# Understanding the Current State of Knowledge and Future Directions of Doxing Research: A Social Cognitive Theory Perspective

Yuan Fang
University of Queensland
yuan.fang2@uq.net.au

Marten Risius
University of Queensland
m.risius@business.uq.edu.au

Christy M.K. Cheung
Hong Kong Baptist University
ccheung@hkbu.edu.hk

## Abstract

*Doxing is the public release of personal information with harmful intentions. It is an emergent online practice that is used in social protest movements, for personal revenge, or even as a means of cyber-warfare. To amalgamate the ambiguous multi-disciplinary research, we summarize the current state of knowledge and identify directions for doxing research. To that end, this study applies social cognitive theory in a systematic review of 28 doxing papers and provides an overview of current doxing research trends. The review shows that doxing research has been primarily focused on the environmental perspective, particularly the legal regulation of doxing while neglecting personal and behavioral factors. We identify a series of research questions to guide and inspire future research on the role of digital technologies in this emerging issue.*

**Keywords:** doxing, doxxing, social cognitive theory, systematic literature review, research framework.

## 1. Introduction

Doxing has been defined as "*the intentional public release onto the internet of personal information about an individual by a third party, often with the intent to humiliate, threaten, intimidate, or punish the identified individual*" (Douglas, 2016, p. 199). Studies have shown that this deviant online behavior can have severe physical and mental consequences for its targets (Chen et al., 2018; Eckert & Metzger-Riftkin, 2020). In 2010, in one of the first reported doxing cases, a 10-year-old U.S. girl had her personal information disclosed online in response to her posting a video in which she alleged having been a victim of sexual assault by a popular musician (*Jessi Slaughter Cyberbulling Controversy*, 2010). The family was subjected to online and offline abuse, with their personal details, including postal address, email, and phone numbers, being made public. Ultimately, the girl's father died after a stress-induced heart attack, and the girl sought treatment for mental health issues.

Doxing has also emerged as a social protest movement strategy. During the 2019 Hong Kong protest movement, the Office of the Privacy Commissioner of Personal Data reported more than 4,000 doxing cases, 36% of which targeted members of the police force and their families (PCPD, 2020). The publication of the addresses of police officers allowed protesters to surround their houses and threaten their wives and children (CGTN, 2019; Thomas, 2019). In response, the High Court issued an interim injunction on doxing in October 2019 to ban protesters from posting the personal details of members of the police force and their families online (HKSAR, 2019). Similarly, when legislation was issued in the U.S. to protect state court judges in early 2022, some of the bills criminalized the doxing of judges or their families (Raftery, 2022). However, following the U.S. Supreme Court's overturning of *Roe v. Wade*, the judges voting to overturn the constitutional right to an abortion were doxed on TikTok. This led to an assassination plot against one of the judges (Roscoe, 2022).

Doxing is also used as a means of revenge. The *New York Post* recently reported on major purchases by civil rights activist Shaun King (including an $842,000 lakefront house) (Vincent, 2021). King claimed that his family suffered grave personal consequences from these reports (e.g., distressing visits from white supremacists) and retaliated by calling on his over six million social media followers to dox the journalists (Kerr, 2022). Doxing has even evolved into a cyber-warfare tactic in the Russian invasion of–Ukraine. Russian government officials have endorsed and supported a doxing operation called Underside, which targets Russian individuals and organizations that have been influenced by or associated with the U.K. government (ISD, 2022).

Doxing is a novel information technology (IT)-enabled behavior (Anderson & Wood, 2021). Online technologies facilitate the retrieval, publication, and spread of personal information. Accordingly, doxing occurs on various digital platforms, such as Facebook, Twitter, Telegram, Instagram, Forums, YouTube, and

URI: https://hdl.handle.net/10125/103306
978-0-9981331-6-4

newspaper websites (Chen et al., 2019; Demydova, 2021; Lee, 2020; McNealy, 2017).

Doxing differs from other abusive online behaviors, such as cyberbullying, online harassment, and cyberstalking (Bailey & Liliefeldt, 2021; Sari & Camadan, 2016), in that it is an online technology-mediated phenomenon that has no offline precedent. Doxing can support abusive online behaviors by de-anonymizing the victim and providing personally identifying information for subsequential harassment and attacks (Colton et al., 2017; Fish & Follis, 2016). Accordingly, our aim in this study is to direct the attention of Information Systems (IS) scholars to the role of digital technologies in doxing and how the practice relates to other phenomena, such as digital activism, cyberbullying, online harassment, and hacktivism.

The threatening consequences and unique technology-facilitated practice of doxing have attracted the attention from various researchers. However, these studies have confounded doxing with privacy violations (Anderson & Wood, 2021), online harassment (Cross, 2019), digital vigilantism (Trottier, 2019), cybercrime (McMahon et al., 2016), and hacktivism (Fish & Follis, 2016). Establishing conceptual clarity on what constitutes doxing and providing an understanding of the current state of knowledge about doxing appears necessary to consolidate and guide future research on this emergent issue. Accordingly, we seek to inform two research questions: (1) *What is the current state of the art of doxing research?* and (2) *What are the promising future directions for doxing research?*

To address these questions, we adopt social cognitive theory (SCT) (Bandura, 2009) as a framework to structure the current doxing literature into three determinants (i.e., personal factors, behavioral factors, and environmental factors) and outline a research agenda within this integrative framework. We find that the nascent doxing research has primarily adopted a descriptive environmental perspective that explores doxing detection techniques and the potential for legal regulation. However, how digital technologies facilitate doxing behaviors and how social media users interact with each other in doxing conduct are still unclear. There is a need for comparative studies that explore the roles of IT and social media affordances in doxing.

