Doxxing, Privacy and Gendered Harassment

The Shock and Normalization of Veillance Cultures

Stine Eckert / Jade Metzger-Riftkin

We conducted 15 in-depth interviews with women and men in Germany, Switzerland, Finland, Canada, and the United States who were victims of doxxing. The goal was to understand their experiences, their responses, and the consequences they faced. We understand doxxing as a complex, gendered communicative process of harassment. Doxxers use digital media technologies to expose personal information without consent given by those to whom the personal information belongs. We apply a feminist approach to surveillance studies to doxxing, focusing on the constructions of daily, habitual, and ubiquitous assemblages of veillances that disproportionately impact vulnerable individuals. We found that gendered aspects shaped the flow and suspected intent of doxxing and subsequent harassment. Victims experienced uncertainty, loss of control, and fear, while law enforcement and social media providers only helped in a few cases to pursue doxxers or remove unwanted personal information. We ultimately extend the definition of doxxing by considering the ubiquitous nature of information shared online in gendered veillance cultures. Our findings lead us to advocate for protecting the contextual integrity of entering personal information into expected, intentional, or desired spaces.

Key words: Doxxing or Doxing; Surveillance Capitalism; Online Harassment, Privacy, Internet of Things

1. Introduction

In a 2018 national survey with 4,151 U.S. adults, the Pew Research Center found that 85 % said posting others' telephone numbers and home addresses is online harassment (Smith & Duggan, 2018). A 2016 national survey of 3,002 Americans 15 years and older found 30 % of respondents said they experienced an "invasion of privacy", including "being hacked, having information about or images of the person exposed online without their permission, being impersonated" (Lenhart et al., 2016, p. 3). These incidents describe doxxing, a term rooted in 1990s hacker culture (Douglas, 2016). Doxxing received increased attention during The Fappening and #Gamergate controversies in 2014 (Massanari, 2017), which were online harassment campaigns specifically targeting women through a release of their personal information online, leading to massive and sustained attacks online and offline. #Gamergate was a reaction by misogynist video game enthusiasts against perceived favoritism towards women in gaming journalism. For months, harassers sent feminist activists and game developers Zoe Quinn, Anita Sarkeesian, and Brianna Wu abusive messages, defaced their online spaces, and hacked their accounts. Further, harassers coordinated to search for the victims' locations and telephone numbers (Kidd & Turner, 2016). The Fappening refers to the online release of nude photographs of women celebrities including U.S. singer Rihanna and U.S. actress Jennifer Lawrence (Blake, 2016). As these two events unfolded in the same year and were widely covered by news reporters, they brought doxxing into broader public awareness. Since then doxxing has also become a business as dox-for-hire services aggregate personal information which can be purchased for as little as $5 (Snyder et al., 2017).

Doxxing is a complex process in which personal information is assembled from multiple channels and publicly distributed online without consent from the person to whom the information belongs. Typically, a call to action accompanies the dissemination of information.

DOI: 10.5771/1615-634X-2020-3-273

Victims face varying levels of harassment, which can escalate into physical attacks: 3 % of respondents in a 2016 representative U.S. survey reported experiencing a physical attack related to online harassment; 4 % experienced sustained online attacks from multiple loosely coordinated people, sometimes called brigading (Lenhart et al., 2016) or a cybermob (Sarkeesian, 2012).

While media technologies have been presented as positive for increased inclusivity in democratic discourse (Gillmor, 2004, Shirky, 2009), they are often designed without consideration for users' needs, especially those of women and minorities. Instead, online media technologies are often designed to increase, save, and capitalize on interactions on platforms, thereby maximizing corporate profit and turning data into a hot commodity (Zuboff, 2019). What happens when an individual in a highly technologized, data-driven society gets doxxed?

We conducted in-depth interviews with nine women and six men who have been victims of doxxing and applied a feminist surveillance studies approach to analyze participants' sensemaking of their experiences. We found that gendered aspects shaped the flow and suspected intent of doxxing and the ensuing harassment that victims experienced. Victims' outreach to law enforcement and social media providers only helped in a few cases to pursue doxxers or remove unwanted personal information. We ultimately extend the definition of doxxing by considering the ubiquitous nature of information shared online in gendered veillance cultures. Our findings lead us to advocate for protecting the contextual integrity of entering personal information into expected, intentional, or desired spaces online and offline.

2. The evolution of doxxing

The term doxxing is shorthand for "dropping documents", i.e. releasing documents with personal information about an individual online – a tactic of hackers to spread information for the purpose of deanonymizing previously anonymous people, making the physical location of people widely known, and/or delegitimizing the credibility of a person (Douglas, 2016). The exposed information can then be used to facilitate extortion, coercion, and harassment (Eveleth, 2015), for instance, threatening to send or sending unwanted items or calling authorities to homes or workplaces (Merlan, 2015).

Some countries have developed laws to sanction doxxing or other forms of online harassment. In 2016 the U.K. implemented new guidelines to prosecute doxxing incidents (Tyson, 2016). Germany's 2018 so-called Facebook Act [NetzDG] heavily fines social media providers that do not remove hate speech, fake news, and illegal content within 24 hours of its posting (BBC, 2018). Additionally, since May 2018 the E.U. implemented its General Data Protection Regulation (GDPR) to provide users more control over personal data online, including the so-called "right to be forgotten"[1] that gives persons a process to have information removed from the results of search engines. In the U.S., Congresswoman Katherine Clark (2017) introduced a bill for the Online Safety Modernization Act in the House of Representatives to "combat the rise in online crimes that disproportionately affect women and girls", including doxxing and swatting. It is still being considered by a subcommittee.

