Introduction

Victims of cybercrime on the small ‘i’ internet

Elena Martellozzo and Emma A. Jane

Two decades ago, academic texts about The Internet usually started with some solid ‘ooh-ing’ and ‘ahh-ing’. ‘My goodness!’ late 1990s Elena Martellozzo and Emma A. Jane might have gushed. ‘The novelty, possibility, and sheer size of the thing! Whoever can believe it?!’ Before long, however, we would have moved onto the important business of ‘oh no!-ing’. ‘Don’t start celebrating too early,’ we would have warned. ‘This place of limitless possibility has a dark side.’ Cue the scholarly equivalent of Macaulay Culkin’s screaming face from the Home Alone franchise (this was the late 1990s, after all). Then, as we walked you through the futuristic new world of ‘computer crime’, you might well have wondered how any of these cutting edge offences could ever possibly be understood, regulated, or prosecuted using existing apparatus because they were occurring in that hallucinogenic parallel universe known as The Cybersphere.

We’ll talk more about these bipolar swings in thinking about cyberspace (it’s all good/it’s all bad) in a moment. For the time being, we draw your attention to the fact that something extraordinary has happened: the place that was once thought to have the power to both fix and break everything has become ordinary. In 2011, the communications professor Klaus Bruhn Jensen observed that – in stark contrast to early visions of the internet as an extraordinary place full of identity experiments, avant-garde artworks, and innovative business models – the cybersphere was in the process of ‘becoming ordinary’ (2011, p. 47). More recently, the technology writer Nilay Patel marvelled at the way the ‘research science pipe dream’ of networking all the world’s computers had become ‘a necessary condition of economic and social development, from government and university labs to kitchen tables and city streets’ (2014). Given that the network is interwoven into every moment of our lives, Patel’s neat point is that we no longer do things on the internet, we just do things (2014).

In fact, the internet has become so run-of-the-mill, so what’s-all-the-fuss-about, that – after a lengthy, linguistic tug-of-war – it is gradually succumbing to the irresistible force of decapitalisation. While ‘Internet’ is still deployed in contexts requiring formal and prescriptive usage, the linguist Susan C. Herring notes that the use of the capital ‘I’ in such cases can make a writer or publication appear ‘stuffy and out-of-date’ (2015). Her view is that the lower-case version will ‘eventually win the day … driven by age-old principles of language change’
We concur. What’s more, we think this process of decapitalisation – so closely linked to the process of ‘ordinary-fication’ – also works well as a metaphor for the changing nature of scholarly research into crime and victimisation online.

In the early years of internet studies, many scholars in many disciplines seemed struck by both shock and awe when they cast their concepts and their research questionnaires around the cybersphere (Barker and Jane 2016, p. 463). Indeed, it may be hard for digital natives – that is, those who have always known the internet – to understand just how revolutionary these new digital technologies were to those of us who grew up in households without a computer, let alone a computer connected to everyone else’s computers. (Jane, for instance, started her career as a cadet journalist at a time when people in open plan offices smoked cigarettes at their desks, and newsrooms still contained some actual typewriters and rotary dial phones.) The ‘shock of the new’ posed by cyberspace helps explain why so much early thinking about the internet – particularly thinking about regulation, crime, and victimisation on the internet – seesawed so wildly between cyber-utopianism and cyber-dystopianism.

For an example of the cyber-utopian view, we can look to John Perry Barlow’s ‘A declaration of the independence of cyberspace’. This famous/infamous manifesto from 1996 introduced cyberspace as ‘the new home of Mind’, a place where all could enter ‘without privilege or prejudice accorded by race, economic power, military force, or station of birth’. It was to be a world ‘where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity’. Firmly throwing down the gauntlet to industrial governments, Barlow declared that traditional regulators had no moral right to rule online, and no methods of enforcement cyberspace dwellers had true reason to fear:

You are not welcome among us. You have no sovereignty where we gather.... You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don’t exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

(Barlow 1996)

The optimism/naiveté is striking. In the context of this edited collection, it is also interesting to note who and what are being framed as the victims here. Barlow’s implication is that it is traditional regulators – those ‘weary giants of flesh and steel’ – who have become antiquated and atrophied, outwitted by virtual citizens connected via the hive mind. They are presented as victims of their own hubris and materiality. Yet another set of victims in this scenario are those citizens in the offline world who have fallen foul not only of the putative legislative overreach of the weary giants, but of the race, gender, and class inequities that would
supposedly be eliminated online. In this view of the cybersphere, e-citizens are not victims but agents empowered via the dual forces of self-governance and virtuality.

Compare Barlow’s idealistic vision of a problem-free, self-regulating cybersphere to one presented around the same time in a book on cybercrime called *I-Way Robbery: Crime on the Internet* (Boni and Kovacich 1999). The foreword of this volume, by Professor Emeritus John P. Kenney, begins with a textbook version of the ‘ooh-ing’ and ‘ahh-ing’ described in the first paragraph of our introduction. Kenney marvels at the profound impact of the ‘global Internet or “I-Way”’ on personal relationships, international politics, and business (Kenney in Boni and Kovacich 1999, p. ix). He notes that the internet is user-friendly for many people ‘from children and housewives in the home … to corporate managers and farmers’. Kenney quickly warns, however, that in addition to the exploits of ‘hackers, phreakers, and crackers’, ‘ominous’ new crimes and criminal enterprises mean most industrial nations have become ‘vulnerable to the ravages of techno-terrorists and cyber-criminals employing the “I-Way” to wreak havoc’ (Kenney in Boni and Kovacich 1999, p. ix). The book goes on to offer, among much else, a chapter which profiles the various ‘miscreants’ one may encounter while using the I-Way for business or government purposes (Boni and Kovacich 1999, pp. 69–100).

Two decades or so later, neither the utopian nor the dystopian framings of cyberspace pass the ‘Goldilocks standard’ of seeming quite right. Barlow was correct about its revolutionary nature, as well as about the issue of ‘sovereignty’ (as it relates to jurisdictional issues) and the relative impotence of traditional regulators in online domains. Sadly, he was wrong to imagine this would be a place free from ‘real’ problems like crime or structural discrimination. Contrary to his idealistic vision, violence and victimisation are occurring online in ways which directly mirror or are very similar to the offline world, and have not been solved in-house. Indeed, as Jane discusses in her chapter of this book, some internet dwellers are making things much worse for people who have already been victimised online. Books such as *I-Way Robbery*, meanwhile, were right to identify the threats posed by various bad actors online (even if language such as ‘ominous’, ‘ravages’, and ‘miscreants’ seems somewhat overblown). Yet they fail to capture the fact that most internet transactions are notable only for their absolute lack of note-ability.

