Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms

Abstract
This article describes domestic violence as a key context of online misogyny, foregrounding the role of digital media in mediating, coordinating, and regulating it; and proposing an agenda for future research. Scholars and anti-violence advocates have documented the ways digital media exacerbate existing patterns of gendered violence and introduce new modes of abuse, a trend highlighted by this special issue. We propose the term "technology facilitated coercive control" (TFCC) to encompass the technological and relational aspects of patterns of abuse against intimate partners. Our definition of TFCC is grounded in the understanding of domestic violence (DV) as coercive, controlling, and profoundly contextualised in relationship dynamics, cultural norms, and structural inequality. We situate TFCC within the multiple affordances and modes of governance of digital media platforms for amplifying and ameliorating abuse. In addition to investigating TFCC, scholars are beginning to document the ways platforms can engender counter-misogynistic discourse, and are powerful actors for positive change via the regulation and governance of online abuse. Accordingly, we propose four key directions for a TFCC research agenda that recognises and asks new questions about the role of digital media platforms as both facilitators of abuse and potential partners in TFCC prevention and intervention.

Keywords: coercive control, domestic violence, digital media, platform governance, misogyny
Introduction

Scholars and anti-violence advocates have begun to document the ways digital media technologies and platforms exacerbate existing patterns of gendered violence and introduce new modes of abuse. There is also evidence that digital media can play a
powerful role in responding to and preventing violence and abuse (e.g. Hand, Chung and Peters 2009; Southworth, Dawson, Fraser and Tucker 2005), trends highlighted by this special issue. This article describes domestic violence (DV) as a key context of online misogyny, foregrounding the positive and negative roles of social media and internet companies in mediating, coordinating, and regulating it. First, we synthesise the extant research on digital media technology and domestic violence to identify four challenges for platform governance. Next, we identify four pressing issues which complicate efforts to address digital platforms’ facilitation of domestic violence. Finally, we propose an agenda and methodological innovations for future research on technology and domestic violence.

**Terminology**

The debates about how to refer to and define violence and abuse against intimate partners are well-rehearsed and long-running (Dragiewicz 2011; DeKeseredy, Dragiewicz and Schwartz 2017). Scholars use a range of different terms that have come to be associated with various theoretical and methodological approaches. While a full discussion of the pros and cons of different terms is beyond the purview of this article, we acknowledge that: there is no scholarly consensus about which term(s) to use; different terms point to different contexts of violence and abuse and therefore different phenomena; and no term is perfect, each having advantages and limitations. Accordingly, scholars use different terms depending on the type of violence and abuse they are studying and the contexts they wish to foreground. We propose the term "technology facilitated coercive control" (TFCC) to encompass the technological and relational aspects of abuse in the specific context of coercive and controlling intimate
relationships. TFCC refers to violence and abuse by current or former intimate partners, facilitated by digital media. It includes such behaviours as harassment on social media, stalking using GPS data, clandestine and conspicuous audio and visual recording, threats via SMS, monitoring email, accessing accounts without permission, impersonating a partner, and publishing private information (doxxing) or sexualised content without consent (Southworth et al. 2005; Woodlock 2017). Our definition of TFCC is grounded in the understanding of the social problem of domestic violence as a pattern of coercive and controlling behaviours, often backed by the threat of violence. Like other forms of coercive control (Stark 2007), TFCC is inextricably contextualised in relationship dynamics, culture, and structural inequality.

We situate TFCC within the multiple affordances and modes of governance of digital media platforms for amplifying and ameliorating abuse. Affordances are the characteristics of online platforms that make behaviours possible, shaping users' options and actions (boyd 2015). TFCC sits within the broader context of patriarchal gender inequality, which includes sexist and heterosexist social norms, gendered structural inequality, and the traditionally male-dominated digital media industry.