While legal efforts to sanction doxxing specifically has progressed slowly, government entities have also been directly involved in doxxing. For instance, police in Canada and the U.S. have released photos of faces and names of suspects on social media (Arvanitidis, 2016; Stewart, 2014) and have become, unknowingly, part of harassment schemes through swatting, an extreme form of doxxing. In these cases, harassers falsely report an ongoing severe crime at

1 The "right to be forgotten" flows out of a philosophical position which suggests internet users should have the right to negotiate which of their information about themselves should remain or be removed from online spaces (see Jones, 2016).

a person's address resulting in a Special Weapons and Tactics (SWAT) team being deployed. For example, in 2017 Kansas State Police fatally shot Andrew Finch when he was swatted after his address was doxxed in an online dispute (Ellis, 2017). While the FBI (2016) issued a warning to the public and agencies that swatting is a tactic of intimidation, no federal U.S. law explicitly prohibits swatting.

Women *and* men[2] both experience doxxing (Duggan, 2017) but women are more likely to have certain types of private information posted online and to receive higher amounts of unwanted, vitriolic messages (Lenhart et al., 2016). Women are also more likely to experience other sexualized forms of online harassment such as revenge porn (Citron, 2014). Black and LGBTX people are disproportionately affected by online harassment than their white and heteronormative peers (Lenhart et al., 2016; Duggan, 2017), thus, intersecting demographic markers, such as race and sexual orientation, result in the heightened victimization of queer women and women of color. Scholars have repeatedly shown that misogyny toward and abuse of women who speak online has become a major problem (Banet-Weiser, 2015; Eckert, 2018; Gardiner et al., 2016; Harmer & Lewis, 2020; Jane, 2014; Mantilla, 2013; Phillips, 2015; Turton-Turner, 2013). Yet, the public, social media providers, legislators, and police do not adequately recognize online harassment as punishable offenses and do not recognize the particular impact online harassment has on women and/or minorities (Clark, 2017; Eckert, 2018). More often, misogyny and harassment of women online has been trivialized and calls to address these behaviors have been cast as attacks on freedom of speech online (Jane, 2014; Eckert, 2018; Massanari, 2017; Turton-Turner, 2013). And yet, more than a quarter of U.S. adults reported refraining from expressing their views online after witnessing online harassment (Duggan, 2017), effectively silencing discourse.

3. Feminist approaches to technologies and veillances

The history of technology, and particularly of computer science, has been highly gendered, often rendering women as inventers, designers, and users, and their experiences, including of discrimination and abuse, invisible (Hicks, 2017; Light, 2003). Most recently, studies show that the architecture of technology and software design enable online harassment (Massanari, 2017; Mortensen, 2016), rather than being apolitical in design. Massanari's (2017) analysis of Reddits' toxic technocultures found that the design of media technologies encourage misogyny, racism, and heteronormativity: features like upvoting, filters, and the ability to generate multiple accounts game seemingly democratic processes, and permit users to capitalize on "platform policies that often value aggregating large audiences while offering little protection from potential harassment" (p. 333). Wikipedia's gender gap and hostility to women contributors have been similarly attributed to the design and culture of the platform (Eckert & Steiner, 2013). Social media providers built a technology that prompts users to share openly and authentically (Marwick & boyd, 2010). Further, techno-cultural influences shape gendered expressions online. In Germany, a study of girls' self-representation on Instagram found that the availability of filters and editing tools combined with rewarding comments of peers funneled girls into posting personal, sexualized content catering to narrow beauty ideals (Götz, 2019). Sharing this content comes with varying control over its long term (in)visibility (boyd & Ellison, 2008) or the contextual integrity of the information. Nissenbaum (2009) defined contextual integrity as "a right to appropriate flow of personal information," which relies on examining both "social contexts and context-relative informational norms" (p. 127). Expectations for privacy may vary between contexts but are rarely developed recklessly. Rather,

2 We recognize that there is a range of genders, rather than a binary. Most studies still refer to women and men.

people develop sophisticated risk assessments of self, audience, place, time, and control, and weigh these factors against the type of information they are prompted to share. Especially vulnerable groups make highly context specific decisions when interacting online and facing potential hostile interactions (Eckert et al., 2019). Hence, self-surveillance has become a feature of "being online". At the same time, vulnerable groups, which can include women, are most susceptible to being monitored (Dubrofsky & Magnet, 2015).

The core definition of surveillance is to combine watching with controlling or regulating human behavior in a power relationship (Monahan & Wood, 2018, p. xix). Mulvey's (2009) male gaze concept emphasized how cinema catered to a powerful, pleasurable, and active viewer position for men's desires while women were cast as passive subjects to be viewed. Since then, more complex forms of veillance have been recognized, beyond individual peeping and government surveillance. As Dubrofsky and Magnet (2015, p. 2) explained: "Surveillance emphasizes its broad aims, defining it as the 'collection and analysis of information about populations in order to govern their activities' – a collection of information that is disaggregated and decentralized – a 'surveillant assemblage' rather than a singular Big Brother" (citing Haggerty & Ericson, 2006, p. 8). Rather, as Zuboff (2019) calls it, a "Big Other" has evolved, a vast surveillance capitalist company landscape. The ubiquity of social media in the Western world has led to a massive aggregation of large amounts of personal data for commercial surveillance and exploitation while also serving as channels for societal peer veillance: "Women on these sites generate a significant amount of the user traffic and profit for social-networking companies, and in fact, endure significant pressure to behave in ways that actively invite a sexualized gaze" (Nakamura, 2015, p. 223; see also Götz, 2019). Social media providers have created technologies that users "depend[ed] on for access to friends and community" (Nakamura, 2015, p. 224). Users are rewarded socially for creating online content, which is "real" or authentic, i.e. to willingly disclose personal information despite knowing that they are being surveilled (Dubrofsky & Wood, 2015; Marwick & boyd, 2010). The push to use social media stands in stark contrast to the material and psychological harms which can accompany a breach of privacy through online exposure. Thus, "for women on social-networking sites, there is a constant negotiation between the desire to connect and the need to self-regulate" (Nakamura, 2015, p. 222).

