Children groomed by online predators, revenge porn victims extorted by unscrupulous internet entrepreneurs, Muslim community members targeted for racialised cyberhate…. Many of the contributors to this book have painted a grim picture of the various ways victims of cybercrimes are suffering, and the multiple ways law is failing to assist. Clearly something is not right here. However, while it is one thing to identify new problems, it is quite another to figure out what to do. Especially when the domains in which these problems are playing out are novel, complex, and extremely volatile.

It could be argued that those victimised online are currently being neglected because insufficient attention is being paid to their plight. Yet the existence of this book is testimony to the fact that – while victims of crime and other problems online may not be receiving as much recognition as they need and deserve – they are not entirely invisible. Continued awareness-raising is essential for bringing attention to the plight of victims in online spaces. This might help address the relative lack of knowledgeability on the part of front-line respondents such as police and prosecutors (Citron, 2014, pp. 83–91), as well as the sorts of victim-blaming outlined in Chapter 3. But sensitisation and education strategies alone will not constitute a remedy.

Others might make the case that it is legislators who are dropping the ball, and that what is urgently needed are new or revised laws. We are not so sure. Implicit in Chapter 1 is a provocative question. Namely: are the sorts of social problems outlined in this collection best understood as having come about as a result of deficits in law, or are they more to do with a surplus of unrealistic expectations of law? Our view is that both the first and second part of this question can be answered in the affirmative. That is, we agree that some new and improved legislation is required to better reflect the realities of the cybersphere (laws relating to horse-drawn carts only retaining utility for so long after a dirt track becomes a six-lane highway). But we also suspect there is overconfidence in exactly how much can be achieved by law – particularly when it comes to meeting the needs of victims.

Given that the focus of this collection is international, we will not here be offering specific suggestions about which laws in which nations are deficient or non-existent, and therefore require attention from policy makers. Neither will we
be providing precise details about exactly how these laws should be written or revised. While we acknowledge that law reform is important, the staggeringly large number of jurisdictions and legislative contexts involved in cybercrime scenes means that meaningful research, critique, and recommendations must be situated at the local level (even if what are ultimately required are inter-jurisdictional responses). Attempting to sketch all the cybercrime-related legislative change that might be beneficial for all people in all nations of the world is beyond the scope not only of this single text, but, we would argue, of any single text. Instead, we urge our colleagues to prioritise research in this area, and to communicate with and lobby policy makers as a matter of urgency. By the same token, we urge policy makers to take these matters seriously and begin the processes necessary to determine what changes might be required in law – both in terms of regulating the conduct of individuals, as well as of service providers and platform managers.

While law might offer some benefits for some victims of some crimes in some jurisdictions, however, our overall argument is that these must be supplemented by a multitude of non-legislative responses in order to truly make a difference. In this final section of the book, therefore, we return to the two harsh, legislative realities detailed in Chapter 1. First, that criminal law – by its very nature – does not make a good ally for victims of any crimes. And, second, that the special features of online environments present yet another set of obstacles to the prosecution of those who have committed cybercrimes (these relating to jurisdictional issues, the identification of offenders, and the high standards of proof required to secure criminal convictions).

While we do acknowledge that the legislative odds are stacked against the victims of cybercrime, we also explain why this does not mean we should give up in despair. Specifically, we outline a non-legislative approach which shifts the focus away from the slow-moving mechanisms and blunt instrumentality of the criminal justice system, and towards a focus on – among other strategies – designing technology in a way that ‘nudges’ people towards better behaviour online.

In a nutshell, our proposal is that criminologists, social scientists, and ethicists work alongside engineers and technology experts in designing, deploying, testing, and engaging in the ongoing re-evaluation of information communication technologies so as to produce better ‘moral technologies’ – that is, devices, platforms, and systems that encourage ethical conduct and provide fewer opportunities for unethical behaviour. Such approaches are guided by work in political philosophy, philosophy of technology, and ethics of technology, and have a number of advantages. Unlike changes in criminal law, for instance, technological interventions can be devised and implemented swiftly. Technology-based approaches are also unconstrained by state borders which greatly inhibit legislative responses. As such, rather than being a runner-up or second-best to legislative responses, we argue that such approaches are as or even more important than legal responses for assisting the victims of cybercrime in a timely, sensitive, and effective manner. Further, they are approaches which are likely to be
extremely useful for many other social problems stemming from technological innovation.

