International Review of Law, Computers & Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Remote justice: information rights as a tool of empowerment

Mo Egan

To cite this article: Mo Egan (2022): Remote justice: information rights as a tool of empowerment, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2022.2060465

To link to this article: https://doi.org/10.1080/13600869.2022.2060465

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
https://doi.org/10.1080/13600869.2022.2060465

Remote justice: information rights as a tool of empowerment

Mo Egan

Division of Law & Philosophy, University of Stirling, Stirling, UK

ABSTRACT

The coronavirus pandemic has resulted in a compulsory retreat from public spaces. While, for some, this displacement has brought about engagement with digital technologies in new and interesting ways, for others, digital technologies have proved to be the site of technology-facilitated abuse (TFA). Consequently, there are renewed calls for regulation of TFA, with a great deal of this discussion focussing on the design and enforcement of criminal law. However, the scope of behaviour perpetrated with, or through, digital technologies is much broader and demands a range of responses that offer access to justice. This paper argues information rights offer significant potential to enable victims/survivors to gain control over personal information, feel empowered, and improve their mental health and wellbeing. First, it defines information rights and how they are accessed from an EU perspective. Second, it addresses the relationship between legal rights and empowerment in this context. It reflects on if, and how, information rights have been used within the UK specifically, to provide reflections on harnessing their potential. And lastly, explores the viability of advocacy in this area.

KEYWORDS

Technology; empowerment; advocacy; access to justice

Introduction

The coronavirus pandemic has resulted in a compulsory retreat from public spaces. There has been greater pressure to find alternative routes to conduct our working and social lives. For many, the solution has been presented by engagement with digital technologies that allow remote communication. However, as the engagement with such technologies has increased so too has the opportunity for their exploitation with those with 'limited digital skills more at risk of cyberviolence' (UN Women 2020). Indeed, in the UK, the Law Commission has recognised that digital technologies have reportedly been the site of increasing levels of a broad range of online harm and that there is a renewed need to consider how best to regulate harmful conduct in digital space (Law Commission 2021b). Yet, it has long been recognised that 'traditional' routes to justice such as criminal law or civil litigation often provide little solace to victims/survivors in general. More recently, limitations have been recognised specifically in the context of technology-facilitated abuse (TFA) (McGlynn and Westmarland 2019). In light of these evolutions in TFA,

CONTACT Mo Egan mo.egan@stir.ac.uk

and the limitations on traditional justice delivery, it is an opportune time to consider how victims/survivors can be better supported and how access to justice can be improved (Bracewell, Hargreaves, and Stanley 2020; Akiwowo 2021). It is argued that empowerment is a critical component of this access to justice and that advocacy is the necessary mechanism to secure it. Empowerment can be achieved through a process that allows participation, as well as through the outcomes of that process. Therefore, in the context of TFA, regaining control over one's information and identity offers such empowerment and enhances access to justice. However, the utility of information rights and their incorporation into advocacy provision specifically demands greater exploration.

To embark on such an exercise, it is necessary to set the boundaries of TFA. There are certainly some noticeable trends in the type of conduct and the persons to whom that conduct is directed. For example, as Sugiura and Smith observe, 'those whose appearance does not meet the capitalist, mediatized societal ideal of being white, heteronormative, slim and able-bodied are more vulnerable to abuse' (Sugiura and Smith 2020, 47). Specifically, there is evidence to suggest that black and ethnic women are more likely to be the subject of abusive tweets and that homophobia and transphobia are endemic online (Sugiura and Smith 2020). Moreover, concerns have been raised that technologies increasingly facilitate the perpetration of domestic violence, a position that has been exacerbated by the pandemic (Dragiewicz et al. 2018; Woodlock et al. 2020; Slakoff, Aujla, and PenzeyMoog 2020; Akiwowo 2021). Certainly, Refuge (a charity providing support services to those suffering domestic abuse), stated that in 2019, 72% of their clients had been subjected to TFA (Refuge 2020).

Much research has been undertaken focusing on definitional boundaries, prevalence, and consequences of TFA (Henry and Powell 2018; Patel and Roesch 2020; Snaychuk and O'Neill 2020). Focusing on sexual violence, Henry and Powell have suggested that TFA would encompass: '(a) the unauthorised creation and distribution of sexual images (including non-consensual sexting or "revenge porn"), (b) the creation and distribution (actual or threatened) of sexual assault images, (c) the use of a carriage service to procure a sexual assault, (d) online sexual harassment and cyberstalking, (e) gender-based hate speech, and (f) virtual rape' (Henry and Powell 2015, 759). However, TFA does not always have a sexual element. For example, in addition to Henry and Powell's list, it would include doxing and identity fraud. Therefore, in this paper, TFA is understood as 'harmful … behaviour that has been enabled, assisted, prompted, or promoted by communicative technology' (Zhong, Kebbell, and Webster 2020, 2).

Although a predominance of the research in this area suggests that criminalisation of conduct will provide a solution, this paper argues that such a view is misplaced (McGlynn, Downes, and Westmarland 2017). The scope of abusive behaviour perpetrated with or through digital technologies is much broader and demands a range of responses that offer access to justice, with information rights offering significant potential. An information rights approach to providing access to justice in relation to TFA is critical because it is able to harness the empowerment of the individual in ways that are not accommodated within traditional approaches.

Defining information rights

Information rights is used here to capture a specific set of rights that allow an individual to gain or protect access to information. Focusing on the EU General Data Protection

Regulation (GDPR), as the most globally influential legal framework, information rights include core data protection rights (Schwartz 2019).[1] These are the right to be informed (about how your data is used), the right to get a copy of data held, the right to have data corrected, the right to have data deleted, the right to object to data being used, the right to restrict the way your data is used, the right to data portability, and the right not to be subject to automated processing/profiling (Wolters 2018).[2] However, information rights extend beyond this core set of data protection rights to include mirror provisions that apply to any public body or entity entrusted by EU member state laws to prevent, investigate, detect or prosecute, criminal offences or the execution of criminal penalties.[3] In addition to these EU data protection measures, there are contractual rights that arise from service agreements (such as when you sign up to social media platforms, particularly community standards) as well as provisions that allow you to request that information is removed because of the nature and scope of that content (notice and takedown). Both of which also have the potential to assist victims/survivors in asserting control over their information (Otero 2016; Lambert 2019; O'Connell and Bakina 2020).

While it is not possible to examine each of these information rights in detail within this article, it must be acknowledged that the process of accessing these rights varies. By way of example, the EU GDPR provisions, ensure that individuals should be able to access their rights through a direct request to the controller.[4] The regulatory framework requires regulated entities to take certain steps in the design and implementation of their services to ensure individuals are informed of their rights and how they can be exercised in their specific service (Article 12 and Article 13(2), GDPR). This means that an individual should be able to make a request for information about how their personal data is being used, complain about the way it has been handled, or have that information deleted, amended, or transferred through a clearly defined reporting mechanism. Where the regulated entity fails in making it clear how such rights are exercised or fails to address the requests of the individual adequately, then a complaint can be made to the supervising authority (Article 77 GDPR). The sanctioning powers of the supervisory authority in the EU framework are significant. Where a regulated entity has failed in the obligations concerning the individual (data subject's) rights they can be fined up to 20 000 000 EUR or 4% of their annual turnover, whichever is higher (Article 83(5) GDPR).