To counter, feminist activists have spearheaded initiatives to aid victims of online harassment that often involve invasions of privacy. For instance, Sarkeesian co-founded the Crash Override Network (www.crashoverridenetwork.com) to support victims of doxxing. Earlier initiatives, such as Take Back the Tech! (www.takebackthetech.net), similarly dedicated themselves to "tak[ing] control of technology to end violence against women". Such interventions, however, can overemphasize the agency of the individual to protect themselves or the agency of the state. While such initiatives pursue legislative or enforcement changes, the result might increase state scrutiny of vulnerable people (Dubrofsky & Magnet, 2015). Even when activists create new platforms, people most vulnerable to surveillance may lack digital or cultural literacy to use such alternatives (Nakamura, 2015). Without considering the nuances of the doxxing process and how victims respond to contextual integrity violations, activists risk reusing technologies that facilitate online harassment or proposing impractical or unfeasible solutions. Our study highlights doxxing victims' detailed experiences, which to our knowledge have not yet been explored by scholarly research. We ask the following research questions:

What are the experiences and responses of victims during a doxxing episode?

How does identity shape victims' experiences with doxxing and the social media technologies involved?

4. Method

Guided by feminist scholarship principles of researching situations-at-hand, we focused on personal accounts of everyday internet users who were doxxed. We recruited participants via snowball sampling, starting with contacts from the researchers' personal and professional networks and victim advocacy groups, followed by asking each participant for new contacts. We encountered some difficulty in recruiting as some initial responses indicated that victims were interested in participating in a study on doxxing, but found it too painful to recount their experiences. We were able to conduct in-depth interviews with 15 doxxing victims, which were audio recorded by native speakers in English (12) or German (3) via phone or Skype. Interview duration ranged from 21 to 85 minutes.

We used a narrative interviewing technique and analysis to understand how participants made sense of their experiences; narrative interviews start with open-ended questions to give the participants the opportunity to retell their experience of an event and their reactions and understanding of what was happening as it was unfolding (Brinkman & Kvale, 2015). We began interviews by asking: "Can you please walk me through your doxxing incident?" We used probes to gain more insight, including "Why do you think you were targeted?" and "Who did you turn to for help?" This resulted in a semi-linear narrative with a beginning and middle but not always a clear ending as some interviewees said they still expect potential fallout and remained hypervigilant. We analyzed the transcriptions narratively for overlapping experiences and connected threads (Brinkmann & Kvale, 2015). These threads were thematically organized, leading to these themes: specific contexts; contextual integrity breach; harassment, fear and silence; responses and recovery; and misogyny and sexism.

In self-reports nine participants identified as woman, womanish, or cis-woman; six identified as man or cis-man. Age ranged from 22 to 58 years (mean=36 years, median=35). Fourteen identified as Caucasian, one as Asian. Eight said they identified as lesbian, gay, bisexual, or queer. Eleven said they were in a relationship; four identified as single. Participants resided in the global West: USA (9), Canada (2), Switzerland (2), Finland (1), and Germany (1). Participants ranged in formal education levels from no high school diploma to holding a graduate degree. Thirteen participants identified as feminists, eight as activists (Table 1).

5. Specific contexts

The majority of victims said doxxing occurred in specific, overlapping contexts linked to political or oppositional activism (17 cases, Table 2). But contexts were not always discriminate: friendships and political activism overlapped in several cases, making the collapse of social contexts more harmful for some victims. For instance, a bisexual woman with disabilities in Canada said the doxxing isolated her from the feminist community:

> Radical feminism is really controversial, and I was afraid for my safety to have my name attached to it. … my ex-friend from high school …he pretended to wanna be my friend again and somehow got my home phone number and asked me my thoughts on some transgender issues …I guess I admitted to him on Facebook chat who I was but didn't expect him to post my full name on his Facebook.

A minority (4) attributed their doxxing to rivalries between feminist movements over transgender issues, abortion, and sex work. A third of women participants (3) said their doxxing was related to being an outspoken woman in the men-dominated spaces of Wikipedia and gaming. Gender plays an important role in becoming a target: Women who speak out as feminists and men who vocally support feminisms or other social justice movements online appear to be

Table 1: Demographics of participants (N=15)

Gender	**Participants**
Woman	9
Man	6
Age	
Mean	36
Median	35
Range	22-58
Country of residence	
USA	9
Canada	2
Germany	1
Finland	1
Switzerland	2
Reported ethnicity or race	
Caucasian/Western European	14
Asian	1
Highest level of formal education	
None/some high school	2
Some university	1
B.A./Vocational Degree	7
Graduate Degree (M.A. & Ph.D.)	5
Sexual orientation	
Gay/Lesbian	1
Bisexual/Pansexual	7
Straight/Heterosexual	7

Table 2: Context of doxxing

Context of doxxing	**Participants***
Political Opposition	9
Activism Opposition	8
Personal Relationship	3
Recreational Activity	3
Mistaken Identity	1

*participants reported overlapping contexts hence numbers do not add up to 15

likely victims. The majority of victims said they were targeted due to their activism rather than at random or due *only* to personal relationships.

Three interviewees said they were doxxed accidentally, through a case of mistaken identity, an innocuous tweet, and a careless moderator, showing that users unrelated to activism become victims, too. A Finnish woman whose information was disclosed accidentally by a group host said: "Before, I tried not to tell things that shouldn't be published in a paper. But in that secret support group I told more. I regret now, a little." The design of online media technologies to easily share personal content, also from others, without their consent, and little recourse to

retract once shared details, created easy flows of information out of the control of the victim, leading to contextual integrity breaches.