Cybercrimes or cyberwrongs?

To set the stage for this discussion, we revisit the broad concern that, technically-speaking, it is an open question whether the sorts of things we have in mind when we speak of ‘cybercrimes’ are indeed even bona fide crimes. We then argue that trying to get them recognised as crimes may be very difficult. Even if we recognise that serious things are at stake in cybercrimes, it could be (and indeed very often is) argued that these are things involving acts that are not as unequivocally serious as threats to life and limb. As such, progressives and conservatives are both likely to be disinclined to accept the curtailment of liberty that recognising these as criminal offences would necessarily entail. To further spell out this argument, we return to the case studies of sextortion and cyberhate, and make use of the discussion of John Stuart Mill’s harm principle (1859, I.9) from Chapter 1.

As explained in the Introduction and Chapter 3, sextortion involves obtaining sexually explicit pictures of a victim, and then threatening to post them onto public fora unless the victim provides yet further sexually explicit material, thus exposing themselves to even greater potential to be sextorted by the offender in the future (Wittes et al., 2016). Currently, although offenders who commit sextortion can be charged with and prosecuted for such offences as computer hacking, wiretapping, stalking, paedophilia, and harassment, they cannot actually be charged and prosecuted specifically for sextortion-specific offences because (at least in the US) no such offence is currently defined within state or federal criminal statutes. Benjamin Wittes and colleagues thus observe that, as a consequence:

There is no consistency in the prosecution of sextortion cases. Because no crime of sextortion exists, the cases proceed under a hodgepodge of state and federal laws. Some are prosecuted as child pornography cases. Some are prosecuted as hacking cases. Some are prosecuted as extortions. Some are prosecuted as stalkings. Conduct that seems remarkably similar to an outside observer produces actions under the most dimly-related of statutes. (2016, pp. 4–5)

This state of affairs is arguably bad for everyone involved. The public has no guidance about what conduct is prohibited, victims lack certainty about whether and what kind of protection and remedies they might seek and obtain, and people found guilty of essentially identical conduct receive punishments of widely divergent kinds and severities. From an economic perspective this ad hoc approach is also tremendously inefficient since, for each case, state prosecutors’ and defense attorneys’ time is taken up in debate that may have simply been avoided with better-formulated laws that function effectively as guides and deterrents. To remedy this problem, Wittes and colleagues thus recommend that:
Given that these cases are numerous, many are interstate in nature, and most being prosecuted federally anyway, Congress should consider adopting a federal sextortion statute that addresses the specific conduct at issue in sextortion cases and does not treat the age of the victim as a core element of the offense. [T]his statute should combine elements of the federal interstate extortion statute with elements of the aggravated sexual abuse statute and have sentencing that parallels physical-world sexual assaults. State lawmakers should likewise adopt strong statutes with criminal penalties commensurate with the harm sextortion cases do. In our view, states should both criminalise the production and distribution of nonconsensual pornography and give victims of it reasonable civil remedies against their victimisers. In combination with a federal statute, this would create a number of avenues for victims to pursue.

(2016, pp. 26–27)

The case that Wittes and colleagues are making is that because sextortion is harmful, legislation should be enacted so that courts can recognise this cyberwrong as a cybercrime. Similar reasoning could presumably also be used to support a case in favour of criminalising other cyberwrongs, for instance like the gendered cyberhate discussed in Chapter 3. At present, women and girls worldwide are not uniformly protected from explicit, sexualised vitriol, rape threats, and revenge porn by the criminal justice system qua ‘gendered cyberhate’ because no crime of gendered cyberhate currently exists. Individual cases of rape threats have been successfully prosecuted, as have jilted lovers who posted sexually explicit photographs of their ex-partners on revenge porn web sites. However, the cases are prosecuted under the banner of existing criminal offences, not specifically under the banner of ‘gendered cyberhate’ offences. Thus, extending Wittes and colleagues’ reasoning, it could be argued that because gendered cyberhate is also harmful, legislation should be enacted to enable courts to recognise this cyberwrong as a cybercrime too.