Importantly, individuals have a right to an effective judicial remedy as well as a right to compensation by way of damages (Article 79 and Article 82). Individuals are not obliged to wait for the supervisory authority to carry out their enforcement action and even where they have done so it does not preclude civil proceedings from being raised. That being said, there is some evidence to suggest that where an individual has not made a complaint to the data controller/processor, this may influence whether the supervisory authority decides to take its own enforcement action.[5]

Certainly, there are limiting factors in the utility of the EU GDPR in the context of TFA. The regulation will not apply to data that is processed 'by a natural person in the course of a purely personal or household activity' (Article 2(2)(c) GDPR). Specifically, it is explained that this would mean 'social networking and online activity' are not regulated by the EU GDPR unless it is connected to a professional or commercial activity (Preamble 18 GDPR).

The effect of this is that a survivor cannot exercise GDPR rights against another individual who is communicating in a purely personal capacity in relation to their online activity. However, action can be taken against the service that has facilitated that activity provided

their involvement has been more than 'merely as a conduit', 'caching' or 'hosting'.[6] Even in such circumstances, if an individual identifies content that is illegal to a 'caching' or 'hosting service' then those specific intermediary services will be compelled to remove it.[7] In all three cases, their limitation of liability would not override an order from a court or administrative authority in a member state.[8]

In responding to requests from data subjects, the GDPR requires that controllers act without 'undue delay' in the case of rectification and erasure of personal data (Article 16 and 17, GDPR). And they must restrict the processing of data at the request of a data subject where that data is required to pursue legal claims (Article 18(c)). These provisions indicate that the timeliness of response is important. While not establishing specific timescales it does suggest that in assessing compliance with the regulation, this factor will influence whether there has been a breach. Notably, there are more stringent provisions in relation to the supervising authority in that they are required to respond to complaints within a period of 3 months. If they do not comply with this timescale, the data subject has the right to pursue judicial action against the supervisory authority (Article 78(2) GDPR). Similarly, there is a requirement that supervisory authorities cooperate with one another in a cross-border context and that they respond to requests within a period of one month (Article 61(2) GDPR).

Importantly, the provisions of the GDPR allow scope for representative actions to be raised on behalf on a data subject with their consent, offering additional protection to those individuals (Article 80(1) GDPR). There is also the possibility of representative actions being raised without the data subject's consent if provisions have been introduced by individual member states (Article 80(1) GDPR).

Where information rights have arisen as the result of Terms of Service or the Community Standards (which usually form part of such Terms of Service), those rights will usually be accessed by reporting the incident to the service provider. The service provider will then be able to sanction perpetrators in accordance with those provisions (Dragiewicz et al. 2018). Since they are ultimately contractual in nature if a non-contentious remedy cannot be found then civil proceedings may be necessary. Nevertheless, information rights offer a route to empowerment in the context of TFA because they offer an alternative to the enforcement of judicial remedies (whether that be through civil or criminal proceedings).

Legal rights and empowerment

There are two main bodies of literature that examine the concept of empowerment. There is literature that examines specifically legal empowerment and that which examines psychological empowerment. As one would expect, the literature on legal empowerment considers whether laws have been secured that provide necessary rights and whether those rights can be meaningfully operationalised (Khair 2009; Banik 2009; Golub 2010; Goodwin and Maru 2017). Legal empowerment has been defined as 'the process of systemic change through which the poor are protected and enabled to use the law to advance their rights and their interests as citizens and economic actors' (United Nation 2009, 2). Alternatively, it has been described as 'giving people the power to use and understand the law' (Goodwin and Maru 2017, 158).

Researchers examining psychological empowerment have tended to define empowerment as 'a mechanism by which people, groups, and communities gain control over their

affairs' (Christens and Peterson 2012, 623). However, Wright et al are critical of those who define empowerment so narrowly (Vaile Wright, Perez, and Johnson 2010). In their view, empowerment goes beyond political advocacy or participatory practices. For this reason, they favour the work of Kasturirangan that argues empowerment should be recognised as a continuous process that involves repetition and reflects the 'personal values and needs' of the individual (Kasturirangan 2008).

Significantly, empowerment is considered to have a positive impact on survivors of abuse since it is a process providing them with the possibility of regaining control of certain aspects of their lives. Cattaneo & Goodman hypothesise that 'if abusers were taking power from survivors, healing entail[s] restoring it' (Cattaneo and Goodman 2015, 85). Critically, they highlight that 'empowerment invokes ideas that resonate with feminist and social justice ideals: personal choice [and] finding voice' (Cattaneo and Goodman 2015, 85).

Key characteristics can be identified that are common to these bodies of work where empowerment requires recognition of autonomy, knowledge (of rights) and resources (to facilitate/exercise those rights). Collectively, these allow choices to be made. If information rights can harness these characteristics, they can be viewed as an opportunity for empowerment that has the potential to improve the mental health and wellbeing of survivors and offer access to justice.

Access to justice

Evaluating access to justice means considering whether the systems in place to enable people to vindicate their rights and/or resolve disputes is effective (Bryant and Cappelletti 1978). Such an evaluation must consider the two basic principles on which access to justice is founded. First, there must be equality in the systems accessibility, and second, the results of the system must be 'individually and socially just' (Bryant and Cappelletti 1978, 182). Bryant and Cappelletti argue that 'the possession of rights is meaningless without mechanisms for their effective vindication' (Bryant and Cappelletti 1978, 185). Significantly, they point out the importance of procedure in securing access to justice. They emphasise that 'procedural techniques serve social functions … and that every procedural regulation, including the creation or encouragement of alternatives to the formal court system, has a pronounced effect on how substantive law operates' (Bryant and Cappelletti 1978, 185). The procedure can be determinative in how often it is enforced and for whose benefits (Bryant and Cappelletti 1978).

A victim of TFA has a number of options. These options are not mutually exclusive. For example, if an individual is subjected to abuse online, they can report the issue to the police (in pursuit of prosecution – if it is recognised as criminal), they can pursue civil proceedings either against the perpetrator or the Internet Service Provider (ISP), or they can contact the ISP with a view to having information removed/deleted or the perpetrator sanctioned in terms of community standards. Information rights offer the potential of an alternative resolution to TFA that can complement criminal or civil measures by allowing a victim/survivor to seek redress through information control. These rights can be used to allow the person who has been subjected to TFA to regain some control over that information and in doing so empower that individual. While criminal and civil measures are often considered to be the appropriate route to justice there are many hurdles in their respective paths.

Criminal law approach

Since TFA takes place in a problematic legal space, law enforcement bodies in any jurisdiction are presented with substantial challenges in terms of skills and resources that allow them to investigate, gather evidence and pursue prosecution in a timely fashion (Bunn 2021). Yet, efficiency can play an important role in satisfaction with, and perceptions of, justice (Casey, Ferraro, and Nguyen 2009). Communication technologies present a problematic legal space because it can be difficult to determine jurisdictional boundaries, agree if certain behaviour is criminal, identify the source of material, and ultimately, establish who has policing responsibility (Wall 1997). Law enforcement efforts are likely to be reserved for only, what they would term as, the most serious of offences, and even in those cases, the prosecution is not guaranteed (Casey, Ferraro, and Nguyen 2009; Woodlock et al. 2020). In any case, the seriousness of an offence does not always correlate to the impact that TFA can have on an individual victim/survivor's physical, mental, and emotional wellbeing (Bates 2016). For access to justice to be achieved, survivors must have access to alternative resolutions.

Non-consensual images: an example

The distribution of intimate images without consent (often referred to as revenge porn) has received a great deal of academic and media attention and for many has become the archetypal form of TFA. Therefore, its treatment offers important insights into the operation of measures seeking to address TFA and whether there is access to justice for victims/survivors.

In its primacy, it was argued that non-consensual image abuse demanded criminalisation (Brown 2018; Keats Citron and Franks 2014; Law Commission 2021a). Indeed, across the world, we have gradually seen the development of specific offences attempting to address this behaviour most recently with the South African Cybercrime Act 2020 (Powell et al. 2020). However, recognition of the offence and its boundaries are still being established in individual jurisdictions. Even where specific legal provisions have been created, the way those provisions are enforced still raises questions about the scope of the offence and the appropriate level of punishment.

