5-11-2023

Doxing and Doxees: A Qualitative Analysis of Victim Experiences and Responses

Anjuli Franz
Technical University of Darmstadt, franz@ise.tu-darmstadt.de

Jason Bennett Thatcher
Temple University, jason.b.thatcher@gmail.com

DOXING AND DOXEES: A QUALITATIVE ANALYSIS OF VICTIM EXPERIENCES AND RESPONSES

Research Paper

Anjuli Franz, Technical University of Darmstadt, Germany, franz@ise.tu-darmstadt.de

Jason Bennett Thatcher, Temple University, USA, jason.b.thatcher@gmail.com

Abstract

Doxing, a form of adversarial online behavior, is the aggregation and release of an individual's personal information with malicious intent. It is increasingly used to intimidate, punish, or silence individuals. Such weaponization of personal information can result in extreme and intertwined cyber harassment and physical threats, significantly affecting doxees' participation in both cyber and physical communities. While prior research has examined the underlying motives of the doxer, the doxee's perspective has remained largely unexplored. Drawing on data from 14 individuals who have experienced doxing, this study examines the consequences of doxing from the doxee's point of view. Employing the lens of approach and avoidance coping, we explore how doxees respond to doxing threats and adapt their behavior. Our research provides novel insight and themes related to doxing. Based on our analysis, we offer an agenda for information systems (IS) research and practice, paving the way for exploring doxing and potential remedies.

Keywords: Doxing, Adversarial online behavior, Cyber harassment, Privacy, Coping theory, Qualitative study

1 Introduction

In the summer of 2022, a Kiwi Farms[1] user opened a thread on trans activist Clara Sorrenti. "The first thing that they did […] was find the obituary for my dead father and use it to find his memorialized Facebook page," Sorrenti explained (O'Sullivan and Naik, 2022). "They were able to find a picture of my dad on the front porch of my childhood home and from that use Google Maps and figure out where that was located." Sorrenti experienced months of harassment and threats, eventually leading to armed police showing up at her home in Ontario after her harassers had called in a fake emergency, a tactic known as swatting. After being interrogated by the police, Sorrenti fled to a nearby hotel. Within hours, Kiwi Farms users determined which hotel in her city had matching bed sheets from Sorrenti's photo of her cat (Collins and Tenbarge, 2022). Through hacking her Uber account, her harassers were then able to obtain her and her family members' phone numbers and email addresses, which again were posted on Kiwi Farms. Sorrenti, like many other people, had been repeatedly doxed.

Doxing refers to the intentional and malicious disclosure of an individual's personal information with the aim of causing harm (Douglas, 2016). Doxing incidents can range from releasing a person's phone number in public feeds, such as live stream chats (Twitch, 2022), to the creation of extensive dossiers containing any information a doxer can find about an individual, which is then tagged and posted online to encourage others to take action against the victim. The disclosed information may include contact

[1] Kiwi Farms is an online forum where groups of users target minorities, such as trans or neurodivergent people, to harass, stalk, and dox them. Founded in 2013, it was taken offline in September 2022 by its hosting provider Cloudflare due to its "imminent and emergency threat to human life" after a month-long public debate, but has since been brought back online by a different provider (O'Sullivan and Naik, 2022).

details, intimate photos, home addresses, or employers, all of which can be used for malicious purposes, from cyber harassment to physical harm. Beyond the Clara Sorrenti doxing campaign, the weaponization of personal information has been utilized to harass activists and police officers involved in political protests (Cheung, 2021), female game developers during the GamerGate incident[2] (Jeong, 2019; Romano, 2021), and has inflicted such harm that at least three suicides have been attributed to doxing (Yousef, 2022).

While prior research has examined the experiences of cyberbullying victims (Chan et al., 2021), privacy and social media research has left unexamined doxees. Whereas some studies have investigated the attacker's viewpoint, such as doxers' underlying goals and motives (Douglas, 2016; Anderson and Wood, 2021), the victim's perspective is largely missing. Such work is necessary because doxees face extreme, severe, cross-domain threats that impact all aspects of life (personal, social, and professional). For instance, we do not yet understand how a doxing incident influences the subsequent behavior of doxees. To gain such insights, we conducted a qualitative study of doxing from the victims' point of view. Three research questions guided our phenomenon-driven study:

RQ1: What are the reasons individuals are doxed, by whom, and how do incidents unfold?

RQ2: What are the consequences of a doxing incident for the doxee?

RQ3: How do doxees respond to and cope with being doxed?

Moving beyond widely documented cases of doxing reported in the news, we gathered data from 14 doxees to uncover various forms of doxing and their implications. Through the lens of approach and avoidance coping, we disentangle the short-term and long-term ramifications of doxing and analyze how it transforms how people participate in their communities.

Our research contributes to the literature on information security in general and on doxing in particular. First, this paper introduces novel issues and themes related to doxing, an emerging and poorly understood phenomenon. Second, we present a research agenda for investigating doxing and the experiences of doxees. Finally, we offer practical implications for social media platform providers, regulators, and employers.

2 Theoretical Background

2.1 Doxing

Doxing is a hacker slang-based neologism derived from "dropping dox [documents]" (Anderson and Wood, 2021). It refers to the "intentional public release of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual" (Douglas, 2016, p. 199). Since doxing often involves disclosing location data, such as a home or work address, it represents a threat that intertwines the cyber and physical domain. Doxing has also been described as technology-facilitated violence (Anderson and Wood, 2021), online abuse (Snyder et al., 2017), or digilantism (digital vigilantism, Nhan et al., 2017). In contrast to other forms of adversarial online behavior, such as cyberbullying, blackmailing, or data breaches, doxing is unique in weaponizing an individual's data with malicious, personally targeted intent. Typically, the released information was already publicly available but distributed across various sources, such as social media profiles or public registries, that might be difficult to access (Douglas, 2016). Other doxing incidents involve the breach of personal information via hacking or social engineering attacks. The "compilation, maintenance, use, and dissemination of personal information on individuals" is also referred to as "dossier building" (Douglas, 2016, p. 202). The opportunities created by the internet effectively enable every user worldwide to assemble a dossier about an individual and to release it to the public.

