UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović

November 2, 2017

For all inquiries related to this submission, please contact:

Dr. Ronald J. Deibert
Director, The Citizen Lab, Munk School of Global Affairs
Professor of Political Science, University of Toronto
r.deibert@utoronto.ca

Contributors to this report (in alphabetical order):

Dr. Ronald J. Deibert, Professor of Political Science; Director, The Citizen Lab
Lex Gill, Research Fellow, The Citizen Lab
Tamir Israel, Staff Lawyer, Canadian Internet Policy and Public Interest Clinic (CIPPIC)
Chelsey Legge, Clinic Student, International Human Rights Program (IHRP), University of Toronto
Irene Poetranto, Senior Researcher and Doctoral Student, The Citizen Lab
Amitpal Singh, Research Assistant, The Citizen Lab

Acknowledgements:

We would also like to thank Gillian T. Hnatiw (Partner, Lerners LLP), Samer Muscati (Director, International Human Rights Program, University of Toronto), Miles Kenyon (Communications Officer, The Citizen Lab), Sarah McKune (Senior Researcher, The Citizen Lab), Jon Penney (Assistant Professor of Law; Director, Law & Technology Institute, Schulich School of Law) and Maria Xynou (Research and Partnerships Coordinator, Open Observatory of Network Interference (OONI)) for their support in the creation of this report.

Table of Contents

Executive Summary

In this brief submission to the United Nations Special Rapporteur on violence against women, its causes and consequences, we review some of the barriers to addressing the problem of technology-facilitated violence, abuse, and harassment against women and girls, drawing on examples from Canada and abroad.

At the outset, we raise questions about narratives that capitalize on the vulnerability of women and girls in order to justify new powers to surveil, de-anonymize, police, and censor in the digital sphere. There is limited evidence to suggest that providing greater generalized powers to law enforcement leads to better outcomes for women or other marginalized and vulnerable groups. In some cases, doing so may also increase opportunities and technological capabilities for abuse. We put forward that new powers (whether afforded to the state or deployed in the enforcement of private wrongs) should be demonstrably necessary, evidence-based, rights-protective, proportionate, and targeted.

Second, we stress the critical importance of promoting encryption, anonymity, and digital security tools to defend the safety of women and girls online; to strengthen their human rights; and to protect the work of human rights defenders working on issues of gender-based violence and discrimination worldwide.

Third, we note that systems for the lawful disclosure of personal information can help to efficiently identify perpetrators of online violence, abuse, and harassment against women in some cases. Similarly, effective systems for the removal of illegal and harmful online content provide essential remedies to survivors. However, when systems that impose legal obligations on intermediaries and service providers are not carefully implemented and lack sufficient oversight and accountability, they may be ineffective, counterproductive, overbroad, or in conflict with human rights in the digital sphere.

Fourth, we draw the Special Rapporteur's attention to some of the threats posed by commercial spyware (sometimes referred to as "stalkerware") in the context of gender-based violence, noting the serious challenges these technologies pose for law enforcement, frontline workers, human rights defenders, and targeted individuals. We emphasize the urgent need for greater political and legal intervention on this issue from states and the international community, and note the importance of holding vendors of commercial spyware accountable for the human rights abuses facilitated by their products.

Finally, we identify high-priority areas for education, training, and capacity-building. In particular, we highlight the urgent need for greater technical literacy among law enforcement, legal professionals, and frontline workers related to issues of online and technology-facilitated violence, abuse, and harassment. Conversely, we note that technologists, engineers, designers, and corporate leadership in the information and communications technology (ICT) sector also require extensive training related to the experiences and particular risks faced by women and girls online.

Throughout this submission, we identify examples of legal mechanisms and policy frameworks for harm mitigation, prosecution and redress, while recognizing that in most jurisdictions both the existing legal models and their practical implementation remain highly inadequate.

We hope these brief comments assist the Special Rapporteur in the preparation of her report to the Human Rights Council in June 2018.

About the Citizen Lab

Founded in 2001 by Professor Ronald J. Deibert,[1] The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research combining methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

We are committed to integrating a gender and diversity-based analysis into our work. Our research has frequently demonstrated that when emerging technologies are abused by states, corporate actors and malicious third parties, that abuse tends to disproportionately impact vulnerable groups—including women and girls. For example, Citizen Lab research has exposed efforts to target women in digital espionage campaigns,[2] revealed the use of surveillance tools against those seeking justice for slain women's rights advocates,[3] mapped Internet censorship systems that filter out information related to women's rights and sexuality,[4] and supported partners in the Global South who study online threats faced by women human rights defenders.[5]

The nature of technology-facilitated violence, abuse, and harassment against women

Online and technology-facilitated violence, abuse, and harassment can take many forms—including, but not limited to cyber stalking, non-consensual sharing or distribution of intimate photos and videos ("revenge porn"), harassment, hacking, denial-of-service attacks, the use of gender-based slurs, the publication of private and identifiable personal information ("doxing"), impersonation, extortion, rape and death threats, electronically enabled trafficking, and sexual exploitation or luring of minors.[6]

Women are both disproportionately targeted by these behaviours, and suffer disproportionately serious consequences as a result. However, gender is not the only variable which makes technology-facilitated violence, abuse, and harassment more likely or the consequences more severe. Discrimination on the basis of gender identity, gender expression, sexual orientation, disability, race, ethnicity, Indigenous status, age, religion and other factors also compound, exacerbate and complicate experiences of gender-based violence.[7] In some cases, inadequate legal protection, systemic bias, or experiences of police violence create additional barriers that limit women's abilities to seek the support of law enforcement. Studies demonstrate that Indigenous women,[8] women of colour,[9] women with precarious immigration status,[10] and sex workers[11] are among those groups.

Harms resulting from online and technology-facilitated violence, abuse, and harassment may be physical (e.g., stress-related illness, injury, and physical trauma), psychological or emotional (e.g., experiences of

shame, stress, and fear; loss of dignity; costs to social standing), and/or financial (e.g., costs related to legal support, online protection services, missed wages, and professional consequences). Online and technology-facilitated violence, abuse, and harassment can also have an adverse impact more broadly by increasing needs for health care, judicial, and social services; impeding the exercise of free expression and other human rights; and disturbing the sense of peace and security required to fully participate in economic, social, and democratic life.[12]

Attempting to draw clear boundary lines between "online" and "offline" conduct in this context is often difficult and frequently unhelpful. In some cases, online behaviour may amplify, facilitate, or exacerbate traditional categories of problematic conduct. In other cases, technology allows for entirely new forms of violence, abuse, or harassment to take place.[13] As a result, the language of "technology-facilitated" violence may be more inclusive or appropriate in some cases.