We share Wittes and colleagues’ view that sextortion is harmful (as is cyberhate, cyberbullying, racialised abuse, and other examples discussed in this volume). As Chapter 1 argued, however, appeals to harmfulness as a basis for criminalising conduct are likely to strike unhelpful hurdles. After all, laws that protect people from cyberhate and/or other cyberharms wouldn’t just make some people (i.e. potential victims) better off. They would also make other people (namely, those who would otherwise engage in that conduct) worse off. For instance, cyberhaters routinely insist they are actually cybercommentators who are harmlessly exercising their right to freedom of speech. If laws were created that removed their freedom to engage in this conduct, they – alongside staunch supporters of free speech as an ideal – would likely strongly object to the state taking steps that would deprive them of their current freedoms. For this reason, when the state contemplates creating legislation that prohibits certain conduct for the benefit of one group of people through the mechanism of the criminal law, it must also consider how much harm this course of action would inflict.
Conclusion beyond law

onto another group of people whose liberty would be curtailed by such legislation. But since the degree of harm in cyberhate is not as unambiguously great as, for instance, murder, attempts to gather broad public support for such legislation will likely get mired in lengthy, murky, and ultimately unproductive debate; for instance, over whether what is at stake for potential victims is truly harmful as opposed to merely offensive, and, if harmful, over whether the degree of harm is sufficiently great to warrant inflicting the correlative harm of restricting potential cyberhaters’ liberty.

Regardless of whether we think cyberhate is harmful, and regardless of whether we think that the freedom to engage in cyberhating conduct is not a freedom that anyone should be entitled to exercise in the first place, the state (which creates laws that govern everyone) must adopt an impartial position and thus consider opposing views if such exist. Unfortunately, what this means in practice is that if others don’t see things our way, and if they can present a sufficiently plausible case to warrant further inquiry, then the debate that is likely to ensue is bound to be long and unproductive. Abstracting away from the example of cyberhate, our point is that criminalisation of cyberwrongs is not a promising strategy for cases which are likely to generate murky debate about whether the conduct in question is sufficiently harmful, whether victims can mitigate their harm just by choosing to not take offence, and whether it is more harmful than curtailing the liberty of those whose conduct would be criminalised.

Furthermore, it is also important to keep in mind that law reform is a very slow and resource-demanding process because of the built-in legal inertia which favours the status quo over the new and reformative. It may be tempting to view this legal inertia as a fault with how the law functions. However, when considered against the backdrop of constant political pressures to accept change in this or that direction driven by populist appeal to views du jour, this inertia may actually be a source of comfort even to progressive folks, since it offers protection from potentially reactionary changes being made to society. Finally, given that internet phenomena are often fast-paced and short-lived, reform of the criminal justice system has little chance of keeping pace with technological changes. This includes keeping pace with responding to new ways in which online fora may create opportunities for cyber-victimisation, and thus taking adequate account of the interests of victims of cybercrime.

For such reasons, investing much effort into criminal justice system reform so that it can take better account of the harms suffered by victims is not an ideal plan, at least not if this is the only thing we plan to do.

Civil remedies

But if not (only) through criminal law reform, then how else could we respond to cyberwrongs, cyberharms, or cyberoffences (or whatever other terminology we adopt to recognise the plight of those who have been victimised – though not necessarily as the result of a criminal offence)? Wittes and colleagues also recommend providing ‘victims … reasonable civil remedies against their
victimizers’ (2016, p. 27). As argued in Chapter 1, civil remedies do indeed give plaintiffs more explicit recognition, control, and pride of place than what the criminal law does. Furthermore, the threat of being sued is likely to have some general deterrence effects, as long as potential offenders know they may be sued and they are in a situation to think far enough ahead before they act, to stop themselves from doing what they would otherwise regret (see below for further discussion).