[2] GamerGate was an online harassment campaign in 2014 to 2015 directed towards outspoken feminist women of the gaming industry. It has been argued to be a watershed moment that showed the trend towards systematized online harassment based on ideological polarization (Eckert and Metzger-Riftkin, 2020).

The dynamics of a doxing incident range from relatively simple (e.g., a user doxing a streamer's real name in an online chat) to highly complex (e.g., hundreds of users coordinating the compiling of a doxee's dossier in an online forum). Figure 1 displays a model of the stakeholders involved in a doxing incident. The 'public' refers to a broad range of people, such as the doxee's social network, employer, or arbitrary internet users who have access to the disclosed information. The public's perceptions (e.g., an employer viewing the doxee as untrustworthy following the incident), reactions (e.g., a friend supporting the doxee), and potential actions (e.g., other users participating in the harassment) can significantly influence the impact of the incident the doxee, as well as the doxee's response to it.

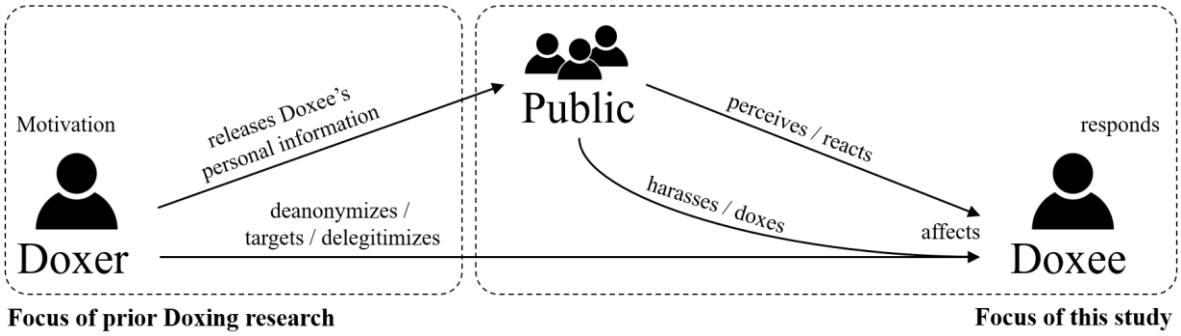

Figure 1. Model of a doxing incident

While the malicious release of others' personal information has existed long before the internet, technologies such as people search websites or image recognition software facilitate the search of individuals' personal information. Moreover, affordances of social media (e.g., like / comment / share; Karahanna et al., 2018) act as a catalyst for its aggregated disclosure and dissemination, and allow the doxing incident to gain campaign-like character. Surprisingly, however, IS literature on doxing is scant. Researchers from information technology ethics (Douglas, 2016), criminology (Trottier, 2020), or law (MacAllister, 2016), have started to study doxing, mainly focusing on the left side of our model above. For example, Douglas (2016) has introduced a typology of doxing based on the value that doxing endangers: He distinguishes between deanonymization doxing, where the formerly anonymous identity of an individual is released; targeting doxing, which reveals information about an individual that allows them to be physically located; and delegitimizing doxing, which reveals intimate personal information that damages the credibility of the doxee. Diving deeper into doxers' motivation, Anderson and Wood (2021) present several underlying motives such as silencing or controlling the doxee, or building oneself a hacker reputation. Although previous research has demonstrated that doxing elicits negative emotions, such as depression, anxiety, or stress among doxees (Chen et al., 2018), the right side of the model has remained largely unexplored.

2.2 Approach and Avoidance as Mechanisms for Coping

To investigate doxees' responses to a doxing incident, we employ approach and avoidance as mechanisms for coping with trauma as a theoretical lens. Approach and avoidance are two basic modes of how individuals respond to a threat (Roth and Cohen, 1986). They are opposed forms of cognitive and emotional activity oriented either towards or away from the threat. Previous works have formulated approach strategies (that is, orientation towards the threat) as being vigilant and overly alert, taking self-responsibility, and seeking knowledge about the threat to be able to appraise and carefully plan one's behavior (e.g., Cohen and Lazarus, 1973; Miller, 1980). In contrast, avoidance strategies (that is, orientation away from the threat) have been characterized as restricting one's behavior to avoid anxiety-arousing stimuli, practicing detachment from the threat, or giving up personal responsibility (e.g., Mullen and Suls, 1982). While the approach mechanism is associated with the benefits of reacting and actively dealing with one's trauma, it comes along with increased stress and potentially nonproductive worry. In contrast, whereas the avoidance strategy typically reduces stress, it impedes appropriate reactions and might foster disruptive avoidance behaviors (Roth and Cohen, 1986).

3 Research Method

Considering the limited literature on doxing from the subject's perspective, we adopted a qualitative approach. This method allows us to illuminate individual and contextual factors that characterize doxing as an emerging cybersecurity phenomenon (Cram et al., 2021; Straub and Welke, 1998). We gathered data from 14 individuals (coded as I1-I14) who had experienced doxing. Our data collection was shaped by two primary challenges: First, doxees are hard to find and contact. Due to their negative experiences disclosing their personal information online, many doxees do not share details of their doxing incident on social media, public forums, or websites. If they do, they are hesitant to respond to interview requests. Second, individuals' doxing experiences often touch on very personal and vulnerable topics, which might make them uncomfortable being interviewed for a study. Hence, we relied on three data-collection techniques: (1) in-depth semistructured interviews (n = 3; I2, I8, I14), that should encourage participants to speak freely and allow the interviewer to ask follow-up questions; (2) anonymous online surveys (n = 7; I1, I3, I6, I9, I11-13), where participants typed their answers to open-ended questions which they may not be comfortable to reply to in person; and (3) archival data (n = 4; I4, I5, I7, I10), e.g., blog articles from or about doxing subjects with a focus on their personal experience of the doxing incident.

