enact harms upon the victim; and (3) the *diffusion* of the PII breach, which may invite further harms or breaches against the victim. This diffusion of PII may have no foreseeable endpoint, as it is remediated and rewrought in a cyclic repetition of harm. Indeed, the lack of a foreseeable endpoint may constitute one of the chief psychological harms wrought by doxxing. Within this cycle of repetition, remediation and reception, the harm is not experienced as a discrete event. Rather, it is an iterance of disclosure that may occur—and be experienced—repeatedly.

Like both critical victimology and corporeal victimology (Spencer 2015), our approach to understanding these harms is informed by Bhaskar (2008) and Archer's (1995) critical realist social theory. However, unlike corporeal victimology, our approach does not foreground the body. Rather, our approach focuses on the potential of technological mechanisms to *elongate* harms and generate non-subjective harms that are not experienced by their victims. This is not to minimise the embodied nature of harms experienced by victims but rather to emphasise the *range* of harms and *potentialities* for harm opened by new forms of technology-facilitated violence. To this end, Bhaskar's (2008) critical realist ontology offers a useful framework for understanding harms that go on 'behind our backs' (Walklate 2003: 122). Indeed, such an ontology proves particularly useful when we address the harms of doxxing and image-based abuse, which may occur without a victim's direct experience of them. Further, a critical realist ontology exhorts us to shift from focusing on harmful (Actual) events to the (Real) generative mechanisms that give rise to these events. In doing so, it emphasises the potentialities for harm encased in digital objects created to harm. Building on Walklate's (2006) use of critical realism to inform critical victimology, we can readily map these layers of harm onto Bhaskar's (2008) three-tiered ontology of the Real, Actual and Empirical:

- Real = generative mechanisms giving rise to harm
- Actual = harmful events
- Empirical = subjective experiences of harm

In conceptualising the Real generative mechanisms that give rise to harm, we can further benefit from considering Deleuze's (1994) distinction between the actual and the virtual. As Deleuzian scholars such as DeLanda (2016: 122) have explained, we can understand the ontological status of the virtual as 'real but not actual'. Elsewhere, DeLanda and Harman (2017: 68) have expounded on the virtual by analogising it as the power a knife has to cut—it lies dormant but possible, until its power is actualised by being picked up and used. For Deleuze (1994: 209), 'the reality of the virtual is structure'—a statement that is redolent of Bhaskar's notion of the generative or causal powers of structures. Translated into Bhaskar's terms, the virtual represents Real causal powers that, while present in the structural makeup of an Actual event, have *not* contributed to generating this event. When read through Bhaskar's (2008) critical realist ontology, 'the actualization of the virtual' (Deleuze and Parnet 2007: 149) constitutes the moment when concatenations of Real generative mechanisms give rise to Actual events. Consequently, we suggest conceptualising the virtual as *dormant generative powers*; that is, generative mechanisms that are not exercised (Archer 1995), activated or actualised. Indeed, Deleuzians such as DeLanda (2016) have explained the virtual in similar terms, with Bryant (2011) going so far as to argue that Bhaskar's notion of generative mechanisms can only make sense through recourse to a notion of the virtual.

Here, it is important to acknowledge that our approach to the virtual aligns with Bryant's (2011) approach to the concept. Bryant is a speculative realist who, though influenced primarily by Deleuze, has also listed Bhaskar as an influence. Bryant's work has identified key homologies between Bhaskar and Deleuze's work, and through identifying aporias in Deleuze's ontology, he has provided a means of incorporating Deleuzian concepts—such as the virtual—into (critical) realist accounts of structures. In Bryant's (2011: 112) reading of the Deleuzian concept, 'the virtual must … be strictly conceived as a part of discrete entities such that each object has its own virtual dimension'. 'The virtual', Bryant (2011: 105) explained, 'is always the potential harbored or carried by a discrete or individual being'. This conceptualisation of the virtual as 'the potential harbored or carried by a discrete or individual being' is wholly compatible with Bhaskar's claim that (Real) objects and structures can be 'out of phase' with the events they have the ability to produce.

What is the benefit of bringing Bhaskar and Deleuze into dialogue in this way? We might consider the following hypothetical to understand why it is necessary to invoke the virtual in understanding harm. Unbeknown to an individual, they are doxxed, and their PII is disclosed on a social media platform. However, the doxxed information is not viewed by others on the platform—amid the constant deluge of information created by users, it is quickly buried beneath new data. If an individual's doxxed information is not viewed by others and the individual is unaware that they have been doxxed, has harm occurred? An empiricist might say that the initial act of doxxing the information is harmful because it breaches the

individual's privacy. This would locate the harm primarily in the act of doxxing itself—releasing the information. However, what about after the information has been doxxed? Can we say that the information remaining in the public domain is harmful, even if nobody views it? If we think it is, then we already presuppose the virtual because we acknowledge that the doxxed information carries the potential to harm—a potential that remains even if it is not actualised. If, as we suggest, doxxed information is a harmful structure even when it does not (continue to) generate harmful events, then we must consider how harm can virtually reside in structures. When it is understood in this way, virtual harm-generating powers are no less real than actual harms. While they have not actualised, such virtual harm-generating powers are real harms because they represent a threat to the future security interests of an individual.