In England & Wales (with the offence being passed in 2015) there are only 3 published case reports at the time of writing, only two of those related to the use of digital technologies, and each were guilty pleas.[9] Similarly in Scotland, with the offence established in 2016, there are also only 3 published case reports (each being an appeal against a sentence). Only one offers insight into the treatment of the offence with clarification of the need to demonstrate a sexual element if it is to be sentenced as a sexual offence (with associated listing/supervision consequences).[10] This is interesting because there is a dominant strand of literature that has examined TFA with a sexual element and frames much of the academic debate on responses to addressing such behaviour. The impact of this narrative is that it is only through the application of criminal law that an appropriate level of condemnation can be achieved.

There are significant differences between the scope of the offence in England and Wales and that in Scotland. In England and Wales, the offence requires proof of intention whereas in Scotland it extends to conduct that is reckless.[11] In England and Wales, it only

applies in circumstances where the image is disclosed but in the Scottish provision, it extends to the threat of disclosure.[12] In the Scottish provision, it extends to images that 'appears to show another person in an intimate situation' and so is capable of capturing 'deepfakes' but the English provision only covers disclosure of 'a private sexual photograph or film' and so is thought to be more limited (Law Commission 2021a). And in England and Wales, the maximum penalty is 2 years whereas in the Scottish provision it is a period of 5 years.[13]

In 2017–2018, there were 421 new crimes reported of disclosing, or threatening to disclose an intimate image in Scotland, and in 2018–2019, there were another 596 (Scottish Government 2019). Although in England and Wales, there were 541 cases specifically relating to children, reported to the police in 2019, there were only 376 prosecutions relating to the disclosure of private sexual images by the end of that year (Office for National Statistics 2019; Webb and Weale 2020). This suggests a significant disparity between reported cases and prosecution. It is not uncommon for there to be such a disparity given the role of prosecutorial discretion. However, there are additional concerns about how the views of law enforcement may interact with that discretion. For example, in one comparative survey of Australia, New Zealand and the UK, it was demonstrated that there is a 'lack of awareness among some [Law Enforcement] officers of the serious harms to victims' caused by such offences and there also appeared to be limited awareness of the existence of 'new laws on image based sexual abuse' (Flynn, Powell, and Hines 2021, 13). In another study focusing on the perception of Law Enforcement in Israel, a gender disparity was evidenced that males tended to blame the victim more than females (Zvi and Shechory-Bitton 2020). The researchers also found that whether the images were self-taken or not, impact the extent to which the officers thought that the perpetrator should be punished (Zvi and Shechory-Bitton 2020). This is important because officers' perceptions can impact how the victim is treated and how cases progress through the system since they are often gatekeepers (Taylor and Gassner 2010).

In England and Wales, the Crown Prosecution Service guidelines recommended that the actions of internet service providers should be taken into consideration in whether to prosecute. This seems to suggest that action taken by those providers would reduce the likelihood of action being taken through criminal sanction. Despite the guidelines also requiring that consideration should be given to the 'circumstances of and harm caused to the victim' the role given to the actions taken by ISP seems to suggest that those actions reduce the public interest in addressing the behaviour. Such a premise detracts from the victim/survivor's position (Crown Prosecution Service 2018). Though, in many ways, the factors taken into consideration in the Crown Prosecution guidelines reflect the functions of the criminal law. It has to be recognised that it is an exercise in demonstrating public condemnation of socially unacceptable conduct, as opposed to a mechanism for the recognition or remedy for individual wrongs. While such recognition and remedy may be a side effect of criminal sanction, they are not the foundation on which the domestic criminal law has been built. Indeed, Bunn argues that 'although criminal offences certainly have a role in deterring or punishing the unauthorised publication of images in some situations, they are of limited utility in giving individuals the ability to control how or whether their images are published or how they are subsequently used' (Bunn 2021, 352). Bunn suggests that this is because 'the criminal process is essentially

a public one and the ability of individuals to be direct participants within that process is limited' (Bunn 2021, 352).

Limitations and potential

The utility of legal measures addressing violent and abusive behaviour is frequently called into question (Yar and Drew 2019; Walklate, Fitz-Gibbon, and McCulloch 2017). Of particular interest, Lewis *et al* have argued that debates have been 'limited by their tendency to view women survivors of abuse as passive recipients of legal intervention' (Lewis et al. 2000, 179). Dissatisfaction with the treatment of victims/survivors is evidenced extensively in academic literature and by those providing support services, with the criminal justice system specifically seen to be lacking (McGlynn, Downes, and Westmarland 2017; Antonsdóttir 2020). Indeed, within the Australian context, there have been calls for greater clarity concerning the application of the criminal law and the need for relevant training by academics, law enforcement, and the support services sector (Powell and Henry 2018).

In terms of the criminal laws' ability to empower, the scope is narrow. If the key characteristics of empowerment are, as suggested earlier, the recognition of autonomy, knowledge (of rights) and resources (to facilitate/exercise those rights) criminal law has little to offer in the UK. It is well documented that there is generally no representation of victims/survivors in criminal proceedings (Raitt 2013; Ferguson 2021). The prosecution represents the interests of the state as opposed to the victim/survivor's interests. While those interests may be the same, it is equally possible for those interests to conflict. Although the introduction of victim impact statements is thought to go some way to recognising the interests of the victim/survivor, to suggest that these statements offer recognition of autonomy would be a stretch (Geeraets and Veraart 2021). Victim impact statements have no bearing on whether action is taken against an accused party.

The ability to identify whether criminal offences capture TFA is complicated. As discussed above using the example of non-consensual images, the picture, even within the UK, is conflicting. If you set this within a wider cross-border context, there is likely to be even less consensus on raising criminal proceedings except for in the most serious of cases. That being said, the UK, as with many other jurisdictions is going through a period of renewed interest in addressing the regulation of online harms.

In July 2021 the Law Commission (of England and Wales) published its report on the modernisation of communication offences (Law Commission 2021b). As a statutory body assigned the responsibility for the promotion of law reform, the Law Commission play a central role in driving the development of law in the UK (Dyson and Wilson-Stark 2016). Its central goal was to make recommendations for law reform that would ensure that the criminal law can be used effectively to protect people from genuine harm and abuse in the 'new technological paradigm'(Law Commission 2021b, 1). The Law Commission are clear that only communications that are harmful should be criminalised (Law Commission 2021b, 6). They acknowledged that the scope of criminalisation was necessarily limited because criminal law is a 'cumbersome and expensive tool' and therefore 'can only be reserved for the most seriously culpable communications' (Law Commission 2021b, 7). However, the Law Commission expressly excluded platform liability from consideration. (Law Commission 2021b).

Overlapping with this Report, the Law Commission is consulting specifically on image-based abuse and how best to address this issue. At this stage, they have suggested proposed reforms and have published them for consultation, but they do not intend to be in a position to report their conclusions until 2022. In the meantime, The Unsolicited Explicit Images & Deepfake Pornography Bill was introduced in June 2021. The purpose of this bill is to 'create the offences of sending unsolicited explicit digital images and of producing digitally-altered images or videos in which an individual is depicted pornographically without their consent' (The Unsolicited Explicit Images & Deepfake Pornography Bill, Long Title). The details of its provision remain unclear as a draft of the bill is only due to being presented to Parliament in February of 2022. However, we can infer that the function of this bill is to address the identified gaps in the English approach to the criminalisation of non-consensual images.