There are, however, problems with civil remedies, too. One is that civil litigation is costly (Willging and Lee, 2010), and this can create barriers to entry for plaintiffs who cannot afford up-front fees to finance litigation. This costliness is also likely to present a barrier to victims of relatively more minor cyberharms. For instance, in potential cases that would involve defendants who inflict many tiny cyberharms on many separate victims (Wall, 2007), no individual plaintiff would ever have sufficient financial incentive (in the form of a prospect of receiving compensation from a successful lawsuit) to warrant litigating. Furthermore, for the civil law approach to work, we would still need to build up society’s recognition of the way in which things like gendered cyberhate and sextortion genuinely harm their victims, and thus why they should be treated as potentially compensable harms. Admittedly, the barriers to recognition here, by comparison to those present in the context of the criminal law, are likely to be smaller. After all, recognising that these are genuine harms will not result in anyone being prohibited from engaging in the respective conduct, but only potentially open them up to being sued. However, the decision to protect people by offering them the remedy of pursuing a lawsuit, rather than by outright prohibition of the harmful behaviour, is problematic too because it converts objectionable behaviour into de facto permissible behaviour — permissible, that is, as long as whoever engages in it is prepared to compensate their victims. The prospect of converting objectionable behaviour into in-effect, retrospective judge-brokered financial transactions, where people can commit offences with impunity as long as they subsequently compensate their victims, is distasteful and wrong.

What is needed is for these offences to simply not happen in the first place, and, given the concerns we expressed above regarding the effectiveness and propriety of legal approaches (i.e. criminal sanctions and civil law remedies), it might be tempting to suppose that perhaps another way to change people’s behaviour is through better education campaigns targeted at potential offenders. However, although we do not wish to discourage such efforts – just as we do not intend to discourage efforts to reform the law – our concern with this suggestion is that educating people about the consequences of their actions still has limited capacity to effect behavioural change. After all, people may simply remain unconvinced. But even when people are genuinely convinced, they still often fail to act in accordance with their own considered judgments (see below).

For this reason, in the next section we will consider two groups of theories from political philosophy and ethics of technology regarding how to effect behavioural change through smarter design of environments and technologies –
namely, so-called ‘nudge’ techniques and value sensitive design (VSD), both of which fall under the broader umbrella heading of ‘moral technologies’. Instead of trying to change people’s minds at the conscious level through reason-giving practices – for example, by creating threats of criminal sanction or of being sued, or by trying to convince anyone through explicit education (and then hoping that convincing them to think differently will lead them to act differently) – these moral technologies aim to alter people’s behaviour and its outcomes by changing the environments in which people act. Specifically, they aim to change environments and artefacts in order to prompt better behaviour, to foster better outcomes, and to promote the values that we as a society wish to promote.

Enter nudge

To understand what nudge techniques are and why they might be useful, we shall begin by considering an example from the political domain (concerning retirement savings plans) developed by Richard Thaler and Cass Sunstein (2009), as discussed recently by Jeremy Waldron (2014). After the example is presented, we will then comment on the core ideas that nudge techniques employ, and indicate how we think these same ideas could also be deployed to foster better behaviour and better outcomes in interactions in online environments. We will finish by considering some objections to nudging.

Here is Thaler and Sunstein’s (2009) example: presumably, few people would savour the prospect of being poor in their old age, and, from this perspective, it makes sense to put a small portion of our income away into a retirement savings plan dedicated specifically to providing adequately for our financial needs in our old age. However, despite this, and despite the fact that governments go to considerable lengths to educate and entice the public to subscribe to better retirement plans, many people still fail to do this. Why? Evidently, not because they remain unconvinced that this is what would serve their own best interests, but for such mundane and all-too-human reasons as because they get distracted and fail to sign up for a savings plan, or because their resolve to do so weakens in the face of temptations (for example, purchasing airfares for a luxurious holiday), or because they lack the relevant knowledge and thus under-estimate their future needs or over-estimate the minor proximal costs of making slightly larger contributions to their retirement savings plans to finance the distal outcome of having an adequate income in their old age.

