Internet Crime Enabling: Stalking and Cyberstalking

Raphael Cohen-Almagor[1] and Daniel Trottier[2]

1 The University of Hull, Hull, HU6 7RX, United Kingdom

2 Erasmus University Rotterdam, 3062 PA, Rotterdam, The Netherlands

Abstract. Cyberstalking is practiced by Internet abusers to harass, victimize and to mock peers, teachers, co-workers, neighbors and others. While typically framed as an individual pursuit, we suggest that it can best be understood as a collective process, both as a result of internet users' reliance on platforms and third-party services, as well as their engagements with other internet users engaged in related data practices, including doxing. We discuss the Amy Boyer tragedy, a well-known case that led to changes in law designed to better protect individual privacy. Subsequently, the paper discusses the responsibility of data companies within the broad business dimension of Internet companies. Corporate Social Responsibility (CSR) is suggested as a model to follow. Ethical leaders are people who care about the greater good of their employees, organization, and society rather than their own self-interests.

Keywords: Cyberstalking, Data Companies, Doxing, Harassment, Internet, Responsibility, Stalking

1 Introduction

This paper aims to address the social problem of cyberstalking as a multi-stakeholder and cross-disciplinary social harm. By drawing upon digital sources that are often widely available, cyberstalking is linked to more collective and coordinated practices like cyber harassment, cyberbullying and doxing. Sometimes, cyber harassment and cyberbullying include electronic stalking [1]. In some cases, collective forms of harassment and doxing will lead to individual stalking, while in other cases a stalker may decide to 'go public' and mobilize others in their sustained pursuit of a target.

The following section (II) explains the concepts of stalking and cyberstalking. Subsequently (section III), the tragic story of Amy Boyer serves as a poignant example. This tragedy raises several concerns that have significant ethical and legal implications. These include long-standing issues involving personal privacy in public space, security, anonymity, free speech, and the flow of information. In section IV, questions are raised about moral responsibility. Should Internet Service Providers (ISPs) give platform to data companies designed to intrude on the privacy of individuals and reveal information about them without trying to explore the motives of those who seek personal information about certain individuals? Social responsibility is emphasized. The moral and legal responsibilities of data companies to handle privileged information sensibly are accentuated. From a business perspective, it is argued (section V) that companies benefit from adopting principles of Corporate Social Responsibility (CSR).

CSR is one of the main tenets of a relatively new field of studies that emerged during the 1980s: business ethics. Like other aspects of applied ethics, this field is rooted in in

moral philosophy, combining philosophical principles with the study of business and corporations. Business ethics describes managerial activities as they became more visible thanks to the expansion of technology and media. Carroll [2] contends: "It is concerned with the rightness or fairness of business, manager and employee actions, behaviors and policies taking place in a commercial context."

This paper is cross-disciplinary in nature, drawing on the fields of Internet studies, psychology, business ethics, criminology and law. Given the severity of the problems associated with cyberstalking, ethics and self-regulation need to be supplemented with sufficient legal mechanisms to prevent Internet abuse and to save lives. Governments, especially liberal democratic governments, have a duty of care to their citizens, and an obligation to protect vulnerable third parties.

2 Stalking and Cyberstalking

We define stalking as the repeated harassment of individuals which would cause them to fear for their safety. Cyberstalking is defined as the repeated use of Internet capable devices with the intent to harass or threaten another [3]. Stalking and cyberstalking are in excess of curiosity, fascination or interest. Social networking platforms such as Facebook exacerbate the problem. While thankfully the vast majority of Facebook users are not stalkers, the platform's affordances [4] facilitate harmful pursuits of others. Not only does Facebook make personal information about individuals widely accessible, but it also routinely solicits further information about users and their associates.

Stalking is the result of curiosity, fascination or interest that has developed into an unhealthy, negative and destructive *obsession*. Stalkers are obsessed or fixated with the victim [5]. It is about obsession that has a negative impact on the stalker that might lead him or her to inflict harm on the person or persons who evoked that unhealthy obsession. Risk factors for violence in stalking include a prior intimate relationship, the stalker's feeling of being rejected or chastened, and susceptibility for violent behavior. Low educational level and substance abuse are contributing factors to violence [6][7]. In the focus is the conduct, not the awareness of the targeted person. Such a conduct would be stalking notwithstanding whether the targeted person is aware of the conduct.

Stalking is often a pattern of prolonged repeated harassment. It may include following or lying in wait for the target or the victim. Sometimes they let their victims know that they are been stalked and observed. But sometimes stalkers hide themselves from the victims who might not be aware that they are the target of intense attention and possibly vile intentions. When victims become aware of the stalker, they might be required to change their day-to-day routine. Stalking also involves intrusive communications from the perpetrator to reveal information about the victim and it may also involve intrusive and frightening communications directing at the victim [8]. These communications may typically be directed at the target but may also reach out to members of the target's social network, or even to a broader community of digital media users. Such a community may provide moral justification for the stalker's

behavior or may otherwise provide technical means or vital information in order to continue their pursuits [9]. As obsession escalates, stalking might involve obtaining the victims' personal information in order to follow them, harm them and damaging the victims' property; making direct or indirect threats to harass, intimidate or harm the victims and/or their families, friends and pets; repeatedly sending the victims unwanted messages and items; sexual overtones or other unwanted, persistent, and intrusive contact [10].