The majority of participants in groups (1) and (2) were found either through directly contacting individuals who reported their experience with doxing in online discussion forums or news articles, or through responses to our survey link posted in online forums, such as r/Twitch or r/Teachers on reddit.com. We broadly sampled individuals with many characteristics to increase the scope of our findings and inform a more general theory (Urquhart et al., 2010; Davison and Martinsons, 2016). Our sample age ranges from 20 to 59 years old (average: 40) and is primarily female (57%). Most participants are US citizens, except for I3, who is Irish. Some participants chose not to disclose their demographic information. For the interview and qualitative survey techniques, we employed an evolving set of open-ended questions that changed as we learned more about doxing. In alignment with *RQ1-3*, the questions inquired about the doxing incident itself, its impact on doxees' personal, social and work life, changes in their day-to-day as well as online behavior, and how they coped with the incident. To build a theory for explanation (Gregor, 2006) for the victim perspective on doxing, we employed an iterative, inductive approach in our data analysis (Urquhart et al., 2010; Kaplan and Maxwell, 2005; Glaser and Strauss, 1967). We coded data based on the techniques offered by Kuckartz (2012), using the software MAXQDA. In the first rounds of coding, we analyzed our material line by line and developed preliminary conceptual labels for meaningful units of text. This process allowed us to gain a deep understanding of our data and guided us in discovering common themes. By overlapping our first rounds of analysis with data collection, we allowed emerging themes to inform both our acquisition of further study participants and the development of our question catalog. In later rounds of our first-order coding, we derived second-order categories and overarching themes from our coding structure (Kuckartz, 2012).

4 Results

4.1 How, by whom, and for which reasons do people get doxed? (RQ1)

In Table 1, we offer detail on our sample and their experiences with doxing. We briefly summarize each doxing incident and offer an overview of the type and the source of the doxed information, the medium where the doxing incident took place, and the doxee's view of the doxer's identity and motive.

Looking at the type and source of the doxed information, we find that almost all doxing incidents involve the disclosure of **contact information**, such as the subject's phone number or email address. Moreover, more than half of the doxing incidents include a physical location, which is mostly a **home address**. For subjects whose identity had been anonymous (e.g., content creators who had been working under an alias), being doxed involved the disclosure of their full name and **identity**. Other types of doxed personal information include **pictures** (among them **intimate pictures**), **social media profiles** or **social media posts**, the doxee's **profession**, **employer**, or **salary**, their **sexual orientation**, **gender identity**, **political**

views, or **private correspondence**. For several subjects, this was not limited to doxees' personal information but also **family members', friends', or colleagues' data**.

Some doxed information had previously been self-disclosed by the doxee, for example, on their **social media profile** or via a prior **confidential exchange of information** between doxee and doxer. Beyond that, doxers assemble information from **public sources** that doxees do not necessarily have control over, such as their work website, a family member's obituaries, the voting registry, or public archives of real estate transactions. **People search engines** (e.g., peoplefinder.com) often list individuals' addresses or relationship status without them being aware. More active approaches to compiling a doxee's personal information include **hacking their accounts** (e.g., via brute-force password guessing or social engineering tactics, such as sending a fake friend request), or **stealing their personal devices**.

Once the doxee's data is in the hands of the doxer, the platforms where the information is disclosed, are manifold. For many of our subjects, the doxed information was spread across several media, including **mainstream social media platforms** (e.g., Twitter or TikTok), **messenger services** (e.g., online chats, WhatsApp groups), **online forums** (e.g., Reddit), or **online forums that are specifically dedicated to doxing** (e.g., Kiwi Farms, 4chan). I2 stated that the **local news** reported on her doxing incident, with articles amplifying the dissemination of her personal information. Two incidents occurred at **school**, with I11 and I12 being teachers who were doxed by a student toward other students and school staff.

With regard to the timeline over which an incident unfolds, we find **one-time-only** incidents (that are, however, often embedded in months-long harassment campaigns), as well as individuals being **repeatedly doxed for several weeks, months, or even years**. For the latter, the doxing activity mostly occurs in waves, which tend to be driven by either **news coverage** or the **doxee's confrontational behavior**. I9 describes: *"After seeing multiple other people being harassed for similar things, I felt the need to take a bigger stand and get more involved. Me becoming more vocal absolutely played a part in making me a bigger target."* While most subjects named a timespan when asked about the duration of their doxing incident, I13 states: *"This is a confusing question. I do not see the doxing as an incident, but an ongoing threat to my privacy. There is no way to actually have the information removed."*

Diving deeper into *why* people get doxed, our sample divides into **issue-based** and **person-based** doxing. In issue-based doxing, doxers target the doxee because of a specific issue or group they represent. Examples in our dataset include being doxed for promoting a certain political opinion, advocating for marginalized groups, or one's sexual orientation or gender identity. The doxer uses the doxee as a political pawn to discredit that issue or opinion. Issue-based doxing can overlap with **vigilantism**, such as I1, who was doxed by a pacifist group who assumed his firearm collection violated the law, or I9, who was targeted for allegedly being a sexual predator. In the case of person-based doxing, the doxer targets the doxee for personal reasons, such as seeking revenge, trying to get someone fired from their job, or bullying. An example is I2, whose political group was doxed by a disgruntled former member.

While some doxing incidents are committed by single persons or small fixed groups, we find that other incidents gain **campaign character**, that is, a doxee's "dossier" is gradually assembled in online threads by multiple users. In contrast to some campaigns being of **spontaneous, amorphous, leaderless nature**, others are **initiated and led by one coordinator.** Whereas, in the first case, doxees report that their doxers *"seem to be doing it just for fun or out of fear of being targeted by the group"* (I9), in the second case, the doxers are described as a coordinated *"mob"* (I5), with one coordinator targeting the victim, *"pointing their followers in your direction, and making [them] descend on you"* (I7). In I2's case, the coordinator first disclosed an initial set of her personal information and instigated his Twitter community to *"go get her"* her, then tagged her employer, and called radio stations and local newspapers to disseminate the story. While some coordinators are overt about managing a doxing campaign, others **try to make the campaign look like a leaderless, organically grown movement**: *"[Person X] sent an email to [person Y] with a link to one of my columns, and he said "please mock this fat feminist". Which is significant, because it's sort of evidence that [Y]'s campaign […] was a deliberately coordinated silencing campaign, and not, as he wanted us all to believe, just a bunch of random boys on the internet having spontaneous fun"* (I7).