Both the nature of the misconduct and the nature of the resulting harms frequently evade neat legal categorization. In some cases, a flexible, contextual, and purposive application of existing laws can be sufficient to address problems of online and technology-facilitated violence, abuse, and harassment. In other cases, justice demands reform and modernization of both law and practice.

Efforts toward prevention, investigation, prosecution, and redress for gender-based violence, abuse, and harassment tend to face the same barriers as other forms of crime and misconduct online. In particular, complex legal tensions related to identification, jurisdiction, enforcement, competing rights, and the role of intermediaries are inherent to the digital policymaking arena. Where these issues interface with gender-based violence, abuse and harassment, they become even more complex. Aggravating factors include the absence of political willpower to address threats faced by women and girls; stereotypes and discriminatory attitudes about gender-based violence; and a lack of digital literacy among policymakers.

Ensuring that new powers are necessary, proportionate, rights-protective, and evidence-based

While the Internet has created new forms of information and new opportunities to gather it, it has also created new investigative barriers, both for law enforcement and in the enforcement of private rights. These challenges are frequently cited to justify new powers of general application for law enforcement and other actors.

In Canada, narratives which emphasize the vulnerability and victimhood of women and girls have been repeatedly employed in order to support claims for greater generalized government powers to de-anonymize, identify, track, and surveil individuals online. Most recently, these efforts have taken the form of Bill C-30 and Bill C-13, which were promoted as measures to target "child predators" and "cyberbullying" in 2012 and 2014 respectively.[14]

Bill C-13 introduced new provisions related to the non-consensual distribution of intimate images ("revenge porn") which filled a significant gap in Canadian criminal law.[15] However, both bills also proposed new "lawful access" provisions, despite little evidence that the new electronic search powers proposed for law enforcement were rationally linked to the specific challenges faced in investigations of gender-based violence, abuse or harassment online.[16] The surveillance powers in Bill C-13 in particular

were presented to the Canadian public as a response to the incidents of online abuse that led to the tragic suicide of Rehtaeh Parsons.[17] However, an independent inquiry into the police response concluded that law enforcement had already possessed the necessary search powers and grounds to investigate at the time of Ms. Parsons' complaint; they simply failed to use them due to a lack of training in identifying legal wrongs in a technologically mediated context.[18]

Legislation purported to protect against gender-based violence may have deleterious collateral impacts on other human rights, if not properly tailored. For example, Citizen Lab research fellow Jon Penney has recently demonstrated that women and young people are disproportionately likely to experience "chilling effects" of Internet surveillance and regulation and to engage in digital self-censorship as a consequence.[19] Bill C-13's more expansive surveillance powers might therefore do more harm than good, if they neither significantly extend the state's ability to address technology-facilitated violence, abuse, and harassment against women, and operate to chill the online activities of women and girls. Bill C-30 (which did not ultimately become law) would have similarly threatened the freedom of expression, safety, and privacy rights of all people in Canada—including the rights of women and girls—by requiring telecommunications service providers to intentionally weaken user security and to comply with extraordinary new surveillance powers.[20] In addition to Bill C-13, the death of Rehtaeh Parsons also generated comprehensive 'cyberbullying' legislation in the Canadian province of Nova Scotia. However, the courts ultimately struck down that law on the basis that it was overbroad and lacked procedural safeguards commensurate with its impact on free expression and liberty.[21] A new United States bill proposing amendments to the *Communications Decency Act* is similarly described as addressing illegal sex trafficking, but would profoundly jeopardize long-established protections for freedom of expression online and has been heavily criticized by women's rights advocates.[22]

Claiming that a policy measure is beneficial for the protection of vulnerable individuals does not make it so in practice. For example, in collaboration with OpenNet Korea,[23] Cure53,[24] and other researchers, Citizen Lab investigated security vulnerabilities in government-mandated South Korean child monitoring applications, which are intended to protect children online.[25] One such application is Smart Sheriff, which was released by the Korean Mobile Internet Business Association (MOIBA), an influential consortium of mobile telecommunications providers and phone manufacturers. Our joint audit in collaboration with Cure53[26] found that authentication, registration, and communications with Smart Sheriff's servers are all unencrypted. As a result, names of minors and parents, dates of birth, mobile device information, gender, and telephone numbers are all visible to anyone controlling the network that the device uses and thus vulnerable to interception. Our investigation also revealed security and privacy issues in Smart Dream, which is another MOIBA-developed child monitoring application. The app monitors children's messaging applications and online search history against a database of keywords. These keywords include those related to body parts and functions, such as menstruation, as well as gender and sexual expression (e.g., homosexuality). Our analysis of Smart Dream revealed serious security vulnerabilities that could allow unauthorized access to stored messages and search history.[27]

In short, even well-intentioned policy measures meant to protect vulnerable groups can have serious negative consequences when not properly implemented.

New powers to de-anonymize, track, monitor, and surveil also create new avenues for abuse. Tools which provide government actors unchecked access to vast quantities of personal information create attractive targets for malicious third parties, which can then use that data to commit fraud, identity theft, blackmail, and other exploitative crimes.[28] Finally, law enforcement officers or other state agents may

themselves be perpetrators of violence, abuse, and harassment—and there are unfortunately many examples where such individuals have leveraged state surveillance tools in order to stalk former partners or to engage in other forms of professional misconduct.[29] Within the intelligence community, this form of abuse of power is so common that it has its own name: LOVEINT.[30]

There are often major institutional barriers within law enforcement agencies that limit their ability to effectively respond to complaints of gender-based violence, abuse, and harassment more generally—whether online or off. Though appeals for greater investigative powers are commonplace, it is not clear that police forces consistently make use of the full range of existing powers at their disposal to address threats to women and girls online.

Recommendation 1: The Special Rapporteur on violence against women should collaborate with the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the right to privacy when formulating policy responses

Complex legal problems—including those related to identification, jurisdiction, enforcement, and the role of intermediaries—are inherent to policymaking in the digital arena. Where new powers are insufficiently targeted or fail to account for the unique characteristics of the online ecosystem, they may also threaten human rights, including—but not limited to—freedom of opinion, expression, and privacy. The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the right to privacy have both engaged in extensive study of these issues which are likely to be of invaluable guidance in determining appropriate policy responses to technology-facilitated violence, abuse, and harassment against women and girls.[31]

We recommend that the Special Rapporteur on violence against women work closely with these other experts, attempt to harmonize their findings where possible, and account for the possibility of collateral impact on other human rights in the formulation of policy responses.