In addition to investigating TFCC, scholars are beginning to document how platforms can engender counter-misogynistic discourse, and are potentially powerful actors in the regulation and governance of online abuse. Accordingly, we propose a TFCC research agenda that recognises and asks new questions about the role of digital media platforms as both facilitators of abuse and potential partners in TFCC prevention and intervention.

Our framing of domestic violence recognises it as a course of abusive conduct that Evan Stark (2007) has termed "coercive control." Stark articulated the coercive
control model in an effort to shift the collective understanding of DV away from a narrow focus on decontextualised acts of physical violence. Despite early feminist articulations of violence against women as the interpersonal manifestation of a political problem, criminal justice responses (e.g., Dobash and Dobash 1979) and much DV research continue to focus on individual behaviours. Stark foregrounded patterns of behaviour and the constellation of abusive tactics that emerge within the cultural context of structural gender inequality and the systems that reproduce it (Stark 2007: 14). Domestic violence perpetrators use tactics including, but not limited to, physical and sexual violence to entrap partners and ultimately limit their freedom. Stark argues that in order to understand abuse, "it is necessary to know not merely what a party does— their behaviour—but its context, its sociopolitical as well as physical consequence, its meaning to the parties involved, and particularly to its target(s), and whether and how it is combined with other tactics" (2007: 104). Digital media offer a variety of everyday options for effectively controlling partners. Some of these are contemporary iterations of traditional forms of abuse, like stalking and verbal abuse. However, the accessibility and immediacy of mobile, digital, and social media may result in abuse perpetration with greater ease, using new methods and channels (Woodlock 2017).

The ubiquity and social convergence of digital media can enable perpetrators to increase their control in victims’ lives, even when they are physically separated. The characteristics of digitally mediated communication such as storage, synchronicity, replicability, mobility (Baym 2015) enhance abusers’ ability to persistently intrude on their targets regardless of their location. As a result, TFCC expands abusers’ sphere of control beyond previous spatial boundaries (George and Harris 2014; Woodlock 2017). Technology can also be used in hybrid forms of digital/physical stalking, for example,
abusers may use the geolocation of posts on Facebook to track the activity of their intimate partners, using the information to show up in person or let the victim know they know where they are (Woodlock 2017). Consequently, victims have reported feeling constantly unsafe, and unable to truly escape the abuser regardless of their physical location (Dimond, Fiesler and Bruckman 2011; Hand, Chung and Peters 2009; Harris 2016). Synchronous communication "can enhance the sense of placelessness that digital media can encourage, making people feel more together when they are apart" and "make messages feel more immediate and personal" (internal citations omitted, Baym 2015: 15). In the context of abusive relationships, this characteristic can amplify the harms of abuse.

The storage, reach, and replicability (Baym 2015: 16) of digital media communication and content means that texts and media objects used in abuse may be persistently visible and connected to the victim’s identity. For example, some victims of image based sexual abuse experience constant anxiety about who has seen an image and where it may next appear (Bates 2017). Young women interviewed about abusive text messages from violent partners say that "it gets into your head" more than it does in person as they have a permanent record on their phones. Because they have their phones with them all the time, they say, the abuse "stays with you" (Stonard, Bowen, Walker and Price 2015: 21).

As digital media technologies are rapidly integrated into everyday life, interpersonal communication and relationships are changing alongside them (Baym 2015). Communication and monitoring behaviours in dating relationships, for example, are highly ambiguous and context dependent, and their implications shift with the use of different communication technologies. Picard’s 2007 representative survey of 615
American teenagers found that 36% of respondents who had ever had a boyfriend or girlfriend had a partner check up on them about "where you are, what you're doing, who you're with, etc." more than 10 times a day. 30% had a boyfriend or girlfriend email or text them more than 10 times per hour (Picard 2007: 8). However, prevalence and frequency measures alone don't reveal the meaning, context, or impact of such behaviours. Indeed, what older people might consider to be excessively frequent texting is common and unproblematic for many young people (boyd 2015). It is the context and meaning of the behaviour that determines whether it is abusive or not. Accordingly, Reed, Tolman and Ward highlight the limitations of the most common approach to measuring the prevalence of ambiguous behaviours they label “aggression” and “monitoring/control” (which they aggregate into what they call Digital Dating Abuse or DDA) among adolescents. Reed et al. note that, "With widespread use of daily digital media among U.S. teens, one might ask whether DDA behaviours are benign modern dating interactions in most circumstances" such as where they are infrequent occurrences or do not cause distress (Reed, Tolman and Ward 2017, p. 88). Reed et al. suggest that,