If proposed measures were to be adopted, they can only contribute to empowerment where the victim/survivor knows that the measure is in place – allowing them to report the matter to the police. However, in turn, the police have to be sufficiently trained to be able to embrace the new measures.

It is difficult to assess whether there are sufficient resources for a victim/survivor to be empowered in criminal proceedings because many of these resources are dictated by the state. Inevitably the state will have insufficient resources including finance and technical expertise to pursue every complaint concerning TFA with resources only allocated to the most serious incidents.

A victim/survivor's capacity to choose a course of action in criminal proceedings is very limited. In effect, their main choice will be the decision to report the incident or not. However, because of the nature of digital space and the location of intermediaries within it, it is also important to acknowledge that their choice may be dictated by those intermediaries if illegal conduct comes to their attention. Ultimately, criminal law provides little scope for empowerment in the context of TFA.

Civil litigation and its limitations

Recently, in the UK, there has been a resurgence in rape cases being pursued in the civil courts as an alternative way of finding justice.[14] The civil courts have been considered advantageous to victims/survivors in that unlike in criminal matters, they are able to have legal representation and that, as a result, they can have more meaningful participation providing a sense of control (Godden-Rasul 2015). There are of course a wide range of actionable grounds that may capture TFA. For example, misuse of information, breach of confidence and defamation are arguably the most pertinent (Brown 2018). Setting aside the complexity of selecting the appropriate ground of action, and the intricacies of proving the same, a critical determinant in choosing to pursue civil proceedings is money. Representation costs money. Although tentative, in Iceland, there is some indication that financial support may be made available to survivors of sexual violence to pursue civil claims but even if some form of legal aid was to be made available, there will still be issues surrounding what level of experience/expertise can you afford (Antonsdóttir 2020). The cost of bringing proceedings to court can be prohibitive. The nature of TFA can be such that expert witnesses may be required to reach the necessary standard of proof. While civil legal aid is theoretically available, in practical terms its allocation is

restricted by its limited budget. In the UK, civil legal aid is often a casualty of political priorities, facing cuts as the Government's budget is reallocated (Baksi 2014; Bowcott 2018).

Still, importantly, Antonsdóttir's study has found that victims/survivors of sexual violence have 'profoundly ambivalent views' on pursuing civil claims and the potential of associated compensation (Antonsdóttir 2020). Although it cannot be presumed that the same finding would apply to victims/survivors across the full spectrum of TFA, it does provide pause for thought as to the motivations and expectations of those victims/survivors. Indeed, there is evidence to suggest that in the context of TFA 'survivors also want an active voice, seeking more ownership and control within a justice process in order for them to feel empowered' (McGlynn, Downes, and Westmarland 2017).

The time taken from an action being raised in a civil court to disposal has been negatively impacted by the COVID 19 pandemic (Ministry of Justice 2021). In England and Wales, it took an average of 51.5 weeks between a small claim being issued and the claim going to trial (Ministry of Justice 2021). For multi-track or fast track claims it took an average of 73.4 weeks to reach a trial (Ministry of Justice 2021). These delays can have a critical impact on victims. It can extend the length of the traumatic event (particularly when required to give evidence) and can incur further costs leading to the possibility of the 'economically weak having to abandon their claims or settle for much less than that' which they would otherwise pursue (Bryant and Cappelletti 1978). In each of these circumstances, there is little doubt that it cannot be claimed that justice is achieved.

Civil proceedings do offer more potential for empowerment than criminal proceedings in that there is a clear recognition of autonomy through representation (Herman 2005). However, the scope for empowerment remains limited in that the ability to know one's rights is still restricted. There is likely to be a financial burden connected to the provision of legal advice on which grounds to found action and further expense in respect of representation should the matter proceed. There certainly is more scope to be involved in civil proceedings but this is tempered by the available resources of the victim/survivor.

Information rights – potential and limitations

Information rights are not a panacea: There are also limitations to these rights. The anonymity of perpetrators of TFA can result in difficulties in terms of accountability. Without being able to identify the perpetrator, an individual is dependent on the framework attributing responsibility to intermediaries, a position that is notoriously problematic since perpetrators can, for example, create multiple accounts to avoid identification (Dragiewicz et al. 2018; Levmore 2010). Indeed, since perceptions of justice are positively associated with retribution, the 'internet's anonymity problem' can lead to disempowerment because of limitations in accountability of the specific individual perpetrator (Strelan and Van Prooijen 2013).

There are further limitations in that, in order to exercise information rights, it is necessary to know about them in the first instance (Ni Loideain 2019). In turn, it is necessary to understand the process by which these rights can be exercised and to understand the limitations of potential outcomes. For instance, in making a request for data to be removed from a social networking site, while there can be requirements for responses to be timely, there can also be a delay (for example if the user who posted content was to appeal). Or, if for example, an individual was to attempt to remove an intimate

video on the grounds of copyright, this is likely to result in significant costs because individual requests would be required to each location it has been uploaded and the nature of the digital society is such that reposting can escalate quickly. (Romero-Moreno 2019; Bunn 2021). Consequently, managing expectations is critical in determining levels of satisfaction.

The Information Commissioners Office (the UK organisation responsible for monitoring the implementation of data protection rights), has commissioned Annual Track Reports seeking to understand people's trust and confidence in data protection (as well as how they interact with those rights). There are interesting dynamics evidenced in their reports, with gender and age presenting implications for the utility of information rights in the context of TFA.

Gender

Males have a greater level of trust in organisations storing and processing data compared to females (37% to 30%) (ICO 2018). This is significant in the context of TFA because if (as evidence suggests) women tend to suffer more widely from TFA, and they have a low level of trust in organisations dealing with their data, it would seem that they may be less likely to utilise their data protection rights since it will require interactions with those organisations. It is worth noting that over the period 2018–2020 the trend is one of reducing trust in organisations (ICO 2018, 2019, 2020). This is pertinent because while these reports were being conducted the ICO were carrying out a campaign to advertise the availability of data protection rights. This seems to suggest that as knowledge of data protection has increased – trust has decreased.

However, a higher percentage of males perceive themselves as 'having a good understanding of how their data is used' (23% of males to 14% of females) – the importance of this is that it is necessary to know how one's data is being used in order to consider if one can challenge it (ICO 2018). If these perceptions held by participants are an accurate reflection of the wider society it would suggest that males are better placed to exercise their data protection rights than females.

Age

Age can be a significant factor in the level of engagement with digital technologies and the resulting exposure to online abuse (Jatmiko et al. 2020; Snaychuk and O'Neill 2020; Bunn 2021; UK Safer Internet Centre 2021; Law Commission 2021b). Age has the potential to play a significant role in the use of data protection rights because trust and confidence is seen to be higher in younger age groups when compared with older age groups (18–34-year-olds, 49%, 35–54 31%; 55+ year olds, 25%) (ICO 2018). This would suggest that younger groups may have a greater willingness to engage with organisations in an effort to control their information because they trust them. However, as with gender, the trend is that trust and confidence has decreased across all age groups.

Knowledge of how data is used is lower in the older age groups when compared with the younger age groups. With 31% of over 55s knowing 'very little or nothing about how their personal data is used' compared to 21% of 18–24-year-olds (ICO 2018). This would tend to indicate that older age groups would be less likely to be in a position of having the

necessary awareness to exercise their rights. Although, it is notable that the trend across all groups is that an increasing percentage of participants feel they have little or no knowledge of how their data is used.

It seems that gender and age are likely to be significant considerations in the design of any intervention seeking to promote the use of information rights such as through dedicated advocacy.