Recommendation 2: States should ensure that all new powers conform with the International Principles on the Application of Human Rights to Communications Surveillance ("Necessary & Proportionate Principles")

The International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles") provide civil society groups, states, the courts, legislative and regulatory bodies, industry, and others with a framework to evaluate whether current or proposed electronic surveillance laws and practices are compatible with human rights.[32]

In September 2013, the Necessary & Proportionate Principles were presented by representatives from Access, Privacy International, the Electronic Frontier Foundation, the Association for Progressive Communications, Reporters Without Borders, the Center for Democracy and Technology, and Human Rights Watch on various occasions, and at a side event at the 24th session of the UN Human Rights Council in Geneva.[33] Today, the principles have been endorsed by over 600 organizations, over 40 experts, and 6 elected officials or political parties from over 100 countries, along with over 270,000 individuals from around the world. The Principles were also cited favourably in a report by the President's Review Group on Intelligence and Communications Technologies, the Special Rapporteurs on free expression for the UN and the Organization of American States, the UN High Commissioner for Human

Rights, and by members of the European Court of Human Rights.[34] The Necessary & Proportionate Principles encode the need to adopt surveillance powers only where these are demonstrably necessary and effective, the need for prior merits-based authorization from a judicial authority, the need to notify affected individuals promptly, and the need for statistical reporting on the use of surveillance powers.

We recommend that in all cases where the Special Rapporteur encourages the adoption of new investigative powers for law enforcement that they operate in conformity with these thirteen principles.

Recommendation 3: States should adopt legislative obligations for data collection and transparency reporting

Transparency reporting is an essential tool to ensure the lawful and appropriate use of police investigative powers.[35] In Canada for example, some invasive surveillance capabilities (such as a wiretap) can only be authorized in order to investigate specific, serious offences from among a list enumerated in the *Criminal Code*.[36] The Minister of Public Safety is also required to produce an annual report on the use of some electronic surveillance powers which indicates the offences in respect of which authorizations were granted, and the number of authorizations granted for each type of offence.[37]

Problematically, many new search and seizure powers—including an overhaul of Canada's framework for production and interception of transmission and tracking metadata which came into force in 2015 as part of Bill C-13[38]—do not require annual reporting on their use and are not restricted to an enumerated list of offences. As a result, though the legislation was purportedly designed to address "cyberbullying," there is no way to determine the extent to which these powers are actually used to investigate and prosecute cyberbullying-related crimes (or, for that matter, entirely unrelated offences).

We recommend that the Special Rapporteur encourage States to adopt legislative obligations for internal data collection and transparency reporting whenever new powers are afforded to law enforcement in order to counter online violence, abuse, and harassment. Detailed transparency reporting provides essential data to women's advocates and researchers, allows the public to better understand the extent to which new powers are actually used to address the problems which first justified their adoption, and helps to better evaluate their utility in achieving stated objectives and their general effectiveness in achieving their harm reduction objectives. In sum, transparency reporting helps to ensure that new powers are evidence-based and rationally connected to their stated objective.

Recommendation 4: States should modernize existing legislation to ensure that it remains effective and inclusive in light of technological change

In some cases, legislative modernization will be necessary to ensure that laws designed to protect survivors of gender-based violence, abuse, and harassment remain effective and inclusive in light of technological change. For example, prior to the adoption of the *Criminal Code* provisions related to the publication, distribution, transmission, sale, and advertisement of non-consensual intimate images ("revenge porn") in 2014, Canadian law enforcement did not usually take any criminal action following a complaint "unless the images qualif[ied] as child pornography or [were] accompanied by additional aggravating factors."[39] While introducing new offences does not remedy historical deficiencies in training and prioritization, explicitly defining such activity alleviates the need to fit harmful conduct into more generalized offences (e.g. criminal harassment, extortion, or mischief in relation to computer data) and thereby extends recourse to a greater number of women.[40]

Another example is the newly proposed Bill C-51, which would make several amendments to the sexual assault provisions in the Canadian *Criminal Code*.[41] While the potential implications of Bill C-51 for sexual offence trials are complex, of particular relevance is the expansion of the "rape shield" provisions, which provide that evidence of a complainant's prior sexual history cannot be used to support an inference that the complainant was more likely to have consented to the sexual activity at issue, or that the complainant is less worthy of belief, commonly referred to as the "twin myths."[42] The Canadian Supreme Court has found that the rape shield provisions of the *Criminal Code* enhance the fairness of hearings by excluding misleading and irrelevant evidence from trials of sexual offences.[43] If adopted, Bill C-51 would revise these provisions to include communications of a sexual nature or for a sexual purpose (e.g., text messages, emails, video recordings) within the definition of the complainant's prior sexual history.[44] In many cases, justice will not require the creation of entirely new offences or civil wrongs, but rather careful updates to existing provisions in order to fill gaps created by technological change.

The importance of encryption and anonymity tools to the security of women online

In 2015, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, released his seminal report on encryption, anonymity, and the human rights framework. The report recognized that while encryption and anonymity tools can be used as shields by perpetrators of harassment, they are also vital to human rights and to members of groups vulnerable to technology facilitated violence, harassment and abuse, who can "use [these] tools to ensure their privacy in the face of harassment."[45] The availability and use of such tools should generally be encouraged, rather than undermined.

Encryption uses a mathematical process to transform data into a form which is unreadable by parties that are not in possession of the encryption key. Encryption can be used to protect the confidentiality, authenticity, and integrity of data both while it is at rest (i.e., while stored on a device) and in transit (i.e., while being transmitted over a network). It is a foundational technology of the Internet, and is essential not only for the protection of human rights, but also to the economy, public safety, and global security more broadly.[46] Anonymity tools such as Tor use both encryption and routing techniques to conceal an individual's location and behaviour online, enabling anonymous communication and allowing users to circumvent Internet censorship in countries where online content is blocked.[47] "Onion services" are a related technology that allow Tor network users to access and offer various kinds of services (such as file sharing, web publishing, or instant messaging) while hiding their location from eavesdroppers and intermediaries.[48] Encrypted messaging services such as WhatsApp and Signal confound censorship filters that would otherwise block the exchange of dissenting or minority views in private conversations.[49]

In his report, the Special Rapporteur found that "encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief,"[50] enable freedom of expression, and facilitate the freedom to seek, receive, and impart information and ideas regardless of frontiers.[51] He highlighted the essential link between the security afforded by these technologies and other rights, "including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity."[52] In 2016, The UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein similarly

stated that "it is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered."[53]

However, in many jurisdictions, law enforcement agencies have continued to raise alarm about the rise of strong encryption and anonymity tools, arguing that they pose a threat to their ability to conduct investigations online. They claim that the Internet is "going dark" as a result of these technologies, and that widespread access to effective digital security tools threaten law enforcement's ability to de-anonymize individuals, monitor communications, and access evidence required to bring wrongdoers to justice—including wrongdoers engaged in gender-based violence, abuse, and harassment.[54] In response, they have asked for dramatic powers and regimes for "exceptional access," which would require service providers to intentionally weaken the security of the technologies they develop in order to make law enforcement investigations easier. In the last year alone, calls to undermine, weaken, or subvert encryption technology have come from various political leaders in countries such as Australia and the United Kingdom among others.[55]

Proposed measures to undermine encryption and anonymity tools are neither necessary nor proportionate, and would profoundly threaten privacy rights, freedom of expression, and the security of persons, including the security of women and girls. The consensus that exists among computer scientists, security researchers, industry experts, and human rights activists in opposition to these government proposals has been analogized to the scientific consensus on climate change.[56] Measures designed to weaken, circumvent, or undermine encryption systems inherently increase system complexity (by extension, increasing risk) and create strong incentives for malicious actors to target government credentials and other "lawful access" tools with potentially disastrous consequences.[57] In short, legislative and technical attempts to weaken, circumvent, or undermine encryption technology jeopardize the safety and security of all Internet users.