A consequence of this is that many people have woefully inadequate retirement savings plans. Not because they want things that way, but because the way things are currently arranged is such that, unless people explicitly choose to save up for their retirement, by default they will be saving nothing (or not enough). This outcome, in other words, is not a consequence of people’s express choices – it is not what people genuinely want and what they explicitly choose – but it is rather just a consequence of the way that things are currently set up, so that by default, nothing (or not enough) is put away for retirement. However, things could be set up differently: by default, more money could automatically be set
aside from people’s incomes, and, if some people really do object to this, then there is nothing preventing us from giving them an option to alter their contributions (i.e. an option to opt-out from the default setup). At least setting things up this way would ensure that by default (i.e. even if nobody makes any decisions whatsoever) everyone would have sufficient income in their retirement. Furthermore, to ensure that people do not make weighty decisions whimsically, we could also set things up such that to lower one’s retirement plan contributions, a person must go through a more complicated and involved process. Not to prevent anyone from lowering their contributions if that is what they truly desire, since that would be paternalistic and objectionable on grounds that it would infringe on individual liberty. But just to give them time to fully think through this weighty decision.

At the core of nudge techniques are three closely-linked ideas. One, that people generally act in predictable ways, and that the mind sciences and social sciences – for example, psychology and anthropology – can be used to illuminate this. Two, that all actions, including inaction, have some outcome by default, and that this outcome is not an immutable fact of nature, but something that it is in our power to set as we see fit. And, three, that for liberty to be respected, nobody should be forced to engage in any action, nor to pursue any particular outcome, though they should be given sufficient opportunity to consider the ramifications of their decisions. Interplay between these three ideas explains why Sunstein and Thaler suggest that governments should set up default retirement savings plans from which people can, by going to some effort, withdraw, in order to ensure that citizens get a better outcome vis-à-vis retirement incomes through a liberty-preserving process – i.e. one that nudges people into doing what they would most probably want to do anyway, but that at the same time also enables anyone who wants to resist the nudges to do so.

In summary, ‘nudge’ techniques make use of research in the mind and social sciences to reveal how people behave as a general rule and what factors can influence people’s behaviour. This information is then factored into the design of environments in which people live and interact. And the intention is that, by default, people’s interactions would then take desirable rather than undesirable forms, and generate desirable rather than undesirable outcomes. While the option to pursue undesirable forms of conduct would still remain, engaging in these forms of conduct would take additional effort (since they would be a departure from the default) and thus would be less attractive (but not impossible) to pursue.

Turning now to our re-deployment of this idea, as a first approximation to what this might look like vis-à-vis the design of online interactive environments, consider a computer interface deliberately formulated to encourage the use of standardised responses. That is, the fastest and easiest method of using this interface to interact with other people would be to express opinions through likes, favouriting, re-tweeting, thumbs-ups, +1s, and so on, and presumably also through negatively-valenced variants such as dislikes, thumbs-downs, and –1s. Users would still have the option of entering text responses, but this option
would require a greater investment of time and effort, perhaps because permission would be required from the post’s author for the comment to appear, or perhaps because entering text would simply require a more convoluted and time-consuming procedure which would discourage users from engaging in that mode of interaction. A minor variant on this approach might be to create a more nuanced dictionary of iconic expressions which still give people the option of expressing a wide array of disapproving sentiments, but which remove some of the sting involved in highly-personalised textual comments. These particular suggestions are untested, and they are only intended to convey some initial ideas, rather than to solve concrete problems. As such, we strongly encourage further empirical studies to ascertain precisely which methods of shaping human conduct in online environments might have the potential of reducing the incidence and/or severity of cyber-victimisation and cyberharm.

Critiques of nudge

Nudging is a subtle form of influence, and this gives rise to at least two distinct forms of criticism. On the one hand, one disadvantage of subtle techniques is their fallibility – i.e. that it is quite possible to resist them. In other words, internet users who wish to be vile and harmful will still be able to do so with relatively little effort. However, it is precisely the subtlety of the verb “to nudge” that makes this technique easier to defend (at least from a perspective that is mindful of infringements on liberty) than, say, something along the lines of a ‘coerce technique’ or a ‘shove technique’. Yes, internet users intent on being vile and harmful would still be able to act in these ways. But, given the incidence of violent crime throughout the world, those who strongly wish to be vile and to do harm to others will (unfortunately) probably always find ways to do so. Consequently, we think it is more realistic to aim not at 100 per cent compliance or 100 per cent eradication of cyberoffences, but rather at a significant reduction of their occurrence through the design of interactive environments in such ways that they discourage undesirable conduct and guide users into pro-social interactions. Again: the aim of our earlier critique of legal responses to cyberharms in this conclusion was not to discourage efforts to reform the legal system altogether, but only to highlight the limits of these approaches so that we do not end up relying solely on those strategies. Hence, even if nudging does not provide a fool proof method for completely eradicating cyberharms, we do not see this as a problem since our ultimate aim in this chapter has been to draw attention to other remedies we could also develop in order to ensure that this group of victims is catered for more adequately, as opposed to finding one, single fool proof strategy.