6. Contextual integrity breach

All participants said their doxxers posted information on social media (15); mostly on Facebook and Twitter (11 cases each). Additionally, a majority said doxxers uploaded their information on message boards and websites/blogs (9 each). Doxxers revealed a variety of information: addresses (9), legal names (8), employment information (4), telephone numbers and email addresses (5), and personal images (3). In a minority of cases, affecting three women and one gay man, sexual information was posted without consent: nude photos and videos were shared only in the case of women victims.

The revealed information, however, was not always limited to the victims themselves. The majority of victims said doxxers revealed names, addresses, telephone numbers, and images of family members, leading victims to feel anxious for their privacy and safety. For instance, as one American woman who worked as an artist described: "I'm still very scared especially because the address that was associated with the information they put out isn't my address but my father's address who lives alone." Doxxers exploit a design that makes social links highly visible and findable, a main feature of social media technology architecture (boyd & Ellison, 2008), which may lead to injury for adjacent social networks who may be less equipped or prepared to protect themselves. A white man in our study, an anti-racism activist, concluded: "I think if you want privacy you really have to be offline. The problem is in the 21st century it's very difficult to be offline… even for basic services"

Most doxxers gathered and disseminated information which was already online: a majority of victims (11) suspected that doxxers found personal information on websites (7), through hacking (2), or in online groups that participants assumed to be closed and trustworthy (2). Several said they had posted information in the past and had forgotten about it or that privacy settings had changed since. For instance, a U.S. man who edits Wikipedia said the doxxed information was available on Wikipedia's editor pages, a mailing list, Facebook (prior to the site adding privacy settings), and an old college profile. Similarly, another American man said: "This is stuff that I think went back to like 2004 or 2005. You know the internet doesn't forget things in the way we might sometimes like."

In a minority of cases[3] (5), doxxed information was previously offline and obtained through stalking (2) and/or previously trusted relationships (3). For instance, a U.S. instructor speaking at an anti-racism conference said the doxxer secretly taped her and posted the clip online. A Swiss blogger using an online pseudonym led an offline workshop after which a participant thanked her via Twitter unintentionally revealing her legal name. Using a website that mimics a phone book, a man who had stalked her for two years used the tweeted name to locate her. He posted her full legal name, home address, and telephone number on Twitter with the comment "interesting where this woman lives". She said: "I had my address removed from the website but I still was scared [that something could happen]…I had panic attacks in the first days, I was really, really afraid and I was not able to go grocery shopping anymore by myself."

In sum, the vast majority of participants said they had submitted information for personal or professional reasons to what they considered to be specific *expected, intentional, or desired* but protected online spaces. This confirms the argument made by feminist surveillance scholars that "seemingly mundane forms of data collection, observation, entertainment, and sorting that increasingly characterize daily life in informated and technologized societies" (Andrejevic,

3 Cases overlapped as some victims experienced doxxing several times or by multiple people.

2015, p. xi) flush large amounts of data into *unexpected, unintentional, or undesired online spaces* that need to be viewed critically.

7. Harassment, fear, and silence

All participants said they felt shocked when they first became aware of the doxxing, entering into crisis or emergency mode and trying to regain control over their information or at least making sense of what had occurred and what the consequences might be. For some this only lasted a few days, for others it stretched to months and years, involving repeated doxxing.

The majority of participants said they were harassed through email, phone calls, social media, or messaging systems following the doxxing. They described feeling scared, intimidated, and hypervigilant *both* online and offline. For some, harassing messages were sporadic as an American man who worked as a librarian described: "I got a few nasty emails, a few nasty messages on Facebook from people that I didn't even see until like two months later." For others, abusive messages were more frequent and also affected family members. A Canadian with a disability said when his doxxer was unable to reach him, the doxxer called his mother several times a week, leaving death threats, resulting in strained family relations: "My mother just pretty much took it out on me…it was just my fault."

Doxxing also isolated victims from their support groups. For instance, a U.S. gamer said that when her sex tape was doxxed her gaming team ostracized her. Responding to our question about the worst impact that the doxxing had on her, she said:

> I struggled and still do with severe depression among many other mental health issues and the problem was that I didn't have any friends in real life. So, when you remove my support network, my friends, my ability to communicate with other people you isolate me to a dangerous level. And I would say my suicide attempt in 2015 was strongly motivated by the fact that I had no one and the main thing that had given me gratification, some sort of reason to latch on, that was gone.

The overwhelming majority (12) said the doxxing was intended to intimidate/silence them or to enact revenge. Almost half of the women and a third of men in our study said they were doxxed and harassed to stop them from speaking out online; in one case a woman said doxxing was a punishment for her going to the police with charges of sexual assault against a man who was a politician. In the case of revenge, one situation exemplifies particularly well the chain of events doxxing can offset: A U.S. man was "back-doxxed" unintentionally because he bore a similar name as the intended victim who had initially doxxed someone from an opposing political group. Similar cases of back-doxxing have been reported, for instance followers of popular lifestyle bloggers in Singapore shamed critics of the bloggers this way (Abidin, 2013).

Finally, almost half of our women participants (4) attributed material damage to doxxing, having to return unwanted items, annul bills, and losing job opportunities. Perhaps the most extreme case involved a U.S. gamer who said she suffered financially and emotionally when a SWAT team broke down the door to her home and her online business became inoperable.

8. Responses and recovery

A minority of participants (3) said doxxing did not change their online behavior or encouraged them to be more open online, arguing that they had "nothing to hide". The majority of victims, however, said they altered their behaviors online and offline following the doxxing. They said they avoided writing about specific topics online, ceased activities in specific online spaces, tightened the security of their passwords, purchased VPN technology, and/or used pseudonyms. For instance, a Canadian activist who regularly posts political views on YouTube, said he no longer discusses transgender issues and stopped using Tumblr. A

U.S. man said he deleted his LinkedIn and Twitter accounts. A U.S. artist, who said she was doxxed for her pro-abortion stance, said she virtually stopped using social media: "I don't have any social media accounts using my legal name. I don't connect with people that I know in real life. I don't really use social media except for the promotion of my work now." Several said they remain hypervigilant of their online and offline surroundings. For example, a U.S. professor said she stopped teaching face-to-face and moved most of her other work online.