While it is true that encryption and anonymity tools make some forms of online investigations more difficult for law enforcement, it is more accurate to characterize that challenge as increased investigative *friction*, rather than investigative impossibility. There is no data to support the claim that strong encryption poses an insurmountable barrier in the vast majority of criminal investigations, and an increasingly large range of alternative measures and data sources remain available to law enforcement.[58] Those technological and legal alternatives include metadata analysis, location record tracking, and the use of well-established human intelligence techniques, all of which are more minimally impairing of the fundamental rights and interests at stake.[59] The use of encryption and anonymity tools are also essential to law enforcement's ability to operate effectively online: for example, Tor is used to facilitate anonymous police tip lines and sting operations conducted in the course of digital investigations.[60]

End-to-end encrypted messaging platforms like Signal Messenger are increasingly used by at-risk populations to communicate via text and voice securely.[61] End-to-end encryption ensures that messages can only be read by their intended recipients, and features like "disappearing" and "revocable" messages help women to exercise greater control over the information they share with others.[62] Encrypted storage tools help women keep personal information and evidence of abuse safe, and may allow them to carve out private spaces for self-expression despite surveillance by abusive partners and others.

Anonymity software also provides critical protections for survivors of sexual violence, abuse, and harassment; tools like Tor are becoming vital tools to help women leave dangerous relationships safely.[63]

New software solutions are also increasingly being deployed to allow women to securely and anonymously report instances of sexual assault and violence; Project Callisto provides one such example on university campuses in North America.[64] Another example is SecureDrop, a tool developed by Freedom of the Press Foundation, which facilitates anonymous whistleblowing to journalists using onion services over the Tor network.[65] SecureDrop has been adopted by prominent media organizations worldwide,[66] and tools like it may increasingly be used to facilitate anonymous whistleblowing related to gender-based violence, abuse, and harassment.[67]

Websites relating to women's rights, sexuality, and reproductive health (including access to abortion and birth control) have been frequent targets of government censorship. Encryption and anonymity tools allow women to shield their location and identity from governments seeking to limit their speech and curtail access to information: in a recent study exploring the use of ICTs among reproductive rights activists in Latin America, nearly half of those interviewed indicated that they used anonymous browsing tools like Tor.[68] Onion services can also be used to conceal the physical location of a host, defend against website takedowns in the form of domain name seizure, and encrypt communications end-to-end between users and websites. As a result, they also offer a robust opportunity for censorship-resistant and secure hosting—ensuring access to information, protecting the voices of women online, and shielding them from threats to their physical safety or liberty in response.

Examples of content related to women's rights, sexuality, and reproductive healthcare issues which are unavailable in certain jurisdictions, provided by the Open Observatory of Network Interference (OONI)

URL:	Not available in:
http://www.feminist.com	Iran
http://www.feminist.org	Iran
http://www.ifeminists.com	Iran, Cuba
https://www.awid.org	Iran
http://www.womeniniran.com	Iran (blocked even through the domain is squatted)
http://www.unpo.org	Iran, China
https://www.amnesty.org	China
http://guerrillagirls.com	Pakistan, Iran, Indonesia
http://www.itsyoursexlife.com	Iran, Indonesia, Saudi Arabia
http://www.scarleteen.com	Iran, South Korea
http://teensource.org	Iran
http://sfsi.org	Iran, Indonesia
http://plannedparenthood.org	Iran
http://www.siecus.org	Iran, Indonesia
https://www.sexualhealth.com	Iran
http://www.positive.org	Iran, Indonesia
http://www.premaritialsex.info	Iran, Indonesia

The examples included in the table above are drawn from data recently analyzed from the Open Observatory of Network Interference [OONI] in October 2017. More examples from different jurisdictions are likely available through OONI's publicly available dataset (see https://ooni.torproject.org/ and https://api.ooni.io)

Finally, efforts to undermine encryption and anonymity tools may set a dangerous international precedent for authoritarian and repressive governments unconstrained by due process or the rule of law, creating particular risks for civil society organizations and other actors (including women's advocacy groups) working to defend human rights. As the Citizen Lab's 2015 response to the Special Rapporteur's call for submissions on encryption and anonymity describes in detail, encryption and anonymity tools are vital to the protection of civil society organizations, activists, and human rights defenders.[69]

Recommendation 5: States should protect and encourage the development of technologies—including encryption and anonymity tools—that protect the rights of women and girls online

As a recent UNESCO report has noted, "much of the debate about encryption has, until now, been gender-blind, or perhaps worse, male-dominated," despite the fact that women and girls experience both disproportionate and qualitatively distinct threats to their privacy, security, dignity, and ability to participate fully in the online sphere.[70] However, a review of the resources created by grassroots advocacy organizations to support women seeking to improve their digital safety makes it clear that encryption and anonymity tools play a profound role in protecting women's safety online.[71]

A more thorough accounting of the ways in which encryption and anonymity tools might better contribute to the security and human rights of women and girls in the digital sphere is necessary and overdue. The Special Rapporteur on violence against women is in a unique position to provide strategic expertise in those efforts, and to encourage the development of technologies which more fully account for the experiences and needs of women online.

We recommend that the Special Rapporteur consider the specific importance of encryption and anonymity tools to the protection of women and girls online, and affirm the findings of the Special Rapporteur on freedom of expression on this matter, including the recommendation that:

> "States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education."[72]

Recommendation 6: States should adopt legal mechanisms to protect the anonymity of complainants in both civil and criminal proceedings

Anonymity facilitates the capacity of women and girls to report instances of violence, abuse, and harassment—both on and offline. In Canada, the Supreme Court has recognized that protecting the identity of a young complainant in a civil proceeding was necessary to realize the right to privacy and prevented the serious harms of re-victimization while minimally limiting the open court principle or freedom of the press.[73] The Court has also affirmed the constitutionality of *Criminal Code* provisions which shield the identity of complainants in criminal sexual offence proceedings from publication, while preserving press access to the hearing and ability to report on all other aspects of the trial.[74]

The complex role of online service providers in identifying users and removing content

Internet intermediaries play a crucial and central role in our digital interactions. As a result, they are often at the centre of attempts to address individual instances of online abuse, as well as of broader policy debates regarding technology-facilitated violence, harassment, and abuse. However, finding appropriately balanced mechanisms that scale to the operational realities of online intermediaries has been challenging.