This spectre of object-inscribed harm comes close to the two directions of hauntology Fisher (2014: 19) described: first, 'that which is … no longer, but remains effective as a virtuality', and second, 'that which (in actuality) has not yet happened, but which is already effective in the virtual'. The harmful event of PII being released may have passed, but the potential for this PII to harm remains effective as a virtuality. Conversely, the doxxing of an individual's PII might not have yet led to them experiencing harm, but such experiences are already effective in the virtual. However, in drawing together Bhaskar and Deleuze, we are able to see how these harm-generating virtualities are no less real than harmful events because they are, as Bryant (2011: 105) noted, virtualities harboured by discrete—and very real—objects or structures.

The Virtualisation of Violence

If the virtual represents the forces and tendencies in an object that may be actualised, what precisely do we mean by virtualisation? Building on Deleuze, Lévy (1998: 26) defined virtualisation as 'the transition from the actual to the virtual'. This transition, Lévy (1998: 26) argued, signals 'a displacement of the center of ontological gravity of the object considered', whether through delocalisation, desynchronisation, multiplication, exteriorisation or mediatisation. Crucially, this displacement of an object's centre of ontological gravity is generative. When something is virtualised, new potentialities are generated, heralding shifts in the object's identity. For Lévy (1998: 98), the emergence of 'humanity' can be attributed to a progressive process of virtualisation through language, technology and social institutions. As Lévy (1998: 98) argued:

> Three processes of virtualization led to the emergence of humanity. The first is associated with signs: a virtualization of real time. The second with technology: the virtualization of action, the body, and the physical environment. The third process increases with the growing complexity of social relations. To express this as concisely as possible, we could say it involves the virtualization of violence. Ritual, religion, morality, law, economic and political regulations are social mechanisms for virtualizing relations of force, immediate impulses, instincts, desires.

For our purposes, we might readily recalibrate this notion of the *virtualisation of violence* to account for how violence has been virtualised, first through language, then through writing, and then later, again, through digitisation. In other words, though the mediatisation of crime into digital domains has increased the virtualisation of harm, it is important to emphasise that digitisation is *not* a necessary condition for the virtualisation of harm. As Lévy (1998: 164) argued, 'the process of virtualization is only completed with the construction of the object, an object that is independent of the perceptions and acts of the individual subject, an object whose sensible image, its manipulation, causal effect or concept, can be shared by other subjects'. Therefore, harm is virtualised when it is concretised into a structure that may generate future harmful events. Such structures need not be digital. However, there are several characteristics of digitisation and digital structures that render them a powerful source of harm virtualisation. Key among these is the *generativity* of digital technologies: their ability to foster the creation of new structures, innovations, connections, socialities and other outputs not envisioned by their creators (Msiska and Nielsen 2018; Zittrain 2008).

For Deleuze (1991, 1994; see Deleuze and Parnet 2007: 148), generativity is a core characteristic of the virtual—an argument that accords with Bhaskar's (2008) view that generative mechanisms comprise the Real. This emphasis on generativity is not foreign to discussions of digital technologies. Indeed, the potentially generative qualities of the internet have figured in numerous accounts of digital technologies, most notably in the work of Zittrain (2006, 2008). For Zittrain (2008: 1980), generativity denotes 'a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences'. It is this technological generativity of the internet that underpins its *programming power*: its ability to engineer new networks and new socialities (Castells 2009; see Thompson and Wood 2018). Indeed, for Terranova (2001: 109), computer-mediated communication virtualises through creating new potentialities for connectivity. However, when speaking of the generativity of the internet, Zittrain (2008) focused primarily on the issue of technological innovation.

Generative technologies, Zittrain (2006) argued, are modifiable technologies that facilitate rather than constrain innovation and development on the part of unaccredited users. However, Zittrain's conception of technological generativity is certainly consonant with a Deleuzian emphasis on the generativity of the virtual. Such a 'parallax view' (see Karatani 2005) of Zittrain via Deleuze via Bhaskar helps us emphasise that the generativity of digital technologies lies in their capacity to generate not only innovations but also harm-generating structures that threaten the security of individuals. Indeed, Zittrain himself acknowledged the Janus-faced nature of technological generativity. In fostering innovation, Zittrain (2008: 8) noted, a generative internet also encourages disruption and security threats—an issue he framed as the 'generativity-as-vulnerability problem' (Zittrain 2006: 2017). Digital technologies, in other words, are also generative of security threats, or what Gross termed 'second-order harms' to individuals' security interests.