If a DDA behavior is upsetting, causes a negative emotional response, and/or alters behavior, it is of concern to those interested in the intervention in and prevention of dating violence. Research that only reports the frequency of DDA behaviors therefore provides an incomplete picture of DDA experiences among high school students. (2017: 88)

This observation reflects challenges for earlier theoretical and methodological debates about how to define and measure abuse against intimate partners. The same behaviours can be healthy, protective, or abusive depending on the context.
TFCC affects people across age groups, cultures, and geographic locations. Woodlock (2017) surveyed 152 DV support practitioners and 46 adult TFCC victims in Victoria, Australia, and found most perpetrators were using technology to control, stalk, and intimidate victims. Another Australian survey of 546 DV support practitioners found the most common forms of TFCC were abusive and persistent text messages and the use of Facebook to harass victims; and that surveillance and tracking with GPS via mobile phone apps was also common (Woodlock 2015). Patterns of online abuse reflect offline social inequality: women from non-English speaking backgrounds, women with disabilities, and Aboriginal women were disproportionately likely to experience TFCC (Woodlock 2015). A study interviewing 30 DV victims across rural Victoria, Australia, found that TFCC was used by perpetrators to increase the victim’s social and geographic isolation, which has particular risks to the safety of women in regional and rural areas (George and Harris 2014); and there are distinctive challenges to "cyber-safety" in Aboriginal remote communities, including in the context of intimate and family relationships (Rennie, Hogan and Holcombe-James 2016).

**Social media and online misogyny**

Social media platforms (Facebook, Twitter, Instagram, WeChat) are a specific and dominant sub-category of digital media technologies that are designed to facilitate communication and content sharing among networks of users, and are characterised by the convergence of personal, public, and professional communication within a single platform. Since the late 1990s, social media platforms have become immensely popular, influential, and profitable. For example, Facebook is predicted to register 2 billion monthly users in 2017 (Fiegerman 2017), and has been valued at US$485 billion dollars
Other popular social media platforms report hundreds of millions of monthly users. Early social media networking sites shared a number of characteristics in common: namely, they were web-based (usually requiring only a PC and browser), they enabled users to construct a public or semi-public profile and develop a network of users or "friends" with whom they communicated and interacted (boyd and Ellison 2007). Social media have become almost ubiquitous in everyday life as they have been embedded into mobile phones as apps, and they have become part of basic communications infrastructure of societies, spanning not only interpersonal but also public and professional communication (Burgess and Banks 2014).