To alleviate the duress, some reached out to family and friends. A gay immigrant to the U.S. said he asked friends to monitor social media and alert him to fake profiles of him. Similarly, a U.S. gamer whose sex videos were leaked employed a graphics expert to post arguments on a site where she was harassed to convince other users that the tapes were fake. She said that without the legitimacy of a "real leaked" tape, the harassment decreased. While this helped victims in the moment, it also fed into posting more content and spending more time online to monitor others' behavior, contributing to the surveillance and interaction driven dynamics that social media technology is designed for to bring profits to providers. Victims inadvertently increased user traffic to platforms which enabled their harassment in the first place, possibly heightening the visibility of the information and potentially exposing friends and families to harassers. The majority of victims focused on who their individual harasser was, rather than challenging the structures that enabled the perpetrator's harassment of them. These responses reflect a normalization of a culture of daily, habitual, and miniscule forms of technology assisted veillances in the information and technology driven societies described by Andrejevic (2015), Dubrofsky and Magnet (2015), and Zuboff (2019).

8.1 Inaction of law enforcement and social media providers

The majority of victims turned to institutions for help, most often police and social media providers. In the U.S. and Canada, most participants viewed police and lawyers as unwilling or unable to help. A U.S. anti-racism activist went to local and federal police recalling:

> I said, "Hey, you know, I'm getting these threats." And [the police] said, "Oh really, how about that?" I said, "Well, think you could do something about this?" and they said, "Well, not really. But you let us know if you get new threats."

A U.S. woman, whose nude photos were doxxed, similarly said:

> I talked to a guy [officer] who was probably in his 60s and I told him the whole story and he didn't understand exactly what happened even though I spent at least 45 minutes explaining things to him over and over. He ended up giving me a 15-minute lecture about: "Oh well, nothing you post online is private, blah blah blah." Stuff that parents say to their five-year olds. It was kind of embarrassing and not really worth my time.

This type of interaction led another U.S. woman to hire a private investigator to aid police in finding her doxxer's identity, albeit unsuccessfully. Similarly, a Canadian said he paid a hacker to confirm that the doxxer was a former friend but did not go to the police as he saw them as impotent. By contrast, in Switzerland two women won court settlements after going to the police. One, however, also faced sexualized insults and trivialization when first reporting the doxxing:

> The policeman said he cannot imagine that this is happening when people don't know each other. [The policeman] was young, very friendly and polite but he asked me three times if I am sure that I was not sleeping with that person.

While men and women had trouble being taken seriously by police, only women reported sexist and misogynist behavior that dismissed the violence they faced, further victimizing them.

More than half of the victims (9) said they contacted the websites or social media providers where their information was posted without their consent to request its removal; six said they did not contact site providers as they thought providers would not remove information or settled the dispute in private. Of the nine who contacted site providers, the majority (8) said that they received no or a declining response, often an automated message from Twitter or Facebook. A Swiss blogger said even after a prosecutor determined that the posted content was illegal according to Swiss law neither Facebook nor Twitter heeded requests to remove it. Another woman in Switzerland noted that Facebook did not possess the cultural and linguistic competency to understand a misogynist threat in regional languages: "When someone threatens to rape me using Swiss German, then it stays online on Facebook." Only for two men victims was the information deleted from undesired websites after they proved their identity; in one case doxxers had information removed after noticing that they had doxxed the wrong person.

By contrast, social media providers offered no protection to accounts with pseudonyms. For instance, a Canadian with disabilities said her legal name was doxxed by linking her online profiles to her "real" identity. She reached out to Twitter but "because I was using a fake name for my privacy I couldn't do anything about it. They [Twitter administrators] didn't help me." Similarly, in the U.S., Facebook removed the page of an activist who used a pseudonym although she did not request the removal. She said that without the pseudonym she was not able to use the site. Ironically, she said Facebook declined her request to remove information revealing her legal name that the doxxer had disclosed. As Dubrofsky and Wood (2015) and Marwick and boyd (2010) have emphasized, social media providers reward users for selling "real" or authentic online content, i.e. disclosing personal information to feed the data beast. Zuboff's (2019) theory of surveillance capitalism as rogue capitalism emphasizes that these companies' aggressive data collection is a means to a commercial end that disregards any social norms to treat users – who are only data points – as humans with human requests.

9. Misogyny and sexism

With nine women compared to six men participating in our study (albeit women are known to be more likely to volunteer), this may point to a power asymmetry online: women may be more likely victims of doxxing than men. At the same time, a majority (11) of victims said they suspected or knew their doxxer was a man; a minority (3) said it was a woman. The most frequent combination (7) was a woman victim and a man doxxer (Table 3). Although our interviews are not representative, they indicated that doxxers were most often men, no matter the gender of the victim. Additionally, almost half of our women participants but only a third of men encountered multiple doxxers or doxxing episodes while only a third of our men participants did so.

With only one exception – a gay man – men who were victims did not face sexualized personal information being doxxed. By contrast, a third of our women (3) said doxxed content included nude photos or sex tapes, sexist comments, or threats of sexual violence. This is in line with Pew's findings that women are twice as likely as men to experience sexual harassment online, and young women three times as likely (Duggan, 2017). Our interviewees' cases are exemplary of the misogyny and sexism linked to doxxing: through technological designs that allow misogynist spaces (Banet-Weiser, 2015; Mantilla, 2013); a rape culture of verbal sexualized harassment and threats (Citron, 2014; Jane, 2014); and online spaces that appear to be for a general public but are in fact men-dominated where women are punished for "intruding" (Eckert & Steiner, 2013).