Liability-based mechanisms have almost uniformly led to poor outcomes. There is ample evidence of the extensive over-enforcement that occurs when intermediaries are compelled to identify allegedly abusive users or to remove allegedly illegal content under threat of liability. This is particularly so in the absence of narrowly defined court orders or other legal safeguards. Such over-enforcement inevitably leads to disproportionate interference with the rights to privacy and free expression, including the rights of women and girls. On the other hand, current mechanisms are predominantly voluntary, leading to inconsistent outcomes and under-enforcement related to harmful and abusive content. In either case, the various economic, social, and moral harms that flow from online and technology-facilitated violence, harassment, and abuse often remain unmitigated.[75]

States should exercise caution when enlisting intermediaries in attempts to address online abuse, as well as when engaging in certain targeted measures to mitigate the harms of such conduct.

Recommendation 7: Mechanisms for states and private litigants to access identification data from Intermediaries should be rights-protective, effective and tailored

In some situations, identification of an unknown perpetrator is necessary to address online or technology-facilitated gender-based violence, harassment, or abuse. For example, a study conducted by the Swedish National Council for Crime Prevention in 2015 found that while a high proportion of police-reported online threats and incidents in the dataset were alleged to have been committed by a known acquaintance (40% in general, 43% among girls), a substantial volume were attributed to anonymous or suspected but unidentified individuals (33% in general, 44% among girls).[76] Generally, the identification process will require the ability to link digital identifiers such as an Internet Protocol (IP) address or IMSI number to physical devices and real-world identities.[77] A variety of carefully tailored legal tools can facilitate this identification process.

Where the conduct in question is potentially criminal in nature, law enforcement may rely on various investigative tools and specialized powers. Law enforcement mechanisms for digital identification can be mandatory, permissive, or court-order based. In many cases, it should be noted that the underlying nature of the implicated conduct can provide sufficient grounds to engage court-ordered early-stage criminal investigative powers such as production orders. The added safeguard of a ‘grounds’-based court order for digital identifiers is not a substantial impediment to investigating anonymous online or technology-facilitated violence, harassment or abuse.[78] Indeed, state investigations will often stall due to a lack of law enforcement expertise, and not because of an unmet need for broader surveillance powers or unfettered access to digital identifiers.[79] On the other hand, the anonymity generally protected by such identifiers engages significant privacy and expressive values, and generally demands a commensurate level of protection.[80]

Online or technology-facilitated violence, harassment, or abuse against women can also implicate rights protected by a private cause of action, and such rights are increasingly evolving to encompass such activity even in scenarios where no direct economic or physical harm can be demonstrated.[81] Such private causes of action can overlap with or extend criminalized conduct,[82] and allow individuals to engage legal identification powers on their own initiative, substituting cost and personal effort for barriers such as police disinterest, lack of expertise,[83] and obligation to respect the procedural safeguards engaged where the state investigates criminal conduct.[84] Where the underlying conduct engages a potential civil wrong, a cause of action can be filed with relatively minimal cost and increasingly with safeguards to protect the anonymity of the complainant.[85] This, in turn, engages third party discovery powers at an early stage of the litigation that can be used to obtain identification data from entities such as social media sites, email service providers and Internet service providers. Third party discovery orders should carry adequate safeguards to ensure they are not abused to identify anonymous online conduct in the absence of a wrong.[86] However, such safeguards remain a relatively minimal and therefore proportionate impediment to identifying a perpetrator in situations where the anonymous conduct clearly demonstrates a potential legal wrong.[87] As such, voluntary identification of anonymous customers accused of civil wrongs should generally be prohibited as they are not required to identify anonymous perpetrators of online abuse.[88]

Other specialized rights and mechanisms can be leveraged to identify the perpetrator of gendered technology-facilitated violence, abuse or harassment in certain contexts. For example, abusers will often take control of an account belonging to their target as a means of facilitating harassment or even surveillance. In such instances, individual access rights found in many data protection regimes can be used to identify the IP address used to access the account.[89]

In some jurisdictions, specialized tribunals have been developed to assist in the rapid removal of violent, harassing, or abusive material from online platforms. This approach recognizes that in many instances, the rapid removal of abusive online material will be the primary objective of the complainant, and that often identification of the distributor of such material will not be feasible regardless of how broadly identification powers are formulated.[90] While such rapid response mechanisms are not appropriate for all types of content removal,[91] they may provide effective relief even in the absence of broad identification powers.

Recommendation 8: Intermediaries should not be compelled to remove content in the absence of a narrowly tailored and specific court order, issued further to a clearly defined legal prohibition

Intermediaries can play a role in mitigating the harms of online abuse. However, the scope, scale and distance at which most intermediaries operate poses challenges to effective and proportionate removal of illegal content in ways that are not substantially over- or under-inclusive. Many online platforms already remove abusive online content on their platforms, and many include dedicated tools to flag abusive online comments, images, videos, or accounts. However, the opacity and inconsistent application of the voluntary mechanisms that assess and respond to such ‘flagging’ provide no assurance that the removal of abusive content will be conducted fairly or proportionately, and often operate as a deterrent to reporting by those experiencing abuse.

At the same time, however, a long history of experience with liability-based takedown mechanisms in a range of contexts shows such mechanisms consistently lead to overbreadth when applied to intermediaries. Even in the absence of liability, great caution must be exercised when enlisting intermediaries to enforce the removal of illegal content, and compelled intermediary content removal should perhaps be reserved for the most egregious and unambiguous instances of online abuse, such as the non-consensual publication of intimate images.

Recommendation 9: All new measures adopted by states to regulate online content removal should conform with the Manila Principles on Intermediary Liability

The Manila Principles on Intermediary Liability provide a useful reference point for minimal requirements that should be met in any effort to enlist intermediaries as content enforcement agents.[92] The Principles have been endorsed by organizations and experts worldwide working on human rights in the digital sphere, including Article 19, Asociación por los Derechos Civiles, the Centre for Internet and Society, ONG Derechos Digitales, Kenya ICT Action Network, OpenNet Korea, and the Electronic Frontier Foundation.