Without wishing to underplay the very real harms caused by crime and victimisation online, it is important to remember that the vast bulk of online engagement and interactions are banal, often taking forms such as shopping, banking, making small talk with friends, and reminding significant others to please pick up some tofu on their way home from work. Just as Hollywood’s canon of serial killer movies can give a false impression of the true extent of Hannibal Lecterism, the ‘shock horror’ media coverage given to the most extreme examples of cybercrime can obscure the fact that most of our time online is positive and problem-free. In curating this book, therefore, we have done our best to offer nuanced contributions that are neither overly triumphalist nor sensationall
alarmist in tone. We proceed from the view that the online world is much the same as the offline one: mostly fine, but occasionally profoundly not fine (with members of traditionally marginalised, excluded, and oppressed groups far more likely to be victimised than those with greater privilege).

One obvious advantage of the ‘ordinary-fication’ of the internet is that the increasing familiarity of the territory is lending itself to more textured scholarly work less reliant on unhelpful binaries such as the cyber-utopian versus cyber-dystopian framings discussed above. This is certainly the type of scholarship we have aimed to showcase in this volume. That said, we note that familiarity presents its own research challenges. For instance, certain features of the cyber-sphere can quickly seem so natural and indisputable that it is assumed these features always have and always will be part of cyberspace. Writing on Google and ‘the culture of search’, for instance, Ken Hillis, Michael Petit, and Kylie Jarrett note that to search has become ‘so natural and obvious a condition of using the Web, and the Web such a natural and obvious feature of the internet, that the specific contingency of these everyday practices has become obscured’ (2013, p. 2). This is the flipside of overemphasis, exaggeration, and sensationalisation.

Consider, for example, the proliferation of hate speech online, and the way many users have learned to ‘see but not see’ the graphic misogynist, racist, and homophobic comments that now swamp comment sections (Barker and Jane 2016, p. 463). Such habituated blindness may well assist internet users navigate the internet efficiently, but it can also result in the downplaying or overlooking of significant social problems (Jane 2015, p. 73). As we in academia recover from being shocked by the new, therefore, we must also ensure we are not blinded by the obvious – or to assume that all the important questions about the internet have already been answered.

With regard to knowledge gaps, for instance, we note that while there is now a great deal of awareness about the internet’s role in giving rise to potentially empowering new forms of self-identity and social relationships, the ways in which online social relationships are engendering new forms of violence and victimisation are less clearly understood. Certainly the general topic of the intersection of the internet and law could do with more attention. In Matthew Lippman’s Contemporary Criminal Law: Concepts, Cases, and Controversies (2013), for example, ‘computer crime’ and related terms appear on only nine pages (this includes cyberstalking and cyberbullying). The other main topics covered are copyright infringements, trespass (unauthorised access to computers), and causing computers to malfunction. And this is in a text book for college students with 560 pages not including notes or index!

Fortunately, other texts are emerging which respond not only to the urgent need for greater scholar coverage of cybercrime, but to the necessity of constantly updating this coverage. In the preface to the second edition of Cybercrime and Society, for example, Majid Yar, acknowledges the ‘perishable’ nature of books on internet crime (2013). He notes that the 2005 edition of his text made no mention of Facebook because the social media platform was then in its infancy. As we know, baby platforms can grow up fast in the cybersphere. These
days, Facebook is a behemoth and well on the way to – as one writer puts it – ‘eating the internet’ (Lafrance 2015). In late 2016, there were more than 1.71 billion monthly active Facebook users, with 300 million photos uploaded every day and five new profiles created every second (‘The top 20 valuable Facebook statistics – updated September 2016’ 2016).

Like Yar, we acknowledge that there is only so much a book about the internet can do to remain up-to-date (especially if that book also happens to be made out of dead trees). Literature relating to the cybersphere inevitably dates extremely quickly and it is easy for a text such as this to seem embarrassingly outdated to student readers who are constantly exploring new platforms and apps online. Indeed, some internet insiders joke that internet years are like dog years in that each single year sees about seven years’ worth of change (Bland 2016). This would mean we have been working on this book for nearly two decades! Aware that new legislation and platform changes are occurring constantly, we have attempted to make this volume as time-resistant as possible, partly by focusing on the sorts of broad trends and principles we believe will continue to have relevance over time, even if the examples best used to illustrate them change.

Our aim is to help fill knowledge gaps relating to victimisation online by exploring the social construction of violence and victimisation in online spaces in three key ways. First, we examine the ways in which the unique social structures, spaces and interactions that have taken shape in cyberspace over the past two decades have engendered distinctive forms of problematic behaviour, violence and victimisation. Second, we show how social processes of violence and victimisation in online spaces are tied into broader social formations of crime and violence. Third, we consider new and enhanced approaches to the prevention of violence, crime, and victimisation in online spaces.

To achieve these ends, we adopt a transnational and interdisciplinary perspective, exploring cybercrime, and violence and victimisation in a range of international settings. Our intentions are to foreground the experiences of victims and targets, to offer insight into emerging criminal practices, and model the usefulness of interdisciplinary perspectives and interdisciplinary conversations in this area. The tricky balancing acts we undertake include attempting: to avoid being alarmist without facilitating complacency; to offer a big picture perspective without losing sight of individual experiences and case studies; and to balance empirical and prevalence data and statistics with the human faces of cybercrime. At all times, we endeavour to avoid unhelpful extremes. That is, we avoid framings of the cybersphere which are either overly utopian or overly dystopian, which formulate discrete divisions between the online and offline, or which buy into all-or-nothing approaches to intervention. This recognises that the internet is not all safety or all danger; all risk or all possibility. Instead, like any other place where humans congregate, it involves shades of grey rather than stark blacks and whites.