The First- and Second-Order Harms of Doxxing

As Gross (1979: 125) explained, first-order harms represent direct setbacks to an individual's interests and bodily integrity. By contrast, second-order harms are setbacks to an individuals' security interests. As Ramsay (2011: 207) explained, such second-order harms can be distinguished into two categories: setbacks to an individual's objective security interests and setbacks to their subjective security (see Zedner 2009). First conceptualised well before the advent of the World Wide Web, Gross' (1979) concept of second-order harms nonetheless has great utility in understanding the virtualisation and imbrication of technology-facilitated harms such as doxxing. Doxxing can constitute both first- and second-order harms through disclosing and compromising PII. Here, we might consider one of the harms of doxxing to be its deleterious effects on the *integrity* of PII; once breached, the anonymous online abuse of PII can, uninterrupted, interfere with an individual's livelihood and personal life. Following this breach, an individual might encounter setbacks to a number of tenets of security, including the expectation of anonymity, the right to a private life and the right to be forgotten—a concept already upheld in the EU *General Data Protection Regulation* (GDPR): Regulation (EU) 2016/679 and the *Data Protection Act* (UK) 2018.

We can frame these future risks attached to the diminished integrity of PII as *harm potentialities*, marked as distinct from 'actualised' harms. Harm potentialities entail virtual risks to the objective and subjective security of individuals that can be actualised in first- and second-order harms. In the case of doxxing, these potentialities be can actualised simply through learning that one's PII has been compromised—a setback to the doxxing victim's subjective security. Indeed, the anxiety wrought through these virtual potentials for future harm represents one of the key second-order harms of doxxing. Such second-order harms were vividly recounted by Wu (2015: 47), who described the deleterious present and future effects of her doxxing:

> You have to constantly ask yourself if your post will put you or your loved ones in danger. After 150 death threats, after people have called your private phone while masturbating, after the stories written about your murder, you worry. You ask yourself if pictures taken will give away addresses, you worry about your pets when you leave your house. Knowing that hate-

> speech sites continually monitor everything you tweet or write, you constantly second-guess everything you say publicly.

Importantly, to understand the harms of doxxing, we must consider not only the nature of the loss or injury experienced by a victim but also the role technologies play in co-producing these losses and injuries. One framework for doing this is the technology–harm relations approach, which analyses relations with technology that are harmful by virtue of what they contribute to bringing about (Wood 2021a). To understand the role technologies play in co-producing harms, the technology–harm relations approach distinguishes between instrumental relations and generative relations on one axis and utility relations and technicity relations on another (see Figure 1). Instrumental relations arise when technologies are used in a manner that harms, whereas generative relations refer to relations with technology that are harmful by virtue of what they do to actors (Wood 2021a: 4-5). Instrumental and generative relations can then be distinguished along a second axis that considers whether or not a technology's contribution to a harmful event results from the technology functioning as its designers intended. Here, we can distinguish between utility relations—which stem from a technology functioning as intended by its designers (Wood 2021a)—and technicity relations—which result when technologies do not function as their designers intended. Given the multiply determined nature of (harmful) events (see Elder-Vass 2010), harmful events can be underpinned by multiple technology–harm relations (see Wood 2021a).