Doxed information	Source of doxed information	Medium	doxer identity and motive	Demographics
I1 was targeted by an anti-gun group that believed his firearms collection violated the law. His home address was leaked in online chats, which resulted in individuals physically arriving on his property, damaging his house and cars, and injuring his wife. After the doxing incident, I1 and his wife changed their property location and identity for safety. He has been very reluctant to share his data ever since, and uses strict privacy protection measures online.				
• Home address • List of firearm collection	Unknown	• Online chat	Issue-based: Anti-gun group who assumed I1 to violate the law.	Age: 50-59 Gender: Male Year: 1995
I2 held an executive role in external affairs at a cancer treatment center. During the COVID-19 pandemic, she posted an article on former President Trump's reluctance to finance ventilators on her private Facebook page, along with the comment "Trump supporters need to pledge to give up their ventilators for someone else". A Republican operative shared a screenshot of this post as well as I2's contact information on Twitter, urging his followers to bring to account I2 and her employer. This resulted in I2's employer terminating her contract, strangers assembling her data online, and her family and colleagues being harassed.				
• Home address, Google Earth picture of the house • Phone number, email addresses, social media profiles • Pictures of self, spouse, and children • Family members' phone numbers • Employer, work address and phone number, boss's and secretary's phone number, salary	• Self-disclosed on social media and wedding website • Public archive of real estate transactions • Voting registry • Listed as reference in another person's online resume	• Twitter • Facebook • LinkedIn • Reddit • Alt-right forums • Local news	Issue-based: Political operative of the opponent party, who initiated a coordinated doxing campaign supported by many others. I2 felt like she was being used as a political pawn, and as if she was clickbait.	Age: 40-49 Gender: Female Year: 2020
I3 is a member of a left-wing political activist group. A disgruntled former member of that group disclosed the personal data of group members and internal documents. This caused reputational damage for the group and its members and damaged members' trust in each other, impeding future collaboration. The doxing incident severely impacted I3's mental health and social life and caused him to withdraw from speaking out on social media and attending public events.				
• Names of group members, email addresses • Political beliefs • Professions and employers • Internal documents (e.g., strategy)	• Access to internal documents and personal information of group members through previous group membership	• Far-right magazine • Twitter • WhatsApp	Person-based: Upset previous group member took revenge by doxing the group and its members.	Age: unknown Gender: Male Year: 2020
I4 was doxed by a stranger who impersonated her by disclosing her picture and phone number on Craigslist ads that portrayed her as a sex worker. The doxer posted numerous ads in major cities across the country over four months, resulting in I4 becoming the target of online sexual harassment and rape threats and fearing for her physical safety. Although her picture and phone number have been disclosed, her identity (i.e., her name) has been concealed.				
• Phone number • Photos	Unknown	• Craigslist	Person-based: I4 stated that she does not know the doxer's identity and motive.	Age: unknown Gender: Female Year: 2016
I5's Twitter account was hacked by her doxers, who used it to broadcast tweets with discrediting messages and her personal information. This began "GamerGate", a year-long online harassment campaign against outspoken feminist women in the gaming industry.				
• Home addresses of self and family • Pictures of home • Phone numbers of self and family • Intimate photos	• Self-disclosed or disclosed by friends on social media • Hacked online accounts • Public spreadsheet with safe	• 4chan • Twitter • Reddit	Person- and issue-based: I5's ex-partner published a defamatory blog article that inspired a mob, partly rooted in the alt-right, to start a	Age: 30-39 Gender: Female Year: 2014

• Social media accounts	addresses after a terrorist attack • People search websites		coordinated doxing campaign.	
I6 is a writer who used to promote her work on Reddit. After criticizing someone online, she received harassing and vulgar responses. One user posted her name, location, and profession, and created an account in her name with which he proceeded to harass other women.				
• Full name (previously known by alias) • Location (not specified) • Profession	• Self-disclosed online due to promotion of own work	• Reddit	Person-based: doxer (identity unknown) took revenge on I6 for her criticizing comments.	Age: unknown Gender: Female Year: 2022
I7 is a comedian and activist who writes about feminism, racism, and body image. She was part of a group of people targeted by a former editor of the alt-right news site Breitbart News in the form of a coordinated silencing campaign. The campaign made her leave Twitter, an online platform that previously was key to her work.				
• Home address, children's home addresses • Phone number, email address • Pictures of self and spouse	Unknown	• Twitter and other online platforms	Issue-based: I7 was targeted as a media figure who advocated for marginalized groups.	Age: 30-39 Gender: Female Year: 2017
I8, a former WNBA player, uses TikTok to support female athletes. In one of her live streams, an anonymous user posted her home address and phone number in the chat. Whereas I8 changed her privacy behavior, she was determined to keep speaking out on TikTok. The incident helped her account grow in the long term.				
• Home address • Phone number	• Found on a work website	• TikTok	Issue-based: I8 suspects her doxers to be teenage boys that harassed her for misogynist and racist reasons.	Age: 40-49 Gender: Female Year: 2020
I9 is an artist who was targeted after defending another artist's work online. The latter had been accused of being a pedophile after drawing an underaged cartoon zombie character. I9's personal information was dug up on multiple old accounts, and the doxers attempted to trick him into admitting guilty to crimes that they assumed he condoned. Becoming more vocal towards the doxers only fueled the harassment, which only died down when he started hiding and deleting his profiles.				
• Full name (previously known by alias) • Date of birth • Hometown, former high school • Pictures	• Self-disclosed on social media • IP grabber sent via email • Hometown guessed based on slang I8 used online	• Twitter and other online platforms	Issue-based: I9 assumed his doxers to be teenagers who were convinced that they were protecting themselves from sexual predators.	Age: 20-29 Gender: Male Year: 2019
I10 is a trans woman and journalist who got doxed on Kiwi Farms, where users document and mock minorities. She immediately started to cleanse her 13-year-long online presence to limit the damage. Nevertheless, her Kiwi Farms thread resulted in over 80 online pages of harassment and users trying to dig up her personal data.				
• Full name (previously known by alias), pre-transition name • Home address, phone number	• Self-disclosed on social media • People search websites	• Kiwi Farms • Twitter	Issue-based: I10 was targeted by Kiwi Farms users for being a trans online personality.	Age: 30-39 Gender: Female Year: 2017
I11, a teacher, was doxed by a student who gained access to his Facebook timeline by using a fake profile pretending to be someone I11 knew. The student divulged I11's posts of several years to other students and teachers, among other things outing I11 as gay. I11 described that "it was hell for [him] from that point forward", and that he eventually left the school the following year. He states that "the student was class president with a vast network at our school and never was punished".				
• Sexual orientation • Political views	• Social engineering to obtain access to private Facebook profile	The doxee's workplace (school)	Person-based: The student's goal was to ridicule I11 and to make him quit or be fired.	Age: 40-49 Gender: Male Year: 2008