Rather than being prescriptive, or offering simplistic solutions, therefore, we wish to propose a series of open-ended questions that prompt readers to
contemplate the complexity of cybercrime. These include (but are by no means limited to):

- Does cyberspace make us more or less vulnerable to crime and violence?
- Under what circumstances might ‘cyberwrong’ (see Chapter 1) be a better term than ‘cybercrime’?
- In what ways does cyberspace challenge prejudice and the stereotyping of marginalised groups, and in what ways does it reproduce, reinforce and amplify these offline phenomena?
- In what ways (if any) should online regulatory interventions differ from the offline variety? That is, are there special circumstances relating to crime on the web or should cyberspace be considered as just another jurisdiction or criminal context?
- How much regulation online is too much or too little?
- What are some of the competing values involved in questions around regulation online? For example, when should freedom of speech and expression be protected at the expense of those suffering abuse, harassment and victimisation? Is the free speech defence being misused? Or is it not being given adequate consideration by regulators?
- Given the increasing public pressure on states to act, is there a danger of ad hoc, knee-jerk policy making that is not fit-for-purpose, or which rapidly dates? How might we best avoid this type of policy making?
- Where should the role of state regulation end and the role of communities, schools, and individual users begin?
- Should platform managers be held responsible for the activities of their users?
- How do crime and violence in online spaces give rise to new forms of surveillance and social control?
- What role might technology design have in preventing crime and violence online in future?

The complexity of crime online

To understand the perspective of the victims of cybercrime (as well as the victims of what Nicole A Vincent calls cyberwrongs) it is first necessary to understand the offences; how they occur, and how the internet may enable perpetrators to commit them. Again, the dynamism of the cybersphere makes this task daunting given the dizzying speeds at which platforms and usage patterns materialise and de-materialise. (At the time of writing, for instance, Jane’s nine-year-old daughter was fixing her mother with a withering look of techno-contempt while explaining that the term ‘muser’ referred to a user of the app ‘musical.ly’ [‘duh, mum’] which happened to be 2016’s answer to ‘Dubsmash’ and whose intricacies could not possibly be comprehended by anyone as ancient as her parent.)

The internet and its multitude of interconnected devices are indeed singular in terms of speed and uptake. For example, it took broadcast radio 38 years and
television 13 to clock up their first 50 million users, while the web achieved this number in just four years (Naughton 2014). This makes the internet the fastest growing medium ever recorded. In 2016, around 40 per cent of the world’s population had an internet connection (compared to less than 1 per cent in 1995), and there were nearly three-and-a-half billion internet users across the globe (‘Internet Users’ n. d.). As the stop watch-style counter at www.internetlivestats.com/internet-users/ demonstrates so graphically, this figure was continuing to rise at a rate of knots (for want of a more digitally savvy metaphor).

New technologies have always posed a challenge for regulators at the state level (police and policy makers) as well as those presiding over domestic jurisdictions (in the form of parents and caretakers). (For example, Martellozzo, in her chapter, observes that children and young people are often more technosavvy than their caregivers, as well as being more physically mobile, in that they are able to use internet-enabled devices in potentially riskier contexts outside of home environments.) Yet while new modes of criminality are indeed coming into being far faster than various regulators are able to keep pace with them, many instances of online crime bearing striking resemblances to offline variations – and vice versa. The Australian Crime Commission (now part of the Australian Criminal Intelligence Commission), lists a number of traditional crimes and their cybercrime equivalents (‘Cyber and technology enabled crime’ 2013, p. 2). These include: fraud (the cybercrime equivalents being online fraud, and mass marketed fraud including auction fraud, advance free fraud, and phishing); burglary and malicious damage (online hacking, denial of service attacks, viruses); child sex offences (online grooming, child pornography websites); money laundering (through online payment systems and e-cash); and theft (identity theft, bank website phishing, and movie, music and software piracy).

Stalking, bullying, and domestic violence have also developed distinct online versions, including various forms of technology-facilitated and technology-amplified abuse, harassment, and coercion. There is, for example, emerging research into the links between online abuse and offline domestic violence against women. The UK organisation Women’s Aid, notes that 48 per cent of UK women who suffer violence at the hands of a partner experience harassment or online abuse during their relationship as well as once they have left it, with 38 per cent of women being stalked online after they leave their relationships (Smith 2014). Such figures also demonstrate the way violent partners and ex-partners are able to use the internet to incite others to join their attacks: in effect, to crowdsources harassment. There have also been increases in the use and abuse of new communication and surveillance technologies to stalk, intimidate, harass, humiliate, and coerce intimate partners, particularly girls and women (Ostini and Hopkins 2015). This includes: using electronic means to remove women’s access to their bank account funds; preventing friends and family members from being able to reach women via their phones and computers; installing GPS trackers on women’s vehicles; and circulating false and/or intimate information about women online (Ostini and Hopkins 2015). Understanding these sorts of offences requires thinking beyond a simple and arguably overly narrow framework of
"cybercrime" and understanding their overlap with more traditional offences and wrongs, as well as their reflection of broad, structural inequalities.

A useful case study which provides insights into some of the key features of – and regulatory challenges posed by – cybercrime concerns the online trade of illicit drugs. Intriguingly enough, the world’s first commercial transaction online is said to have been a drug deal. Students at Stanford University used Arpanet accounts to arrange the sale of ‘an undetermined amount of marijuana’ to their counterparts at Massachusetts Institute of Technology (John Markoff cited in Power 2013b). Since then, vast quantities of recreational drugs have been traded on encrypted sections of the net using the untraceable online currency Bitcoin (Martin 2014; Ball 2013). Indeed, one 2013 survey suggests that nearly a quarter of all users are buying drugs online, making the internet a rival to laneways and street corners as a place to buy illicit drugs (Ball 2013). These purchases often occur via channels such as Silk Road which has been dubbed an ‘eBay for drugs’ and has been closed down multiple times by multiple authorities (Ball 2013). The online drug trade poses challenges for regulators in that the substances available online are often technically legal because their chemical compounds are very similar to illicit substances yet are different enough to bypass existing laws (Power 2013a, 2013b). Without wishing to take sides in the heated debate about whether adult drug users constitute ‘victims’, it is worth noting that the unknown and unpredictable formulations in what are known as ‘synthetic’ drugs can make them potentially very dangerous for users (Barker and Jane 2016, p. 185). Again, however, it is important not to overinflate the risks associated with new drugs being sold in new domains given that substances purchased in offline contexts may also be cut with unknown and potentially harmful substances.