The specific affordances of social media have generated new opportunities and tactics for control and humiliation in DV. Online abuse is increasingly characterised by abuse and harassment by perpetrators known to the victim (Salter 2017a). A recent survey on online harassment in the United States found that the most common perpetrators of digital abuse and stalking are current and former partners (Lenhart, Ybarra, Zickuhr and Price-Feeney 2016: 40). Additionally, the dense connectivity of social media networks across multiple spheres of life - family, work, friends and so on - blurs the divisions between "public" and "private" life, and creates an environment in which content shared on social media aimed at one audience (such as family and friends) may have untoward consequences when viewed by other audiences (such as work colleagues). This convergence of social worlds and the "networked publics" (boyd 2007) that connect them results in the phenomenon Marwick and boyd call "context collapse" (Marwick and boyd 2011) - where different audiences or social groups who would be dealt with separately in “offline” contexts are co-present within a single social media platform. While, as Marwick and boyd (2011) show, social media
users develop ways of managing their online personae for these different audiences, context collapse and networked publics can exacerbate the effects of DV, as perpetrators can upload defamatory or humiliating content "that effectively poisons the user’s social world" (Salter 2016: 18). Girls and women are at particular risk of reputational damage when personal information, images or video are made public (Salter 2016), and this has become a point of leverage for DV perpetrators as social media platforms amplify their ability to harass and humiliate partners (Woodlock 2017). This strategy has been documented in research on so-called "revenge porn," which involves the abusive, non-consensual sharing of intimate images. While they problematise the label, Salter and Crofts (2015) documented the ways that men had used social media to circulate sexualised images or video of partners and ex-partners in retaliation for leaving the relationship. Abusers have also been known to circumvent Facebook’s real name policy by impersonating friends of the person they want to harass (National Network to End Domestic Violence 2016). A major risk in TFCC on social media is that individual perpetrator tactics designed to abuse and humiliate a partner or ex-partner can intersect with broader cultures of online misogyny. At this point, TFCC can take on a "viral" form as misogynist peer networks on social media mobilise to harass women using information and images provided by DV perpetrators (Salter and Crofts 2015; Salter 2017b). A number of high-profile "revenge porn" victims have described anonymous online groups of men, motivated by a shared misogyny, persistently re-circulating images released without their consent to maximum reputational damage (Salter and Crofts 2015). Salter’s (2017b) analysis of the "Gamergate" controversy provides a case study of viral TFCC, in which an embittered video game developer wrote and circulated a
defamatory post about his ex-partner, ultimately recruiting tens of thousands of social media users into a sustained campaign of targeted abuse and harassment that attracted global media attention. Such misogynist campaigns can be highly organised and coordinated across multiple online platforms, exploiting the specific affordances and loopholes of each platform (Burgess and Matamoros-Fernández 2016; Massanari 2017; Quodling 2016). For instance, the high level of anonymity on Twitter, the ease with which a user can create multiple accounts, and the platform’s historical reluctance to police the free expression of their users, have combined to make the platform a hotbed of abuse and harassment (Mortensen 2016). Malicious users have appropriated Twitter’s targeted advertisement feature to abuse transgender people, since it enables them to promote abusive posts that cannot be traced back to them (Quodling 2016). Other harassment tactics include "tweet and delete" practices, in which abusers temporarily make available the private information of their targets but remove the content before it can be flagged and any disciplinary action taken by the platform (Matias, Johnson, Boesel, Keegan, Friedman, and DeTar 2015).

However, social media platforms can also be used to mobilise against misogyny (Huntemann 2015; Dragiewicz and Burgess 2016; Salter 2013) and women have long used the internet as a platform for mutual support, self-expression and activism (Döring 2000; Harcourt 1999). Quodling (2016) suggests that social media users’ collective counter-abuse tactics fall into three categories: advocacy, circumvention, and intervention. With regard to the first of these, advocacy, Twitter hashtags offer a new set of possibilities to enhance feminist discourse, denounce sexual assault, and coordinate shared experiences among victims of domestic violence (Bowles Eagle 2015; Clark 2016; Dragiewicz and Burgess 2016; Megarry 2014; Rentschler 2015;
Rodino-Colocino 2014; Thrift 2014). In terms of circumvention, users have also used Twitter’s technical architecture to build bot-based collective blacklists to tackle online abuse and coordinate action against harassers (Geiger 2014) and to create bots engaged in sanctioning bad behaviour online (Munger 2016). An example of intervention is the anti-trolling website hatr.org reposts hateful comments towards women that were originally posted in other online spaces to make them visible and examine their discursive patterns (Sadowski 2016). However, other scholars note the complexity of such interventions, arguing that reproducing this type of harassment, even if the purpose is to denounce it, involves "cycles of amplification" (Phillips 2015). Other tactics against online misogyny include the hacking of revenge porn sites and doxxing of abusers (Salter and Crofts 2015). As Whitney Phillips reflects, her own practices of ‘actively trolling trolls’ (Phillips 2015: 206) were difficult to pull off without remaining captive to the rules of the trolls’ game. More aggressive interventions like doxxing abusers raise additional ethical questions about the line between collective justice and revenge. The scope for vernacular and collective counter-abuse tactics, then, is wide but fraught with complexity.