Imposing liability on platforms and other intermediaries for user-generated content frequently leads to overbroad censorship. Platforms faced with a choice between assuming the potential liability of a user as their own and preemptively removing contested content more often than not err on the side of content removal.[93] Premising liability immunities for third party content in this manner also encourages automation of takedown responses—particularly by central intermediaries who are used by billions of individuals around the world and who therefore face large volumes of allegedly infringing content with no incentive to conduct case-by-case assessments of the underlying legitimacy of allegations.[94]

Imposing generalized takedown obligations on intermediaries also encourages the use of undiscerning categorization mechanisms that generate a significant number of false positives, leading to negative consequences for a wide range of legitimate conduct.[95] The problem with these monitoring schemes is context—the intermediaries are unable to assess the contextual variations that arise when particular content is flagged, which becomes all the more problematic when applied to online abuse.[96] The use of decontextualized blanket prohibitions to address obscene content, for example, has led to arbitrary restrictions on non-harmful expression by women on matters relating to bodily autonomy and women's health (for example, censoring images of breastfeeding as "obscenity").[97] Generalized monitoring obligations of this nature can also disproportionately impact the right to privacy, as their development will often require a level of pervasive monitoring of sensitive user activity.[98]

Legal systems are increasingly acknowledging and recognizing the harms that can result from online abuse and crafting legal protections to address these harms.[99] While challenges remain on this front,[100] establishing clear, concise and narrowly targeted standards with respect to online content that is abusive of women can not only address such challenges, but also provide clarity for all affected stakeholders and individuals as to the scope of their rights. Intermediaries should not be compelled to remove content absent a specific and targeted order issued by an independent and impartial judicial authority arising from a clear prohibition set out in law.[101]

Recommendation 10: Intermediaries engaged in the moderation of online conduct should be encouraged to adopt transparency reporting mechanisms, publish clear and comprehensive content moderation policies, and develop explicit review and appeal processes

The Recommendations for Responsible Tech—a set of guidelines crafted by the Centre for Law and Democracy which incorporates the work of Citizen Lab researchers—provide a useful framework for effectively addressing the moderation and removal of content.[102]

Currently, complaints regarding online abuse are predominantly addressed by opaque and voluntary decision-making premised on secretive internal policies. While some online platforms solicit input from relevant stakeholders in the formulation of internal policies for removal of abusive content and accounts, these policies generally develop in a vacuum and without public debate or discussion despite their wide-ranging public impact. It is perhaps not surprising that the product of these internal and closed processes can be unprincipled, and that threats against women in particular often receive insufficient attention.[103] At minimum, consistently publicizing these policies will allow for necessary public dialogue on the scope of content removal activities, their excesses, and their shortcomings.[104]

Finally, the current absence of any meaningful appeal mechanisms and clearly established, consistent and participatory processes for intermediary assessment of claims from women experiencing online abuse confounds many of the challenges inherent in this context. Only the parties involved can provide the necessary context for a complaint, and such input can only be obtained through clearly defined and consistent complaint management processes.[105] The absence of a clear and guaranteed right for complainants to provide detailed input into assessments of reported abuse also contributes to a general lack of faith that complaints will be taken seriously.[106] The lack of any meaningful transparency in these decisions can also allow abuse of mechanisms designed to mitigate technology-facilitated violence, abuse, and harassment and "often obscures discriminatory practices or political pressures affecting the companies' decisions."[107] For example, recently leaked Facebook content moderation training materials overtly emphasize the severity of generalized threats against political figures over comparable threats against women.[108]

The obligation to establish clear and consistent complaints-handling mechanisms, inclusive of an obligation to provide rationales underlying decisions and the adoption of internal appeals processes, is therefore critical to any effective attempt to address online abuse through voluntary mechanisms.

Recommendation 11: All policy frameworks related to the removal and moderation of online content should account for the global nature of intermediaries

A final challenge to effectively and proportionately addressing technology-facilitated violence, harassment, and abuse emerges from the global nature of online intermediaries. The absence of a clearly defined consensus over the legal parameters of online abuse poses challenges for global platforms seeking to reconcile the numerous overlapping standards and norms governing tolerance for technology-facilitated violence, harassment, and abuse, for freedom of expression and for privacy. In navigating this complex overlapping matrix of norms, there must be minimal baselines rooted in international human rights norms that apply regardless of the domestic context in which they arise: online abuse of a degree that is simply never acceptable, expression that must be preserved regardless

of jurisdiction, and privacy safeguards that must be navigated as necessary prerequisites to investigations of online abuse.

Within these limits, some latitude for domestic contexts should be respected. This remains a rapidly emerging area of law, and the development of standards and guiding principles can help ensure realization of these goals. For example, where an online platform is compelled to remove abusive content due to violation of a state's laws, access to that content should generally only be restricted for residents of that state. At the same time, states should develop international norms around the most egregious and uncontroversial abusive online conduct such as the non-consensual distribution of intimate images.[109] Second, global platforms must respect the right to free expression as enshrined in international human rights instruments, even when assessing demands from states that lack formalized domestic human rights instruments.[110] Third, where a global platform faces data access demands from foreign jurisdictions, processes can be developed to expedite assessment of such data requests by courts, and mechanisms such as those set out in Mutual Legal Assistance Treaties can be streamlined to facilitate more efficient access. However, legal protections and safeguards in both the requesting and the data host jurisdiction must be respected prior to the disclosure of said data and cross-border access should never be used as a means of bypassing minimal safeguards in one jurisdiction by relying on weaker safeguards in another.[111]

A need for urgent action on the use and sale of commercial spyware and "stalkerware"

Governments worldwide are increasingly requiring telecommunications operators and Internet service providers to develop new tools in the name of fighting cybercrime and countering terrorism. This emerging market demand for spyware and surveillance tools has been met by a number of private firms worldwide, who specialize in the production of highly-sophisticated intrusive software capable of targeting the devices of users and granting access to personal information.

The commercial surveillance industry is estimated to be worth at least US$5 billion.[112] Its products have been developed largely in Western nations and marketed for sale to law enforcement and intelligence agencies worldwide, including to those operating in autocratic regimes with questionable human rights records. As Citizen Lab's Senior Legal Advisor Sarah McKune and Director Ronald Deibert have written, "where some see insecurity, others see a welcome market opportunity. Indeed, business is booming for a specialized market to facilitate the digital attacks, monitoring, and intelligence-cum-evidence-gathering conducted by government entities or their proxies."[113] Examples include Remote Control Systems, made by the Italian company Hacking Team,[114] the German-developed FinFisher suite,[115] and Israel-based NSO Group's Pegasus spyware.[116]

These tools have various features—for example, they can be used to covertly track an individual's GPS location, monitor and intercept their communications (including e-mails, phone calls, text messages, and social media activity), send fake messages on behalf of the target, remotely activate device microphones and cameras, access photos and videos, steal application passwords, duplicate call and message logs, and notify a monitoring party if the device is turned off.