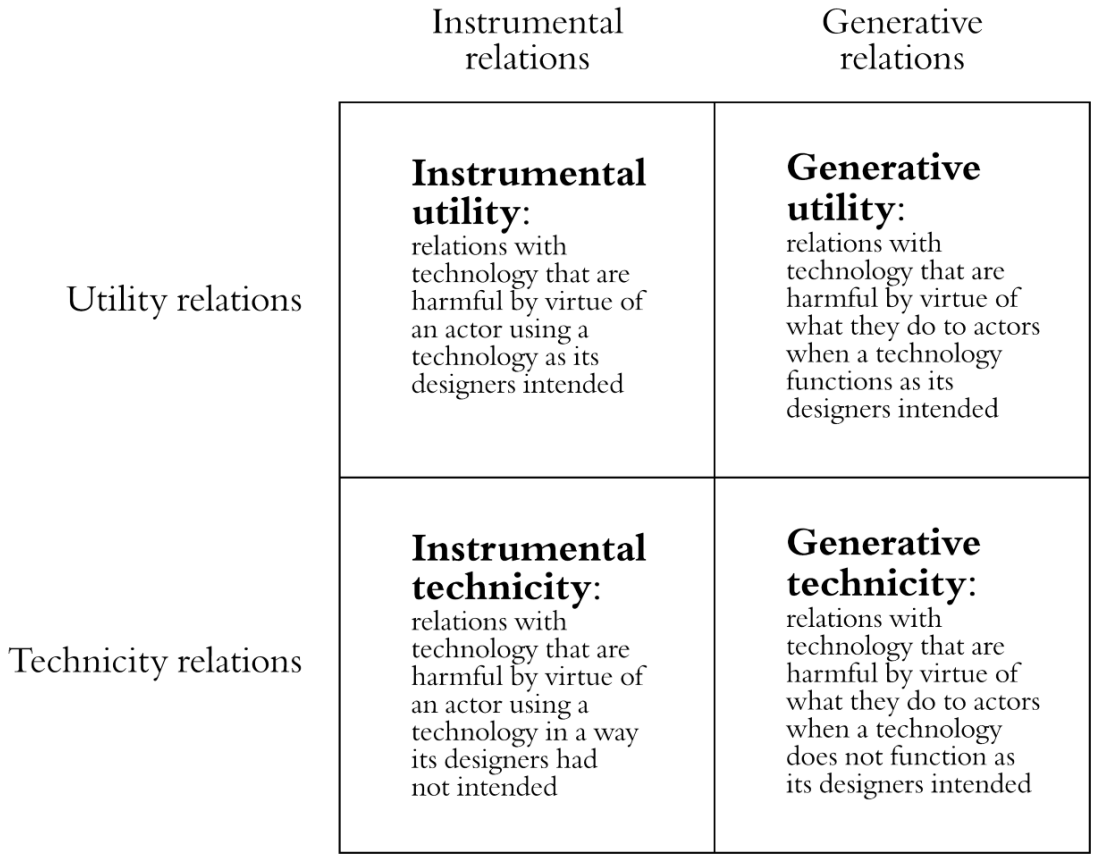

Figure 1. A typology of technology–harm relations

In the case of doxxing, first-order harms to an individual's interests and bodily integrity result, first, when an individual uses new media to disclose PII about an individual publicly, and second, when additional individuals use the affordances provided by this newly available information to physically or emotionally harm the subject of this information. In many instances, the first-order harms to a victim's bodily integrity and identity represent a product of what can be termed instrumental technicity relations, wherein 'harm

results from an unintended use of a technology' (i.e., a use of the technology that was not intended by its designers) (Wood 2021a: 4). While the affordances of mainstream new media platforms readily enable doxxing, such platforms are not designed *for* doxxing, and many – including Facebook, Twitter and Reddit – prohibit the practice. Doxxing, in other words, rarely represents one of the preferred or acceptable uses platform designers consider in (re)designing their platforms. Rather, doxxing emerged from the internet's technicity: its ontological force in generating new uses and functions in its wake.

However, as the notion of second-order harms captures, the harms of doxxing are not exhausted by these first-order harms. Rather, they extend to encompass the prospect of further first-order harms (objective security), as well as the emotional and psychological harms resulting from this setback to a targeted individual's security interests (subjective security). While these setbacks are put into motion by the doxxer's first breach of PII, they may be sustained, elongated and intensified by the internet's generativity, its power to create or generate new behaviours, socialities and needs among its users. Key among these new behaviours, Eckert and Metzger-Riftkin (2020b) argued, are the information sharing behaviours promoted by technologies of surveillance capitalism (see Zuboff 2019). Such information sharing behaviours not only increase the reach of doxxed information but, as Eckert and Metzger-Riftkin (2020b) noted, also increase the likelihood of doxxing occurring through encouraging individuals to share PII on digital platforms. For this reason, they conceptualised doxxing as:

> a gendered process enmeshing online and offline spaces in which others' personal information is shared intentionally or unintentionally but non-consensually, triggering negative fall out for affected users and their networks. In violation of contextual integrity, personal information, accumulated online and offline, is moved from expected, intentional, or desired online spaces to unanticipated, unintentional, or undesired online spaces, typically making it available to hostile or exploitative individuals or entities through media technology designed to prompt users to share personal information. (Eckert and Metzger-Rifkin 2020b: 285)

In this respect, the second-order harms of doxxing are conduced by what can be termed generative utility relations, wherein 'harm results from a technology functioning as its designers intended' (Wood 2021a: 4). In this sense, the second-order harms of doxxing can be an unintended consequence of an intended function of most social media: increasing the production and flow of user-generated behavioural data through social algorithms and social media buttons (see Gerlitz and Helmond 2013; Powell, Stratton and Cameron 2018; Wood 2017; Wood, Rose and Thompson 2019). Thus, when considering the role of technologies in the harms of doxxing, we cannot readily reduce doxxing to either the intended or unintended effects of technologies. Rather, as we detail in the following section, the harms of doxxing arise from *imbrication* of different relations with technology.

Harm Imbrication

In geology, the concept of imbrication refers to geological strata that overlap in the manner of toppled dominos. Beyond geology, imbrication refers to the process of overlapping, layering and staggering many discrete items to form a larger whole. A roof tile or a fish scale is both an individual item and constitutive object that, in concert with other items, sustains and supports a larger structure. This analogy of imbrication, we suggest, can help us understand the relationship between doxxing's first- and second-order harms. However, to do so, a better-developed conceptualisation of harm imbrication is needed. We can again turn to the ontology of critical realism to develop this concept.

In developing the notion of harm imbrication, we can—following critical realism's distinction between horizontal explanations and vertical explanations—distinguish between instances of *vertical* and *horizontal harm imbrication*. As Collier (1994: 109) explained, 'it is important to distinguish the way in which one mechanism explains another (which we may call *vertical explanation*) from the way in which a mechanism plus a stimulus explain an event (*horizontal explanation*)'. Adapting the notion of vertical explanation to understanding harm, in vertical harm imbrication, a higher-order harm emerges from a

structure containing properties and powers generating a lower-order harm. In line with the principles of weak emergence, higher-order harms emerge from particular structural relationships between multiple parts (see Elder-Vass 2010), parts which include one or more powers generating lower-order harms. Importantly, for two harms to be vertically imbricated, there must be a relationship of supervenient dependence between the higher-order harm and the lower-order harm(s) it partly emerges from. In other words, for the higher-order harm to manifest, the lower-order harm must also manifest – the powers that produce the lower order harm must be activated, rather than unexercised.