**The challenges of platform governance**

Recent digital media scholarship has emphasised the relationship between platform design, the cultures of online communication supported by those platforms, and platform governance. By platform governance, we mean both how platforms shape and regulate our information and social environments, and how they are subject to regimes of governance themselves (Gillespie 2017). The design of each platform’s front-end, user-facing features and affordances, as well as its back-end architectures and
algorithms, shapes the possibilities and constraints of private and public communication on that platform, including the ability to spread and share abuse, to engage in creative counter-abuse tactics, or to report and block abusers. On the other hand, users frequently exploit features of the platform in ways that are not intended or adequately contemplated by the platform. These intended and unintended consequences suggest the need to pay more attention to the design choices of platforms in facilitating or limiting abuse by intimate partners. Similarly, telecommunications providers are the intermediaries through which abuse and stalking take place, and hence important sites of TFCC prevention and intervention. Beyond digital media scholarship, there is increasing policy and commercial pressure on online platforms and telecommunications providers to improve their responses to online harassment (United Nations Development Programme and UN Women 2015).

In policy debates, digital intermediaries like social media platforms often represent themselves as passive facilitators of communications, and use this rhetorical framing to limit their responsibility for users’ actions (Gillespie 2010). In legal terms, those platforms that are incorporated in the United States benefit from a strong legal immunity from liability for harm caused by users under the Communications Decency Act, s 230. Online intermediaries outside of the US, on the other hand, often do not have such strong immunity (Authors 2017). For the last two decades, commercial providers have sought to minimise their legal liability and social pressure to police how their users behave on their networks, while reserving the absolute right to enforce rules and moderate content as they see fit (Suzor 2010). The dominant approach has been informed by a libertarian vision of free speech and private property that emphasises the freedom of platforms to set the rules of participation and de-legitimises explicit external
regulation and censorship of abusive speech (Suzor 2017). Moreover, challenges of regulating the internet (Hiller and Cohen 2002; Lessig 2000) and the lack of international legal mechanisms to enforce the removal of abusive material complicates the prosecution of abusive behaviours online (Citron 2009; Citron and Franks 2014; Salter and Crofts 2015).

As the regulatory work that platforms do to moderate user content and behaviour becomes more visible, there is increasing social pressure on platforms to do more to address harassment and abuse on their networks. Controversies over digital abuse and gendered harassment, including the online misogyny associated with the alt-right precursor movement "Gamergate" (Salter 2017b, Burgess and Matamoros-Fernandez 2016; Massanari 2017) as well as image-based abuse (Langlois and Slane 2017; Salter and Crofts 2015) including the widely-reported instance of non-consensual image sharing centred around female celebrities and known colloquially as ‘the fappening’ (Massanari 2017), have greatly increased the pressure on platforms. To protect their public image, platforms are increasingly reacting to make public statements about their commitment to addressing gender-based violence (e.g. Hess 2014; McDonald 2014). The major platforms have responded by creating advisory bodies that include women’s groups, in efforts to improve their policies and responses to abuse (Cartes 2016; Laville 2016). In 2015, Google announced that it would remove from its search results revenge porn links that have been reported (Singhal, 2015), and many of the major search engines and social media platforms have now introduced similar procedures (Suzor, Seignior and Singleton, 2017). In June 2016, YouTube clarified its harassment and bullying policy (Lim 2016) and other platforms have progressively strengthened their hate speech and harassment rules in recent years (Johnston 2016).
Despite these promising moves and progressive public statements, inter-user social media abuse is still rampant, and there is little agreement about how platforms should act. For Twitter, at least, the perceived ineffectiveness of these responses has substantial ramifications: Disney’s decision not to purchase Twitter is rumored to have been informed by Twitter's inability to deal with trolling and abuse (Ingram 2016). This is such a persistent issue for the company that it led one commentator to call it a "honeypot for assholes" (Warzel 2016) and one that appears to relate to a deep existential dilemma located at the heart of Silicon Valley libertarianism. Many of the major platforms are clearly sensitive to the demands that they improve their services, but neither the law, their internal cultures, nor the media controversies that threaten their very existence provide clear guidance about what, exactly, they should do. Indeed, efforts to address institutionalised sexism have been met with ambivalence, with praise and criticism issuing from the public and tech company employees alike (Marwick 2013).