I12 is a teacher and Twitch streamer. A student watched him enter his phone passcode, stole the device, and obtained access to his personal data, correspondence, and online accounts. He disclosed I12's information, including intimate photos of I12 and his wife to fellow students via I12's Google Classroom account and shared it with the school administration. The doxed information outed I12 and his wife as members of the LGBTQ+ community. The doxing incident left I12 in poor standing with school administrators, colleagues, and parents, and he is concerned that this will harm his future job prospects.				
• Home address, phone number • Intimate pictures and sexual identity of self and spouse • Social media profiles, private correspondence	• Stolen password via shoulder surfing • Stolen device	The doxee's workplace (school), via Google classroom	Person-based: The student remained anonymous, I12 suspects his motive to be anger that he had replaced a teacher they liked.	Age: 20-29 Gender: Male Year: 2022
I13 had been following an author online who had been doxed, swatted, and harassed for over 3 years. After I13 took a stand for that author by speaking out online, he and his wife were targeted by a mob of doxers, who created a thread on an online forum disclosing their personal information, harassed them via calls and text messages, signed them up to hateful newsletters and advertisements, and appeared at their home to take pictures.				
• Home address, email addresses, age, phone number, former high school • Spouse's name, phone number, work phone number, and LinkedIn profile	• People search websites	• Online forum	Not clear if person- or issue-based: I13 was targeted after defending a long-term doxing victim online.	Age: 40-49 Gender: Male Year: 2022
I14 maintained an online friendship with a social media influencer. When she criticized his hostile behavior towards others, he doxed her and encouraged his followers to harass her. The influencer also targeted I14's husband, who is a top executive with a well-known company. When the influencer continued to repeatedly occasionally dox her several times per year, I14 decided to take him to court. This resulted in the second wave of intense doxing, six years after the initial incident.				
• Full Name (previously known by alias), home address, phone number • Spouse's name, license plate • Parents' home address	• Information confidentially shared between doxee and doxer • Employer's website	• Facebook • Instagram • Twitter	Person-based: I14 stated that the doxer's motives were retaliation for criticism, as well as generating engagement among his followers.	Age: 50-59 Gender: Female Year: 2016, 2022

Table 1. Sample overview

Another motive that emerged from our data, but has not been found in prior literature, is **doxing for engagement**. For person-based and issue-based doxing incidents, doxees report that *"in my experience with him, he did this for engagement. Like, the more drama, the more people clicked, the more people watched"* (I14). I2 describes: *"Someone brought to the local news reporter's attention that I was getting doxed in the comments of his thread. They told him, 'manage your thread, report it, take it down'. But I had to report all my doxing myself. And this reporter, it was happening, and meanwhile – I wanna swear right now – and meanwhile he was giddy he had a number one trending story. He never responded to people that were saying, 'her address was just given out on your Facebook page'. […] I felt like I was just clickbait".*

Regarding the identity of the doxer, our data reveals that in four out of 14 cases, the doxer was **underaged**. This applies both to doxing in a school setting, where teachers were doxed by their students (I11, I12), as well as to doxing on online platforms, where two doxees report that *"most [of them] seem to be kids and teens, and […] doing it just for fun"* (I9). In all four cases, the doxing activity was directed from minors toward adults.

4.2 What are the consequences of a doxing incident for the doxee? (RQ2)

Immediately after the doxing incident, doxees mainly feel **scared** and **angry** (see Figure 2). While their anger is directed toward the doxer, their fears are more complex. Doxees are *"frightened that the revealed information might find its way back to [their] family, which would likely lead to [them] being disowned"* (I12), fear losing their job, or, when the doxers start to dig into friends' and family's lives, are *"afraid of how much information other well-meaning people might share"* (I5). With regard to the doxer, doxees are most scared of the doxing incident translating into **physical violence**. They are afraid of *"people coming to [their] house physically"* (I8), or begin *"fearing for [their] safety every time [they] go to the grocery store, refuel [their] car, or go hiking"* (I4). I10 argues that the doxers *"want a target to feel threatened, because that feeling of threat ensures that targets are always on edge, consumed with watching out for them"*. Such cross-domain effects of doxing distinguish it from related adversarial behavior, such as cyberbullying, which are mostly confined to the cyber domain.

While our data paints a broad emotional landscape of how doxees feel concerning their own life, they also feel **responsible for consequences on other peoples' lives**: *"It's one thing to be the target; it's another thing to have to warn a friend or loved one that hordes of awful people are about to stalk them, too"* (I5). I3, whose political group was doxed by a former member, states: *"As the techie in the group, it was my duty to keep everyone safe, and I felt I had failed at that."* Overall, a doxing incident evokes **extreme emotions** in all subjects. I12 states: *"I feel violated in a way that I haven't felt since I was much younger"*.

Figure 2. Emotions evoked by the doxing incident. The higher the number of doxees who reported the respective emotion, the bigger the font size.

In the short term, a doxing incident goes along with harassment, which occurs in the form of **physical and cyber harassment**, and, for the most part, **spills over to family members, friends, colleagues, or name sharers.** On the physical side, doxees and their loved ones receive **threatening phone calls and text messages**, become a victim of **stalking**, or even become the subject of **physical violence**. Online, doxees and their family and friends receive **threatening messages and comments**, such as I2, who describes that *"there is a whole discussion group saying 'we are going to keep an eye on her, and if she ever gets another job again, we are going to bombard her employer and make sure she never works again'"*. For six of the 14 doxing incidents analyzed in our study, the online persecution involves **sexual harassment**, such as **rape and death threats**. Doxees state that *"It actually got darker: Her firing isn't enough. She needs to be raped. She needs to be killed. She needs to be deported"* (I2), and that *"the rape and death threats started to feel terrifyingly real now that every conceivable detail of my life was at the mob's disposal"* (I5). Doxees also become a target of **cyberattacks**, such as attempts to breach their online bank account or them being signed up for newsletters and advertisements.