Conversely, we can use the notion of horizontal harm imbrication when, in explaining harmful events, a harmful *event* is comprised of several discrete harms, each co-produced by the powers of different structures. Unlike vertical harm imbrication, in horizontal harm imbrication, these harm-generating structures are not rooted in or emergent from one another. As such, neither vertical nor horizontal harm imbrication is merely a harm-focused analogue of vertical and horizontal explanation. If this were so, there would be a risk of tautology; horizontal harm imbrication would simply refer to explanations acknowledging that harmful events are multiply determined by numerous mechanisms, and any mechanism that co-produces a harmful event could be described as a 'harm-generating mechanism'. Rather, horizontal harm imbrication captures the imbrication of multiple harms in a single event, each multiply determined by discrete structures, such that this imbrication compounds or otherwise transforms the overall harm done to the harmed entity.

Our concept of (horizontal) harm imbrication differs from, yet remains compatible with, intersectional approaches to harms (see Collins and Bilge 2020; Goff, Thomas and Jackson 2008). Elaborating this distinction is important given that the analogy of imbrication has been used to describe intersectional understandings of harm (see Carastathis 2014). When explaining an intersectional approach to understanding oppression, Mann (2012: 178), for example, stated that 'rather than viewing separate oppressions as distinct categories, "intersectionality describes a more fluid, mutually constrictive process" whereby every social act is imbricated by gender, race, class, and sexuality'. Like the notion of imbricated harms, intersectional harms are similarly characterised by an emergent as opposed to an additive structure. However, contra our conceptualisation of harm imbrication, intersectional approaches to harms specifically concern harms that affect an individual on account of their membership within different but inseparable identity categories (e.g., an individual's intersecting gendered, racialised and class identities). While intersectional harms can, therefore, represent an important example of harm imbrication, the latter notion is considerably broader in also encompassing harmful events that do not affect individuals on account of their intersecting identity categories. In other words, though animbricated harm may be experienced differently on account of an individual's identity categories, a distinct configuration of intersecting identify categories is not a necessary condition for the harm to occur.

Importantly, this is not to discount the utility of intersectionality in understanding the harms of doxxing. Doxxing *is* shaped by the different but inseparable identity categories of the targeted individual (Eckert and Metzger-Riftkin 2020a: 1, 2020b). For one, abuse and harassment facilitated by a PII breach are often informed by the victim's intersectional identity. Such doxxing-facilitated abuse can be gendered, racialised *and* classist in character, for example, when it overtly targets someone specifically as a black, working-class woman. Further, even when such abuse is not overtly intersectional, it can be informed by the abuser's views on these intersecting identity categories—views that are themselves informed by 'multiple interlocking systems of privilege and oppression' (Bowleg 2012: 1267).

Beyond the abuser's motivations, such first-order harms facilitated by doxxing may differentially affect victims on account of their intersectional identity. The intersectional identity of a doxxing victim may, for example, help or hinder their attempts to curtail the spread of their doxxed PII through reporting the breach to the police or social media platforms. Here, we need to consider how the technologies and platforms that distribute doxxed PII are in no way value-neutral but are characterised by 'platform politics' (see Gillespie 2010) that can be implicated in the spread of doxxed information. Such platform politics are, as Massanari (2017: 336) explained, 'the assemblage of design, policies, and norms that encourage certain kinds of cultures and behaviors to coalesce on platforms while implicitly discouraging others'. Further, as

Massanari (2017) detailed in her analysis of #Gamergate and The Fappening, the platform politics of social media can amplify the harms of doxxing and the forms of harassment it may facilitate. When a social media platform allows the doxxing of certain identities but intercedes to bar the doxxing of other identities, we again need to acknowledge the intersectional operation of doxxing's harms.

As signalled earlier, the notion of harm imbrication offers a means to understand the relationship between the first- and second-order harms of doxxing. In doxxing, setbacks to an individual's security interests (second-order harms) are rooted in a doxxer's initial disclosure of their PII. Yet importantly, this setback to their security interests, in turn, exposes them to further first-order physical and psychological harms—harms that hinge on the doxxing victim's newly disclosed PII. These first-order harms perpetrated against a doxxing victim emerge from a particular structural relationship between multiple parts that include – but are not limited to – the doxxed information itself. As the release of this PII into an unanticipated, unintentional, or undesired space itself constitutes a second-order harm to the doxxing victim, doxxing's first and second-order harms are vertically imbricated.

As detailed earlier, doxxing's ability to produce ongoing second-order harms owes much to the generativity of digital media platforms. These second-order harms to the individual's security are, we argue, characterised by a generative utility relation, stemming from the internet's capacity to engineer new networks and connections, including connections with the doxxed PII. The generativity of digital media broadens the scope of who can see and, therefore, partake in the PII disclosure. However, in doing so, it also increases the potentialities for future harm by virtue of visibility and the implications of 'digital eternity' (Corbridge 2018: 17). In the context of a 'digital eternity' of generative second-order doxxing harms, we might observe a fundamental difference in the power relations between the doxxer and the doxxed. The doxxer provides the catalyst for harm in the first breach of PII—but the cumulative effects of the second-order doxxing harms extend beyond this, constituting a generative malaise of virtualised violence.