New horizons in Online Safety

The protection offered to individuals suffering from TFA is about to be significantly enhanced in the UK with the introduction of the Online Safety Bill 2021. Adopting a preventative approach, the bill places duties of care on regulated services that are intended to ensure the prevention of harm to individuals using these services. OFCOM are the designated regulatory body furnished with the responsibility of ensuring regulated business compliance and sanctioning non-compliance (Part 4 Online Safety Bill 2021). However, there will of course be concerns here that they are sufficiently resourced to accommodate this expansion to their role (Harbinja 2021).

While the measures implemented through the Online Safety Bill 2021 apply only to regulated services where those services have a link to the UK (Clause 3 Online Safety Bill 2021) the definitions given are such that there is a degree of an extraterritorial effect than one would expect in a dynamic digital environment. Perhaps most importantly, its provisions apply to those user-to-user-services or search services where they 'are capable of being used by individuals in the United Kingdom' and 'there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the United Kingdom' (Clause 3(6) Online Safety Bill 2021). However, there are also some significant exemptions. For example, its provisions do not extend to email services, SMS, or MMS (where that is the exclusive service offered) (Schedule 1, Clause 1–2; Online Safety Bill 2021).

Regulated services are obliged to 'take proportionate steps to mitigate and effectively manage the risks of harm to individuals' (Clause 9(2) Online Safety Bill 2021). In operating their services, they have a duty to adopt processes and systems to minimise the presence of illegal content, minimise the length of time that content is present, minimise the dissemination of 'priority illegal content', and 'swiftly' take down illegal content when notified of it (Clause 9(3) Online Safety Bill 2021). From the perspective of information rights, the bill proposes that services will be obliged to narrate the steps that will be taken to protect individuals from illegal content within their terms of service (Clause 9 (4) Online Safety Bill 2021). This is critical because it effectively creates a contractual, as well as a compliance obligation, on the regulated service and will help to improve the accessibility of information rights.

There is a duty placed on regulated user to user services to ensure that users can report content that is illegal or potentially harmful to adults or children (Clause 15(2) Online Safety Bill 2021). However, regulated search services have a more restrictive reporting mechanism only requiring a mechanism to report illegal content or that which is harmful to children (Clause 24(2) Online Safety Bill 2021). In addition, regulated user to user services are required to operate an easily accessible and transparent complaints system. Importantly, their complaints system must provide 'for appropriate action to be

taken by the provider of the service in response' (Clause 15(3)(b) Online Safety Bill 2021). Individuals with standing to make complaints should include users and those who are the subject of the content in question or a member of the class or group of people targeted by the content. In addition, the definition extends to a parent or another individual with responsibilities for a child who is a user or subject of the content, or an adult who is representing another adult user or individual subject of the content, provided they are in the UK (Clause 15 Online Safety Bill 2021). This is significant in the context of TFA because it would allow scope for actions to be taken on behalf of victims/survivors.

Part of the Government's preventative approach to online harm includes the promotion of media literacy. OFCOM are furnished with a duty to promote media literacy to the public. Specifically, and of particular relevance to TFA, media literacy is considered to include 'an awareness of the impact that such material may have (for example, the impact on the behaviour of those who receive it)' (Clause 103; Online Safety Bill 2021). Taking on board the findings of the ICO work on trust and confidence in information rights, it will be crucial for any such promotion to be tailored appropriately to relevant demographics.

Perhaps the most significant aspect of the proposed legislation is the facilitation of 'super complaints' allowing eligible entities to make complaints to OFCOM about the compliance of regulated services (Clause 106; Online Safety Bill 2021). This is likely to be particularly useful should victim advocates/victim support organisations be captured within such eligible entities. The Secretary of State will hold the power to determine what or who constitutes an eligible entity albeit that they are required to consult with OFCOM (Clause 107(3)(a), Online Safety Bill 2021).

This is important because it means that individuals do not have to enter into an adversarial process such as that presented by pursuing civil proceedings independently. However, although this may offer comfort to some, it also may result in dissatisfaction in that the individual perpetrator is not being held to account. Research suggests that although many individuals find court proceedings challenging (whether criminal or civil) they also value the opportunity for the perpetrator to be publicly held to account (O'Hara 2005; Strelan and Van Prooijen 2013).

Collectively, information rights, and their potential enhancement through the draft Online Safety Bill, offer more potential for empowerment than either criminal or civil sanctions. This is because they give greater recognition to the autonomy of the individual. They have become embedded within the design and operation of internet services. That being said, there is still a potential gap between the legal recognition of autonomy, the legal framework supporting raising awareness and accessibility of information rights and an individual having the necessary trust and confidence to engage with those mechanisms.

Facilitating empowerment through advocacy

Advocacy is likely to offer the most robust route to empowerment through information rights (Henderson and Pochin 2001). This is because advocacy recognises the role of the individual, seeking to support them in pursuing their goals. However, such advocacy cannot stand alone because as with the rights themselves, there has to be an awareness of its existence for it to be utilised. Therefore, any development of information rights

advocacy services will need to engage with those organisations that currently provide a range of support services to victims/survivors to ensure the service is connected to affected individuals and to foster their trust and confidence.

There are already a number of initiatives that seek to provide information to those suffering TFA, services that provide access to resources, and services that provide mechanisms for the removal of online content. Some initiatives are located within organisations with another remit, or some are established within a specific product or service. For example, Facebook has a selection of resources accessible through their 'Staying Safe' pages and a mechanism through which you can report abuse.[15] Facebook have 35,000 people engaged in ensuring safety and security on their services.[16] Yet, with a reported 1.91 billion daily users it does beg the question of whether this complement is likely to be sufficient.[17]

Flynn et al provide insights into the nature and scope of TFA support in the Australian community and the barriers and challenges to such support from the perspective of providers. It is important to highlight that their research captures not only their important insights but is framed by the context of bushfires and COVID-19. This is significant because of the potential for each of these experiences to influence what support is available, how that support is accessed, and their influence on the future direction of service provision in terms of sustainability (Flynn, Powell, and Hines 2021). Their survey was completed by 338 support services workers with the majority focusing on domestic and sexual violence provision (Flynn, Powell, and Hines 2021). These workers expressed that the biggest challenges in supporting those suffering TFA include 'finding up-to-date information, not being taken seriously by the police and court and inadequate responses from technology providers' (Flynn, Powell, and Hines 2021, 5). Participants indicated that in their experience 'there remains a substantial gendered nature to TFA, demonstrating a clear need for focused policy efforts that prioritise TFA as a subtype of men's violence against women' (Flynn, Powell, and Hines 2021, 5).

In the UK a similar picture emerges in that 'concerns about responses to violence against women more generally have provided the impetus for developing advocacy services to assist victims in their interactions with criminal justice, health and other agencies'(Brooks and Burman 2017, 210). Consequently, many advocacy services focus on the context of domestic violence and rape. Resources to support victims are numerous. Some of the most prominent include Refuge (Tech Abuse and Empowerment Service), Paladin (National Stalking Advocacy Service), Revenge Porn Helpline, Internet Watch Foundation, and the Queen Mary Legal Advice Centre SPITE project.[18] Although many support services provide training to staff on the nature of TFA, only some provide training on the legal framework and fewer still on how that framework can be utilised without the need for legal representation in the context of information rights. For example, RSVP (Rape and Sexual Violence Project) based in Birmingham, provides regular training on 'online sexual abuse'.[19] In the context of domestic violence, Refuge provides a range of resources seeking to assist those who are supporting individuals affected by TFA.[20] In addition, Refuge has produced a Chatbot that can assist individuals in keeping their devices safe (Refuge 2019-2020). Beyond addressing individual concerns, the SPITE project is an important initiative providing tailored educational workshops on image-based sexual abuse providing an awareness-raising function.