The remainder of this paper is structured as follows. Section 2 presents the conceptualization of doxing and the confounding tendencies in its definition. It also introduces the theoretical foundation of our framework for doxing research. Section 3 describes the literature collection and selection procedures. Sections 4 and 5 cover the status of doxing research and the gaps identified therein. Section 6 discusses future research directions and details the contributions and limitations of this study.

## 2. Background

### 2.1. Introducing doxing

Doxing (sometimes rendered as “doxxing”) is a neologism created from an altered spelling of “dropping docs” (with “docs” as an abbreviation for “documents”) (Garber, 2014). It was first observed in an act of publicly disclosing an internet user’s personal information in the 1990s on Usenet (Amanda, 2013). In addition to the investigation of doxing from the perspective of malicious behaviors (Colton et al., 2017; Fish & Follis, 2016), doxing has also been introduced as a form of digital vigilantism (Cheung, 2021; Huang, 2021; Trottier, 2019). People tend to resort to doxing when the authorities are seen as failing to uphold justice. Consequently, people use doxing to take justice into their own hands (Trottier, 2019) with strongly personalized motivations (Douglas, 2016). In the form of vigilantism, doxing can be the private enforcement of public law with personalized motivation (Douglas, 2016). However, when doxing becomes seen as a vigilante approach, there can be a lack of clarity in the terms and rules.

Douglas (2016) examined the nature and forms of doxing and defined it as the intentional disclosure of other people’s private information, often with malicious intent. However, this definition appears overly broad, as it covers almost any information disclosure behavior. For example, amber alerts publish detailed personal information online about suspects, and police publish notices to locate and arrest wanted persons, yet people do not regard these as acts of doxing or violations of the subject’s right to privacy (Blake & Hereth, 2020).

Moreover, the prevailing definitions sometimes overlap with other malicious online behaviors, such as trolling (Morch et al., 2018), swatting (Jaffe, 2016), defamation (Solo, 2021), and other privacy violations (e.g., privacy breaches and de-anonymization). Therefore, in this study, we distinguish the doxing phenomenon and refine the definition of doxing by highlighting its fundamental characteristics: *doxing is the public online release or dissemination of a target’s private information without consent or legal authorization that intends to cause harm to the target and emanates online without offline precedent.*

## 2.2. Social cognitive theory

We apply SCT to better understand how doxing has been investigated in the literature. SCT describes individual behavior as the product of reciprocal interactions between (personal) cognitive determinants, environmental influences, and behavioral factors (see Figure 1) (Bandura, 2009). Personal factors refer to the cognitive, affective, and biological events of an individual; environmental factors describe the external social events and facts, such as social norms, access to resources, and influence on others; and behavioral factors include practice and the person's self-efficacy (i.e., perceived capacity and skills to engage in the behavior).

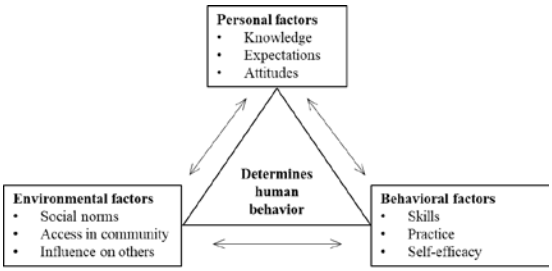


**Figure 1. Social cognitive theory (Bandura, 2009)**

SCT has been applied successfully to conceptualize the impact of the digital environment on various online behaviors, such as cybersecurity (Maalem Lahcen et al., 2020), cyberbullying (Chan et al., 2021), and internet addiction (Yang, 2020). Doxing is a complex phenomenon. During the 2019 Hong Kong social movement, a police officer was doxed for shooting a protester, having his personal information spread on Twitter with trending hashtags to get attention (PCPD, 2020). The personal information was also posted on other social media platforms, such as Telegram and Forums, on which the doxers applied legitimization strategies to justify their behaviors (Lee, 2020). In this case, the conflict between protesters and the police was the personal factor that initiated the doxing; the digital environment (i.e., Twitter, Telegram, and Forum) facilitated the information exposure; and the linguistic strategies were the behavioral factors that contributed to the doxing. The risks associated with doxing are decreased by it taking place in the digital IT environment, which is characterized by a lack of social censure and physical connection; in this environment, users' behaviors highly depend on their self-regulation, which is a personal (cognitive) factor of doxing behavior (Bussey et al., 2015). Therefore, understanding the role of humans (personal factor) and the digital IT environment (environmental factor) is important for understanding doxing behavior and forms the basis for our categorization framework and coding scheme.

# 3. Methodology

## 3.1. Literature collection and selection

The literature review was conducted through a systematic and transparent process according to the guidelines of Webster and Watson (2002). Figure 2 describes the detailed approach to the literature collection and selection processes.