The trade of illicit (and illicitish) drugs online also draws attention to the nature and significance of what is known as the ‘deep web’. This term refers to the fact that only about four per cent of the information available on the internet can be accessed using commercial search engines. The other 96 per cent of content comprises what is known as the deep web (Bradley 2014). Given that nearly five billion pages are available in the visible, surface or clear web, the size of this hidden dimension is truly extraordinary (Barker and Jane 2016, p. 492). It is important to remember, however, that most of this content in this part of the web is banal in that it includes material such as user databases, webmail pages, registration-required web forums, pages behind paywalls and website pages that have been created but are yet to go ‘live’ (Egan 2015).

There is, however, a subsection of the deep web known as the ‘dark web’. Material here cannot be found using traditional search engines. Access, therefore, requires a degree of cyber savvy as well as the use of browsers such as The Onion Router (Tor) which obscure physical locations, as well as permitting access to sites that might otherwise be blocked (Bradley 2014). While there has been no shortage of sensational media reports drawing attention to those sectors of the dark web used for the trade of drugs, child abuse images, weapons, and criminal services, people are also making use of this intriguing – and currently extremely understudied – sector of the internet for political reasons. In ‘closed,
totalitarian societies’ the dark web can be used to communicate with the outside world (Egan 2015). Internet users are also said to be moving their communication onto the dark web in the light of ‘recent revelations about US and UK government snooping on web use’ (Egan 2015).

The deep and dark web offer rich directions for future scholarly inquiry as very little academic research has been conducted on these aspects of the internet. An exception is the work of Robert W. Gehl (2014) who conducted an ethnographic study of a social networking site only accessible to web browsers equipped with Tor. Gehl’s conclusions about the Dark Web Social Network (DWSN) are that its norms and ideals have much in common with the early days of the internet in participants’ rejection of state-based intervention and call for disembodied communication dissociated from putatively superficial identity markers such as race or gender. Unlike the pioneers of the early internet, however, the critical stance is being taken not in opposition to the offline world but to the intensely corporatized and surveilled ‘clear web’ (Barker and Jane 2016, p. 493).

While many crimes online do have similarities with those committed offline, some aspects of digital spaces are singular in nature. As such, offences committed online may have elements and idiosyncrasies which their offline counterparts do not. Consider, for instance, the ‘always-on’, omni-connected aspects of contemporary existence. As various contributors to this collection show, the reach enabled by technology combined with the ‘always-on’ nature of modern life means perpetrators have the potential to tyrannise targets in new and perfidious ways.

A cogent example is sextortion – an emerging criminal practice in which perpetrators gain remote access to computers to obtain intimate or compromising footage of targets who are then blackmailed into performing sex acts (thereby becoming entrapped even further). The US coder Luis Mijangos, for instance, hacked into hundreds of computers and installed sophisticated, antivirus software-resistant malware that allowed him to track targets’ keyboard activity, to search their hard drives, and to remotely operate their web cams (Kushner 2012). Wheelchair-bound and living at home with his mother in California, Mijangos – later dubbed a candidate for the title ‘world’s creepiest hacker’ – spent days on end watching multiple targets on up to four web cams at once – each spying on a different victim (Kushner 2012). He boasted to his peers that he had found a way to control up to 600 computers simultaneously and spread the word that his services were available to others wishing to spy on girlfriends, wives, or unsuspecting strangers (Kushner 2012). When US law enforcement agents finally arrested Mijangos in March 2010, he had more than 15,000 webcam-video captures, 900 audio recordings, and 13,000 screen captures associated with around 230 women and teenaged girls from around the world – 44 of whom were minors and one of whom lived as far away as New Zealand (Wittes et al. 2016, p. 2).

The case study of sextortion shows the way a single offender is able to use technology to victimise large numbers of people located anywhere in the world.
It also demonstrates the fact that new modes of online violence and victimisation may not fit easily into pre-existing criminal categories such as ‘theft’, ‘sexual assault’, or ‘stalking’. Sextortion, for instance, can involve elements of stalking, home invasion, theft, blackmail, paedophilia, domestic violence, sexual exploitation, harassment, and abuse, and organised crime. This creates obvious problems for police and prosecutors, and has resulted in regrettable inconsistencies with regards to sentencing. In a 2016 report analysing 78 sextortion cases, researchers from the Brookings think tank note that – given no crime of ‘sextortion’ exists in the US – cases in that nation have proceeded under a ‘hodgepodge’ of state and federal laws including ‘actions under the most dimly-related of statutes’ (Wittes et al. 2016, pp. 4–5). This has produced what the researchers condemn as ‘indefensible’ disparities in sentencing (Wittes et al. 2016, p. 5). Mijangos, for instance, was sentenced to six years’ imprisonment which is ‘dramatically lighter’ than he would have received for multiple physical attacks on even a fraction of the number of people he was accused of victimising (Wittes et al. 2016, pp. 2, 5). In another case analysed by Brookings Institution, a perpetrator received only three years in prison for victimising up to 22 young boys (Wittes et al. 2016, p. 5).

Like many other emerging crimes in digital spaces, sextortion is dramatically under-studied. Brookings’ researchers note that while sextortion is an acknowledged problem within law enforcement and among private advocates, no government agency or private advocacy group publishes data on its prevalence, and the subject lacks a body of academic literature (Wittes et al. 2016, p. 4). The lack of understanding about new forms of violence and victimisation online is due, in part, to various issues of visibility. The crimes themselves may be invisible if they are so new they are yet to register on the public’s radar (let alone be written into law). If arrests are not being made, and offenders are not being processed by the courts, neither will such crimes be visible to the public. Further, as Brookings points out in relation to sextortion, the frequency with which offences are occurring cannot be measured to determine prevalence.