Mullen, Pathe, Purcell and Stuart [11] studied 145 stalkers who were referred to receive treatment in a forensic psychiatry center. Most of the stalkers were men (79%), many of them were unemployed (39%) and the majority, 52%, had never had an intimate relationship. Victims included ex-partners (30%), professional (23%), colleagues at work (11%), and strangers (14%). The researchers identified five motivational types: (1) The **rejected stalker** has high levels of narcissism and jealousy. The act of stalking aims to reconcile damaged self-esteem and to feel better about the stalker's conduct. (2) The **intimacy seeker** usually lives a secluded existence which lacks close connection with others, and s/he usually has an introverted personality. The intimacy seeker desires a relationship with a person who has engaged his/her affection and already does, or will, reciprocate that love so the intimacy seeker is convinced despite obvious evidence to the contrary. (3) The **incompetent suitor** also stalks to establish a relationship. Unlike the Intimacy seeker, the stalker is seeking a date or a sexual encounter. (4) The **resentful stalker** wants to intimidate and distress the victim to exact revenge for an injury he suffered. Unlike the rejected stalker, here the cause for stalking does not lie in rejection from an intimate relationship. (5) The **predatory stalker** engages in stalking to have sex. The predatory stalkers frequently exhibit low self-image, are ineffective socially and particularly in romantic life, and their intelligence possibly below-average [12].

The Mullen *et al* classification is the most commonly used in relation to cyberstalking. It illustrates the distinction – as well as the potential connections - between private motives like intimacy and revenge among stalkers, in contrast to more collective harms such as doxing and harassment, which are typically fueled by public outrage [13]. Doxing is defined as the "intentional public release" of a target's personal details [14]. The term came into use in the 1990s to describe a behavior aimed to humiliate or intimidate a person by linking online personas to sensitive personal information [15]. The public nature of these harms implies that they command an audience, and provide motives, means, and opportunity to take follow up steps against a target. Potential stalkers who hold personal grievances may attempt to scale up their assault by mobilizing a collection of likeminded individuals to engage in doxing and harassment [16]. Individual members of this group may in turn branch off and stalk the target based on the aforementioned motives.

Mullen *et al* found that delusional disorders were common among stalkers (30%), particularly among intimacy-seeking stalkers. Rejected stalkers exhibited personality disorders. The stalking duration varied from 4 weeks to 20 years (mean = 12 months), longer for rejected and intimacy-seeking stalkers. Sixty-three percent of the stalkers issued threats, and 36% were assaultive. Threats and property damage were more frequent when resentful stalkers were involved. Rejected and predatory stalkers

committed more assaults. Other predicators to potential assaults were previous convictions, substance-related syndromes, and threatening behavior.

Since the advance of communication technologies, especially after the Internet was popularized in the mid-1990s, it is much easier for stalkers to find information about their targets and to stalk their victims [17].

Cyberstalking, also called online stalking and Internet stalking, is a crime-facilitating speech. It is a form of stalking involving computer communication. Using the Internet, stalkers can operate anonymously, retrieving information about the victim by using their digital literacy without the need to venture into the physical world. Cyberstalkers use emails, social networking sites, chat rooms and other forums facilitated by technology. They abuse the Internet to locate personal information about their victims, to follow them, to communicate with the victims, to damage their victims' reputation, and to cause them other harm. Christine Hammond [18] lists 23 ways that people can be cyberstalked. Thus, for instance, cyberstalkers may subscribe their victims to services without their knowledge. They may plant tracking devices in their victims' cars. They may spread false accusations about the victims' conduct. Perpetrators might pretend to be representatives of the victims' bank and ask for them to verify personal information. Then they use the information to gain access to bank accounts. They may depict the target as a prostitute or a swinger who is interested to experiment various sex acts on adult websites. They may also issue public appeals to other digital media users to (a) locate and share information about the target, (b) circulate already published information about the target, and (c) to send vitriolic messages to the target, or engage in similarly abusive practices [19]. Because of these practices cyberstalking does not just concern a single perpetrator and target, but rather a scenario in which a stalker temporarily mobilizes a community to pursue the target, or where a communal exposition of a target mobilizes an individual stalker. This community may either be likeminded in disposition and ideology, or may unknowingly participate in disproportionate abuse, for instance, if the target is wrongly or unjustly presented by the perpetrator as a criminal or immoral.

Cyberstalking is considered an individual misdeed, yet it is shaped by the media landscape in which it occurs. In addition to practices that relate to or overlap with cyberstalking, we also need to address digital services that make personal information accessible. Prominent digital platforms such as Facebook enable users to obtain personal information about other people. The practice of seeking and disclosing personal information (about one's self or others) is justified and normalized through the rhetoric of sharing [20]. Sharing is good for the business model of these platforms as it facilitates advertising. This practice not only enable users to gather information about others, which may be an innocent practice motivated by human curiosity; but it also lead to abuse and exploitation, including stalking. Stalking via social media is an amplified and malicious version of more acceptable practices such as "creeping" or simply "using" the site [21].

Collective pursuits such as doxing can inform stalking, and vice versa. A private pursuit may go public if stalkers bring their obsession to a public forum, especially in framing it as a personal and relatable grievance. Likewise, a public appeal to dox and harass someone can easily result in private pursuits if a stalker adopts collective

grievances as a personal obsession. Consider the doxing of vulnerable communities such as sex workers [22] where individual pursuits may extend from collective harassment. These outcomes speak to the inherent risk associated with any online site or service that gathers and publishes personal information, whether as a for-profit scheme, on moral grounds, or as a combination of the two [23]. Once information is published on public or even private fora, it is difficult for any single actor to control the flurry of activity that may follow. This includes the target, who is unlikely to persuade (and in many cases may not be aware of) a group of users denouncing, doxing and harassing them.

Stalkers who wish their targets to know that they are been stalked might place victims in a reasonable fear of bodily injury or even death. Strawhun *et al* [24] suggest that women experienced greater frequencies of cyberstalking than men. In the United States, one out of every 12 women (8.2 million) and one out of every 45 men (2 million) have been stalked at some time in their lives [25]. According to the National Intimate Partner Sexual Violence Survey, 2011, 15.2% of women and 5.7% of men have been stalked by an intimate partner in their lifetime [26]. Working to Halt Online Abuse (WHOA), an organization that fight against cyber harassment through education and the empowerment of victims receives an estimated 50-75 complaints per week [27].