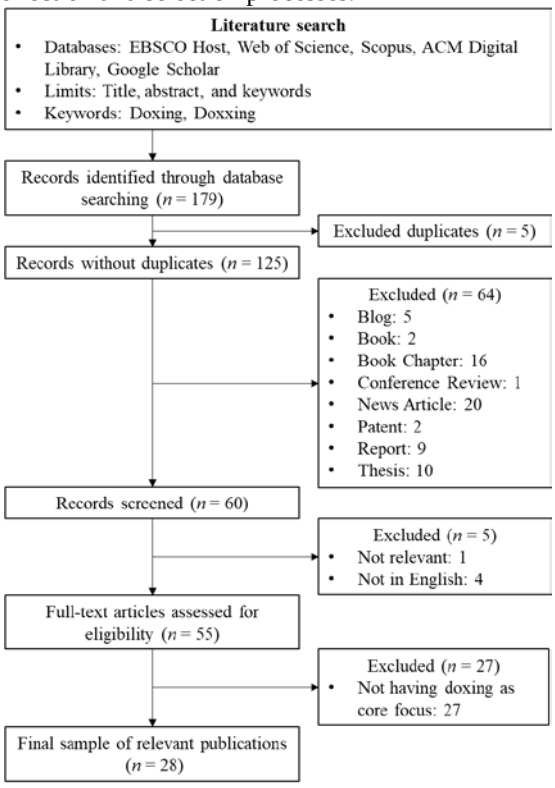


**Figure 2. Literature selection procedures**

We performed literature searches to identify academic papers that had doxing as their core focus. Thus, we selected "doxing" and "doxxing" as the two keywords. The systematic literature searches were conducted on May 12, 2022, in the electronic databases EBSCO Host, Web of Science, Scopus, ACM Digital Library, and Google Scholar. The titles, abstracts, and keywords were searched to ensure that doxing was the main focus of the studies. Publications across all time periods were included. Table 1 shows the search results from each database. The initial literature search returned 179 papers.

With initial search results, we applied following inclusion and exclusion criteria to refine our sample. The criteria aimed to ensure the quality and relevancy

of the studies and helped us to maintain a focus on doxing. The inclusion criteria were (1) papers that were published in peer-reviewed journals and conferences and (2) papers that targeted doxing as a core focus. The exclusion criteria were (1) papers that briefly mentioned doxing in a certain context, (2) papers that were published in languages other than English, and (3) papers that were published as other document types (e.g., book chapters, theses, and reports). We arrived at a final sample of 28 papers and conducted a qualitative content analysis to investigate the state of doxing studies.

**Table 1. Search results from databases**

| Database | Doxing | Doxxing | Total |
|---|---|---|---|
| EBSCO Host | 8 | 20 | **28** |
| Web of Science | 26 | 8 | **34** |
| Scopus | 39 | 12 | **51** |
| ACM Digital Library | 1 | 2 | **3** |
| Google Scholar | 53 | 10 | **63** |
| Total | 127 | 52 | **179** |

## 3.2. Coding approach

Drawing on SCT (Bandura, 2009), we developed a categorization framework and coding scheme to assess the state of knowledge in doxing research. The coding scheme was repeatedly discussed among the authors and aligned with the theoretical background through two iterations to remove discrepancies and ambiguity and to guarantee validity. The final coding scheme (see Table 2) was devised to deliver a descriptive and objective evaluation of each study. We coded each paper under different categories according to its core discussion points and contribution to doxing literature, as introduced in the research questions, abstract, and subtitles.

## 4. Current research trends

Since the first peer-reviewed publication by Khanna et al. (2016) on how digital platforms and software facilitate doxing, the body of academic research on doxing has grown steadily (Anderson & Wood, 2021). In the past seven years, the number of annual publications has stabilized at around 3 and peaked at 7 in 2018 (see Figure 3).

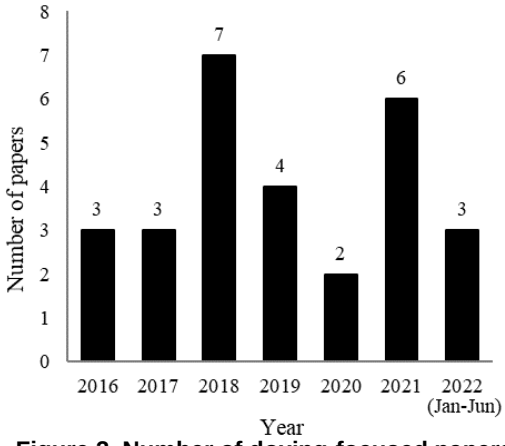


**Figure 3. Number of doxing-focused papers published per year**

Doxing is seen as one of the three major emergent problems of the digital age, alongside defamation and impersonation (Solo, 2021). Accordingly, our findings show that research on doxing has been published in multiple disciplines, of which law has contributed the

**Table 2. Literature coding scheme based on social cognitive theory (SCT)**

| SCT construct | Factor | Definition | Description in the doxing context |
|---|---|---|---|
| **Personal factors** | Knowledge | Learning occurs by observing a behavior and observing the consequences of putting those behaviors into action | The observation of doxing behaviors and the experience of exposure to doxing information |
| | Expectation | Anticipated outcomes of one's behavior | Motivations for doxing |
| | Attitude | The way of thinking or feeling about something | Attitude toward doxing (e.g., whether doxing is permissible or appropriate) |
| | Additional | N/A | Demographic characteristics (e.g., age and gender) |
| **Environmental factors** | Social norms | Rules based on socially shared beliefs on how one ought to behave | Ethical issues of doxing; legal regulation on doxing |
| | Access in community | The ability and right to approach or communicate | Digital technologies that facilitate or counter doxing |
| | Influence on others | The impact of behavior outcomes on the environment | Harm and consequences of doxing |
| **Behavioral factors** | Skill | The ability to use one's knowledge in conducting certain behavior | Doxing tactics and strategies; reactions to doxing |
| | Practice | To perform repeatedly to become proficient | N/A |
| | Self-efficacy | The belief in one's own capacity to conduct certain behavior | N/A |

most studies (39%), followed by the social sciences (21%) and computer science (11%) (see Table 3).