In the long term, doxing has multifaceted ramifications for the doxee. In our data analysis, **effects on mental health**, **social life**, **professional life**, **and political or societal attitudes** emerge as four overarching themes, which we present along with exemplar statements in Table 2.

First-order codes with exemplary statements	Categories	
• **Feeling paranoid** [6] *"I spent nearly four months constantly looking over my shoulder."* (I4) • **Anxiety** [4] *"I still have very bad anxiety and depressive episodes stemming from how close this incident came to ruining our lives financially and personally."* (I12) • **Distorted image of own guilt, reduced self-esteem** [3] *"It wasn't until [I started therapy] that I had this understanding, like, this isn't normal and this shouldn't happen to people."* (I2) • **Suicidal thoughts, self-harm** [3] *"My spouse and I both came very close to committing suicide multiple times during the 2-month peak of this incident."* (I12) • **Depression** [2]	Doxing deteriorates mental health*	**Mental health**
• **Damaged reputation** [3] • **Loss of personal (online) history** [2] *"I even messaged an admin at a sports fan message board to delete my account there, which I had been posting on since 2004 - another 13 years of internet life gone."* (I10)	Doxing affects social self (i.e., self perceived by others)	**Social**
• **Unwilling to trust others** [4] • **Withdrawal from friendships, uncomfortable around others** [2] • **Withdrawal from friendships online** [2] *"I got a lot of enjoyment and friendship from Reddit, […] but I just don't feel comfortable there anymore."* (I6) • **Feeling dismissed by social networks** [1] *"You're constantly dismissed, that no one is going to come hurt you. 'Oh, they're just saying that.' Well, I don't know. They got me fired, I lost my pension, I lost my entire life. […] How do I know?"* (I2)	Doxing challenges social relationships*	
• **Unemployment, loss of career** [2] *"I found a new job, but I had a career."* (I2) • **Bankruptcy** [1] • **Loss of job benefits (e.g., insurance for therapy)** [1] • **Growth of own business** [1] *"My shooting range after my relocation had many donations by 2nd Amendment support groups, and I got hundreds of new members."* (I1)	Doxing impacts career, and with it, financial resources*	**Professional**
• **Negative effect on hireability** [3] *"Kiwi Farms was among the top results when you googled my name. I wonder how many editors at writing jobs I applied for found my thread after my application."* (I10)	Doxing impairs hireability	
• **No support by employer** [3] *"The student was class President with a vast network […]. He never got punished."* (I11) *"The next morning, our newspaper did a story saying I was fired, and that's how I found out I was fired."* (I2)	Doxing concerns employer	
• **Doxers' activity affects what opinions the doxee expresses publicly** [1] *"I limited what thoughts I put out publicly as well. If I knew a particular tweet would draw attention, I would often forgo posting it. No other force in the history of my life has restricted my free speech as much as Kiwi Farms did.*" (I10) • **Downsizing of the political group (loss of members, lockdown on projects)** [1] • **Fewer open discussions within the political group due to loss of trust** [1]	Doxing inhibits political activism	**Political / Societal**
• **Radicalization towards opposing groups** [1] *"I started hating anti-gun assholes even more."* (I1) • **Radicalization toward police and law enforcement** [1] *"This incident also helped to radicalize me in terms of distrust of police and law enforcement in my country. I no longer believe there is a reason for police officers as they exist now to exist in our society, as they offered me no help whatsoever." (I12)*	Doxing exacerbates radicalization	

Table 2. Data structure diagram for consequences of the doxing incident. The numbers in [brackets] denote the number of subjects that the respective code applies to.
**The first-order codes of this category are selected examples; additional first-order codes not listed here for space reasons are similar in character to the ones displayed.*

4.3 How do doxees respond to, and cope with being doxed? (RQ3)

We address our third research question by examining how doxees respond to, and ultimately cope with, a doxing incident. In Table 3, we present our analysis of doxees' statements through Roth and Cohen (1986)'s lens of **approach** and **avoidance** as mechanisms for coping with stress. We thereby code coping mechanisms that imply orientation towards the doxing threat, taking self-responsibility, seeking knowledge, or careful appraisal and planning as an approach. Mechanisms that indicate orientation away from the doxer, avoidance of anxiety-arousing stimuli, detachment from the incident, or submitting oneself to severe behavioral constrictions are coded as avoidance. In between, we place doxees' adoption of privacy measures that, on the one hand, aim at avoiding future doxing stimuli, but on the other hand, indicate a careful appraisal and planning of their strategy to withstand the doxers' attacks.

First-order codes with exemplary statements	Categories	
• **Report doxing incident to online platform, police, or authorities** [7] *"I reported most posts to the respective sites they happened on, but not much was done."* (I9) • **Speak up against doxer in online threads** [2] • **Take doxer to court, try to change the law** [1] *"We did take him to court. Just in dealing with this guy since February, I've spent $28,000. [..] I'm also working with a local senator, to try and change the laws here in [state] about doxing."* (I14)	Confronting the doxer	**Approach**
• **Speak up more strongly about issues that were the motive for doxing** [1]	Speak up for own issues	
• **Keep weapons close at hand, purchase firearm** [4] • **Keep an eye on doxing thread, or have friends monitor it** [2] *"I would routinely check my Kiwi Farms thread. At first, I used the excuse that I needed to monitor the site for dangerous threats. Later, I realized it had become a bit of an addiction. Now I still have a friend who keeps track of it in case I get doxed again."* (I10)	Being vigilant, ready to defend oneself	
• **Start psychotherapy** [3] • **Research about doxing** [2]	Actively dealing with incident	
• **Spread awareness and information about doxing** [5] • **Exchange with and support other doxees** [3]	Supporting others	
• **Rebuild online presence after doxing incident** [2] *"Slowly, I began to take social media accounts off of their private settings and got back to work creating more content to help bury the Craigslist ads."* (I4)	Rebuilding own online presence	
• **Change phone number, use burner number for casual contacts** [3] • **Add spam blocker to phone** [1] • **Use a mail-forwarding service** [2] • **Cut contact with people who are less privacy-aware** [1] • **Dismantle devices to remove cameras and microphones** [1]	Taking physical privacy protection measures	▲
• **Disentangle online presence from identity, use anonymous accounts** [5] *"I constantly use new aliases."* (I5) • **Set social media accounts on private** [5] • **Be selective regarding friend requests, distrustful towards strangers online** [5] • **Increase password hygiene** [4] • **Avoid posts that potentially reveal location** [3] *"Once I posted a selfie from my balcony and then worried someone might comb through Google satellite view to try to find the plants and fake grass in the background."* (I10) • **Use privacy-aware software (e.g., VPN or DuckDuckGo)** [3]	Taking online privacy protection measures*	▼
• **Avoid engaging in public discourse online** [7] *"I no longer publicly advocate for things that are important to me online."* (I12)		