The confluence of technology design and cultural acceptance of misogynist spaces stood out in the case of a U.S. woman who had voluntarily shared nude photos with her boyfriend via

Table 3: Gender of victim and suspected doxxer, all cases and cases with suspected multiple doxxers

Victim	Doxxer	Number of cases (all)	Number of cases (multiple doxxers/ incidents)
Woman	Man	7	3
Man	Man	4	2
Woman	Woman	2	1
Man	Woman	1	0
Man	Unknown	1	0
Total		**15**	**6**

Facebook Messenger. Her boyfriend kept these photos private but a former classmate hacked into his messenger account and retrieved them. The doxxer did so, the victim said, to "trade" them on a website where men exchange nude photos of women. Her example shows how technology design and the continued cultural degradation of women as sex objects merge into misogynist doxxing flows: First, the online site, which facilitated their romantic communication and enticed users to exchange personal information, Facebook Messenger, was able to be hacked. Second, the website that used images of women's bodies as a "currency" without their consent exists with impunity for website providers or users. Third, women are encouraged to share sexualized content to generate traffic and profits (Götz, 2019; Nakamura, 2015). It is for these reasons that, especially for women and the sexualized data they are enticed to share, remain hot commodities online; perpetuating and amplifying misogyny and sexism.

Another example of misogyny online funneling into doxxing is the case of a woman Wikipedia editor in Germany who said that before the doxxing incident, men would post "sexist stuff, with pornographic pictures and innuendo" on her Wikipedia discussion site, making her feel uncomfortable and threatened. As a consequence she said that she temporarily closed her Wikipedia account. A former woman politician in Switzerland, who got sent semen in the mail, summarized:

> Men colleagues are also being insulted online but it's a different type of hate. It's different if a man is told, you are as dumb as they come and incompetent, or if they tell me: You stupid cunt, I will rape you. That's just different…it hits more deeply. Men [victims] don't experience it like that.

This supports Jeong's (2015, para. 21) argument that: "doxing is a tactic to dominate the voice of the Internet. Everyone has his own understanding of what does or does not belong on the Internet – in other words, what garbage needs to be taken out. In the case of misogynists, women are that garbage." A third of women participants said they got doxxed because they were women operating in men-dominated online spaces. A U.S. gamer said only 5 % to 25 % of players in her gaming space were women: "There have been situations in the U.S. top 15 guilds where I am the only girl." She said in this gaming space women have been seen as "easier victims" for harassment because "people are less likely to rally behind a woman in a competitive spot in gaming. …there is also the idea, especially since the [doxxed] content was primarily sexual, that women only get spots in the top guilds through sexual favors." Similarly, a Wikipedia editor said that in the German-language Wikipedia only 10 % to 15 % of contributors are women, confirming Wikipedia's gender gap (Eckert & Steiner, 2013). She said her work on articles about anti-feminist men right's and New Right movements triggered the doxxing: "I was editing areas where you usually don't find women users with an account. …I can discuss quite aggressively if need be with such people and I was persistent and very present and this is how all added up [to becoming a target]."

By contrast, a U.S. Wikipedian said his identity protected him: "It's not particularly dangerous to be a young white man. I'm straight and cis…there's nothing interesting or vulnerable about me." Similarly, a U.S. man who was accidentally doxxed said: "It's given me increased appreciation for women and people of color and LGBTX on the internet who are speaking up. I can't really imagine dealing with this in any sort of sustained way."

Our participants' identities as women, minorities, feminists, and/or activists and their sense-making of the doxxing episodes indicates that these groups are likely victims of doxxing. Online harassment reflects and confirms the misogyny that shapes online spaces (Banet-Weiser, 2015; Eckert, 2018, Gardiner et al., 2016; Harmer & Lewis, 2020; Jane, 2014; Mantilla, 2013; Phillips, 2015; Turton-Turner, 2013). Our study adds to this scholarship and shows that doxxing is an area of highly gendered online abuse in which women are sexualized and their sexualized data are treated as a commodity without impunity in a surveillance culture that exploits women as producers and consumers of content for commercial purposes.

10. Discussion and Conclusion

We use Zuboff's (2019) important theory of surveillance capitalism to ground our interviewees' statements and to tie them to neoliberal ideology. We argue that doxxing is an insidious form of harassment as perpetrators are able to harness information found in enmeshed online *and* offline spaces exploiting current technology design and contemporary culture that makes it difficult to avoid online spaces for school, work, personal connections, or to function as a citizen (Zuboff, 2019). Police are often unable or unwilling to aid victims and social media providers are mostly unwilling to remove doxxed content, supporting contemporary criticisms of internet architecture built to be unforgetful and unforgiving (Jones, 2016). Ultimately, the victim is left to untangle the complexities of the harassment on their own. While the GDPR may give E.U. citizens a new path for the removal of their online information, in the U.S. and other countries, laws protecting privacy online are absent, glacially developing, or only intermittently enforced. California's recently implemented Consumer Privacy Act (Morrison, 2019) was hailed as a victory for consumers in the state to regain at least some control over the data social media and website providers collect. Even when laws are enacted, powerful social media providers, head-quartered in the U.S., may not heed national laws or verdicts made outside the U.S.

Our participants' experiences highlight the harms theorized by Zuboff (2019) as surveillance capitalism through technology design. They also confirm the logic of normalizing surveillance through everyday technology use for aggressive data collection and exploitation (Dubrofsky & Magnet, 2015). Media technologies in surveillance capitalism are designed to shape user behaviors, encouraging people to share personal information that ultimately feeds commercial interests (Zuboff, 2019), while leaving them vulnerable to harassment (Massanari, 2017). In "informated and technologized societies" (Andrejevic, 2015, p. xi) peers watching peers is normalized, rendering privacy moot through peer pressure and computationally directed certainty of behavior, ultimately eroding humans' "right to sanctuary" (Zuboff, 2019, p. 21). Thus, we argue that doxxing needs to be theorized in the broader context of surveillance capitalism, recognizing the many forms of technology assisted and induced veillances and the importance of the contextual integrity of submitted personal data.