The ramifications of stalking and cyberstalking are significant and widespread, affecting psychological, social, interpersonal, and economic aspects of life. Victims experience psychological distress, fear, anger, depression, increased suicidal ideation, anxiety, insecurity, isolation, lowered self-esteem and a loss of trust in other people [28][29]. To adapt, some victims are required to make major changes to both their work and social life. In some cases, they have to change jobs and suffer family relationships breakdown [30]. The widespread negative effects of stalking and cyberstalking highlight that this phenomenon is a concern to high-tech, legal and mental health professionals as well as to security officers. Let us illustrate the problem of stalking and cyberstalking by examining the tragedy of Amy Boyer.

3 The Boyer Tragedy

In October 1999, Amy Boyer, a twenty-year-old resident of Nashua, New Hampshire, was murdered by a young man who had stalked her for a long time. The stalker, Liam Youens, was engaged in stalking activities that led to Boyer's murder by using the Internet for his predatory pursuit. Through the use of standard Internet search facilities, Youens gathered information about Boyer from online databases. He was able to find information about Boyer's residence, her place of work, her car and other personal information. Youens set up two websites about Amy Boyer. On one site, he posted Boyer's personal information. On another website, Youens described in detail his plans to murder Boyer [31]

Boyer was unaware that Youens was stalking her for over eight years. Youens had been infatuated with Boyer since they met in the eighth grade. Boyer did not pay much attention to Youens who thought that she had turned him down. After graduation,

Youens was unemployed and lived with his parents. Having lots of free time, Youens had studied the Internet and learned to use it for his base purposes. Information that he could not find on the Internet was secured by paying an information broker called Docusearch.com [32]. Youens purchased Boyer's date of birth, her social security number as well as her home and job addresses. He became Boyer's shadow while she was oblivious to the obsessive man. Youens announced his murderous intentions on the Internet. On October 15, 1999, Youens murdered Amy Boyer, the subject of his obsession, and then killed himself.

Youens maintained his web presence in a different era of online communication. The archived remains of his web presence suggest limited opportunities for readers to interact directly with him, although guestbooks and other means were available at the time. Had he maintained such an online presence twenty years later, the outcome of this case would almost certainly differ. This is due the affordances of contemporary platforms that promote "human connectedness while pushing automated connectivity" [33]. Through human agency and algorithmic governance, Youens' audience would have surely been amplified. Had he posted on a social media profile like Facebook or Twitter, it is likely that someone would have alerted local authorities about his intentions. On the other hand, platforms like 4Chan and 8Chan might have been more enabling of his intentions, providing moral justification and even guidance for his intent to murder.

We wish to analyze the problematic conduct of Docusearch. What are the responsibilities of such data companies? What can be done to prevent abuse of data for malicious purposes, including murder?

4 Responsibility of Data and Software Companies

The Association of Independent Information Professionals (AIIP) Code of Ethical Business Practice states that members must "uphold the profession's reputation for honesty, competence, and confidentiality" and "Accept only those projects which are legal and are not detrimental to our profession" [34]. Docusearch.com had prided itself on being "America's premier provider of on-line investigative solutions." On its website, it was "sensitively" written: "We provide articles relevant to specific searches and present feature columns written by leaders in the investigative community. If you require the personal touch, you may always contact us. Happy Hunting!."[1] This casual statement, "Happy Hunting!" is anything but ethical or professional. It typifies Docusearch behavior, and it is disconcerting and irresponsible. Such language feeds in to what David Lyon terms "surveillant imaginaries" which:

> have to do with shared understandings about certain aspects of visibility in daily life, and in social relationships, expectations, and normative commitments. They provide a capacity to act, to engage in, and to legitimate surveillance practices. In turn, surveillance practices help to carry surveillance imaginaries and to contribute to their reproduction. [35]

[1] http://www.docusearch.com/basics.html (no longer available).

Shared understanding of digital surveillance - including cyberstalking - are shaped by the marketing efforts of digital media companies. This includes platforms that host personal data as well as services that seek private information from disparate sources. This marketing push is also seen in contemporary media cultures [36], ranging from specialized services to gossip based entertainment, appealing both to private scrutiny of persons of interest, and also to public denunciation on moral or legal grounds.

The business model is simple: companies like Docusearch whose logo claims "We've been helping people successfully find what they need for over 20 years secure, private and online"[2] provide the information people ask for if they pay for it. Hardly no questions are asked. Youens himself was surprised by how easy was it for him to purchase Boyer's personal information without inquiring about his motives. He wrote: "I found an internet site to do that, and to my surprise everything else under the Sun... It's actually obsene what you can find out about a person on the internet. I'm waiting for the results" [37]. Indeed, obscene it is. Financial gains precede social responsibility. The private investigation/information broker did not take any constructive steps to find who Youens was, and why he needed the information about Boyer. Had Docusearch searched "Amy Boyer Liam Youens" online they were likely to have found Youens' website documenting his intent to murder Boyer. In this situation, scrutiny of clients (in a way that is comparable and perhaps proportionate to the scrutiny these clients perform on unsuspecting targets) might have saved Boyer's life.

Equally concerning are software companies that sell stalking tools to customers with complete disregard to the consequences of their actions. A company called Imminent Methods sold an intrusive tool known as the Imminent Monitor Remote Access Trojan (Imrat) for about $25 (£19). The tool gave (ab)users full access to infected devices, letting them steal data, monitor what victims were doing and access their webcam. According to the United Kingdom National Crime Agency (NCA), Imminent Methods sold its spying tool to 14,500 people. The authorities were able to take down the Imminent Methods website, which subsequently stopped the work of the cyber-stalking tools [38].