In addition to this, a doxxing event can take place and not be (re)mediated to any user, including the victim of PII disclosure. In such cases, there *will* be a setback to the doxxing victim's objective security, but not to their subjective security (see Zedner 2009). Therefore, the second-order harms of doxxing are a necessary but insufficient condition of further first-order harms against the interests and bodily integrity of a doxxing victim. In the case of targeting doxxing, individuals may not use doxxed PII to actually harass the doxxing victim. Though the doxxed PII may *allow* individuals to harass or harm the doxxing victim in ways that they formerly could not, such first-order harms will only occur if individuals are willing to perpetrate such harms against the victim. Further, in the case of delegitimising doxxing, the release of PII aimed at harming the victim's credibility or legitimacy may have no such effect and may instead raise the victim's standing among those who view the doxxed information.

Here, the notion of horizontal harm imbrication can come into play and help us understand the ongoing first-order harms opened up by an individual's doxxing. Such first-order harms, including abuse, harassment and sharing-on the doxxed PII, are a product of multiple harm-generating structures and may be perpetrated by a (sometimes large) number of actors. When this is the case, a doxxing victim can be beset by a deluge of abuse, wherein multiple imbricated acts of abuse constitute a single harmful event. To understand these harmful events, we must consider, of course, the doxxed information as a harm-generating structure—the virtualisation of violence through its mediatisation. However, we also must consider a far broader set of harm-generating structures that produce individuals who are willing to harass or otherwise harm doxxing victims.

Conclusion

In this paper, we have brought Deleuzian and critical realist theory into dialogue to offer a framework for understanding the harms of doxxing. Doxxing, we have argued, provides an example of the virtualisation of violence. In doxxing, an individual's PII is concretised into a structure that may generate future harmful events. There is, therefore, utility in distinguishing between a doxxing victim's *experiences* of harm, the

harmful *events* that arise from being doxxed and the *mechanisms* and *powers* that cause these harmful events. In examining the latter, we benefit from not only distinguishing between the first- and second-order harms of doxxing and the technology–harm relations that characterise them but also from examining how these harms are deeply imbricated. Such a conceptualisation of the imbricated harms of doxxing has key implications for legal responses to doxxing. Namely, through addressing the imbricated first- and second-order harms of doxxing, our analysis has indicated that legal responses to doxxing should not reduce the behaviour to a breach of informational privacy but should also acknowledge the second-order harms rendered upon the security interests of individuals.

By attending to the harms of doxxing and offering the concept of harm imbrication, we hope to have expanded ongoing theoretical considerations of technology-facilitated violence. Applied to the harms of doxxing, the notion of harm imbrication offers a framework for addressing both the instantiation of discrete doxxing harms and the compounding effects of multiple, continuous and potential doxxing harms in the present and in perpetuity. However, the concept of harm imbrication has applicability well beyond doxxing and other forms of technology-facilitated violence. It provides a way to examine not only how harm-generating structures can be rooted in, but emergent from, other harm-generating structures (vertical harm imbrication), but also how a harmful *event* may consist of several discrete harms, each co-produced by different structures (horizontal harm imbrication).

Correspondence:
Briony Anderson, PhD Candidate in Criminology, The University of Melbourne, Victoria, Australia.
briony@student.unimelb.edu.au
Dr Mark A. Wood, Lecturer in Criminology, Deakin University, Victoria, Australia.
mark.wood@deakin.edu.au

[1] Calling for such cross-pollination between these two perspectives is now far from novel, as Rutzou and Elder-Vass (2019) noted. In addition to Rutzou (2017) and Elder-Vass' (Rutzou and Elder-Vass 2019) work bringing Deleuze and Bhaskar into dialogue, a variety of theorists associated with speculative realism (Bryant 2011), assemblage theory (DeLanda 2016) and critical realism (Decoteau 2018) have staged productive conversations between these theorists.

References

Anderson B and Wood MA (2021) Doxxing: A scoping review and typology. In Bailey J, Flynn A and Henry N (eds) *The Emerald international handbook of technology-facilitated violence and abuse:* 205-226 Bingley: Emerald Publishing.
Archer MS (1995) *Realist social theory: The morphogenetic approach*. Cambridge: Cambridge University Press.
Bergson H (1991) *Matter and memory.* Cambridge: MIT Press.
Bhaskar R (2008) *A realist theory of science*. London: Routledge.
Bowleg L (2012) The problem with the phrase women and minorities: intersectionality—an important theoretical framework for public health. *American journal of public health* 102(7): 1267-1273. https://doi.org/10.2105/AJPH.2012.300750
Bryant LR (2011) *The democracy of objects*. London: Open Humanities Press.
Calabro SM (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): 55-73. https://sites.suffolk.edu/lawreview/2020/02/27/from-the-message-board-to-the-front-door-addressing-the-offline-consequences-of-race-and-gender-based-doxxing-and-swatting/