• **Avoid engaging in public discourse in person, avoid rallies** [3] *"I haven't been attending protests and public events since the attack. My face is easily findable from a google search of my name, and while there aren't many fascists in this country, the ones who are here are violent."* (I3) • **Give up on voting due to voter registry** [2]	Withdrawing own voice from society (online and offline)	**Avoidance**
• **Move to echo chambers** [1] *"I have moved to more closed communities and, unfortunately, echo chambers. I avoid discussing discourse online unless I know most people will agree with me."* (I9)	Move to echo chambers	
• **Relocate home** [5] • **Avoid outdoor spaces** [2]	Withdrawing from physical space	
• **Search and cleanse one's own online presence** [6] *"I scrubbed what I could from the internet."* (I2) • **Delete social media accounts** [6] • **Stop posting on social media, cease interacting with one's own community** [3] • **Stop using online services (e.g., banking, shopping)** [2]	Withdrawing from cyberspace	
• **Endure doxing incident** [2] *"As a woman, we do what we have to do, we suck it up. So, when you say coping with it. I'm enduring it."* (I14)	Developing numbness towards doxing incident	

Table 3. Data structure diagram of doxees' coping mechanisms. The numbers in [brackets] denote the number of subjects that the respective code applies to.
**The first-order codes of this category are selected examples; additional first-order codes not listed here for space reasons are similar in character to the ones displayed.*

5 Discussion

In this study, we have examined the effects of doxing on both its victims and our society. Our analysis reveals how doxing drives victims into a spiral of isolation and injustice across physical and cyber space. While our exploration shows that some doxees tend to cope by *approaching* a doxing incident with respect to speaking up for their rights, defending themselves, and seeking emotional support, we find that most doxees seek *avoidance* when it comes to engaging in their communities' public discourse or advocating for issues they care about. This has troubling implications for a democratic society that aims to give fair and equal voices to a broad range of opinions.

In Table 4, we present propositions that emerge from our data. By providing insight into this understudied form of adversarial online behavior, our work suggests several directions for IS research.

	Propositions derived from our data	**Research directions and implications for practice**
Doxing Types	1. Motives for doxing are either person-based or issue-based.	How do person-based and issue-based doxing differ? Regarding how doxees respond to the incident? How bystanders perceive the doxee?
	2. Doxing can occur in the form of campaigns which are either leaderless, or coordinated by an initiator. The initiator might operate in the background to make it seem like a leaderless, organically grown movement.	How can we analyze if a doxing campaign is coordinated or organically grown? How do the two forms differ regarding the evolvement of posts, contributors, timeline, and impact on the doxee?
	3. Doxing is not uncommonly committed by minors toward adults.	How does our understanding of doxing need to change if we consider minors as perpetrators? How can interdisciplinary research help us examine this phenomenon?
	4. Employers, online platforms, and authorities are mostly unfit to deal with doxing and hence amplify the doxing incident's negative effects.	How can we equip employers and authorities to support doxees when they need it? What are examples of best practices, despite an insufficient status of the law?

Doxing Effects and Remediation	5. Doxing is followed by physical and cyber harassment that spills over to family members, friends, colleagues, or name sharers. This causes extreme emotions and fears that translate from cyber into physical space, and severely affects mental health.	How does a doxee's specific emotional response towards a doxing incident influence if they employ approach or avoid strategies? How does doxing affect collateral victims and their behavior?
	6. Doxing harms the doxee's social relationships, careers, and hireability resulting in a severe loss of financial resources and a spiral of injustice.	How does doxing affect how individuals are perceived by hiring managers?
Doxing and Social Impact	7. Doxing causes doxees to take drastic privacy protection measures (e.g., deleting social media accounts or refraining from voting). This leads to them withdrawing their voice from both physical and cyberspace, hence becoming invisible to the public.	Which situational or personal factors influence a doxee's choice to speak up versus withdrawing their voice from the public discourse? How can we design online platforms that allow for users' participative safety? What privacy measures are effective against doxing?
	8. Doxing impedes political activism by obstructing trust and open discussions in political groups.	How do members of a doxed group interact with each other after an incident? What are collaboration strategies that make it harder to dox internal information?
	9. Doxing makes people move to echo chambers, radicalizes them towards opponent groups and authorities, and increases possession of weapons.	How do offline politics impact doxing? Does the effect of radicalizing polarizing leaders on online polarization diminish over time?

Table 4. Propositions and research agenda

Our research offers two main contributions to security and privacy literature in general and doxing in particular. First, drawing on real-world qualitative data, we propose novel issues and themes related to doxing that have not yet been investigated in IS research. Besides uncovering critical distinguishing characteristics of doxing incidents (propositions 1-3), our findings show that doxing, an adversarial online phenomenon, heavily impacts doxees physically, for example, by driving them off their jobs, homes or social relationships with little support from authorities, employers or online platforms (propositions 4-6). Furthermore, our study reveals a troubling impact of doxing on society. We uncover multifaceted dimensions in which doxing censors individuals' voices from the public discourse, for example, by causing them to withdraw their opinion from public discussions or move their exchange on closely-held issues to echo chambers, or by obstructing collaborative activism. This affects doxees' participation in both online and offline communities (propositions 7-9).

Second, we present directions for future research on doxing in both IS research and related fields. Our research agenda responds to the current status quo of doxees being left to deal with the implications of doxing themselves by suggesting research to examine (1) the underlying mechanisms of how doxing impacts doxees and their behavior and (2) effective remedies.

Finally, our study has important implications for social media providers and regulators, who should take measures to provide a cyberspace that allows for a participative and safe exchange of opinions, for example, through content moderation and reliable reporting functions. On a similar note, employers should adopt strategies to protect their employees who have been doxed.