There are, however, some paradoxical elements relating to the issue of cybercrime and visibility. While some violence and victimisation online is urgently in need of more attention and exposure, certain offences involve victims who desperately want less eyes on their situations. Two examples are the victims of revenge porn (a term used to describe the malicious circulation of intimate images without the consent of the subject) and doxing (the circulation of targets’ personal details online, sometimes accompanied by an incitement to others to attack targets online or offline). If a victim is a child, their case may be kept out of the limelight for their own protection. In such instances, concealing aspects of a crime makes sense. Other invisibility issues are, however, more insidious. Sometimes victims do not come forward because they want to avoid further shame and embarrassment. As Martellozzo explains in her chapter, victims of online child sexual abuse may never come forward because they do not realise that what they have experienced is abuse. Sometimes victims do report their experiences to police, but no action is taken because they are not believed or taken seriously.
In other cases, victims are invisible because they are not recognised as victims. Consider women targeted for revenge porn. As with offline sexual violence, it is often implied or stated explicitly that such women are to blame for their experiences because they trusted the wrong men, posed for the wrong photos, and so on (see Chapter 3). Victim-blaming also occurs when the targets of various cybercrimes are framed as being insufficiently tech savvy, as over-reacting or being too sensitive to the rough and tumble of online life, or as being opposed to the ideals of free speech. Often they are accused of not being able to take a joke, or of not appreciating the edgy humour of the cybersphere. In these ways, targets are recast not only as the problem but as the solution to the problem, in that they are encouraged to undertake do-it-yourself (DIY) measures to remedy their situations. This is profoundly unfair, and ignores the fact that—among many other potential problems—different internet users have different resources available for self-help in this regard.

Failing to act with regard to online violence and victimisation may also strengthen extrajudicial cultures online as manifest in digital vigilantism—or ‘digilantism’—tactics such as ‘hacktivism’, ‘scam-baiting’, ‘denial-of-service attacks’, and ‘naming and shaming’ (Jane 2016a, 2016b, 2016c). Like offline vigilantism, online versions of vigilantism cannot (by definition) be legally justified. They can, however, be morally justified, and possibly even morally demanded, if there exists a social need alongside deficiencies in the state security system (Jane 2016b, 2016c). Said, our view is that such actions should be regarded as diagnostic of rather than solutions to state security deficits. This is because—again, like offline vigilantism—digilantism has many risks and downsides. Consider, for instance, the rapid formation of vicious online mobs whose public shaming of individuals might be disproportionate to or even worse than the originally objectionable behaviour or action.

Cogent, here, is the case of the PR professional Justine Sacco who, in 2013, tweeted the following comment shortly before boarding a flight to South Africa: ‘Going to Africa. Hope I don’t get AIDS. Just kidding. I’m white’ (cited in Ronson 2015b). Sacco has always insisted the comment was intended to parody American ignorance about HIV, but the wider public viewed it as offensively racist. As a result, Sacco disembarked from her 11-hour flight from Heathrow to Cape Town to discover that mob attacks on her online had rendered her ‘the number-one worldwide trend on Twitter’ (cited in Ronson 2015a, p. 65). Sacco was subsequently sacked. Reflecting on this and other similar public shaming cases, the author Jon Ronson notes the disconnect between ‘the severity of the crime’—frequently some poorly considered joke on social media—and the ‘gleeful savagery’ of the vigilante mob punishment (2015b).

Different but related to digilantism is the problem of corporate exploitation of people who have been targeted for violence and victimisation online. Danielle Keats Citron and Mary Anne Franks, for instance, note the existence of web sites which publish revenge porn and then charge the pictured individuals to have the material removed (2014). A 28-year-old San Diego man, Kevin Bollaert, ran a revenge porn site called ugotposted.com featuring the sexually explicit photographs,
full names, location details, and Facebook profiles of thousands of women and men (`Revenge porn kingpin Kevin Bollaert jailed' 2015). Bollaert also ran a companion ‘takedown’ site called changemyreputation.com which charged up to $350 for the removal of photos. In 2015, he was jailed for 18 years in what was described as the first case of its kind in US criminal history (`Revenge porn kingpin Kevin Bollaert jailed' 2015). The importance of possessing a positive online reputation has also led to a proliferation of professionals who charge clients for cyber ‘makeovers’ which involve promoting positive content while attempt to bury negative search engine results (Barker and Jane 2016, p. 488). While such businesses are neither illegal nor comparable to the unscrupulous business ventures conducted by individuals such as Bollaert, they do show the vulnerability of those victimised online, as well as the fact that the ability to buy oneself out of reputational strife is not an option equally available to all. Such options costs upwards of US$1,000 a month (Lock 2013) and are therefore only feasible for those with the means to pay.

There also exists a regrettable – and deeply unfair – tendency to suggest that victims of cybercrime are not real victims because the offences occur in a virtual domain and therefore cannot possibly involve ‘real’ harm. Heated debates about the differences between ‘harm’ and ‘offense’ have a long history, particularly with regard to how they should impact law-making and freedom of expression. These issues will be addressed in the conclusion of this book where we appraise various regulatory and non-regulatory responses to cybercrimes and cyber-wrongs. While it is beyond the scope of this book to deal with the subject in any depth, we also note advances in neurophysiology and cellular biology which show that cognition, emotion, and social context can be even more influential than tissue damage in terms of producing physical pain (Moseley 2007; Moseley 2011; Moseley et al., 2012; Butler and Moseley 2013). This complicates the ability to make neat distinctions between ‘embodied’ injuries that cause physical pain, and ‘ disembodied’ injuries that cause what might be dismissed as different and/or lesser sorts of suffering. In particular, the ‘medicosociolegal’ nature of the modern world (Moseley et al. 2012, p. 37) means such findings are becoming increasingly relevant in legal contexts involving the consideration of harms or injuries that are not visible to the naked eye or apparent in medical scans (see: Jane 2016; Davis 2016).

In addition to this research, there is good evidence to show that many victims of attacks in online domains suffer real, material harms in the offline world. This is starkly demonstrated by the impact statements of victims of sexually violent crimes online. The Brookings researchers who studied sextortion, for instance, underline the fact that this is a crime of often ‘unspeakable brutality’ (Wittes et al. 2016, p. 3). The prosecutor in the Mijangos case, for instance, noted that some of Mijangos’ victims thoroughly feared him and continued to be traumatised by his criminal conduct on an ongoing basis. One victim reported feeling ‘terrorized’ and did not leave her dorm room for a week after the episode (Wittes et al. 2016, p. 2). Other victims demonstrated signs of immense psychological stress. Disturbingly, the Brookings researchers noted that perpetrators seemed to revel in the desperate pleas of their scared and under-aged victims:
In multiple cases we have reviewed, victims contemplate, threaten, or even attempt suicide – sometimes to the apparent pleasure of their tormentors. At least two cases involve either a father or stepfather tormenting children living in his house. Some of the victims are very young. And the impacts on victims can be severe and likely lasting. Many cases result, after all, in images permanently on the Internet on multiple child pornography sites following extended periods of coercion.