Articles from various disciplines have concentrated on different aspects of doxing. The law publications have been fully focused on contributing to doxing laws and regulations. They have discussed current regulations on doxing (Crompton, 2018; Mery, 2020), called for further regulation on doxing on social media (Yudiana et al., 2022), and provided recommendations and proposals on doxing regulation from various perspectives (Amiruddin et al., 2021; Bei Li, 2018; Calabro, 2018; Corbridge, 2018; Lindvall, 2019; MacAllister, 2016; McIntyre, 2016; Styple, 2021). Different doxing cases have also been reviewed and discussed in the above law papers. Publications in computer science have concentrated on the digital technologies that facilitate doxing. These papers have proposed designs to detect doxing on social media platforms (Karimi et al., 2022; Snyder et al., 2017) and analyzed internet technologies and software used for doxing (Khanna et al., 2016). In comparison, publications in social sciences and other disciplines have covered diverse topics. For instance, a social science publication studied the intertextual strategies of doxing (Lee, 2020), a political science publication conceptualized doxing as a political tool to interfere with an election (Hansen & Lim, 2019), a public health publication discussed the mental harm caused by doxing (Chen et al., 2018), and a philosopher presented an argument on the nature of doxing in the context of revealing racists (Barry, 2021).

**Table 3. Disciplines of doxing-focused papers**

| Discipline | Number of papers |
|---|---|
| Communication | 2 |
| Computer Science | 3 |
| Ethics | 2 |
| Law | 11 |
| Philosophy | 1 |
| Political Science | 1 |
| Public Health | 2 |
| Social Sciences | 6 |

Table 4 shows the methodological approaches taken in the reviewed publications. Our findings show that outside of the notable number of law reviews, there have been few conceptual papers and case studies. The amount of quantitative research (using experiments, interviews, and surveys) on the doxing phenomenon is particularly limited, and theory-driven empirical studies on doxing are generally scarce.

Overall, while the significant number of law reviews proposing regulation on doxing seem to have set a tone for the understanding of the phenomenon, there remain certain situations in which doxing has not been fully explored. This vagueness in the understanding of doxing may result from doxing research being in its infancy and from the complexity of the phenomenon itself. To support more scholars in joining these efforts, we develop a framework that depicts the current state of doxing literature and suggests promising avenues for future research.

**Table 4. Methodologies of doxing-focused papers**

| Methodology | Number of papers |
|---|---|
| Case study | 4 |
| Conceptual | 5 |
| Design science | 2 |
| Experiment | 1 |
| Interview | 1 |
| Law review | 13 |
| Survey | 2 |

## 5. The current state of knowledge

SCT is our guiding framework to analyze the identified doxing literature. We adapted the theory to the doxing context to systematically understand different doxing-related factors. As the factors are not mutually exclusive, any given paper can address multiple factors of doxing and thus be categorized into more than one factor. Table 5 shows the result of our analysis of the current state of doxing research.

### 5.1. Personal factors

The results of our literature review show that doxing studies have focused on multiple personal factors, from demographic information to the motivations for doxing. These personal factors reflect the characteristics of individuals involved in doxing, who can be further classified as doxers and victims. Douglas (2016) conceptualized doxing from the perspective of the doxer's motivation and categorized doxing into deanonymizing, targeting, and delegitimizing forms. Some studies have investigated doxing from both sides. For example, two studies have highlighted the demographic characteristics of people who had performed or suffered from doxing, especially the gender difference between doxers and doxing targets (Chen et al., 2019; Eckert & Metzger-Riftkin, 2020). Both studies observed that males were more likely to engage in hostile doxing and females were more likely to be doxed. As the effect on doxing victims might form part of a doxer's motivation, the characteristics of the doxer and doxing target have a joint effect in determining doxing behaviors.