Previous definitions of doxxing offered concepts that focused on information moving online through perpetrators or the goals of doxxers (Douglas, 2016; Duggan, 2017; Eveleth, 2015). But these definitions need to evolve to account for ongoing techno-cultural changes in which everyday users increasingly depend on social media to access services and people (Nakamura, 2015). At the same time, as Lovink (2016) argues, the problem is not only the ubiquity of internet and social media technologies but how they gather influence in the back-

ground, creating "new states of collective unconsciousness" (p. 10). Thus, we theorize contemporary 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. The intent, process, and subsequent harassment is tailored to the victim's overlapping identities and specific situations. This definition of doxxing exposes the inability of any individual's sole control of the flow of their personal information in an enmeshed, capitalist, and surveilled environment that generates and treats data, and, by extension, humans as a commodity. Additionally, our definition highlights the importance of identity, as the type of doxxing a person experiences is tied to dimensions of their identity such as gender and sexuality, adding to the vulnerabilities that already discriminated groups, including women, experience.

Policy makers and legal authorities must recognize the ways online and offline spaces are inextricably enmeshed, and the responsibilities that social media providers and technology developers have in perpetuating harassment through biased technology design (Massanari, 2017). As one man in our study, who worked as a software developer, said: "I'm in an unlicensed profession. You know, if you build buildings you have to be certified… My profession is too new. Any asshole can call themselves a developer and start building websites." The lack of oversight, regulation, and diversity in technology development are contributing to the continued harassment faced by women and minorities.

Doxxing starkly exposes how essential the internet has become for daily life but also how "psychic numbing [sic] inures us to the realities of being tracked, parsed, mined, and modified" (Zuboff, 2019, p. 11), not only by commercial and state interests but by peers. When done intentionally, doxxing enacts surveillance capitalism on a mini scale: using data to bargain for other data to intimidate or silence – combining watching with attempting to control others' behavior in a grid of human power relations. When done unintentionally, doxxing feeds into the normalization of the erosion of privacy and individual autonomy, which are fundamental to democratic society. Either way, doxxing brings a shock that renders visible the gendered veillance cultures in which we are marinating. When examined through a lens of gendered harassment and peer veillances that feed into surveillance capitalism, doxxing uniquely highlights the urgent need for comprehensive policy, law enforcement, and cultural changes.

References

Abidin, C. (2013). Cyber-BFFs*: Assessing women's "perceived connectedness" in Singapore's commercial lifestyle blog industry. *Best friends forever. *Global Media Journal Australian Edition, 7*(1). https://www.hca.westernsydney.edu.au/gmjau/?p=217 [13.07.2020].

Andrejevic, M. (2015). Foreword. In R. Dubrofsky & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. ix-xviii). Durham, NC: Duke University Press.

Arvanitidis, T. (2016). Publication bans in a Facebook age: How internet vigilantes have challenged the Youth Criminal Justice Act's 'secrecy laws' following the 2011 Vancouver Stanley Cup riot. *Canadian Graduate Journal of Sociology and Criminology, 5*(1), 18–32.

Banet-Weiser, S. (2015, January 21). Popular misogyny: A zeitgeist. *Culture Digitally*. http://culturedigitally.org/2015/01/popular-misogyny-a-zeitgeist [10.07.2020].

BBC (2018, January 1). Germany starts enforcing hate speech law. http://www.bbc.com/news/technology-42510868 [10.07.2020].

Blake, A. (2016, October 27). 'Celebgate' hacker Ryan Collins gets 18 months in prison. *Washington Times*. https://www.washingtontimes.com/news/2016/oct/27/celebgate-hacker-ryan-collins-sentenced-18-months-/ [10.07.2020].

boyd, d., & Elison, N. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer Mediated Communication, 13*(1), 210–230.

Brinkmann, S., & Kvale, S. (2015). *InterViews: Learning the craft of qualitative research interviewing*. Thousand Oaks, CA: Sage.

Citron, D. K. (2014). *Hate crimes in cyberspace.* Cambridge, MA: Harvard University Press.

Clark, K. (2017, June 27). Clark, Brooks, Meehan push online safety roadmap, combat sextortion, internet threats, other online crimes. https://katherineclark.house.gov/index.cfm/press-releases?ID=C0878679-D18D-496F-8096-B996CB985BB6 [10.07.2020].

Douglas, D. (2016). Doxing: a conceptual analysis. *Ethics Information Technology, 18*, 199–210.

Dubrofsky, R. E., & Magnet, S. A. (2015). Feminist surveillance studies: Critical interventions. In R. E. Dubrofsky & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. 1–20). Durham, NC: Duke University Press.

Dubrofsky, R. E., & Wood, M. M. (2015). Gender, race and authenticity. Celebrity women tweeting for the gaze. In R. E. Dubrofsky & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. 93–106). Durham, NC: Duke University Press.

Duggan, M. (2017, July 11). Online harassment 2017. Pew Research Center. http://www.pewinternet.org/2017/07/11/online-harassment-2017/ [10.07.2020].

Eckert, S. (2018). Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the UK and US. *New Media & Society*, *20*(4), 1282–1302. DOI: 10.1177/1461444816688457.

Eckert, S., & Steiner, L. (2013), "Wikipedia's gender gap". In Armstrong, C. (ed.), Media Disparity: A Gender Battleground (pp. 87–98). New York, NY: Lexington Books.

Eckert, S., Metzger-Riftkin, J., Kolhoff, S., & O'Shay-Wallace, S. (2019). A hyper differential counter-public: Muslim social media users and Islamophobia during the 2016 U.S. presidential election. New Media & Society. https://doi.org/10.1177/1461444819892283.