While these tools may be principally developed with purposes of counterterrorism and espionage in mind, by various means—from creative commercial repackaging to black market sale—they fall into the hands of ordinary criminal or abusive actors. The proliferation of spyware technologies poses a distinct threat to the rights of women on at least two fronts. First, they have been used with impunity to target human rights activists, journalists, politicians, lawyers, and civil society organizations—including those working to defend the rights of women and girls. Second, these tools are increasingly being repackaged and sold to facilitate domestic violence, stalking, and other forms of technology-facilitated harassment and abuse that threaten the safety of women and girls.

Our research has found dozens of cases where commercial spyware has been deployed against civil society groups and human rights activists in the United Arab Emirates[117], Mexico,[118] and Ethiopia,[119] among others. In a recent series of reports, Citizen Lab research revealed that both a well-known female journalist as well as a prominent female lawyer representing the families of three slain Mexican women were personally targeted with NSO Group's government-exclusive Pegasus spyware.[120] Notably, journalist Carmen Aristegui's minor child was also targeted using NSO technology, highlighting the additional risks women face as caregivers in this context.[121] In July of 2017, a group of United Nations experts called on the government of Mexico to "to carry out a transparent, independent and impartial investigation into allegations of monitoring and illegal surveillance against human rights defenders, social activists, and journalists," based on the results of research conducted by Citizen Lab and others.[122]

Government-exclusive spyware produced by these companies has also been used to target internationally recognized human rights defenders like Ahmed Mansoor[123] and public health activists challenging the soda industry.[124] These targeted attacks against civil society raise myriad human rights concerns, and the consequences of abuse can be profound. Notably, both Gamma International (developer of FinFisher)[125] and Cisco Systems Inc. (architects of China's "Great Firewall" and a special "Falun Gong module" for surveillance and identification) have been named in multiple proceedings in which they were accused of developing surveillance tools that facilitate torture and other human rights abuses.[126] This pattern of abuse has critical implications for women's rights organizations and other gender advocacy groups vulnerable to these forms of targeted attack.

The proliferation of commercial spyware has implications for the safety of all women. A recent in-depth investigation conducted by VICE/Motherboard shed light on the use of these covert surveillance tools in the domestic violence context, where they are frequently referred to as "stalkerware."[127] Software with precisely the same capabilities as the spyware tools used to covertly monitor state actors or abused to target human rights activists can also be purchased for the purpose of monitoring a spouse or ex-partner—frequently for less than US $100. These tools allow abusers to exercise near-total control over a target's life and are notoriously difficult to detect (and, even in circumstances where a target is aware that she is subject to electronic surveillance, practical constraints may prevent her from taking action in response). Though the use of commercial software is widespread, a review of case law in Canada and the United States suggests that its users and manufacturers are rarely prosecuted.[128]

Yet in the United States, a National Public Radio survey of women's shelters revealed the pervasive state of the commercial spyware problem in the domestic violence context: 85% of shelters said they were "working directly with victims whose abusers tracked them using GPS" and 75% said they were working with "victims whose abusers eavesdropped on their conversation remotely."[129] Countless companies operating under various names are engaged in the sale and distribution of these technologies, and are part of a larger market ecosystem which facilitates domestic violence, abuse and stalking through other

technological means—such as criminal "hacker-for-hire" services that use phishing attacks to steal passwords to e-mail and social media accounts.[130]

One of the most well-known developers of commercial stalkerware is a company called FlexiSpy, which also sells an unbranded, private version of the technology which can be repackaged to meet various purposes (similar software, like Mobistealth,[131] has also been marketed for the purpose of surreptitiously monitoring children or employees).[132] FlexiSpy has a "sister company" called RaySoft that sells surveillance and hacking tools to law enforcement and intelligence, and which may have provided software to Gamma International for the development of FinSpy/FinFisher.[133] In other words, the commercial entities involved in tools used to target human rights defenders and those involved in developing stalkerware that jeopardizes the safety of women and girls are intimately interlinked—and in some cases, may even be one and the same.

Recommendation 12: States should hold manufacturers of commercial spyware accountable and engage legal measures to ensure that these tools are not abused to facilitate surveillance against women and human rights defenders

As McKune and Deibert have written, there is an urgent need to create accountability among private market actors engaged in the sale of digital surveillance tools, which are abused by governments and malicious actors alike.[134] Women—both as individuals in communities, and when working toward larger goals in human rights and civil society—face unique and acute risks as a result of these technologies.

Companies have independent obligations to respect human rights internationally,[135] but holding spyware manufacturers accountable in practice requires both international coordination and strong initiative from states. While "there is no single mechanism best suited to addressing the problems associated with the spyware trade," there is a possibility of developing a "web of constraints" to mitigate harm through a mix of public and private law, at domestic, regional and international levels.[136] At the outset, there is a need to systematically map frameworks for criminal and civil liability for those who abuse commercial spyware to surveil women and civil society actors (and for spyware vendors who are complicit in that surveillance).[137] There are also multiple other avenues through which the activities of spyware manufacturers may be constrained, from export controls[138] and consumer protection law[139] to contract and intellectual property law.[140] The legal frameworks to oversee and constrain the activities of private military and security contractors (PMSCs) will in some cases cover the activities of those in the spyware trade as well.[141]

The Special Rapporteur should engage on this issue to highlight the unique costs to women, calling on states to take action that regulates spyware vendors and minimizes the risk that these tools will be used to facilitate human rights abuses, particularly gender-based violence, harassment, and abuse.

The importance of stakeholder education, training, and capacity-building

Most legal professionals, law enforcement, and frontline workers do not receive basic training on the intersections between technology and violence against women, despite the fact that acts of gender-based violence, harassment and abuse are increasingly likely to have a technological nexus. For

example, a 2016 article in *The Guardian* reported that there were "serious concerns over the lack of skills and capability to properly investigate online abuse" among police officers in England and Wales, noting that less than 8% of the force had specialized training to respond to digital crime.[142] Without adequate training or access to resources on the ways in which technology is misused by stalkers, abusers, and other perpetrators, justice system and frontline anti-violence workers cannot provide the necessary supports to victimized women, children, and youth. A lack of digital literacy can dramatically impair the ability to appropriately identify legal wrongs; limit opportunities available for mitigation and redress; and may result in the provision of inaccurate and dangerous advice, exacerbating harm. Conversely, technologists require better resources to evaluate the potential impacts and risks of the software they develop for women and girls.

Expert-led technical training and educational resources are vital for professional development across many fields. As part of our efforts to improve digital literacy, the Citizen Lab has researched and written extensively on the human rights implications of technologies ranging from smartphones[143] and web browsers[144] to spyware[145] and wearable fitness tracking devices.[146] The need for such materials (adapted for non-specialist audiences) is particularly urgent when the safety and rights of vulnerable groups are at stake.