On the other hand, a less obvious but perhaps more troubling form of criticism of subtle forms of influence, by comparison with more overt forms of influence, is that they can be more difficult to notice, insidious, and thus difficult to resist. This makes them more akin to sinister forms of manipulation and social
engineering, not unlike that depicted in George Orwell’s *Nineteen Eighty-Four* (1949). In this famous dystopian novel, language was itself fashioned and crafted in line with the political ideology of the fictional totalitarian government of Oceania in an attempt to make not only the expression but potentially the very thinking and conceiving of certain things impossible. The way in which Sunstein (2015) deflects the accusation of Orwell-like totalitarianism in relation to nudge is to point out that the aim is not to make it impossible for people to express themselves in violent ways, but only to make it more difficult for them to do so. By creating an outlet for cyberoffending – albeit a difficult or awkward one to use – we do sacrifice 100 per cent effectiveness or 100 per cent compliance. However, we also avoid the dilemma faced by the criminalisation of cyberconduct that sits at the penumbra of harm and offence. People retain the ability to do what is wrong, but they are provided with disincentives to exercise that ability, as well as incentives (for example, in the form of ease of interaction through pre-fabricated responses) to engage in pro-social conduct.

In summary, at the core of nudge techniques are two closely linked – and perhaps somewhat odd-sounding – ideas. These acknowledge: (1) the power of people doing nothing; and (2) the importance of ensuring people still have the option of behaving badly. The first idea recognises that even doing nothing will generate some outcome by default. Thus one way of improving outcomes in any given sphere of human conduct is to alter what comes about by default. (In other words, to change what happens if people do nothing.) The second idea responds to libertarian objections about the use of state force. It notes that compelling people to behave in this or that way violates liberty, even if those violations are supposedly in the name of good. One way to preserve liberty and avoid the charge of compulsion is to give people the option of behaving in ways that go against what is otherwise deemed right. This option should, however, be discouraged by designing-in hurdles that make that conduct more difficult and less attractive.

Taken together, the design of default choice architectures (the first idea) and the deployment of insights into human psychology to discourage bad conduct and encourage good conduct (the second idea), potentially provide a liberty-respecting approach to the design of all kinds of environments. If it is used to fashion interaction in pro-social ways in online environments, it is plausible that this method could reduce the incidence of cyberoffending by funnelling people’s behaviour in pro-social directions. This would not be a fool proof approach, but it could stem the number of offences and even create more opportunities for positive encounters.

**Value sensitive design**

Nudge is a technique intended to shape how humans behave by modifying their environments. Its potential to better respond to the needs of victims and their harms relies on the idea that shaping human interactions in online environments through better design of those environments might reduce cyberoffending.
Another, similar approach is what Batya Friedman et al. refer to as ‘value sensitive design’ (VSD), that is, ‘a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process’ (2008, p. 70). Like nudge techniques, the value sensitive design approach recognises the fact that the way we design technology strongly influences how that technology is used. Thus it is possible to influence usage patterns if we think carefully at the design stage about the types of behaviours we value, and to craft our new devices and systems in a way that supports these.

Given the popular misconception that technology is ethically neutral (and that humans are the source of moral and social problems when they use technology in unethical ways), it is helpful to consider two examples which illustrate the way values are built into the technologies that we make and use. Consider a touch-screen combination lock by the side of a door, and a closed circuit television camera monitoring system. Both examples involve the value of security in one sense or another. However, the first device might score poorly in regards to the value of equality. After all, visually impaired people may have trouble using touch screens. On the other hand, the second device may compromise the value of privacy, perhaps by inadvertently recording the identities of people engaged in normal but private affairs, rather than just those engaged in prohibited conduct. Thus, if the value of equality is also important, then a different security lock might need to be fitted (not one that relies upon its user being sighted). And if the value of privacy is important, then maybe a new security camera system will need to be developed and fitted – for instance, one that automatically blurs the faces of all people and maybe any other identifying markers or private information, unless an incident happens, in which case a supervisor with a sufficiently high security clearance can view the footage without the blurring filters applied.