(Wittes et al. 2016, p. 5, internal references omitted)

We can see that the suffering of victims of crimes such as sextortion and revenge porn is unlikely to end just because a perpetrator is arrested and even imprisoned. In addition to the ongoing impact of the initial degradation and trauma, it is all but impossible to stop intimate images and footage circulating once such material makes its way onto the internet. This is the sort of evil genie that is impossible to return to its bottle and the psychological harm caused to victims aware that their images are freely travelling around the web is severe. Similarly, sexual offences against children and young people recorded on video or in still photographs may be kept for personal gratification, like trophies sitting on a dusty shelf, or may be distributed online to other abusers. Further, producing, downloading, storing, and viewing such material can increase the demand and, as the result, the continuation of the cycle of victimisation (Martellozzo 2012, p. 76). It is well rehearsed in the literature, for instance, that re-victimisation occurs each time an image of child abuse is downloaded and/or shared (Taylor and Quayle 2003, p. 24).

The harms caused by reputational damage online can also be severe and ongoing. Findings from the Pew Research Center, for instance, show that of those people targeted for physical threats and sustained harassment online, about a third feel their reputations have been damaged (Duggan 2014, p. 7). Citron’s research, meanwhile, reveals that female teachers and government employees have been fired after naked photos of them appeared on revenge porn sites or were otherwise circulated publicly (2014b). To understand how the harm in such situations is not just a one-off affair, consider the fact that nearly 80 per cent of employers consult search engines to collect intelligence on job applicants, and about 70 per cent of applicants are rejected because of these findings (Citron 2014c). Common reasons for not interviewing and hiring applicants include concerns about ‘lifestyle’, ‘inappropriate’ online comments, and ‘unsuitable’ photographs, videos, and information (Citron 2014b). These aspects of cybercrime and cyberwrongs underline the fact that – as various contributors argue throughout this collection – criminal law may be of limited use to victims.

Why, then, consider legal remedies at all? Our case is that while law is only one element of what must be a multifaceted approach to cybercrime, it is, none-theless, an important element. Many states are becoming increasingly sophisticated about how the physical infrastructure of the internet is monitored and controlled (Suzor 2016). Yet the atmosphere in many online domains remains one of impunity. As the Australian legal scholar Nicolas Suzor, puts it:
many parts of the open internet are, to put it mildly, not nice places. The infrastructure we’ve built allows everyone to speak, but all-too-often drowns out and silences voices from the more vulnerable groups in our societies. It is used as a highly effective tool to direct abuse and hate against minorities, to invade the privacy of those who speak out, and to enable violence, chilling threats, and coordinated attacks. (2016)

As simplistic as it may sound, a critical first step in bringing perpetrators to account is to identify perpetrators as perpetrators. Among other problems, the victim-blaming narratives and tendencies described above contribute to the invisibilising and exculpation of bad actors online. After all, if people who are attacked or scammed online are also blamed for being attacked or scammed, perpetrators are neatly written out of the narratives. Offenders are also invisibilised when the cybersphere is framed as either a lawless Wild West or as inherently dangerous – that is, a place where trouble should be expected, and people should only visit if they have thick skins, or special training. Once again, these frontier-style framings facilitate victim-blaming in that targets are chastised for having gone to the ‘wrong’ places, for engaging in the ‘wrong’ sort of behaviour online, for clicking ‘reply’ on the wrong sort of email, and so on. At the same time, perpetrators are exculpated and permitted to continue offending without fear of punishment because the danger is linguistically located in the landscape rather than in the harm-producing human agents who inhabit this landscape (see Chapter 3).

An increased understanding about and focus on the perspective of victims is necessary to help provide immediate relief for those people who are currently being attacked or abused and who may need assistance extricating themselves from volatile situations that have the potential to rapidly worsen in a way that can have ongoing and potentially irreversible impacts. To work towards a culture of accountability online, a culture that reinforces the ideals of fairness, justice, and equity of access, victim-blaming needs to stop and, where feasible and appropriate, the punishing of perpetrators needs to start. These punishments might include the loss of certain online privileges, or they might include fines, community service, and/or imprisonment. A range of potential remedies and interventions for cybercrimes and cyberwrongs will be discussed throughout this volume, and particularly in the conclusion.

Like our contributors, we acknowledge that addressing cybercrime is no easy task. As discussed earlier in this introduction, such offences are notoriously difficult to investigate and prosecute because they play out in domains where perpetrators are often difficult to identify, where victims may be reluctant (or may not even realise it is an option to) report offences, and where police often lack the requisite resources and the techno-savvy to act. On those occasions where police are successful in making a cybercrime-related arrest, it may be discovered that an act is legally liminal or not covered by existing legislation – not least because prosecutors in many nations are relying on laws drafted for a pre-internet age. In the UK, the chief constable responsible for fighting digital crime,
Stephen Kavanagh, has admitted that the ‘unimagined scale of online abuse’ threatens to overwhelm the police service (cited in Laville 2016). Noting that existing laws include one dating back to the nineteenth century, Kavanagh has called for new and more simplified legislation in the hope of achieving justice for tens of thousands of targets (cited in Laville 2016).

Without wishing to point fingers, we agree that – while the contours of the cybersphere are indeed novel and constantly changing – there is validity in activist claims that police, policy makers, and platform managers could be working faster and more effectively to assist targets and victims in online environments. Rather than continuing to drag their collective metaphorical feet, we believe these bodies should move faster and more effectively. They must acknowledge the vertiginous pace of developments in communications technology, take it for granted that new forms of criminality will continue to emerge fast and furiously, and plan – and act – accordingly. As various authors featured in this collection argue, community groups, schools, technology designers, online groups, and individual users also have important roles to play.

**On targets, victims, and ‘victims’**

Different contributors to this book are more comfortable with the use of the term ‘victim’ than others. Jane, for instance, explains in her chapter that she prefers the term ‘target’, although she does refer to ‘victim-blaming’ for idiomatic reasons. In her disciplinary areas, there is an emphasis on the tremendous power of words to either enhance or distract from people’s agency, and their ability to not only survive but to thrive after even indubitably dreadful experiences. That said, she notes that the keenness of some cultural studies scholars to emphasise agency and empowerment may inadvertently overlook or underplay the real suffering and harm of those targeted for cybercrime and cyberwrongs.