The business model of companies that handle sensitive issues should include the principle of social responsibility. Social responsibility refers to universality and diversity of provision; democratic accountability to the public as a whole; responsibility for meeting general and special needs as decided by the public; a commitment to quality, not determined by profit or the market; and often some subordination to national needs or priorities in cultural, economic, and political matters [39]. Social responsibility carries a special meaning in the context of the professions. A member of a profession is trained to practice a core skill, requiring autonomous judgment and expertise, in turn governed by ethical standards. Professionalism is maintained and monitored, and companies should accept wider responsibilities to clients and society. Yet in practice this sense of socially rooted responsibility clashes with an ethos of "cyber-libertarianism" [40] among digital media services. This refers to the core beliefs that inform their marketing and lobbying efforts. While transcending any given territory and jurisdiction, these services are also transcending any perceived responsibility to the

[2] https://www.docusearch.com

norms or laws of that territory. In their perception, they are at liberty to overlook the local contexts in which their services may be abused. While we may wish for digital media platforms to espouse a greater sense of social responsibility, they often seem either unable or unwilling to incorporate such social accountability into their operations, thus facilitating stalking and harassment. Recent efforts have sought to hold such platforms legally accountable, including a Federal Trade Commission (FTC) decision to issue a $5 billion USD penalty to Facebook, based on their misrepresentation to users of the handling of their personal information [41].

Not only social responsibilities are at issue. Legal responsibility was pertinent too. After the murder, Amy's parents filed a wrongful death suit against Docusearch and the investigators with which the company subcontracted to obtain Boyer's personal information. In 2003, the New Hampshire Supreme Court ruled that Docusearch was liable for the criminal acts of Youens, holding stalking and identity theft to be foreseeable risks of selling personal information [42]. If the personal information of a targeted person creates a foreseeable risk of criminal misconduct against that person then the private investigator who provided the information should be held liable. In obtaining Boyer's social security details from another party (a credit reporting agency) without the victim's knowledge or consent, Docusearch invaded Boyer's privacy. The court found that Docusearch had "a duty to exercise reasonable care in disclosing a third person's personal information to a client."[3] When Docusearch sold Ms. Boyer's social security number and employment address, stalking and identity theft were "sufficiently foreseeable" risks.[4] This is especially true when the company did not know Youens and did not inquire about his intentions in seeking the information. Thus, Docusearch was negligent in selling Ms. Boyer's personal information, and was liable for its irresponsible conduct.

In 1990, California enacted a specific stalking law. It was the first American state to enact such a law. Since then, all 50 states and the District of Columbia have enacted stalking laws. Most states have specific cyber harassment and cyberstalking laws [43]. The Interstate Stalking Act was signed into law by President Clinton in 1996, stipulating that an "interactive computer service or electronic communication service or electronic communication system of interstate commerce" cannot be used to threaten, cyberstalk and cyber harass people. [5] Two years later, in 1998, President Clinton signed a bill that protects children against online stalking. According to the statute, it is a federal crime to use interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person to solicit or entice a child into unlawful sexual activity.[6]

In 2000, the 106th American Congress passed the Amy Boyer Law. The law bars the public display of any person's social security number, "or any identifiable derivative of such number, without the expressed consent, electronically or in writing, of such

---

[3] *Ibid*.
[4] *Ibid*.
[5] 18 U.S. Code § 2261A.Stalking, https://www.law.cornell.edu/uscode/text/18/2261A
[6] 18 U.S. Code § 2425.Use of interstate facilities to transmit information about a minor, https://www.law.cornell.edu/uscode/text/18/2425

individual. Prohibits obtaining a social security number for purposes of locating or identifying an individual with the intent to physically injure, harm, or use the identity of the individual for illegal purposes. Provides prerequisites for consent, including that the individual be informed of the general purposes for which the number will be utilized and the types of persons to whom the number may be available." The Law further authorizes persons who are aggrieved by violations of this law to bring civil actions in district courts to recover damages.[7]

The aforementioned legislation may target explicit data brokers within the United States, yet the possibility remains for stalkers to use comparable services through the dark web. Nowadays, to some degree the services of Docusearch are not as necessary for would-be stalkers who have sufficient technical skills. People disclose their work details and other personal and sensitive data on a variety of searchable platforms. This information may be the most prominent results when entering a target's name in search engines. Research shows that most doxes include highly identifying information of the victim and family members, including the full legal names, phone numbers and online social networking accounts [44]. Moreover, their employer or other institutions may also publish this information about them by default. Not only is there an increased expectation to be searchable and findable through today's Internet, but stalkers and even those with a casual interest in others have refined their skills to locate others through a variety of open and private sources. This includes a knowledge of technical affordances of platforms, but also arguably a normalization of human engineering to bypass privacy barriers, for instance through use of fake accounts to reach or even entrap a target.

Jurisdiction vary in the way that they define stalking [45]. In Europe, the General Data Protection Regulation (GDPR) [46] aims for better handling of the personal data online, and the transfer of personal data outside the European Union (EU) and the European Economic areas. The GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. The regulation primary aims are to give people control over their personal data and to simplify the regulatory environment for businesses by unifying this Regulation within the EU. The Regulation is said to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" [47]. One of the primary aims of the GDPR is to enforce the protection of individuals' personal information among companies, thus preventing businesses and other organizations from being unwitting – or knowing – enablers of doxing and cyberstalking. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified. This definition relates to one's name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people [48]. However, ensuring compliance and effective enforcements on a per-case basis remains a concern, especially when data

[7] S.2554 - Amy Boyer's Law 106th Congress (1999-2000), https://www.congress.gov/bill/106th-congress/senate-bill/2554

brokers may easily flaunt legal frameworks by operating in the so-called 'dark web' [49].