The point of these examples is twofold. One, to highlight the way in which three particular values – namely security, equality, and privacy – might manifest themselves in different implementations of two kinds of security devices. Two, to highlight how deployment of some technologies rather than others can generate ethical problems, though not because any specific humans use the technologies in unethical ways, but because the technologies were designed in ways that failed to adequately accommodate important values. However, there are other values we could consider such as sustainability and efficiency. It is notable that the more values we consider and try to accommodate in the design of technology, the more we may discover tensions between different values at the design stage. Imagine, for instance, that we do also care about efficiency. A proximity detector-based lock might be very efficient, but it might come at the cost of the value of security. Importantly, we are not here asserting which of these values is more important than the others. Rather, we are pointing out that the values that are embedded into technology – technology that we design – can come into conflict with one another and this conflict among values embedded in technology may be in need of resolution.
When used as a methodology, value sensitive design requires that we make explicit the values we wish our technologies to promote (rather than leaving it up to accident and just hoping for the best). It is also demands that we treat these ethical requirements as sitting side-by-side with functional requirements at the stage when technology is designed. So, from this perspective, instead of bemoaning the fact that a proximity-activated locking device cannot satisfy both of the values we wish it to satisfy (for example, security and efficiency), this ethical dilemma is turned in the eyes of a value sensitive design engineer into a technical problem. Namely, the challenge is to design an artefact that not only satisfies the strict functional requirements of locks, but also the ethical requirements we want locks to meet. Something similar can be said about the CCTV security camera example. If privacy and sustainability are also as important as security, then what we should ask our engineers to design are security cameras that will achieve all three of those moral aims in order to accommodate all of those values.

So how might this work in the context of cybercrime and its victims? The first step would be to use the methods described in value sensitive design literature to identify the kinds of values that are compromised when cyberoffenders harm cybervictims – not least by identifying the harms involved. The next step would involve working alongside software engineers to develop technologies that would safeguard and promote those values. One example of this kind of effort is Mireille Hildebrand’s discussion of a ‘proactive technological infrastructure’ – a ‘so-called “vision of Ambient Law”’ which builds ‘legal protection into the ICT architecture, to safeguard our rights and freedoms within the various cyberspaces we inhabit’ (2011, p. 223). A more recent example is provided by Maryam Al Hinaï and Ruzanna Chitchyan (2015) who describe their design of a software system that caters for the value of equality (even though we personally find their particular suggestions vis-à-vis gender objectionable).

Closing thoughts

Taking a step back from the important question of precisely how environments and artefacts could be designed to better secure the interests of victims of cybercrime, we can make the following observations. One way to view the ethical and moral problems that we encounter in this book – the harms that some people inflict on others through interactions in online environments – is as human-created problems for which solutions should be sought in the human domain. For instance, through the law, which, through its system of rules and punishments and so on, addresses itself to people at the conscious level by creating incentives and disincentives to certain forms of behaviour, with the hope of providing people with consciously salient reasons to act in some ways and desist from other ways of acting. Another way to address these problems, though, is to view these as design flaws (that is, that the environments we live in and the artefacts we use have been designed in a manner which permits and maybe even promotes troublesome interactions). Conceptualising these problems in this way
– as challenges to design better moral technologies – means that these problems can potentially be designed out of the equation. Designed, that is, in such a way that it becomes impossible or at least more difficult to engage in undesirable conduct in the cybersphere, and easier and more inviting to engage in desirable conduct.