Platforms increasingly use algorithms, automation, and machine learning to curate and present content and information to their users; and even to identify and censor objectionable content. This algorithmic turn affects the content and ordering of Facebook newsfeeds, Twitter timelines, as well as the prominence of other users and their content in our personal views of each platform. The functioning of such platform technologies are usually opaque (Pasquale 2015) although their effect on cultural production and access to knowledge is significant (Gillespie 2016). Recent scholarship has begun to highlight that the specific ways that these platform technologies shape social interaction and information access can support different kinds of cultures - for example, Adrienne Massanari observed how Reddit’s algorithms support "toxic
technocultures,” rewarding anti-social behaviours with visibility (Massanari 2017). Further, as Alice Marwick and Rebecca Lewis (2017) argue, the diffuse online subculture associated with the "alt-right," which includes the misogynist "manosphere" of antifeminist men's groups, is significantly empowered by the ability to exploit the affordances and algorithmic characteristics of the contemporary digital media environment, to "manipulate news frames, set agendas, and propagate ideas." Marwick and Lewis argue that these subcultures have "developed techniques of ‘attention hacking’ to increase the visibility of their ideas through the strategic use of social media, memes, and bots" (2017: 1) alongside other lobbying techniques. This sophisticated capacity to game the system’s technological affordances as well as to game the media culture at large (through "weaponizing irony" for example) are significant dimensions of online misogyny and TFCC alike; and present major governance challenges to platforms.

Social media platforms do offer users a range of technical mechanisms to moderate abusive content, either by means of content flagging tools, keyword filters or blocking features. However, the tactics of TFCC are often too complex to report through drop-down menus or simple flagging tools (Matias et al. 2015), which makes these mechanisms insufficient (Crawford and Gillespie 2014). In addition, in the process of reporting, reviewing and responding towards content and users flagged, platforms have the last word in deciding whether action should be taken against these claims, often weighing up the interests of users in a logic that is flawed by false equivalence, and which reflects "disproportionate power" in the governing processes within social media sites (Quodling 2016).
Given their historical continuities with the modes of production associated with Silicon Valley and the early commercial internet, the cultures of US social media companies like Facebook and Twitter are deeply entangled with American ideals of freedom of expression, openness and the free market (Streeter 2011) -- values that in practice often work to favour the prerogatives of privileged groups over the rights of others. Policies that govern user behaviour on social media platforms betray irresolvable conflicts between Silicon Valley’s libertarian ideals and the challenges of inclusion and safety. For example, controversial humour is generally protected in most social media sites’ policies, which facilitates the disguise of online abuse by means of sexist or racist jokes (Milner 2013; Shifman 2013). Often, misogynistic humour is mediated through visual content, such as memes that, due their catchy aesthetics and their potential to go viral, can be a "ceaseless flickering hum of low-level emotional violence" (Haque 2016). Women’s grievances with regards to online abuse have sometimes been contested by evoking libertarian principles of freedom of expression that frame any form of intervention as "censorship" (Baym 2015; Marwick 2013; Herring 1999), and blaming victims by emphasising their personal "responsibility" for the harms that befall them online (Salter 2017a).