5 Business Dimension

Businesses have economic, legal, moral, social and discretionary responsibilities. *Economic responsibility* suggests a duty to produce goods and services that society needs. Society expects business to be efficient, effective and responsive to developments. *Legal responsibility* implies that businesses should obey the law and conduct their affairs within the confines of the law. In *moral responsibility*, the agent's conscience is concerned. When people fail to perform a morally significant act they may be blameworthy for omission [50]. Businesses should assume ethical responsibilities that are extended to actions, decisions, and practices beyond what is required by the law [51][52]. *Social responsibility* assumes that people are not islands to themselves. We have responsibilities to the community. The responsibilities are positive and negative. That is, businesses have a responsibility to better the society in which we live, and a responsibility to refrain from acting in a way that knowingly might harm our community. Finally, *discretionary (or philanthropic) responsibilities* represent voluntary roles and practices that businesses assume although there are no clear and explicit societal provisions as to how to perform these responsibilities. These are left to individual managers' and corporations' judgments and choices in accordance with prevailing social norms. Examples of these voluntary activities include making philanthropic contributions, conducting in-house programs for drug abusers, training the hard-core unemployed, or providing day care centers for working mothers [53].

In terms of social, legal and moral responsibilities, platforms are difficult to pin down to a particular jurisdiction. And practices like doxing and coordinated denunciation may be seen as morally desirable in particular instances, for example in preparing and planning adequate responses to white supremacist and anti-Semitic demonstrations [54]. Drawing and enforcing boundaries between appropriate and inappropriate forms of doxing remains an ongoing issue. Businesses may play a role in making sense of these boundaries, in accounting for new kinds of harms, or new iterations of old harms. Yet they should also listen to, and cooperate with local authorities on these matters, especially in taking steps that are appropriate to given jurisdiction and cultural practices of the region in question.

Business should focus on its core mission and simultaneously be aware of the social needs that first called a firm into existence. Here we can question the extent to which Docusearch was aware of the "needs" they wanted to address, as evidenced by describing use of their services as "hunting". In other words, businesses are acting in and benefiting from society. They need to act morally and responsibly. Their leaders' decisions need to respect human dignity and provide for the common good [55]. Ethical leadership should include care, compassion and foresight. Leaders should have the ability to analyze and be responsible for the consequences of their decisions. These ethical role models adopt socially responsible behavior and strive to balance the various needs of stakeholders in a way that serves the interests of [56].

The business dimension of the Amy Boyer tragedy is obviously of great relevance and importance. Here the tension between freedom of information, and moral and social responsibility is clear. It may have significant business implications not only for information and communication companies. There is often a basis in law, but many responsibilities are assumed by norms and customs, by business interests and by competitive necessities. Ethical principles may also play a part [57]. CSR scholar Keith Davis [58] asserts that it is a firm's obligation to consider the effects of its decisions on society in a manner that will accomplish social benefits as well as traditional economic benefits. This means that "social responsibility begins where the law ends. A firm is not being socially responsible if it merely complies with the minimum requirements of the law, because this is what any good citizen would do."

The main principles of Corporate Social Responsibility (CSR) dictate integrated, sustainable decision-making which takes into consideration the positive and negative potential consequences of decisions; obligations to consider different stakeholders and interests and incorporating them into the decision-making processes; transparency that is vital for ensuring accountability to stakeholders; liability for decisions, and taking on board remedial measures to minimize harm. Beyond the firm's economic and legal obligations, social responsibility also encompasses ethical and discretionary responsibilities [59]. Companies should behave ethically as a good corporate citizen.

Carroll distinguishes between immoral and amoral people. "Amoral managers," Carroll explains "are neither immoral nor moral but are not sensitive to the fact that their everyday business decisions may have deleterious effects on others" [60]. Docusearch managers ignored the ethical dimension of their business and were inattentive to the implications of their conduct on stakeholders.

Information and communication technologies (ICT) should be accountable for the way information is transferred. Members of these professions are trained to practice core skills, requiring judgment and expertise. They should abide by a clear Code of Conduct and they should enforce the Code, using their knowledge and skill. Certain standards and qualifications need to be maintained.[8]

Adopting norms of social responsibility could be beneficial for Internet companies. Maintaining ethical practice contribute to the company's reputation and marketing. Indeed, there is a significant positive relationship between responsible conduct and consumers' purchasing decisions [61]. Stewart Lewis [62] argues that corporate social responsibility is established as a fundamental addition to stakeholders' appreciation of companies, and calls for a continued effort to maintain companies' reputation. Upholding norms of corporate social responsibility benefit both the firm and the societies in which it operates. Take, for instance, Reddit. This digital platform has taken steps to remove communities deemed to be toxic [63]. Other companies introduced explicit rules against doxing. For example, the popular community "/r/covidiots" dedicated to denouncing people who flaunt pandemic-related public health guidelines. This community features the following warning on their front page: "No Doxing or Posting Personal Information - That person will be permabanned. Please help us keep

[8] Compare to the responsibilities of the press; see McQuail [64]; Raphael Cohen-Almagor [65].

this community safe and protected from such people" [66]. This statement suggests that even platforms dedicated to the practice of naming and shaming are aware of ethical and legal boundaries to their actions. Yet a batch of so-called "complaint sites" allow anonymous users to publish personal and sensitive information about targets, citing Section 230 of the Communication Decency Act in the United States [67]. Not only are cyberstalking and doxing intertwined, but even after over a quarter of a century of openly accessible internet these issues remain a contested legal terrain. Nevertheless, the popularization of the internet – including a growing awareness of incidents such as the Amy Boyer tragedy – brings an expectation that any business dealing with personal information online should be reasonably aware of the harms that might emerge because of improper data handling.