Ellis, R. (2017, December 31). Swatting case poses legal challenges for police, prosecutors. *CNN*. https://www.cnn.com/2017/12/31/us/swatting-legal-ramifications/index.html [10.07.2020].

Eveleth, R. (2015). How to deter doxxing. *Nieman Reports, 69*(3), 46–49.

FBI (2016, March 10). The evolution of swatting. https://www.fbi.gov/audio-repository/news-podcasts-thisweek-the-evolution-of-swatting.mp3/view [10.07.2020].

Gardiner, M., Mansfield, M., Anderson, I., Holder, J., Louter, D., & Ulmanu, M. (2016, April 12). The dark side of Guardian comments. *Guardian.* https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments [10.07.2020].

Gillmor, D. (2004). *We the media*. Sebastopol, CA: O'Reilly Media.

Götz, M. (2019). „Man braucht ein perfektes Bild." Die Selbstinszenierung von Mädchen auf Instagram. *Televizion Digital, 1*, 9–20. http://www.br-online.de/jugend/izi/deutsch/publikation/televizion/Digital/Goetz-Perfektes_Bild.pdf [10.07.2020].

Harmer, E., & Lewis, S. (2020). Disbelief and counter-voices: a thematic analysis of online reader comments about sexual harassment and sexual violence against women, *Information, Communication & Society,* DOI: 10.1080/1369118X.2020.1770832.

Hicks, M. (2017). *Programmed inequality*. London, UK: MIT Press.

Jane, E. A. (2014). 'Back to the kitchen, cunt': Speaking the unspeakable about online misogyny. *Continuum: Journal of Media & Cultural Studies, 28*(4), 558–570.

Jeong, S. (2015). *The internet of garbage*. Jersey City, NJ: Forbes Media.

Jones, M. L. (2016). *Ctrl+Z: The right to be forgotten*. New York: New York University Press.

Kidd, D., & Turner, A. (2016). The #GamerGate files: Misogyny in the media. In Novak, A. & El-Burki, I. J. (Eds.), *Defining identity and the changing scope of culture in the digital age* (pp. 117–139). Hershey, PA: IGI Global.

Lenhart, A., Ybarra, M., Zickuhr, K., & Price-Feeney, M. (2016, November 21). *Online harassment, digital abuse, and cyberstalking in America*. https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf [10.07.2020].

Light, J. (2003). Programming. In Lerman, N. E., Oldenziel, R., & Mohun, A. P. (Eds.), *Gender & Technology* (pp. 295–326). Baltimore, MD: Johns Hopkins University Press.

Lovink, G. (2016). *Social media abyss.* Malden, MA: Polity.
Mantilla, K. (2013). Gendertrolling: Misogyny adapts to new media. *Feminist Studies, 39*(2), 563–570.
Marwick, A., & boyd, d. (2010). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 114–133.
Massanari, A. (2017). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society, 19*(3), 329–346.
Merlan, A. (2015, January 29). The cops don't care about violent online threats. What do we do now? Jezebel. https://jezebel.com/the-cops-dont-care-about-violent-online-threats-what-d-1682577343 [10.07.2020].
Monahan, T., & Wood, D. M. (2018). Introduction: Surveillance studies as a transdisciplinary endeavor. In T. Monahan & D. M. Wood (Eds.), *Surveillance studies. A reader* (pp. xix–xxxiv). Oxford, UK: Oxford University Press.
Morisson, S. (2019. December 30). California's new privacy law, explained. Vox. https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained [10.07.2020].
Mortensen, T. E. (2016). Anger, fear and games: The long event of #GamerGate. *Games and Culture*, *13*(8), 787–806.
Mulvey, L. (2009). Visual pleasure and narrative cinema. In R. Warhol-Down & H. D. Price (Eds.). *Feminisms redux: An anthology of literary theory and criticism* (pp. 432–443). New Brunswick, NJ: Rutgers University Press.
Nakamura, L. (2015). Afterword: Blaming, shaming, and the feminization of social media. In R. E. Dubrofsky & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. 221–228). Durham, NC: Duke University Press.
Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Redwood City, CA.
Phillips, W. (2015). *This is why we can't have nice things.* Cambridge, MA: MIT Press.
Sarkeesian, A. (2012, December 4). Anita Sarkeesian at TEDxWomen 2012. https://www.youtube.com/watch?v=GZAxwsg9J9Q [10.07.2020].
Shirky, C. (2009). *Here comes everybody: The power of organizing without organization*s. New York, NY: Penguin.
Smith, A., & Duggan, M. (2018, January 4). Crossing the line: What counts as online harassment? Pew Research Center. http://assets.pewresearch.org/wp-content/uploads/sites/14/2018/01/03141121/PI_2018.01.04_Online-Harassment-Scenarios_FINAL.pdf [10.07.2020].
Snyder, P., Kanich, C., Doerfler, P., & McCoy, D. (2017, November). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. In *Proceedings of the 2017 Internet Measurement Conference* (pp. 432–444).
Stewart, D. (2014, August 13). Mom arrested for letting kid play in park gets doxxed by local news. Jezebel. https://jezebel.com/mom-arrested-for-letting-kid-play-in-park-gets-doxxed-b-1620674465 [10.07.2020].
Turton-Turner, P. (2013). Villainous avatars: The visual semiotics of misogyny and free speech in cyberspace. *Forum on Public Policy, 1*, 1-18. http://forumonpublicpolicy.com/vol2013.no1/women.html [10.07.2020].
Tyson, M. (2016, October 11). CPS publishes new social media guidance and launches hate crime consultation. Hexus. https://hexus.net/business/news/legal/97840-the-cps-publishes-social-media-hate-crime-prosecution-guidance/ [10.07.2020].
Zuboff, S. (2019). *The age of surveillance capitalism*. New York, NY: PublicAffairs.