Evidently, many organisations within the UK offer potential candidates for providing information rights advocacy focusing on TFA. However, it is necessary to take a critical view of how such a co-location of service would be operationalised and the consequences that may flow from that. For example, while there may be an obvious appeal in partnering with for example, the Revenge Porn Helpline, it is clear that the title alone may mean that the wider range of TFA victims/survivors is unlikely to reach out. Similarly, while the SPITE project has a great deal of potential to increase digital literacy and prevent victimisation, as part of a Law School Advice clinic, it is limited by its focus on local schools and term time delivery.

Arguably one of the most important considerations in any advocacy setting is how such a provider will be funded. This is important for two reasons: first, the source of funding can support or indeed impede independence, and second, funding can secure the sustainability of services (Morariu and Brennan 2009; Henderson and Pochin 2001).

Although commenting on the Australian context, Flynn and others have acknowledged that 'recognition of the vital practice-based knowledge that is held by those who work directly with clients experiencing TFA … including domestic and family violence, sexual assault, health, legal services and specialist diversity services' is critical to the development of robust research (Flynn, Powell, and Hines 2021, 4). Accordingly, if information rights advocacy is to be evaluated seriously as part of the support services available to victims/survivors of TFA, then it is necessary to collaborate with support services organisation to do it. It is necessary to address to what extent their service users experience TFA specifically, to what extent those services users are interested in pursuing information rights, and where relevant whether attempts to exercise those rights have been successful. However, the potential of such collaboration in research is limited by the ability of those support services to commit time and resources to such a project.

However, the UK picture may improve. The introduction of the Online Safety Bill and its commitment to the promotion of media literacy offers scope for a structured system of information provision to assist support services (Clause 103 Online Safety Bill 2021). Since OFCOM's duties extend across the spectrum of online harms, albeit only in relation to the role of regulated services, they would have the institutional remit to develop up to date information on the legal regulation of TFA (Clause 56 Online Safety Bill 2021). This could be developed into a toolkit for support services that could then be drawn upon and tailored by individual support services allowing individual advocates to select appropriate material. It would reduce the burden on resources for individual support services and would contribute to the sustainability of services.

Conclusion

As our lives continue to become intertwined with digital space in new and interesting ways, so to methods of exploitation evolve allowing technology-facilitated abuse to flourish. It is necessary to reflect on that evolution and consider if and how such behaviour can be meaningfully challenged and how individuals subjected to such behaviour can determine how that can best be achieved. In this respect, information rights can make an important contribution to access to justice by complementing criminal and civil measures. Information rights are capable of recognising victim/survivors' autonomy to a greater extent than either criminal or civil measures. This is because many information rights allow an individual to pursue these remedies without representation. In turn, since

no representation is required, it also means there is less requirement for money to be a significant factor in whether action can be taken. However, it is unclear to what extent individuals have sufficient knowledge of their information rights to ensure that they are able to access them, with the UK experience suggesting that this is impacted by the issue of age and gender.

Still, the recognition of autonomy offered by information rights ensures the necessary participatory aspect to secure empowerment. Information rights have great potential to empower individuals through the control of their information and, in turn, limit the impact of digital violence. However, this empowerment potential can only be harnessed if the individual is able to meaningfully participate in that process of controlling information. Importantly, for such empowerment to become a practical reality it is necessary to consider what tailored support may be required by specific groups (age, gender, disability, BAME, etc.) to bridge the gap between the existence of the legal framework supporting information rights and the trust and confidence of individuals in utilising those rights. However, to do this, it is necessary to systematically assess current provisions to avoid duplication and dilution of services. If advocacy services are to be seen as a possible route forward, specific consideration has to be given to resourcing to secure investment in skills/knowledge development to ensure their sustainability. A failure to do so could lead to detrimental outcomes where support falls away unexpectedly and results in disempowerment of those they are seeking to support.

The UK's introduction of the Online Safety Bill offers an opportunity to further bolster the operation of information rights. This is because the remit of OFCOM is to include the promotion of media literacy. It is argued here that such media literacy should include an awareness of harmful online conduct but also how such harms can be addressed. With this in mind, it is suggested that OFCOM would be well-positioned to enhance advocacy support services by providing up to date information on the regulation of TFA. By developing a toolkit they would be able to provide a resource to support services that can be tailored to their service users' needs. This in turn reduces the financial burden on support services to develop independent resources and would allow those services to become more sustainable.

While this paper introduces the possible potential offered by the use of information rights, future research is necessary to interrogate that potential. In particular, it is necessary to collaborate with providers of support services who already engage in victim/survivor advocacy and to engage with victim/survivors themselves to test their utility. It is only with those insights that effective interventions can be designed seeking to ensure a robust framework of support for victims/survivors of TFA.

Notes

1. See also China's recently proposed Personal Information Protection Law of the People's Republic of China 2021.
2. Chapter III, Rights of the Data Subject, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *OJ L 119, 4.5.2016, p. 1–88*. Hereinafter GDPR.
3. Article 3(7) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by

competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016, p. 89–131* Hereinafter Directive 2016/680.

4. Defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." Article 4(7) GDPR.
5. ICO, Rancom Security Limited Monetary Penalty Notice, 25 January 2021.
6. Article 12–14, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). *OJ L 178, 17.7.2000*. p. 1–16. Hereinafter E-commerce Directive.
7. Article 13(1)(d), Article 14(1)(a) E-commerce Directive.
8. Article 12(3), Article 13(2) and Article 14(3) E-commerce Directive.
9. R. v Peters (Candess) [2020] EWCA Crim 53; R. v Pointon (Teresa) [2019] EWCA Crim 1601 ; R. v Bostan (Amar) [2018] EWCA Crim 494.
10. Shanks v PF [2018] SAC (Crim) 18 (Guilty plea – appeal against sentence), Kennaway v HMA [2019] HCAC 11 (appeal against sentence – not guilty plea) and Sorrell v PF [2019] SAC (Crim) 2 (guilty plea but appealing re sentencing as a sexual offence).
11. S33(1)(b) Criminal Justice and Courts Act 2015 and s2(1)(b) Abusive Behaviour and Sexual Offences (Sc) Act 2016.
12. S33(1)(a) Criminal Justice and Courts Act 2015 and s2(1)(a) Abusive Behaviour and Sexual Offences (Sc) Act 2016.
13. S33(9)(a) Criminal Justice and Courts Act 2015 and s2(7)(b) Abusive Behaviour and Sexual Offences (Sc) Act 2016.
14. *DC v DG & DR* [2017] CSOH 5; *A v C & B v C,* [2018] CSOH 65.
15. 15. Facebook Website: https://www.facebook.com/help/1753719584844061/?helpref=related Last Accessed 19 August 2021.
16. Facebook Website: https://about.facebook.com/actions/promoting-safety-and-expression/ Last Accessed 19 August 2021.
17. Facebook (2021).
18. https://paladinservice.co.uk/advice-for-victims/; https://revengepornhelpline.org.uk/; https://www.iwf.org.uk/ https://www.refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/ http://www.lac.qmul.ac.uk/clients/advice/revenge-porn-free-legal-advice/ Last accessed 16 August 2021.
19. RSVP website: https://rsvporg.co.uk/training/ Last Accessed 16 August 2021.
20. See Refuge website: https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/resources/ Last Accessed 16 August 2021.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Mo Egan http://orcid.org/0000-0002-9345-4006

References

Akiwowo, S. 2021. "Opinion: COVID-19 Has Fuelled an Epidemic of Gender-Based and Intersectional Abuse Online." *Interdisciplinary Perspectives on Equality and Diversity* 7 (1): 3–8.