6 Results and Discussion

The Amy Boyer tragedy raises questions relating to social responsibility of Internet companies**,** of readers, and of information broker companies. Stalkers wish to exert power and influence over their victims. Bringing stalking to an end requires a mixture of appropriate legal sanctions and therapeutic interventions [68].

Unfortunately, the challenge of stalking is particularly relevant to educators. In 2007, two students at a North Carolina High School, were charged with cyberstalking after creating a MySpace profile which depicted a school administrator as a pedophile [69]. This incident speaks to the public-facing nature of cyber-harassment, as the students sought to harm their administrator through a highly visible form of character assassination, thus inviting other members of the public to harm him. Those two students, Tyler Yannone and Lauren Strazzabosco, were not alone in thinking of such a harmful prank. A year later, a Providence High School freshman was charged with cyberstalking after he set up a website that suggested a male teacher was a pedophile. Four other students were disciplined by the Charlotte-Mecklenburg Schools code of student conduct, which bans students from distributing "any inappropriate information, relating in any way to school issues or school personnel, distributed from home or school computers" [70][71].

In addition, Internet intermediaries should not enable fans to stalk their favorite celebrities in real time through Internet-organized mobile networks and provide similar channels for journalists to organize citizen-reporters [72]. Governments have a responsibility and duty of care to ensure safe Internet that is not open to abuse. A recent British government White Paper sets out a program of action to tackle content or activity that harms individual users, particularly children, or threatens the British way of life. The White Paper holds that the British government cannot allow harmful conduct and content to undermine the significant benefits of the digital revolution. It maintains:

> While some companies have taken steps to improve safety on their platforms, progress has been too slow and inconsistent overall. If we surrender our online spaces to those who spread hate, abuse, fear and vitriolic content, then we will all lose. So our challenge as a society is to help shape an internet that is open and

> vibrant but also protects its users from harm. The UK is committed to a free, open and secure internet, and will continue to protect freedom of expression online. We must also take decisive action to make people safer online [73].

In July 2021, The House of Lords Communications and Digital Committee [74] issued a report that supports the Government's Online Safety Bill. The Lords recommended that the Bill include a robust duty to ensure that powerful platforms make responsible design choices and put users in control of what content they are shown by giving them an accessible and easy-to-use toolkit of settings, including through third-party applications. The Lords further recommended that design changes be complemented by digital citizenship education and stressed that the rights and preferences of individuals must be "at the heart of a new, joined-up regulatory approach, bringing together competition policy, data, design, law enforcement, and the protection of children".

This article is interdisciplinary, drawing together the fields of Internet studies, business ethics, criminology and law. Policy makers should develop collaborative and integrative approaches to combat online and off-line harassment. Law enforcement agencies, Internet intermediaries and counselling services should all be made aware of this growing challenge and devise the appropriate policies and mechanisms to tackle it effectively. Future research will benefit from longitudinal studies that analyze the phenomena of stalking and cyberstalking from different perspectives, with sharper focus on comparative analysis of different manifestations of stalking and cyberstalking in different countries and specific age groups. Multi-dimensional research that brings together Internet studies, business ethics and other fields of studies, including psychology and brain studies, will shed further light on targeting vulnerable populations (people with health problems, different sexual orientations, minorities). It is also important to conduct systematic follow-up evaluations of programs that educate people about the harms of stalking and cyberstalking and provide meaningful support to victims. It is of vital importance to increase awareness of Internet intermediaries' professionals of the harms that cyberstalking, cyberharassment and cyberbullying involve, harms that might result in most unfortunate and avoidable loss of life.

7 Conclusion

Cyberstalking is a growing concern because it is easy, relatively cheap, instantaneous and has a certain utility for the stalker. Only combined efforts of Internet users and readers, Internet companies, governments and the international community at large will be able to provide safe and secure Internet from which we all could benefit and enhance our autonomy and quality of life. Such a concerted, responsible effort is required because of the global nature of the Internet and the technological tools that are available to people to act in a clandestine and malicious manner. Responsible business should not engage with it in any shape or form. Even slight association with cyberstalking might be detrimental to corporate sustainability. Awareness should be

raised as regarding service providers' liability and social responsibility to prevent stalking and cyberstalking and to support stalked victims.

Unfortunately, not all companies adhere to the principles of Corporate Social Responsibility. Therefore, we contend that ethical standards should be anchored in appropriate laws and enforced by responsible governments.

Future research may continue to analyze the services that data companies, such as Docusearch, are offering their clients and whether those services are following local legal frameworks and/or are ethical in nature. Additionally, the marketing and public framing of these services warrants greater scholarly and societal scrutiny. We, the Internet community, should protest against cyberstalking. Liberal democracies have a duty of care to protect vulnerable third parties.