Martellozzo, meanwhile, in her chapter more readily uses ‘victim’ terminology in reflection of its legal meaning, that is, ‘a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence’ (www.cps.gov.uk). She purposely deploys the term ‘victim’ to emphasise the harms children and young people suffer if they are targeted, groomed, and victimised online. Like other contributors in this book, she recognises that developing effective interventions requires looking closely at the empirical evidence that reveals some of the harsh realities of what occurs in the intangible and somewhat obscure word of cyberspace.

Regardless of the different terminology used, however, together we are interested in exploring a textured, mid-ground approach. This is not intended to underplay or overlook the violence involved in cybercrime and cyberwrongs, but to acknowledge that targets and victims are not necessarily forever violated, but potentially able to engage in healing and resistance that might permit them to move on.

Our nuanced approach is also designed to recognise that robust public disagreement exists about who should and should not be categorised as a victim
with regards to emerging social problems online. Consider, as just one prominent example, public dispute over the case of Edward Snowden. In 2013, the former National Security Agency (NSA) analyst leaked classified information showing the full extent of American domestic and global surveillance, specifically, that American spies now have the ability to track the activities and movements of anyone almost anywhere in the world. Snowden’s actions kickstarted highly charged debates about — among many other issues — how best to balance freedom and security in the post-9/11 era. While it seems indubitable that Snowden broke US laws relating to espionage, whether or not he should be seen as a victim or a victimiser is hotly debated. His detractors, for example, see his actions as unforgivably traitorous and guilty of treason that put US troops at risk and worked to the advantage of terrorists. To supporters, however, Snowden is a patriot and courageous whistleblower who sacrificed his career and his life in the US (at the time of writing he was living in exile in Russia) in order to draw attention to America’s ‘digital totalitarianism’ (Sigmar Gabriel cited in Koepf 2013). The Snowden case study shows that the victim/victimiser distinction is not always clear cut.

Further, some individuals who seem more like perpetrators make dubious claims to victim status. An apt example involves the origins of GamerGate — the term for the series of extraordinary and ongoing attacks on, among others, female video gamers, journalists, academics, and social justice activists from 2014. GamerGate began when a software developer named Eron Gjoni posted a 10,000-word blog impugning the personal and professional reputation of his former girlfriend, Zoë Quinn. He implied, for instance, that she had slept with a games journalist in order to obtain positive reviews for a game she had designed — a claim he later withdrew, saying it was a typographical error (Jane 2016, pp. 29–30). Gjoni’s behaviour was extremely questionable. As Quinn later testified in a Boston court while obtaining a restraining order (that Gjoni was to breach on multiple occasions), he had deliberately besmirched her professional reputation as well as coaching and egging on a ‘hate mob’ (cited in Jason 2015). Members of the latter had circulated personal details such as Quinn’s phone number and home address, alongside photos of her naked (Quinn cited in Jason 2015). Gjoni, however, continues to insist that he is the victim — a survivor of Quinn’s ‘emotional abuse’ no less (Gjoni 2014). An addendum to his initial blog apologises if other emotional abuse survivors find his story triggering, and provides a link to a domestic violence hotline (Gjoni 2014).

Another scenario in which the victim/victimiser line is murky involves the en masse leak, in July 2015, of the details of users of a Canada-based website which facilitates cheating in marriage and whose logo is ‘Life is short. Have an affair’. A total of 30 gigabytes of Ashley Madison data (Zetter 2015) — including names, phone numbers, and other personal details — were published online in what one journalist called ‘the most appallingly intimate internet leak of the modern age’ (Lamont 2016). Schadenfreude reigned as media and other commentators said they felt no pity for the individuals exposed, not least because of the ‘stupidity factor’ involved in signing up for such a site (Ellen 2015). Others, however, saw
these millions of users as victims because they had been assured that their use of
the service would be ‘anonymous’ and ‘100% discreet’. It was reported that res-
ignations, divorces, and even suicides followed the exposé (Lamont 2016).
Further, apparently, 1,200 of the leaked email addresses had suffixes indicating
that users lived in Saudi Arabia, a country where adultery is punishable by death
(Girl on the Net 2016). In Alabama, meanwhile, a newspaper decided to print all
the names of people from the region who appeared on Ashley Madison’s data-
base (Lamont 2016). In addition to illustrating the aforementioned risks associ-
ated with vigilante tactics, the Ashley Madison case study shows the special
problems facing those targets who do not fit the stereotype of the ‘perfect’
victim.

Overview of approaches and chapter breakdown

Violence and victimisation in online spaces are of considerable interest to
scholars from many areas of inquiry, including sociology, criminology, and cul-
tural, media, and gender studies. As such, we believe one of the strengths of this
book is its interdisciplinarity. Martellozzo’s background is in criminology and
her particular interests include exploring children and young people’s online
behaviour, and the analysis of online sexual grooming, sexual exploitation, and
police practice in the area of child sexual abuse. Jane comes predominantly from
a cultural, media, and gender studies background, but now works with an
increasing focus on philosophy – especially with regard to aretæic or ‘virtue’
ethics. In addition to formulating concrete interventions for cybercrime in a prac-
tical sense, she is also interested in more abstract ideas relating to the ethics of
online engagement, and how best to cultivate a culture of accountability online.

Some of the challenges we faced in assembling this book are challenges
which also arise in addressing the very problems about which we write. A lack
of communication between scholars from different disciplines working in the
field, for instance, can contribute to the rise of unhelpful knowledge ‘silos’. We
have, however, attempted to turn these challenges to our advantage by deliber-
ately seeking contributions from a range of disciplines, and inviting contributors
to ‘translate’ discipline-specific terms and paradigms. We believe that conversa-
tions between scholars from different departments and nations are important for
tackling the broader problem of violence and victimisation online, just as dia-
logue between institutions (for example, between police, policy makers, platform
managers, community groups, and schools) is also essential.