None of this needs to carry with it the connotation that cyberoffenders are not agents who choose to inflict harm on cybervictims. People can still be blamed for what they do wrong. Rather, the suggestion is simply that if certain uses of information and communication technologies result in forms of harm that we would rather avoid, then one of the methods at our disposal to reduce the incidence of this harm is to investigate how the values that need to be protected from this harm can be secured through the design of better moral technologies. This, to us, is what it would mean to have a truly victim-focused response, rather than an offender-focused one. Just as cyberoffenders should not be treated as devoid of their agency when they commit offenses against their victims, so, too, it is helpful to notice that the technology we create and use is not a value-neutral part of the environment. It is not a piece of nature which, like a hurricane, cannot be blamed when destruction occurs.

Instead of designing artefacts and environments that create, encourage, or enable social problems to occur, and only afterwards stopping to think about how those artefacts could have been designed better to avoid creating those problems, it would be better to think ahead about how these technologies – that is, either the artefacts that we use, or the environments that we inhabit – could be designed in better ways. Lest this sounds vague and fuzzy, consider that even explicitly harmful technologies like guns can these days be designed in ways that make them less likely to be used in prohibited ways – that is, so-called ‘smart guns’ (Sebastian, 2016). As such, there is no in-principle reason why the design of the software through which we engage in internet-mediated interactions with one another could likewise not be designed to be less harmful, that is, to leave less scope for it to be used to harm victims.

In conclusion, our argument is that the best response to cybercrime, and its victims, is the careful deployment of criminal law, alongside: civil litigation; the education of the public and police; the lobbying (and perhaps even the nudging) of internet platform providers to develop their own policies so they are more sensitive to the needs of those who would otherwise be cybercrime victims; and – especially – approaches such as nudge and value sensitive design. This sort of broad, multifaceted response is, we think, the most effective and savvy way to work around the limitations of law so as to address the very real suffering being experienced by victims of cybercrime around the world.

Notes
1 As Wesley Newcombe Hohfeld (1975) famously pointed out, all rights are underpinned by correlative duties. Consequently, the legal protection of one group’s rights invariably comes at the cost of curtailing another group’s liberty. For example, the right to be free from cyberhate imposes a correlative duty on others to not speak to people in ways
that upset them. This curtailment of liberty, rightly or wrongly, is likely to be viewed by potential cyberhaters as a harm.

Producers of cyberhate, for instance, claim that what they produce is merely a form of ‘speech’, and that, as words rather than sticks, stones, or bullets, what is occurring is not the infliction of genuine harm but only the taking of mere offence (Jane, 2017, pp. 109–110). Some opponents of such legislation also argue that the harm suffered by victims of revenge porn and cyberhate could be mitigated by victims if only they chose to not be embarrassed, humiliated, and threatened. Please note that we do not endorse these arguments, but are simply mentioning them as examples of those prosecuted by others.

To proponents of minimal government who view state restrictions of individual liberty as paradigm cases of state wrongdoing, criminalisation of actions that do not involve sticks and stones but only words and hurt feelings (as it would likely be viewed from their perspective) falls into the category of very serious wrongs.

This begs the question regarding whether this is indeed something that people can just choose to not take offence at, though, for brevity, we set this aside.

And a class action may likewise not be attractive for victims to join for precisely the same reason, namely, because the administrative overhead involved with becoming a party to the class action may not be warranted by the small compensation payment one is likely to receive.

The +1 feature allows users of certain internet platforms to either +1 or –1 a comment or a solution in order to up-rate or down-rate the quality of the various responses.

We borrow the second example, and the general shape of the discussion, from Jeroen van den Hoven’s (2014) presentation of the topic. See also van den Hoven (2007) and van den Hoven and Manders-Huits (2009).

Our affront relates to Hinai and Chitchyan’s proposal for how to ensure gender equality in their system. They write, ‘Some values, such as gender equality, can be indirectly supported through ICT by ensuring that gender is not revealed, or is actively hidden when participation or remuneration is concerned’ (2015, p. 35). To our minds, covering up signs of one’s gender on the internet in order to secure equality is almost an expression of the very problem of misogyny online rather than a way of confronting it and securing equality. This is not intended as a criticism, but as an invitation to feminist scholars to engage with those who attempt to secure important values to ensure that patriarchal modes of oppression are not reproduced in the process of trying to secure gender equality.

Or, even less helpfully, asking who is to blame for misusing that technology, which simply pulls focus away from victims and their harms, and redirects it to offenders.

References


Conclusion beyond law 223


Index

to come