Finally, platforms come aground on their own competing logics when attempting to respond to controversial or objectionable content (Gillespie 2010). While platform terms of service typically ban abuse and harassment, they are unevenly and unequally enforced (Salter 2017a). Scholars, journalists, and activists have actively denounced double standards in the enforcement of their rules. For example, researchers have argued that platforms’ failure of governance with regard to online harassment can be attributed to their business models. Hate online triggers traffic to online content and
interaction about it, which translates in economic revenue for platforms and could explain their lack of response to online abuse (Langlois and Slane 2017; Massanari 2017; Shepherd, Harvey, Jordan, Srauy, and Miltner 2015). Similarly, decisions over what content should circulate and what should be removed can reflect cultural biases towards certain issues (Gillespie 2017). For example, Facebook enforces its nudity and obscenity policy in a narrow fashion that often ignores the context and cultural specificities of nude bodies. This was the case when the platform removed photos of breastfeeding (Chemaly 2014) or pictures of female Indigenous elders with uncovered breasts participating in cultural celebrations (Alexander 2016; Waqas 2015). However, when women’s organizations reported a page that glorified DV, Facebook responded by only deleting the most controversial posts (Meachim and Agius 2016). It was not until the media started covering the case that Facebook closed the page (Brook 2016). The challenges of platform governance are therefore located in four main areas: the limitations of platforms’ reporting tools; the algorithmic and automated characteristics of platforms; the existential dilemmas and double standards embedded in their policies; and the inconsistent and contradictory enforcement of their own rules in practice.

**Conclusion and implications**

TFCC has emerged as a major issue compounding the already-serious risks faced by women in abusive relationships. As we have shown, it is vital to situate TFCC in a framework of coercive control (Stark 2007) used by offenders in attempts to intimidate, micromanage, dominate, and isolate victims (Woodlock 2017). Technology can enable DV perpetrators to expand the reach of control and abuse, disrupting women’s efforts to protect themselves. Social media platforms complicate the
boundaries between personal interactions and public information, which has generated opportunities for DV perpetrators to track and humiliate their victims, often articulating to wider networks of online misogyny such as the "manosphere" and broader alt-right movements (Marwick and Lewis 2017). The slow and uneven response of online platforms to women’s complaints of harassment and abuse suggests that the issue of gender-based violence and harassment has not been a priority within the tech industry. This exemplifies how the social context of gendered inequality enables abuse by creating the conditions in which women's efforts to seek assistance are blocked or ignored.

However, there have been positive developments. Legislative change in a number of jurisdictions criminalising "revenge porn," non-consensual "sexting," and other forms of image-based abuse provide a firm foundation for action, although law enforcement needs to be trained, resourced, and willing to enforce such provisions. Online platforms have developed partnerships with women’s agencies to improve users’ safety. For example, the National Network to End Domestic Violence (NNEDV) teamed up with Facebook and Twitter to offer advice on how to use sites and maintain women’s privacy and safety. Some of the safety tips include limiting the audience of posts and tweets, using mechanisms to control tags, hiding profiles from search engines, and activating login notifications (NNEDV, 2016). While some such defensive tactics will afford greater safety, others are little more than advice to abstain, and therefore could potentially diminish women’s ability to participate fully in public and social life, and to reach out for support and strength (which is especially an issue for geographically or socially isolated women). Women’s advocates and agencies have also developed their own initiatives to promote women’s safety and participation online.
Established organisations and networks that work to end DV, such as NNEDV, The Women’s Services Network (WESNET) and organisations like Women’s Aid, are including technology safety tips and resources in their websites that promote a range of positive uses of technology for survivors, from accessing information to seeking support and gathering evidence. Similarly, there are grassroots initiatives from other stakeholders, like feminist digital activists, that offer extensive resources and information to tackle online harassment, such as the websites Crash Override Network, TrollBusters, Speak Up and Stay Safe(r), HeartMob, Tactical Technology, and Take Back The Tech. In addition, the web is increasingly populated with individual advice on how platforms could technically improve their settings to help victims of online abuse (Harper, 2016). Within academia, there are also initiatives to protect those scholars that might be potential targets of harassers for conducting risky research (Marwick, Blackwell, and Lo 2016).