Carastathis A (2014) The concept of intersectionality in feminist theory. *Philosophy Compass* 9(5): 304-314. https://doi.org/10.1111/phc3.12129
Castells M (2009) *Communication power*. New York: Oxford University Press.
Collier A (1994) *Critical realism: An introduction to Roy Bhaskar's philosophy*. London: Verso.
Collins PH and Bilge S (2020) *Intersectionality*. 2nd ed. Hoboken: John Wiley & Sons.
Colton JS, Holmes S and Walwema J (2017) From noobguides to #OpKKK: Ethics of anonymous' tactical technical communication. *Technical Communication Quarterly* 26(1): 59-75. https://doi.org/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. https://ojs.unisa.edu.au/index.php/uslr/article/view/1489
Decoteau CL (2018) Conjunctures and assemblages: Approaches to multicausal explanation in the human sciences. In Rutzou T and Steinmetz G (eds) Crit*ical realism, history, and philosophy in the social sciences*: 89-118. Bingley: Emerald Publishing.
DeLanda M (2016) *Assemblage theory*. Edinburgh: Edinburgh University Press.
DeLanda M and Harman G (2017) *The rise of realism*. Cambridge: Polity.
Deleuze G (1991) *Bergsonism.* New York: Zone Books.
Deleuze G (1994) *Difference and repetition.* New York: Columbia University Press.
Deleuze G and Parnet C (2007) *Dialogues II*. New York: Columbia University Press.
Dodge A (2019) Nudes are forever: Judicial interpretations of digital technology's impact on "revenge porn". *Canadian Journal of Law and Society* 34(1): 121-143. https://doi.org/10.1017/cls.2019.4
Douglas DM (2016) Doxing: A conceptual analysis. *Ethics and information technology* 18(3): 199-210. https://doi.org/10.1007/s10676-016-9406-0
Dragiewicz M, Burgess J, Matamoros-Fernandez A, Salter M, Suzor NP, Woodlock D and Harris B (2018) Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies* 18(4): 609-625. https://doi.org/10.1080/14680777.2018.1447341
Eckert S and Metzger-Riftkin J (2020a) Doxxing. In Ross K, Bachmann I, Cardo V, Moorti S and Scarcelli CM (eds) *The international encyclopedia of gender, media, and communication*: 1-5. Chichester: Wiley-Blackwell.
Eckert S and Metzger-Riftkin J (2020b) Doxxing, privacy and gendered harassment. The shock and normalization of veillance cultures. *M&K Medien & Kommunikationswissenschaft* 68(3): 273-287. https://doi.org/10.5771/1615-634X-2020-3-273
Elder-Vass D (2010) *The causal power of social structures: Emergence, structure and agency*. Cambridge: Cambridge University Press.
Fairbairn J and Spencer D (2018) Virtualized violence and anonymous juries: Unpacking Steubenville's "big red" sexual assault case and the role of social media. *Feminist Criminology* 13(5): 477-497. https://doi.org/10.1177%2F1557085116687032
Faruqi O and Mann A (2019) 'We're watching you': Why doxxing is the new weapon of choice for cyber bullies and trolls. *ABC News*, 22 February. https://www.abc.net.au/news/2019-02-22/doxxing-the-new-weapon-of-choice-for-trolls/10833428
Fisher M (2014) *Ghosts of my life: Writings on depression, hauntology and lost futures*. Winchester: Zero Books.
Floridi L (2014) *The 4th revolution: How the infosphere is reshaping human reality*. New York: Oxford University Press.
Freed D, Palmer J, Minchala D, Levy K, Ristenpart T and Dell N (2018) "A stalker's Paradise": How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems:* 1-13. Paper 667. New York: Association for Computing Machinery. https://doi.org/10.1145/3173574.3174241
Gerlitz C and Helmond A (2013) The like economy: Social buttons and the data-intensive web. *New Media & Society* 15(8): 1348-1365. https://doi.org/10.1177%2F1461444812472322
Gillespie T (2010) The politics of 'platforms'. *New Media & Society* 12(3): 347-364. https://doi.org/10.1177%2F1461444809342738
Goff PA, Thomas MA and Jackson MC (2008) "Ain't I a woman?": Towards an intersectional approach to person perception and group-based harms. *Sex Roles: A Journal of Research* 59(5-6): 392-403. https://psycnet.apa.org/doi/10.1007/s11199-008-9505-4
Gross H (1979) *A theory of criminal justice.* New York: Oxford University Press.
Henry N and Powell A (2018) Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse* 19(2): 195-208. https://doi.org/10.1177%2F1524838016650189
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. https://doi.org/10.1086/686758
Karatani K (2005) *Transcritique on Kant and Marx*. Cambridge: MIT Press.