References

1. Cohen-Almagor, R. Social Responsibility on the Internet: Addressing the Challenge of Cyberbullying. Aggression and Violent Behavior, 39, 42-52 (2018).
2. Carroll, A.B. Corporate Social Responsibility: The Centerpiece of Competing and Complementary Frameworks, Organizational Dynamics, 44: 87-96 (2015).
3. Durkin, K.F. Cyberstalking. The SAGE Encyclopedia of the Internet, Thousand Oaks: Sage: 165-167 (2018).
4. Nagy, P.and Neff, G. Imagined affordance: Reconstructing a keyword for communication theory. Social Media+Society, 1(2), 1-9 (2015).
5. Rosenfeld, B. Violence risk factors in stalking and obsessional harassment: A review and preliminary meta-analysis. Criminal Justice and Behavior, 31(1), 9-36 (2004).
6. Miller, L. Stalking: Patterns, motives, and intervention strategies, Aggression and Violent Behavior, 17(6), 495-506 (2012).
7. Svenja Senkans, Troy E. McEwan, and James R. P. Ogloff, Assessing the Link Between Intimate Partner Violence and Post relationship Stalking: A Gender-Inclusive Study. Journal of Interpersonal Violence (2017), 1–31
8. Coupland, S.H. Stalking and Violence: A 10-year Follow-Up of Stalking Offenders, PhD Dissertation, Department of Psychology, Faculty of Arts and Social Sciences, Simon Fraser University (Summer 2018).
9. Trottier, D. Denunciation and doxing: towards a conceptual model of digital vigilantism. Global Crime, 21(3-4), 196-212 (2020).
10. Pittaro, P.L. Cyber stalking: An Analysis of Online Harassment and Intimidation, International Journal of Cyber Criminology, 1(2), 180–197 (2007).
11. Mullen, P.E., Pathe, M., Purcell, R. and Stuart, G.W. Study of Stalkers, American J. of Psychiatry, 156(8), 1244-1249 (1999).

12. Barnes, J. and Short, E. Who Stalks and Why, in Short E (ed), A Practical Guide to Coping with Cyberstalking (University of Bedfordshire: The National Centre for Cyberstalking Research) (April 2015).
13. Trottier, D. Digital vigilantism as weaponisation of visibility. Philosophy & Technology, 30(1), 55-72 (2017).
14. Douglas, D.M. Doxing: a conceptual analysis. Ethics and information technology, 18(3), 199-210 (2016).
15. Snyder, P., Doerfler, P., Kanich, C. and McCoy, D. Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing, IMC conference 2017 (1-3 November), London (2017).
16. Hern, A. Zoe Quinn on Gamergate: 'We need a proper discussion about online hate mobs', The Guardian, September 12 (2014). https://www.theguardian.com/technology/2014/sep/12/zoe-quinn-gamergate-online-hate-mobs-depression-quest
17. Cohen-Almagor, R. Internet History, International Journal of Technoethics, 2(2), 45-64 (2011).
18. Hammond, C. 23 Ways You Could be Cyberstalked, Psych Central (2019), https://pro.psychcentral.com/exhausted-woman/2019/09/23-ways-you-could-be-cyberstalked/
19. Coupland, S.H. Stalking and Violence: A 10-year Follow-Up of Stalking Offenders, PhD Dissertation, Department of Psychology, Faculty of Arts and Social Sciences, Simon Fraser University (Summer 2018).
20. John, N.A. Sharing and Web 2.0: The emergence of a keyword. New Media & Society, 15(2), 167-182 (2013).
21. Trottier, D. Social Media as Surveillance. Ashhate, Farnham (2012).
22. Schofield, D. 'He Found Out Where I Live' – Sex Workers Are Getting Doxxed by Clients (2021). Vice.com, January 4. https://www.vice.com/en/article/v7m38y/doxxing-
23. Hill, K. A Vast Web of Vengeance. The New York Times (30 January 2021). https://www.nytimes.com/2021/01/30/technology/change-my-google-results.html
24. Strawhun, J., Adams, N. and Huss, M.T. The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse, Violence and Victims, 28(4), 715–730 (2013).
25. Bocij, P. Cyberstalking: Harassment in the Internet Age and how to Protect Your Family, Westport, CT: Praeger (2004).
26. Sacco, L.N. The Violence Against Women Act: Overview, Legislation, and Federal Funding, Congressional Research Service 7-5700 (26 May 2015).
27. Working to Halt Online Abuse (WHOA) (1997-2015), http://www.haltabuse.org/resources/stats/index.shtml
28. Kamphuis, J.H., Emmelkamp, P.M.G. and Bartak, A. Individual Differences in Post-Traumatic Stress Following Post-Intimate Stalking: Stalking Severity and Psychosocial Variables, British Journal of Clinical Psychology, 42(Pt 2) :145-156 (2003).

29. Short, E., Guppy, A., Hart, J.A. and Barnes, J. The Impact of Cyberstalking, Studies in Media and Communication, 3(2) (December 2015).
30. Short, E., Guppy, A., Hart, J.A. and Barnes, J. The Impact of Cyberstalking, Studies in Media and Communication, 3(2) (December 2015).
31. Tavani, H.T. The Impact of the Internet on Our Moral Condition: Do We Need a New Framework of Ethics?, in Cavalier RJ (ed), The Impact of the Internet on Our Moral Lives, New York: State University of New York Press (2005).
32. Tavani, H.T. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, Hoboken, NJ: Wiley (2011).
33. Van, Dijck. J. and Poell, T. Understanding Social Media Logic. Media and Communication, 1(1), 2-14 (2013).
34. AIIP Code of Ethical Business Practice (2002) https://www.aiip.org/about/professional-standards
35. Lyon, D. Digital citizenship and surveillance culture: Engagement, exposure, and ethics in digital modernity. International Journal of Communication, 11: 824-842 (2017).
36. Andrejevic, M. iSpy: Surveillance and power in the interactive era. Lawrence: University Press of Kansas (2007).
37. Douglas, R. The Murder of Amy Boyer, Senate Hearings, 13 April (2005), http://www.davickservices.com/murder_of_amy_boyer.htm
38. BBC. Spying tools website taken down after UK raids, 29 November (2019), https://www.bbc.co.uk/news/technology-50601905?intlink_from_url=https://www.bbc.co.uk/news/topics/c5elz932pjyt/cyber-stalking&link_location=live-reporting-story
39. McQuail, D. Media Accountability and Freedom of Publication, New York: Oxford University Press (2003).
40. Dahlberg, L. Cyber-libertarianism 2.0: A discourse theory/critical political economy examination. Cultural Politics, 6(3), 331-356 (2010).
41. FTC. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (2019). https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions
42. Remsburg v. Docusearch, Inc. No. 2002-255, 2003 N.H. LEXIS 17 (N.H. Feb. 18) (2003).
43. Hazelwood, S.D. and Koon-Magnin, S. Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis, International Journal of Cyber Criminology, 7(2), 155-168 (2013).
44. Snyder, P., Doerfler, P., Kanich, C. and McCoy, D. Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing, IMC conference 2017 (1-3 November), London (2017).
45. McEwan, T. E. , Simmons M., Clothier, T. and Senkans S., Measuring stalking: the development and evaluation of the Stalking Assessment Indices (SAI), Psychiatry, Psychology and Law (2020). DOI: 10.1080/13218719.2020.1787904