We recognize limitations of our research, which provide opportunities for future work. For example, our qualitative data is limited to the doxees' point of view, while examining other stakeholders' perceptions (e.g., the doxer, the public, the doxee's family) might yield complementary findings. Furthermore, our dataset is almost exclusively U.S. American, whereas other cultural or political contexts might hold novel implications (Krasnova et al., 2012). We encourage future research to employ different data sources and lenses when digging deeper into doxing and remedial measures.

References

Anderson, B. and Wood, M. A. (2021). "Doxxing: A Scoping Review and Typology", *The Emerald International Handbook of Technology Facilitated Violence and Abuse*.

Chan, T. K., Cheung, C. M. and Lee, Z. W. (2021). "Cyberbullying on Social Networking Sites: A Literature Review and Future Research Directions", *Information & Management* 58 (2)**,** 103411.

Chen, Q., Chan, K. L. and Cheung, A. S. Y. (2018). "Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong", *International Journal of Environmental Research and Public Health* 15 (12)**,** 2665.

Cheung, A. (2021). "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon", (eds.) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, 577-594. Emerald Publishing Limited.

Cohen, F. and Lazarus, R. S. (1973). "Active Coping Processes, Coping Dispositions, and Recovery from Surgery", in: Lazarus, R. (eds.) *Fifty Years of the Research and Theory of R.S. Lazarus: An Analysis of Historical and Perennial Issues*: Lawrence Erlbaum Associates, Inc.

Collins, B. and Tenbarge, K. (2022). *Anti-Trans Stalkers at Kiwi Farms Are Chasing One Victim around the World. Their List of Targets Is Growing.* [Online] Available: https://www.nbcnews.com/tech/internet/cloudflare-kiwi-farms-keffals-anti-trans-rcna44834 (Accessed October 27 2022).

Cram, W. A., Proudfoot, J. G. and D'Arcy, J. (2021). "When Enough Is Enough: Investigating the Antecedents and Consequences of Information Security Fatigue", *Information Systems Journal* 31 (4)**,** 521-549.

Davison, R. M. and Martinsons, M. G. (2016). "Context Is King! Considering Particularism in Research Design and Reporting", *Journal of Information Technology* 31 (3)**,** 241-249.

Douglas, D. M. (2016). "Doxing: A Conceptual Analysis", *Ethics and Information Technology* 18 (3)**,** 199-210.

Eckert, S. and Metzger-Riftkin, J. (2020). "Doxxing", *The International Encyclopedia of Gender, Media, and Communication***,** 1-5.

Glaser, B. and Strauss, A. (1967). "The Discovery of Grounded Theory: Strategies for Qualitative Research".

Gregor, S. (2006). "The Nature of Theory in Information Systems", *MIS Quarterly***,** 611-642.

Jeong, S. (2019). *When the Internet Chases You from Your Home*. [Online] Available: https://www.nytimes.com/interactive/2019/08/15/opinion/gamergate-zoe-quinn.html (Accessed October 27 2022).

Kaplan, B. and Maxwell, J. A. (2005). "Qualitative Research Methods for Evaluating Computer Information Systems", (eds.) *Evaluating the Organizational Impact of Healthcare Information Systems*, 30-55. Springer.

Karahanna, E., Xu, S. X., Xu, Y. and Zhang, N. A. (2018). "The Needs–Affordances–Features Perspective for the Use of Social Media", *MIS Quarterly* 42 (3)**,** 737-756.

Krasnova, H., Veltri, N. F. and Günther, O. (2012). "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture", *Business & Information Systems Engineering* 4 (3)**,** 127-135.

Kuckartz, U. (2012). *Qualitative Inhaltsanalyse*: Beltz Juventa.

MacAllister, J. M. (2016). "The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information", *Fordham L. Rev.* 85**,** 2451.

Miller, S. M. (1980). "When Is a Little Information a Dangerous Thing? Coping with Stressful Events by Monitoring Versus Blunting", (eds.) *Coping and Health*, 145-169. Springer.

Mullen, B. and Suls, J. (1982). "The Effectiveness of Attention and Rejection as Coping Styles: A Meta-Analysis of Temporal Differences", *Journal of Psychosomatic Research* 26 (1)**,** 43-49.

Nhan, J., Huey, L. and Broll, R. (2017). "Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings", *The British Journal of Criminology* 57 (2)**,** 341-361.

O'Sullivan, D. and Naik, N. (2022). *Trans Activist Celebrates Rare Victory against Online Trolls after Kiwi Farms Deplatforming*. [Online] Available: https://www.cnn.com/2022/09/06/tech/kiwi-farms-clara-sorrenti-keffals/index.html (Accessed October 27 2022).

Romano, A. (2021). *What We Still Haven't Learned from Gamergate*. [Online] Available: https://www.vox.com/culture/2020/1/20/20808875/gamergate-lessons-cultural-impact-changes-harassment-laws (Accessed October 28 2022).

Roth, S. and Cohen, L. J. (1986). "Approach, Avoidance, and Coping with Stress", *American Psychologist* 41 (7)**,** 813.

Snyder, P., Doerfler, P., Kanich, C. and McCoy, D. (2017). "Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing", *Proceedings of the 2017 Internet Measurement Conference*,

Straub, D. W. and Welke, R. J. (1998). "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly***,** 441-469.

Trottier, D. (2020). "Denunciation and Doxing: Towards a Conceptual Model of Digital Vigilantism", *Global Crime* 21 (3-4)**,** 196-212.

Twitch. (2022). *Preventing Doxxing, Swatting and Other Irl Harm*. [Online] Available: https://safety.twitch.tv/s/article/Preventing-Doxxing-Swatting-and-other-IRL-Harm?language=en_US (Accessed October 27 2022).

Urquhart, C., Lehmann, H. and Myers, M. D. (2010). "Putting the 'Theory' Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems", *Information Systems Journal* 20 (4)**,** 357-381.

Yousef, O. (2022). *A Campaign Made It Harder to Access an Anti-Trans Website Linked to Multiple Suicides.* [Online] Available: https://www.npr.org/2022/09/12/1122482174/a-campaign-made-it-harder-to-access-an-anti-trans-website-linked-to-multiple-sui (Accessed October 27 2022).