Antonsdóttir, H. F. 2020. "Compensation as a Means to Justice? Sexual Violence Survivors' Views on the Tort law Option in Iceland." *Feminist Legal Studies* 28: 277–300. doi:10.1007/s10691-020-09442-2.

Baksi, C. 2014. Civil Legal Aid: Access denied, The Law Society Gazette, April 7th . https://www.lawgazette.co.uk/law/civil-legal-aid-access-denied/5040722.article.

Banik, D. 2009. "Legal Empowerment as a Conceptual and Operational Tool in Poverty Eradication." *Hague Journal on the Rule of Law* 1: 117–131.

Bates, S. 2016. "Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors." *Feminist Criminology* 12 (1): 1–21.

Bowcott, O. 2018. "Legal Aid: How Has It Changed in 70 Years?" *The Guardian*, December 26. https://www.theguardian.com/law/2018/dec/26/legal-aid-how-has-it-changed-in-70-years.

Bracewell, K., P. Hargreaves, and N. Stanley. 2020. "The Consequences of the COVID-19 Lockdown on Stalking Victimisation." *Journal of Family Violence*. doi:10.1007/s10896-020-00201-0.

Brooks, O., and M. Burman. 2017. "Reporting Rape: Victim Perspectives on Advocacy Support in the Criminal Justice Process." *Criminology & Criminal Justice* 17 (2): 209–225. doi:10.1177/1748895816667996.

Brown, J. 2018. "'Revenge Porn' and the Actio Iniuriarum: Using 'Old Law' to Solve 'New Problems'." *Legal Studies* 38: 396–410.

Bryant, G., and M. Cappelletti. 1978. Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective. Articles by Maurer Faculty. 1142. https://www.repository.law.indiana.edu/facpub/1142.

Bunn, A. 2021. "Unwanted Distribution of Children's Images and the Right to Development." *The Modern Law Review* 84 (2): 334–370.

Casey, E., M. Ferraro, and L. Nguyen. 2009. "Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence." *Journal of Forensic Sciences* 54 (6): 1353–1364. DOI:10.1111/j.1556-4029.2009.01150.x.

Cattaneo, L., and L. A. Goodman. 2015. "What Is Empowerment Anyway? A Model for Domestic Violence Practice, Research, and Evaluation.." *Psychology of Violence* 5 (1): 84–94. doi:10.1037/a0035137.

Christens, B. D., and A. Peterson. 2012. "The Role of Empowerment in Youth Development: A Study of Sociopolitical Control as Mediator of Ecological Systems' Influence on Developmental Outcomes." *Journal of Youth and Adolescence* 41: 623–635. doi:10.1007/s10964-011-9724-9.

Crown Prosecution Service. 2018. "Social Media – Guidelines on Prosecuting Cases Involving Communications Sent via Social Media." Revised August 21. https://www.cps.gov.uk/legal-guidance/socialmedia-guidelines-prosecuting-cases-involving-communications-sent-social-media.

Dragiewicz, M., J. Burgess, A. Matamoros-Fernández, M. Salter, N. P. Suzor, D. Woodlock, and B. Harris. 2018. "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms." *Feminist Media Studies* 18 (4): 609–625. doi:10.1080/14680777.2018.1447341.

Dyson, L., and S. Wilson-Stark, eds. 2016. *Fifty Years of Law Commissions: The Dynamics of Law Reform*. Oxford: Hart Publishing.

Facebook. 2021. "Facebook Reports Second Quarter 2021 Results." July 28. https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Second-Quarter-2021-Results/default.aspx.

Ferguson, P. 2021. "R(R) v HM Advocate, Case Comment." *SLT* 14: 61–62.

Flynn, A., A. Powell, and S. Hines. 2021. Technology-Facilitated Abuse: A Survey of Support Services Stakeholders. ANROWS Research Report, Issue 2, July.

Geeraets, V., and W. Veraart. 2021. "What Is Wrong with Empirical-Legal Research into Victimhood? A Critical Analysis of the Ordered Apology and the Victim Impact Statement." *Oxford Journal of Legal Studies* 41 (1): 59–79. doi:10.1093/ojls/gqaa048

Godden-Rasul, N. 2015. "Retribution, Redress and the Harms of Rape." In *Rape Justice: Beyond the Criminal Law*, edited by N. Henry, A. Powell, and A. Flynn, 112–126. Basingstoke: Palgrave Macmillan.

Golub, S. 2010. *Legal Empowerment: Practitioners' Perspectives, Legal and Governance Reform: Lesson Learned No 2*. Rome: International Development Law Organization.
Goodwin, L., and V. Maru. 2017. "What Do We Know about Legal Empowerment? Mapping the Evidence." *Hague Journal on the Rule of Law* 9: 157–194. doi:10.1007/s40803-016-0047-5.
Harbinja, E. 2021. The UK's Online Safety Bill: Safe, Harmful, Unworkable? In: Verfassungsblog: On Matters Constitutional. doi:10.17176/20210518-170138-0.
Henderson, R., and M. Pochin. 2001. *A Right Result? Advocacy, Justice and Empowerment*. Bristol: Polity Press.
Henry, N., and A. Powell. 2015. "Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence." *Violence Against Women* 21 (6): 758–779.
Henry, N., and A. Powell. 2018. "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research." *Trauma, Violence, & Abuse* 19 (2): 195–208. doi:10.1177/1524838016650189.
Herman, Judith Lewis. 2005. "Justice from the Victim's Perspective." *Violence Against Women* 11 (5): 571–602. doi:10.1177/1077801205274450.
ICO. 2018. Information Rights Strategic Plan: Trust and Confidence.
ICO. 2019. Information Rights Strategic Plan: Trust and Confidence.
ICO. 2020. Information Rights Strategic Plan: Trust and Confidence.
Jatmiko, M. I., M. Syukron, and Y. Mekarsari. 2020. "Covid-19, Harassment and Social Media: A Study of Gender-Based Violence Facilitated by Technology during the Pandemic." *The Journal of Society and Media* 4 (2): 319–347.
Kasturirangan, A. 2008. "Empowerment and Programs Designed to Address Domestic Violence." *Violence Against Women* 14 (12): 1465–1475. doi:10.1177/1077801208325188.
Keats Citron, D., and M. A. Franks. 2014. "Criminalizing Revenge Porn." *Wake Forest Law Review* 49: 345.
Khair, S. 2009. "Evaluating Legal Empowerment: Problems of Analysis and Measurement." *Hague Journal on the Rule of Law* 1: 33–37.
Lambert, P. 2019. "IP and PI Takedowns: Comparing and Contrasting the Right to Be Forgotten." *E.I.P.R* 41 (6): 381–384.
Law Commission. 2021a. Intimate Image Abuse: A consultation paper. No 253. February 28.
Law Commission. 2021b. Modernisation of Communication Offences, Final Report, Law Com No 399, July. https://www.lawcom.gov.uk/project/reform-of-the-communications-offences/.
Levmore, S. 2010. "The Internet's Anonymity Problem." Chap. 3 in *The Offensive Internet*, edited by S. Levmore, and S. Nussbaum, 50–67. London: Harvard University Press.
Lewis, R., R. P. Dobash, R. E. Dobash, and K. Cavanagh. 2000. "Protection, Prevention, Rehabilitation or Justice? Women's Use of the Law to Challenge Domestic Violence." *International Review of Victimology* 7 (1-3): 179–205. 10.1177/026975800000700310.
McGlynn, C., J. Downes, and N. Westmarland. 2017. "Seeking Justice for Survivors of Sexual Violence: Recognition, Voice and Consequences." In *Restorative Responses to Sexual Violence: Legal, Social and Therapeutic*, edited by Estelle Zinsstag and Marie Keenan, 179–191. Routledge frontiers of criminal justice. Abingdon: Routledge.
McGlynn, C., and N. Westmarland. 2019. "Kaleidoscopic Justice: Sexual Violence and Victim-Survivors' Perceptions of Justice." *Social & Legal Studies* 28 (2): 179–201.
Ministry of Justice. 2021. National Statistics: Civil Justice Statistics Quarterly. January to March 2021. https://www.gov.uk/government/statistics/civil-justice-statistics-quarterly-january-to-march-2021/civil-justice-statistics-quarterly-january-to-march-2021.
Morariu, J., and K. Brennan. 2009. "Effective Advocacy Evaluation: The Role of Funders." *The Foundation Review* 1 (3): 100–108. doi:10.4087/FOUNDATIONREVIEW-D-09-00031.1.
Ni Loideain, N. 2019. "A Port in the Data-Sharing Storm: The GDPR and the Internet of Things." *Journal of Cyber Policy* 4 (2): 178–196. doi:10.1080/23738871.2019.1635176.
O'Connell, A., and K. Bakina. 2020. "Using IP Rights to Protect Human Rights: Copyright for 'Revenge Porn' Removal." *Legal Studies* 40: 442–457.
Office for National Statistics. 2019. Domestic Abuse and the Criminal Justice System, England and Wales: November. Last accessed August 19, 2021. https://www.ons.gov.uk/

peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseandthecriminaljustice systemenglandandwales/november2019.
O'Hara, E. 2005. "Victim Participation in the Criminal Process." *Journal of Law and Policy* 13 (1): 229–247.
Online Safety Bill. 2021.CP 405. ISBN 978-1-5286-2563-0
Otero, D. 2016. "Confronting Non-Consensual Pornography with Federal Criminalization and a "Notice-and Takedown" Provision." *University of Miami Law Review* 7: 585. https://repository.law.miami.edu/umlr/vol70/iss2/9.
Patel, U., and R. Roesch. 2020. "The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Systematic Review." *Trauma, Violence, & Abuse*, 1–16. doi:10.1177/1524838020958057.
Powell, A., and N. Henry. 2018. "Policing Technology-Facilitated Sexual Violence against Adult Victims: Police and Service Sector Perspectives." *Policing and Society* 28 (3): 291–307. doi:10.1080/10439463.2016.1154964.
Powell, A., A. J. Scott, A. Flynn, and N. Henry. 2020. Image-Based Sexual Abuse: An International Study of Victims and Perpetrators: A Summary Report, February 2020.
Raitt, F. 2013. "Independent Legal Representation in Rape Cases: Meeting the Justice Deficit in Adversarial Proceedings." *Criminal LR* 9: 729.
Refuge. Annual Report 2019-2020. Available at: https://www.refuge.org.uk/our-story/annual-reports/.
Refuge. 2020. Written Evidence Submitted by Refuge (DAB33) to the Domestic Abuse Bill. June 11. https://publications.parliament.uk/pa/cm5801/cmpublic/DomesticAbuse/memo/DAB33.htm.
Romero-Moreno, F. 2019. "Notice and Staydown' and Social Media: Amending Article 13 of the Proposed Directive on Copyright, International Review of Law." *Computers & Technology* 33 (2): 187–210. doi:10.1080/13600869.2018.1475906.
Schwartz, P. 2019. "Global Data Privacy: The EU Way." *New York University Law Review* 94: 101–146.
Scottish Government. 2019. Recorded Crime in Scotland 2018-2019. Last Accessed: August 19, 2021. https://www.gov.scot/publications/recorded-crime-scotland-2018-19/pages/4/.
Slakoff, D. C., W. Aujla, and E. PenzeyMoog. 2020. "The Role of Service Providers, Technology, and Mass Media When Home Isn't Safe for Intimate Partner Violence Victims: Best Practices and Recommendations in the Era of COVID-19 and Beyond." *Archives of Sexual Behavior* 49: 2779–2788.
Snaychuk, L. A., and M. L. O'Neill. 2020. "Technology-Facilitated Sexual Violence: Prevalence, Risk, and Resiliency in Undergraduate Students." *Journal of Aggression, Maltreatment & Trauma* 29 (8): 984–999. doi:10.1080/10926771.2019.1710636.
Strelan, P., and J. Van Prooijen. 2013. "Retribution and Forgiveness: The Healing Effects of Punishing for Just Deserts." *European Journal of Social Psychology* 43: 544–553.
Sugiura, L., and A. Smith. 2020. "Victim Blaming, Responsibilization and Resilience in Online Sexual Abuse and Harassment." Chap. 3, in *Victimology Research, Policy and Activism*, edited by Iacki Tapley, and Pamela Davies. Portsmouth, UK: Palgrave MacMillan.
Taylor, C., and L. Gassner. 2010. "Stemming the Flow: Challenges for Policing Adult Sexual Assault with Regard to Attrition Rates and Under-Reporting of Sexual Offences." *Police Practice and Research* 11 (3): 240–255.
UK Safer Internet Centre. 2021. Report on Reporting of Online Harms by Young People. March.
United Nations. 2009. Report of the Secretary-General on Legal Empowerment of the poor and eradication of poverty, A/64/133 Sixty Fourth Session.
Unsolicited Explicit Images & Deepfake Pornography Bill. 2021. Long Title. https://bills.parliament.uk/bills/2921.
UN Women. 2020. Online and ICT* Facilitated Violence against Women and Girls during COVID-19. Accessed September 10, 2021. https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19.
Vaile Wright, C., S. Perez, and D. M. Johnson. 2010. "The Mediating Role of Empowerment for African American Women Experiencing Intimate Partner Violence." *Psychological Trauma: Theory, Research, Practice, and Policy* 2 (4): 266–272. doi:10.1037/a0017470.

Walklate, S., K. Fitz-Gibbon, and J. McCulloch. 2017. "Is More Law the Answer? Seeking Justice for Victims of Intimate Partner Violence through the Reform of Legal Categories." *Criminology & Criminal Justice*, 1–17. doi:10.1177/1748895817728561.

Wall, D. 1997. "Policing the Virtual Community: The Internet, Cyberspace and CyberCrime." Chap. 9 in *Policing Futures*, edited by Peter. Francis, Pamela Davies, and Victor Jupp, 208–236. London: Palgrave Macmillan.

Webb, C., and S. Weale. 2020. "More Than 500 Child Victims of 'Revenge Porn' in England and Wales Last Year." *The Guardian*, October 9. https://www.theguardian.com/society/2020/oct/09/more-than-500-child-victims-of-revenge-porn-in-england-and-wales-last-year.

Wolters, P. T. J. 2018. "The Control By and Rights of the Data Subject under GDPR." *The Journal of Internet Law* 22 (1): 6–18.

Woodlock, D., M. McKenzie, D. Western, and B. Harris. 2020. "Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control." *Australian Social Work* 73 (3): 368–380. doi:10.1080/0312407X.2019.1607510.

Yar, M., and J. Drew. 2019. "Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Crime Prevention and Criminalisation in Australia and England & Wales." *International Journal of Cyber Criminology* 13 (2): 578–594. doi:10.5281/zenodo.3709306.

Zhong, L. R., M. R. Kebbell, and J. L. Webster. 2020. "An Exploratory Study of Technology-Facilitated Sexual Violence in Online Romantic Interactions: Can the Internet's Toxic Disinhibition Exacerbate Sexual Aggression?" *Computers in Human Behavior* 108. doi:10.1016/j.chb.2020.106314.

Zvi, L., and M. Shechory-Bitton. 2020. "Police Officer Perceptions of Non-Consensual Dissemination of Intimate Images." *Frontiers in Psychology* 11: 2148. doi:10.3389/fpsyg.2020.02148.