46. General Data Protection Regulation (GDPR) (2018). https://gdpr-info.eu/
47. General Data Protection Regulation (GDPR) (2018). https://gdpr-info.eu/
48. Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR) (March 22 2018).
49. Galov, D., Tushkanov, V. and Bezvershenko, L. Dox, steal, reveal. Where does your personal data end up? Securelist, 1 December (2020). https://securelist.com/dox-steal-reveal/99577/
50. Cohen-Almagor, R. *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway,* New York and Washington DC.: Cambridge University Press and Woodrow Wilson Center Press. 2015.
51. Cohen-Almagor, R. Freedom of Expression, Internet Responsibility and Business Ethics: The Yahoo! Saga and Its Aftermath, *Journal of Business Ethics*, 106(3) (2012), 353–365.
52. Carroll, A.B. Corporate Social Responsibility (CSR) and Corporate Social Performance (CSP), in Kolb RW (ed), The SAGE Encyclopedia of Business Ethics and Society, Thousand Oaks: SAGE Publications: 746-754 (2018).
53. Carroll, A.B. Corporate Social Responsibility (CSR) and Corporate Social Performance (CSP), in Kolb RW (ed), The SAGE Encyclopedia of Business Ethics and Society, Thousand Oaks: SAGE Publications: 746-754 (2018).
54. Milbrandt, T. Make them famous': Digital vigilantism and virtuous denunciation after Charlottesville. In Trottier D, Gabdulhakov R and Huang Q (eds) Introducing vigilant audiences. pp.215-258. Cambridge: Open Access Publishers (2020).
55. Mea, W.J. and Sims, R.R. Human Dignity-Centered Business Ethics: A Conceptual Framework for Business Leaders, Journal of Business Ethics, 160, 53–69 (2019).
56. De Roeck, K. and Farooq, O. Corporate Social Responsibility and Ethical Leadership: Investigating Their Interactive Effect on Employees' Socially Responsible Behaviors, Journal of Business Ethics, 151, 923-939 (2018).
57. McQuail, D. Media Accountability and Freedom of Publication, New York: Oxford University Press (2003).
58. Davis, K. The Case For and Against Business Assumption of Social Responsibilities, Academy of Management Journal 16, 312-322 (1973), http://uweb.txstate.edu/~ek10/socialresponsibility.pdf.
59. Crane, A. (ed) The Oxford Handbook of Corporate Social Responsibility, Oxford Handbooks Online (2009).
60. Carroll, A.B. The Pyramid of Corporate Social Responsibility: Toward the Moral management of Organizational Stakeholders, Business Horizons 34, 39-48 (1991).
61. Lee, K.H. and Shin, D. Consumers' Responses to CSR Activities: The Linkage between Increased Awareness and Purchase Intention, Public Relations Review, 36 (June), 193-195 (2010).
62. Lewis, S. Reputation and Corporate Responsibility, Journal of Communication Management 7(4), 356-394 (2003).

63. Dewey, C. These are the 5 subreddits Reddit banned under its game-changing anti-harassment policy — and why it banned them. The Washington Post, (June 11 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/06/10/these-are-the-5-subreddits-reddit-banned-under-its-game-changing-anti-harassment-policy-and-why-it-banned-them/
64. McQuail, D. Media Accountability and Freedom of Publication, New York: Oxford University Press (2003).
65. Cohen-Almagor, R. The scope of tolerance: Studies on the costs of free expression and freedom of the press. Routledge, London (2005).
66. Covidiots. Idiocy is Contagious: r/CovIdiots (2021). https://www.reddit.com/r/CovIdiots/
67. Hill, K. A Vast Web of Vengeance. The New York Times (30 January 2021). https://www.nytimes.com/2021/01/30/technology/change-my-google-results.html
68. Mullen, P.E., Pathe, M., Purcell, R. and Stuart, G.W. Study of Stalkers, American J. of Psychiatry, 156(8), 1244-1249 (1999).
69. Fox News. 2 North Carolina High School Students Charged with Cyber Stalking for Fake MySpace Page, Fox News (13 January 2015), https://www.foxnews.com/story/2-north-carolina-high-school-students-charged-with-cyber-stalking-for-fake-myspace-page
70. Cohen-Almagor, R. Confronting the Internet's Dark Side. Cambridge University Press (2015).
71. Riedel, C. The Fight Against Cyberbullying, The Journal (5 January 2008), http://thejournal.com/articles/2008/05/01/the-fight-against-cyberbullying.aspx
72. Rheingold, H. The Emerging Wireless Internet Will Both Improve and Degrade Human Life, in Head T (ed), The Future of the Internet (Farmington Hills, MI: Greenhaven Press (2005).
73. Department for Digital, Culture, Media & Sport. Online Harms White Paper (2020). https://www.gov.uk/government/consultations/online-harms-white-paper
74. House of Lords Communications and Digital Committee. Free for all? Freedom of expression in the digital age (July 22 2021), https://publications.parliament.uk/pa/ld5802/ldselect/ldcomuni/54/54.pdf