As mentioned earlier (and explored in detail in Chapter 1), many of the cases
discussed in this volume are legally liminal or better referred to as ‘cyberwrongs’
– that is, they cannot be classified as ‘cybercrimes’ in an uncomplicated way.
Again, we believe this is one of the strengths rather than one of the limitations of
the book. One of our aims is to stimulate thinking and debate about how best to
classify emerging practices online. As such, we invite readers to consider the
problematic acts discussed in this book as belonging to two broad categories.
The first are those acts which are currently recognised as crimes, and perhaps
which have non-computer-related analogues (such as unauthorised trespass/access, damage, theft, and so on). A second group contains those acts which are currently not recognised as crimes or are on the penumbra. In relation to this second group, we can see that there exists a wrong and perhaps we can also see that these acts involve harms to victims. But either they are not currently recognized as crimes and/or they do not have simple analogues in non-computer-related domains. A key dilemma identified by this book is how the slow-moving and largely victim-disregarding criminal law might respond to acts located in this second category.

The book is organised thematically into five main sections. The first aims to address some broad conceptual issues and contains two chapters. Chapter 1 sets the scene for this collection. In it, Vincent offers crucial definitions and critically presents two groups of reasons as to why victims of cybercrime are marginalised by the criminal law. Furthermore, she provides some theoretical background to and perspectives on the many hurdles and needs outlined by other contributors to this collection. In Chapter 2, Chris Brickell presents three theoretical frameworks to help us think systematically about power in relation to the internet, particularly in relation to ‘digital sexuality’.

The focus of Part II – which contains four chapters – is concerned with issues relating to sexual violence, abuse, and exploitation, as well as to sexual expression online. Chapter 3 looks at the problem of gendered cyberhate such as rape threats and revenge porn. Through the use of current case studies, Jane provides an overview of the common manifestations and significant harms of contemporary misogyny online and explains how the inadequate responses of police, policy makers, and platform managers are contributing to the proliferation of those crimes. In Chapter 4, Amy Dobson explores the growing issue of ‘sexting’ media practices within a gendered social, cultural, historical, and technological context. Her contribution unpacks the ways in which the ‘risks’ and ‘harms’ of sexting media practices, frequently understood as inherent to digital sexual image exchange, are socially and culturally determined.

Chapters 5 and 6 examine issues surrounding the sexual exploitation of adults, children and young people. Kristine Hickle, in Chapter 5, looks at the current research on internet-facilitated commercial sexual exploitation, and explains how cyberspace provides a new terrain for traffickers to recruit, blackmail, exchange, and advertise victims to potential sex buyers who are also complicit in the victimisation of both children and adults. It also explores how new technologies play a crucial part in creating new opportunities to exploit people and facilitating exploitation. In Chapter 6, Martellozzo focuses on online sexual grooming, types of online groomers, and some of the risk factors affecting the likelihood of children and young people becoming victims of online sexual abuse.

The third, pivotal section of the book addresses issues related to race and culture. In Chapter 7, Jamie Cleland looks at online racial hatred speech and the way in which virtual spaces may act as platforms for of racial and discriminatory discourses.
Ramaswami Harindranath, in Chapter 8, examines relatively recent concerns regarding the use of the internet and social media for alleged recruitment and propaganda purposes by Islamic extremists, and the ways in which this has contributed to increasing public anxieties, especially in Europe, the US, and Australia. His case is that media and official discourse on counter-radicalisation can impact negatively on minorities of colour, resulting in a double victimisation of such minorities: first by acts of terror and then by policies to counter radicalisation.

The two final chapters of the collection address concern cyberbullying and online suicide – topics we group together as ‘social violence’. In Chapter 9, Robin Kowalski and Gary Giumetti provide an overview of cyberbullying, including how cyberbullying is typically defined, the prevalence rates of cyberbullying across varying demographics, and antecedents and consequences of involvement in cyberbullying. Chapter 10 looks at how some distinctive features of the internet have allowed the formation of close-knit communities meeting in online forums to discuss matters related to suicide. In this chapter, Ronald Niezen argues that suicide forums tend to be rigorous, rational, and instrumentally effective when it comes to exchanging information on the techniques of self-inflicted death. He explores the possibility that the internet facilitates a normalisation of suicide, looking at whether and under what circumstances the cybersphere might encourage or provoke, and/or discourage and hedge against acts of self-destruction.

In the fifth and concluding section of this book, Jane and Vincent argue that victims of cybercrime are, in general, neglected and not receiving the recognition and support they need and deserve. They argue that although continued awareness-raising and education are important for bringing attention to the plight of victims in online spaces, it does not constitute a sustainable solution to the problems targets and victims face daily. Further, they argue that while law might offer some benefits for some victims of some crimes in some jurisdictions, a multitude of non-legislative responses must also be adopted in order to truly make a difference.

The aspiration of this book

As with the ugliest corners of the offline world, the cybersphere contains many dark shadows which are unregulated and unmonitored, and where people have the ability to behave in ways that cause real suffering to others. We sincerely hope that this book will draw some much-needed attention to the various forms of harms that can be inflicted online. In our conclusion, we argue that there needs to be an increase in support of all kinds for victims, as well as an increase in the exposure and punishment of perpetrators. We discuss the role which could be played by not only increased legislation, but by novel approaches such as value sensitive design and ‘nudge’ techniques. Going forwards, we hope this collection feeds into and helps inform policing and policy-making in multiple jurisdictions, as well as inspiring others to engage in more research, especially of an interdisciplinary nature.
Notes

1 While definitions of ‘phishing’ vary, it usually refers to a form of online identity theft that allows the stealing of personal identity data and financial account credentials. This might take the form of sending forged emails to recipients mimicking a legitimate institution and requesting details such as credit card numbers or bank account passwords (Dunham et al. 2009, p. 128).

2 ‘Hacktivism’ – a portmanteau of ‘hacking’ and ‘activism’ – refers to the unauthorized access to and disruption of computer systems in the name of socio-political agendas.

3 Scam-baiting’ is the practice of turning the tables on internet scammers by scamming them back.

4 A ‘denial-of-service’ (DoS) or ‘distributed denial-of-service’ (DDoS) attack results in a computer or online network becoming unavailable to users.

References


Introduction


Jane, E.A. 2016c (in press), ‘Feminist digilante responses to a slut-shaming on Facebook’, Social Media and Society, accepted for publication 1 September, 2016.


Power, M. 2013b, ‘Online highs are old as the net: the first e-commerce was a drugs deal’, *The Guardian*, 19 April, viewed 28 June 2016, www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal


Part I

Conceptual issues