**Table 5. Overview of doxing research**

| Factor | Studies |
|---|---|

| Personal factors (10.7% of studies) | |
|---|---|
| Gender | Doxing as gendered harassment: females are more likely to be doxing targets (Eckert & Metzger-Riftkin, 2020) |
| Intention | Doxing to fulfill social needs and doxing to harass or attack targets the doxer dislikes (Chen et al., 2019) |
| Motivation | Three types of doxing motivation: deanonymizing, targeting, and delegitimizing (Douglas, 2016) |
| **Environmental factors (89.2% of studies)** | |
| Ethics | Revealing the identity of an anonymous poster violates the public media's ethical duty to protect the poster's privacy (McNealy, 2017) |
| | Circumstances making doxing ethically permissible: doxing racists (Barry, 2021), revealing wrongdoings in the public interest (Douglas, 2016) |
| Doxing context | Doxing as a tool of online activism: doxing in opposition to authoritarian legislation (Demydova, 2021) or as a negative byproduct of deliberative digital democracy (Buozis, 2019) |
| | Doxing of target groups: gendered online abuse that targets women, minorities (Eckert & Metzger-Riftkin, 2020), and white supremacists (Carriere et al., 2018) |
| | Doxing as a political tool to delegitimize a candidate (Hansen & Lim, 2019) |
| Law and regulation | Critical assessments of current regulation: analyzing the limitations of current statutes (Amiruddin et al., 2021; Lindvall, 2019; MacAllister, 2016) |
| | Application of current legislation: appeal to regulate doxing from the victim's rights to privacy (Bei Li, 2018; Calabro, 2018; Corbridge, 2018) or the "right to be forgotten" (Pittman, 2018; Yudiana et al., 2022), as a form of cyber-harassment (Mery, 2020), and the intentional infliction of emotional distress (McIntyre, 2016) |
| | Develop novel forms of regulation: proposing to allocate regulatory responsibilities to organizations for institutional doxing (Styple, 2021) and to expend additional social resources for regulation (Crompton, 2018) |
| Technology | Proposing doxing detection methods based on string-matching and encoded heuristics (Karimi et al., 2022; Snyder et al., 2017) |
| | Analyzing digital software (Maltego) that gathers information from open sources and thus facilitates doxing (Khanna et al., 2016) |
| Harm | A framework to conceptualize the harm of doxing in terms of the virtualization of violence (Anderson & Wood, 2021) |
| | Emotional issues (e.g., fear, anxiety, and depression) caused by doxing (Chen et al., 2018; Eckert & Metzger-Riftkin, 2020) |
| **Behavioral factors (10.7% of studies)** | |
| Skills | Intertextual legitimation strategies (e.g., rationalization, redefinition, construction of negative other, and victimizing) and linguistics (e.g., dehumanization and irony) of doxing (Lee, 2020) |
| Practice | The high emotional intensity (i.e., use of shaming and offensive language) in doxing messages (Carriere et al., 2018) |
| Victim's reaction | Target's reactions after doxing: trying to solve the problem, asking for help, and closing social media accounts (Eckert & Metzger-Riftkin, 2020) |

## 5.2. Environmental factors

The majority of doxing papers have examined the environmental factors of doxing (89.2%). The environmental factors considered in the reviewed literature range from doxing ethics to regulation and the effect of doxing on others (i.e., the harms of doxing). Within this segment of the literature, 46.4% of the papers have concentrated on proposing doxing regulation. They have affirmed the negative connotations associated with doxing (Beaujon, 2014) and the scarcity of legal regulation of doxing (Anderson & Wood, 2021). Law reviews have situated the protection of victims in terms of their "right to be forgotten" (Yudiana et al., 2022) and right to privacy (Bei Li, 2018; Calabro, 2018; Corbridge, 2018; Pittman, 2018). In the literature on punishing doxers, scholars have introduced the concepts of privatizing attribution to hold organizations liable for institutional doxing (Styple, 2021) and regulating doxers who inflict emotional distress (McIntyre, 2016).

Doxing cases are often related to social events, and doxing has also been investigated in various social contexts, such as online activism against authoritarian legislation (Demydova, 2021), white supremacism (Carriere et al., 2018; Demydova, 2021), political cybervoting interference to delegitimize candidates (Hansen & Lim, 2019), and deliberative digital democracy (Buozis, 2019). These diverse social contexts highlight the complex nature of doxing.

In addition to the environmental social norms of doxing behavior, a few scholars have studied the digital information technologies and channels that affect the accessibility of doxing information. Common social media platforms, search engines, and browser extensions can be used to facilitate doxing (Khanna et al., 2016). For instance, Maltego has been used to scan and collect open-source information and visualize links between people. Similarly, YouTube has been used to spread doxing information and violate personal privacy (Demydova, 2021). Although IT applications have facilitated doxing and had a

negative influence, they also have the potential to constrain doxing. Karimi et al. (2022) and Snyder et al. (2017) proposed doxing detection methods on Twitter, 4chan.org, and pastebin.com that can identify doxing information from available online information. However, further studies are needed to test the practicality of these detection methods.

Moreover, three studies have examined the harmful effect and consequences of doxing for its targets (victims). Anderson and Wood (2021) developed a framework to conceptualize the harm of doxing by distinguishing first-order harms (to bodily integrity) and second-order harms (to security interests). The other two studies focused on the emotional effects caused by doxing, such as depression, anxiety, stress, and fear (Chen et al., 2018; Eckert & Metzger-Riftkin, 2020). In addition, doxing victimization has led to physical and financial damage, such as returning unwanted items ordered by pranksters, losing jobs, and shutting down personal businesses. A better understanding of the harm of doxing and the effects experienced by victims can also provide insight into the development of legal regulations for doxing.

### 5.3. Behavioral factors

In terms of behavioral factors, victims show different reactions in response to doxing. Snyder et al. (2017) found that doxing victims were very likely to close their social media accounts or set them to private access, and Eckert and Metzger-Riftkin (2020) observed that victims stopped engaging in certain topics online and used fake names and profiles.