Nonetheless, we suggest that there remain four pressing issues which must be addressed in responding to the role of platforms in facilitating TFCC. First, there is a distinct lack of clarity about what platforms are currently doing to combat abuse. The major platforms have strong statements about permissible conduct, and clear prohibitions against abuse in their terms of service, but these rules are typically enforced in secret (Gillespie 2017). Much of what we know about how platforms respond to abuse is limited to press releases and leaks of internal training documents. More research, new methods, and greater transparency are required in order to ground ongoing debates about the responsibilities of platforms (Suzor, Van Geelen, & Myers West, 2017). This type of additional detail is required in order for both government regulators and civil society to hold platforms to account for their policies and
procedures, but it might also help platforms themselves develop industry standards and shared knowledge about effective responses that can improve their practices -- and limit their exposure to growing public criticism and controversy. Second, more work needs to be done to articulate a shared understanding of what platforms *ought* to be doing to combat abuse. This includes design solutions that effectively encode safety measures into the platform, disrupt the development of misogynist and aggressive online networks, and predictively model potential misuses of platform features and functions, as well as effective governance and administration measures. Third, regulators need to consider the extent to which these responsibilities of platforms should be explicitly required by law, and how effective laws can be crafted where necessary. Creating effective regulations for digital platforms requires careful consideration of difficult questions, including jurisdictional problems, agreement about what is technically feasible, negotiations over costs of implementation and enforcement, and ensuring that platforms have sufficient certainty and guidance to confidently operate within the jurisdiction. The jurisdictional problems in particular are complex and difficult to solve. Fourth, some level of international consensus is likely required in order to develop useful standards about what states expect from transnational platforms. In order to secure practical compliance from transnational platforms, some work is likely required to create more uniform standards and to clarify the expectations states have about how platforms should respond to regional differences. Regulators must also ensure that local laws do not create a strong incentive for platforms to ignore regulation -- digital platforms can relatively easily structure their operations to benefit from the safety of a jurisdiction with comparatively more attractive rules. Importantly, ensuring practical compliance requires more than just creating laws; regulators will need to develop more
productive relationships with platforms, with other regulators, and with influential civil society stakeholders.

Although a growing body of literature is investigating TFCC, there is still a lack of empirical evidence about the nature, extent, and consequences of this abuse. The extant research on TFCC is quite limited since most studies so far investigate a broad spectrum of harassing behaviours online rather than the specific dynamics or impact of abusive relationships. Few studies have gathered information directly from survivors. While typologies of online abuse are beginning to appear, a fuller understanding of the positive uses of technology for domestic violence survivors and those who support them is also needed.

A TFCC research agenda must therefore be multi-methodological, sensitised to gender and other forms of social stratification, and conscious of long-standing dilemmas in the study of gendered violence. Most of the research on DV and technology has relied on classic social science research methods, such as interviews, focus groups, and surveys, to account for the strategies pursued by harassers and the harm inflicted on their targets (Southworth et al. 2005). Given the significant, embedded role of digital media technologies in facilitating, amplifying and addressing abuse, mixed approaches incorporating digital methods (Rogers 2013) are essential. Such approaches use "digital traces" of activity, integrating user activity, discourse, and platform affordances as data for understanding the operations of apps or platforms within the context of lived experience. This research agenda could particularly benefit from digital ethnography approaches to the study of platforms (Geiger and Ford 2011) and walkthrough techniques (Light, Burgess, Duguay 2016) to interrogate the affordances, limitations, and shaping effects of digital media platforms and their implications not only for the
abusive strategies of perpetrators but also for the resistance tactics of survivors. These methodological approaches are also useful to examine the gendered logics of software design and platform policies, logic and cultures, which in combination with the testimony of victims and workers in the DV sector could inform new directions in tackling TFCC.
References