Khanna P, Zavarsky P and 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. https://doi.org/10.1016/j.procs.2016.08.071
Lévy P (1998) *Becoming virtual: Reality in the digital age*. New York: Plenum Trade.
Mann SA (2012) *Doing feminist theory: From modernity to postmodernity*. Oxford: Oxford University Press.
Marx GT (1999) What's in a name? Some reflections on the sociology of anonymity. *The Information Society* 15(2): 99-112. https://doi.org/10.1080/019722499128565
Marwick A (2013) There's no justice like angry mob justice: Regulating hate speech through internet vigilantism. *AoIR Selected Papers of Internet Research* 14: 1-16.
Massanari A (2017) #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society* 19(3): 329-346. https://doi.org/10.1177%2F1461444815608807
Matamoros-Fernández A (2017) Platformed racism: The mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube. *Information, Communication & Society* 20(6): 930-946. https://doi.org/10.1080/1369118X.2017.1293130
McGlynn C, Rackley E and Houghton R (2017) Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies* 25(1): 25-46. https://doi.org/10.1007/s10691-017-9343-2
McNealy J (2017) Readers react negatively to disclosure of poster's identity. *Newspaper Research Journal* 38(3): 282-292. https://doi.org/10.1177%2F0739532917722977
Mohammed F (2017) Is doxxing the right way to fight the "alt-right"? *JSTOR Daily*, August 30. https://daily.jstor.org/is-doxxing-the-right-way-to-fight-the-alt-right/
Msiska B and Nielsen P (2018) Innovation in the fringes of software ecosystems: the role of socio-technical generativity. *Information Technology for Development* 24(2): 398-421. https://doi.org/10.1080/02681102.2017.1400939
Phillips W (2011) LOLing at tragedy: Facebook trolls, memorial pages and resistance to grief online. *First Monday* 16(12). https://firstmonday.org/article/view/3168/3115
Powell A, Stratton G and Cameron R (2018) *Digital criminology: Crime and justice in digital society*. New York: Routledge.
Ramsay P (2011) Preparation offences, security interests, political freedom. In Duff RA, Farmer L, Marshall SE, Renzo M and Tadros V (eds) *The structures of the criminal law*: 203-228. Oxford: Oxford University Press.
Rutzou T (2017) Finding Bhaskar in all the wrong places? Causation, process, and structure in Bhaskar and Deleuze. *Journal for the Theory of Social Behaviour* 47(4): 402-417. https://doi.org/10.1111/jtsb.12138
Rutzou T and Elder-Vass D (2019) On assemblages and things: Fluidity, stability, causation stories, and formation stories. *Sociological Theory* 37(4): 401-424. https://doi.org/10.1177%2F0735275119888250
Serracino-Inglott P (2013) Is it OK to be an anonymous? *Ethics & Global Politics* 6(4): 217-244. https://doi.org/10.3402/egp.v6i4.22527
Spencer DC (2015) Corporeal realism and victimology. *International Review of Victimology* 21(1): 31-44. https://doi.org/10.1177%2F0269758014547992
Snyder P, Doerfler P, Kanich C and McCoy D (2017) Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 Internet Measurement Conference*: 432-444. New York: Association for Computing Machinery. https://doi.org/10.1145/3131365.3131385
Terranova T (2001) Demonstrating the globe: Virtual action in the network society. In Holmes D (ed.) *Virtual globalization: Virtual spaces/tourist spaces:* 105-123. London: Routledge.
Thompson C and Wood MA (2018) A media archaeology of the creepshot. *Feminist Media Studies* 18(4): 560-574. https://doi.org/10.1080/14680777.2018.1447429
Trottier D (2020) Denunciation and doxing: Towards a conceptual model of digital vigilantism. *Global Crime* 21(3-4): 196-212. https://doi.org/10.1080/17440572.2019.1591952
Walklate S (2003) *Understanding criminology: Current theoretical debates*. 2nd ed. Buckingham: Open University Press.
Walklate S (2006) *Imagining the victim of crime*. Buckingham: Open University Press.
Wall DS (2001) Cybercrimes and the internet. In Wall DS (ed.) *Crime and the internet*: 1-17. New York: Routledge.
Williams M (2006) *Virtually criminal: Crime, deviance and regulation online*. London: Routledge.
Wu B (2015) Doxxed: Impact of online threats on women including private details being exposed and "swatting". Plus Greg Lukianoff on balancing offence and free speech. *Index on Censorship* 44(3): 46-49. https://doi.org/10.1177%2F0306422015605714
Wood MA (2017) *Antisocial media: Crime-watching in the internet age*. London: Palgrave Macmillan.
Wood MA, Rose E and Thompson C (2019) Viral justice? Online justice-seeking, intimate partner violence and affective contagion. *Theoretical Criminology* 23(3): 375-393. https://doi.org/10.1177%2F1362480617750507
Wood MA (2021a) Mapping technology–harm relations: From ambient harms to zemiosis. *Crime, Media, Culture: An International Journal*. Advance online publication. https://doi.org/10.1177%2F17416590211037384

Wood MA (2021b) Rethinking how technologies harm. *British Journal of Criminology* 61(3): 627-647. https://doi-org.eres.qnl.qa/10.1093/bjc/azaa074
Zedner L (2009) *Security*. New York: Routledge.
Zittrain J (2006) The generative internet. *Harvard Law Review* 119: 1974-2040. https://dash.harvard.edu/handle/1/9385626
Zittrain J (2008) *The future of the internet—and how to stop it*. London: Penguin. https://dash.harvard.edu/handle/1/4455262
Zuboff S (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

Legislation

Data Protection Act 2018 (UK)
EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679