Two studies have contributed to the current understanding of doxing conduct. One of these investigated doxing as a group behavior in the context of the 2019 Hong Kong social movement, adopting the critical discourse analysis approach to study doxing-related messages from a Hong Kong-based forum and analyze the intertextual discourse strategies of doxing (Lee, 2020). Lee identified four legitimation strategies of doxing: rationalization (explaining why doxing is morally right and effective), redefinition (redefining doxing to make it morally acceptable), construction of a negative other (attributing a negative moral evaluation to the doxing target), and victimizing (claiming the doxers as victims and seeking solidarity), and also specified several doxing linguistic tactics, such as dehumanization, euphemism, and irony. In this particular social movement context, doxing appears to have been mostly an emotional reaction. The findings on strong emotional intensity were replicated in a Twitter sentiment analysis on a social protest event that triggered group doxing behaviors (Carriere et al., 2018). However, this study defined doxing as shaming-oriented outrage behavior that discloses personally identifiable information, which might have biased the results. Again, this implies the importance of having an integrated understanding of doxing for future research, specifically regarding the use of terms and the selection of data (i.e., whether the studied behaviors or collected data are actually doxing).

## 6. Discussion

### 6.1. Future research directions

The analysis of the current state of knowledge of the doxing literature presented in the above sections shows that the understanding of doxing is still emerging across multiple disciplines. In this section, we propose a number of promising research questions for future studies (see Table 6). The research questions are guided by the SCT framework.

**Table 6. Proposed future research questions**

| |
|---|
| **Personal factors** |
| How do personality factors affect doxers' engagement in doxing? |
| How do personality factors affect how victims cope with doxing? |
| How does doxers' experience of exposure to doxing information affect their doxing conduct? |
| How does victims' experience of exposure to doxing information affect their reaction to doxing? |
| **Environmental factors** |
| What is the role of social media in facilitating/ sanctioning doxing? |
| How can platform design features help prevent or interfere with doxing? |
| How do online social groups affect doxers' engagement in doxing? |
| How do online social groups help victims to cope with the effects of doxing? |
| **Behavioral factors** |
| What are the structural behaviors involved in doxing? |
| What strategies and tactics have been used in doxing behaviors? |
| What is the role of technical and interpersonal skills in supporting doxing? |
| **Personal and environmental factors** |
| What are the motivations for doxing in different social contexts? |
| What are the effects and consequences of doxing criminals/racists/wrongdoers? |
| Who should be responsible for the consequences of doxing wrongdoers in the public interest? |
| **Personal and behavioral factors** |
| What distinguishes doxing behaviors that target individuals and groups/institutions? |
| How do individual doxers and group doxers conduct the behavior, and what are the differences? |

| |
|---|
| What are the psychological mechanisms driving doxing behaviors? |
| How do doxers' expectations of the loss of victims affect doxing behaviors? |
| **Environmental and behavioral factors** |
| How do doxing behaviors differ between digital activist movements? |
| How do doxing behaviors differ between digital platforms? |
| How do doxers respond to regulatory interventions? |
| How does information privacy literacy influence doxing? |
| How do social media affordances influence doxers to engage in doxing? |
| How does platform features influence doxers to engage in doxing? |
| How do doxers use social media features to encourage others to join in doxing? |
| **Personal, environmental, and behavioral factors** |
| How does the interaction between IT users and technologies shape doxing behaviors? |

### 6.2. Theoretical and practical contributions

Recognizing digital technologies as the fundamental element of doxing, we introduce this emerging phenomenon to the IS discipline. Firstly, we define doxing more precisely by distinguishing it from other online abusive behaviors (e.g., Chan et al., 2022; Chan et al., 2019; Li et al., 2022), addressed by IS research. This can reduce the conceptual ambiguity of doxing and help researchers to investigate doxing behaviors more effectively.

Drawing on SCT, we integrate the current doxing literature into a systematic framework and identify research gaps and promising avenues for future research. As a technology-mediated phenomenon, doxing involves doxers' communicative action and the support of IT features. However, we find that the role of social media and digital affordance in facilitating and countering doxing is still underexplored. IS researchers could enrich the literature by investigating the role of technology in influencing, facilitating, and preventing doxing behaviors.

Finally, this review provides insights for governmental regulation and digital platform providers pursuing active intervention on doxing. In line with the current legal regulation on doxing, studies have shown that the legal approach to doxing cases still uses the frames of online harassment and violations of privacy. In addition, digital platform providers could benefit from doxing detection methods that restrict the spread of doxing information by identifying instances of doxing from the massive amounts of information online. The integrative definition developed in this review has the potential to advance the juristic approach to pursuing a standalone legal definition for doxing and the technical approach to identifying doxing from the many different online malicious behaviors.

### 6.3. Limitations

A few limitations of this study should be considered when interpreting the findings. First, the sample is relatively limited as doxing is an emerging topic. To pursue an integrative and independent understanding of doxing, we included only studies that explicitly examine doxing as a core phenomenon. Second, some studies have investigated similar phenomena using alternative terms, such as human flesh search (Wang et al., 2010), de-anonymization (Qian et al., 2017), and outing (Elwood, 1992). As the definitions of those terms could have a slightly different scope, future studies could explore the similarities and differences between doxing and these other terms. Third, the related literature (e.g., in information security) might offer valuable insights into components, particularly digital technologies, associated with doxing. Literature reviews with an expanded focus might offer additional insights.

## 7. Conclusion

Overall, we answer the two research questions by drawing upon SCT (Bandura, 2009) to structure the current knowledge of doxing. Our review of the doxing literature shows that doxing is a complex phenomenon that is influenced by various social and environmental factors. The current diversity of studies investigating doxing through personal factors and multiple social contexts demonstrates the fragmentation of doxing research. A systematic and integrated investigation of doxing behavior is needed. Understanding how the interaction between humans and IT shapes the doxing landscape could contribute to the implementation of future detection methods and the regulation of doxing behavior.

## 8. Acknowledgement


- Marten Risius is the recipient of an Australian Research Council Australian Discovery Early Career Award (project number DE220101597) funded by the Australian Government.
- This work was also supported by a fellowship award from the Research Grants Council of the Hong Kong Special Administrative Region, China [HKBU SRFS2021-2H03].

## 9. References


Amanda. (2013). *Doxxing*. https://knowyourmeme.com/memes/doxxing

Amiruddin, N., Manaf, A. A., & Adam, Y. C. (2021). TROLLING AND DOXING: PROPOSAL FOR A LAW FOR MALAYSIA. *E-BOOK OF EXTENDED ABSTRACT*, 18.

Anderson, B., & Wood, M. A. (2021). Doxxing: A Scoping Review and Typology. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse* (pp. 205-226).

Anderson, B., & Wood, M. A. (2021). Harm imbrication and virtualised violence: Reconceptualising the harms of doxxing. *International Journal for Crime, Justice and Social Democracy*, *11*(1), 196-209.

Bailey, J., & Liliefeldt, R. (2021). Calling All Stakeholders: An Intersectoral Dialogue about Collaborating to End Tech-Facilitated Violence and Abuse. In *The Emerald International Handbook of Technology Facilitated Violence and Abuse* (pp. 769-786).

Bandura, A. (2009). Social cognitive theory of mass communication. In *Media effects* (pp. 110-140). Routledge.

Barry, P. B. (2021). Doxing Racists. *The Journal of Value Inquiry*, *55*(3), 457-474.

Beaujon, A. (2014). *Redditors furious Newsweek 'doxxed' Bitcoin founder*. https://www.poynter.org/reporting-editing/2014/redditors-furious-newsweek-outed-bitcoin-founder/

Bei Li, L. (2018). Data privacy in the cyber age: Recommendations for regulating doxing and swatting. *Fed. Comm. LJ*, *70*, 317.

Blake, M., & Hereth, B. (2020). Sanctuary Cities and Non-Refoulement. *Ethical Theory and Moral Practice*, *23*(2), 457-474.

Buozis, M. (2019). Doxing or deliberative democracy? Evidence and digital affordances in the Serial subReddit. *Convergence*, *25*(3), 357-373.

Bussey, K., Fitzpatrick, S., & Raman, A. (2015). The Role of Moral Disengagement and Self-Efficacy in Cyberbullying. *Journal of School Violence*, *14*(1), 30-46.

Calabro, S. (2018). From the message board to the front door: Addressing the offline consequences of race-and gender-based doxxing and swatting. *Suffolk UL Rev.*, *51*, 55.

Carriere, T., Walker, K., & Legocki, K. (2018). Doxxing to Deter: Citizen Activism on Social Media.

CGTN. (2019). *How is it for Hong Kong police and their families?* https://news.cgtn.com/news/2019-12-02/How-is-it-to-be-Hong-Kong-police-and-their-families--M4oHkYleMg/index.html

Chan, T. K., Cheung, C. M., & Lee, Z. W. (2021). Cyberbullying on social networking sites: A literature review and future research directions. *Information & Management*, *58*(2), 103411.

Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What adolescents look for and their intentions. *International journal of environmental research and public health*, *16*(2), 218.

Chen, Q., Chan, K. L., & 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. In J. Bailey, A. Flynn, & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (pp. 577-594). Emerald Publishing Limited.

Colton, J. S., Holmes, S., & Walwema, J. (2017). From NoobGuides to# OpKKK: Ethics of anonymous' tactical technical communication. *Technical Communication Quarterly*, *26*(1), 59-75.

Corbridge, Å. (2018). Responding to doxing in Australia: Towards a right to informational self-determination. *UniSA Student Law Review*.

Crompton, M. (2018). Doxing in Australia: A Practitioner's Perspective. *University of South Australia Law Review*.

Cross, K. (2019). Toward a Formal Sociology of Online Harassment. *Human Technology*, *15*(3), 326-346.

Demydova, V. (2021). Doxing as a Form of Online Activism: Case of Alexei Navalny's Film A Palace For Putin. *Electronic Turkish Studies*, *16*(3).

Douglas, D. M. (2016). Doxing: a conceptual analysis. *Ethics and information technology*, *18*(3), 199-210.

Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing, Privacy and Gendered Harassment. The Shock and Normalization of Veillance Cultures. *M&K Medien & Kommunikationswissenschaft*, *68*(3), 273-287.

Elwood, J. P. (1992). Outing, privacy, and the First Amendment. *Yale LJ*, *102*, 747.

Fish, A., & Follis, L. (2016). Gagged and doxed: Hacktivism's self-incrimination complex. *International journal of communication*, *10*, 20.

Garber, M. (2014). Doxing: An Etymology. *The Atlantic*. https://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/

Hansen, I., & Lim, D. J. (2019). Doxing democracy: influencing elections via cyber voter interference. *Contemporary Politics*, *25*(2), 150-171.

Huang, Q. (2021). The mediated and mediatised justice-seeking: Chinese digital vigilantism from 2006 to 2018. *Internet Histories*, 1-19.

ISD. (2022). *Tales From the Underside: A Kremlin-Approved Hack, Leak & Doxxing Operation*. Institute for Strategic Dialogue. Retrieved August 31, 2022 from https://www.isdglobal.org/digital_dispatches/tales-from-the-underside-a-kremlin-approved-hack-leak-doxxing-operation/

Jaffe, E. M. (2016). Swatting: The New Cyberbullying Frontier after Elonis v. United States. *Drake L. Rev.*, *64*, 455.

*Jessi Slaughter Cyberbulling Controversy*. (2010). https://knowyourmeme.com/memes/events/jessi-slaughter-cyberbulling-controversy

Karimi, Y., Squicciarini, A., & Wilson, S. (2022). Automated detection of doxing on twitter. *arXiv preprint arXiv:2202.00879*.

Kerr, A. (2022). *BLM activist Shaun King threatens to dox, inflict 'pain' on NY Post reporters*. Washington Examiner. Retrieved August 31, 2022 from https://www.washingtonexaminer.com/news/blm-activist-shaun-king-dox-reporters

Khanna, P., Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks. *Procedia Computer Science*, *94*, 459-464.

Lee, C. (2020). Doxxing as discursive action in a social movement. *Critical Discourse Studies*, 1-19.

Lindvall, A. J. (2019). Political hacktivism: doxing & the first amendment. *Creighton L. Rev.*, *53*, 1.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*(1), 1-18.

MacAllister, J. M. (2016). The doxing dilemma: seeking a remedy for the malicious publication of personal information. *Fordham L. Rev.*, *85*, 2451.

McIntyre, V. (2016). Do (x) you really want to hurt me: Adapting IIED as a solution to doxing by reshaping intent. *Tul. J. Tech. & Intell. Prop.*, *19*, 111.

McMahon, R., Bressler, M. S., & Bressler, L. (2016). New global cybercrime calls for high-tech cyber-cops. *Journal of Legal, Ethical and Regulatory Issues*, *19*(1), 26.

McNealy, J. (2017). Readers react negatively to disclosure of poster's identity. *Newspaper Research Journal*, *38*(3), 282-292.

Mery, H. C. (2020). The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment. . *Mary's LJ*, *52*, 905.

Morch, C. M., Cote, L. P., Corthesy-Blondin, L., Plourde-Leveille, L., Dargis, L., & Mishara, B. L. (2018). The Darknet and suicide. *J Affect Disord*, *241*, 127-132.

PCPD. (2020). *Privacy Commissioner Responds to Public Concern about Disclosure of a Reporter's Personal Data*. https://www.pcpd.org.hk//english/news_events/media_statements/press_20200108.html

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

Qian, J., Li, X.-Y., Zhang, C., Chen, L., Jung, T., & Han, J. (2017). Social network de-anonymization and privacy inference with knowledge graph model. *IEEE Transactions on Dependable and Secure Computing*, *16*(4), 679-692.

Raftery, B. (2022). *Legislation to protect the home addresses of judges and other court officials.* https://www.ncsc.org/information-and-resources/trending-topics/trending-topics-landing-pg/legislation-to-protect-the-home-addresses-of-judges-and-other-court-officials2

Roscoe, J. (2022). TikTok Users Are Doxing the Supreme Court. https://www.vice.com/en/article/v7vmpm/tiktok-users-are-doxing-the-supreme-court

Sari, S. V., & Camadan, F. (2016). The new face of violence tendency: Cyber bullying perpetrators and their victims. *Computers in Human Behavior*, *59*, 317-326.

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. Proceedings of the 2017 internet measurement conference,

Solo, A. M. (2021). Educating the Public to Combat Online Defamation, Doxing, and Impersonation. *Cases on Technologies in Education From Classroom 2.0 to Society 5.0*, 231.

Styple, K. (2021). Institutional Doxing and Attribution: Searching for Solutions to a Law-Free Zone. *Georgia Journal of International and Comparative Law*, *50*(1), 211-239.

Thomas, H. (2019). *Hong Kong protesters target police families in new tactic*. https://www.theaustralian.com.au/world/hong-kong-protesters-target-police-families-in-new-tactic/news-story/837a54b114b4c6d8209f6fb497563968

Trottier, D. (2019). Denunciation and doxing: towards a conceptual model of digital vigilantism. *Global Crime*, *21*(3-4), 196-212.

Vincent, I. (2021, July 31, 2021). *Activist Shaun King lives lavishly in lakefront New Jersey home*. New York Post. Retrieved August 31, 2022 from https://nypost.com/2021/07/31/activist-shaun-king-lives-lavishly-in-lakefront-nj-home/

Wang, F.-Y., Zeng, D., Hendler, J. A., Zhang, Q., Feng, Z., Gao, Y., Wang, H., & Lai, G. (2010). A study of the human flesh search engine: crowd-powered expansion of online knowledge. *Computer*, *43*(08), 45-53.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *mis Quarterly*, xiii-xxiii.

Yang, S.-Y. (2020). Effects of Self-efficacy and Self-control on Internet Addiction in Middle School Students: A Social Cognitive Theory-Driven Focus on the Mediating Influence of Social Support. *Child health nursing research*, *26*(3), 357-365.

Yudiana, T. C., Rosadi, S. D., & Priowirjanto, E. S. (2022). The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia. *PADJADJARAN JURNAL ILMU HUKUM (JOURNAL OF LAW)*, *9*(1), 24-45.