Recommendation 13: States should commit to supporting the development of specialized legal education materials and clinical resources on issues of technology-facilitated violence, harassment, and abuse

Legal professionals require practical training on the intersections of technology, law, and gender-based violence. In particular, prosecutors and judges need to better understand the ways in which new technologies (a) can be misused by stalkers, abusers, and other violent perpetrators; and (b) can make it more difficult to hold perpetrators accountable for their crimes by creating investigative and evidentiary barriers.[147] Similarly, lawyers and legal clinics need access to up-to-date information in order to provide women with access to effective legal advice and representation. This may take the form of continuing legal education (CLE) courses for counsel and members of the judiciary, as well as the creation and renewal of training resources such as handbooks, guidelines, and manuals.[148]

Digital literacy is also required to ensure that judges and other government actors (such as child and family service workers) implement appropriate safeguards to protect victims. For instance, in the case of a protection order where the subject of the order remains permitted to communicate with his children, notice should be taken regarding who purchases the communication technology used, who owns it, and who is allowed to modify it. Even where the subject of the order is prohibited from installing spyware on a victim's cell phone, he may be able to install spyware on a child's phone, particularly if he bought the device.[149]

Recommendation 14: States should mandate regular, expert-led training for law enforcement on responding to reports of technology-facilitated violence, harassment, and abuse

As discussed above, a major barrier faced by law enforcement is a lack of adequate training in determining what constitutes a chargeable offense in the digital context.[150] As a result, many victims have no choice but to remain in danger and without recourse until online conduct escalates or evolves into more "traditionally" recognizable forms of wrongdoing. Sensitivity training around sexual offences,

harassment, and abuse that includes detailed information about the experiences of women and girls online—and how those experiences map onto legally recognized categories of wrongdoing—would help to prevent inaction and mitigate harm.[151]

Properly trained law enforcement will also be better equipped to work with victims to identify and document relevant evidence. For example, more comprehensive technical knowledge will allow law enforcement to correctly advise victims about methods to document incidents of stalking or harassment.[152] Stalking logs make it easier for law enforcement and prosecutors to establish a pattern of suspicious, threatening, or harassing behaviour, and the logging process can be empowering for some victims by allowing them to take an active role in holding perpetrators accountable.[153]

Recommendation 15: States should invest in resources, education and support for frontline anti-violence workers to develop greater technical literacy

Frontline anti-violence workers (such as social workers and shelter staff) also require technical training to better understand new technologies and the ways in which technology can be abused to endanger women who access their services. Further, frontline workers should be trained to assess the use of technology by survivors when developing a safety plan, and to educate survivors about potential risks and benefits associated with various information technologies.[154]

Anti-violence agencies and shelters are also in need of resources that allow them to bring organizational policies and procedures in line with best practices regarding data security and privacy—without which they are unable to effectively protect their clientele.[155] For example, the Canadian Internet Policy & Public Interest Clinic (CIPPIC)[156] has worked with women's shelters who were compelled to undertake highly sophisticated and rapidly evolving network obfuscation techniques before their clientele could safely use online services without risking exposure of their location to an abusive spouse or partner. Technical challenges of this nature can put women at direct risk of physical violence and often arise on short notice. Yet many shelters lack the in-house resources to address—and often even to assess—such challenges.

Recommendation 16: The Special Rapporteur should encourage actors in the information and communication technology (ICT) sector to take a leadership role in preventing technology-facilitated violence, harassment, and abuse

Technologists and software developers need a more thorough understanding of the ways in which the technologies they build can be misused to harass, impersonate, threaten, locate, and monitor victims. In particular, companies involved in the design and development of applications, communications platforms, and online communities should be educated about how women and girls experience (and risk experiencing) technology-facilitated abuse, harassment, and violence. Technologists and software developers should actively seek feedback from women on potential risks at the design and testing stages prior to product launch, and make the necessary and appropriate modifications to mitigate risk. Systems should also be designed to be responsive to reports of abuse, harassment, and other harmful conduct. The Special Rapporteur on violence against women is well-positioned to encourage, facilitate, and participate in this dialogue alongside leaders in the information and communication technology (ICT) sector.

Summary of recommendations

1. The Special Rapporteur on violence against women should collaborate with the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the right to privacy when formulating policy responses
2. States should ensure that all new powers conform with the International Principles on the Application of Human Rights to Communications Surveillance ("Necessary & Proportionate Principles")
3. States should adopt legislative obligations for data collection and transparency reporting
4. States should modernize existing legislation to ensure that it remains effective and inclusive in light of technological change
5. States should protect and encourage the development of technologies—including encryption and anonymity tools—that protect the rights of women and girls online
6. States should adopt legal mechanisms to protect the anonymity of complainants in both civil and criminal proceedings
7. Mechanisms for states and private litigants to access identification data from Intermediaries should be rights-protective, effective and tailored
8. Intermediaries should not be compelled to remove content in the absence of a narrowly tailored and specific court order, issued further to a clearly defined legal prohibition
9. All new measures adopted by states to regulate online content removal should conform with the Manila Principles on Intermediary Liability
10. Intermediaries engaged in the moderation of online conduct should be encouraged to adopt transparency reporting mechanisms, publish clear and comprehensive content moderation policies, and develop explicit review and appeal processes
11. All policy frameworks related to the removal and moderation of online content should account for the global nature of intermediaries
12. States should hold manufacturers of commercial spyware accountable and engage legal measures to ensure that these tools are not abused to facilitate surveillance against women and human rights defenders
13. States should commit to supporting the development of specialized legal education materials and clinical resources on issues of technology-facilitated violence, harassment, and abuse
14. States should mandate regular, expert-led training for law enforcement on responding to reports of technology-facilitated violence, harassment, and abuse
15. States should invest in resources, education and support for frontline anti-violence workers to develop greater technical literacy
16. The Special Rapporteur should encourage actors in the information and communication technology (ICT) sector to take a leadership role in preventing technology-facilitated violence, harassment, and abuse

Endnotes

[1] Ronald J. Deibert is a Professor of Political Science at the University of Toronto and Director of the Citizen Lab at the Munk School of Global Affairs. He was a co-founder and a principal investigator of the OpenNet Initiative (2003-2014) and Information Warfare Monitor (2003-2012) projects. Professor Deibert was one of the founders and (former) VP of global policy and outreach for Psiphon, one of the world's leading digital censorship circumvention services. For his full biography, including notable publications, see: https://deibert.citizenlab.ca/bio/.

[2] See for example: John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," The Citizen Lab (19 June 2017), online: <https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/>.

[3] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware," The Citizen Lab (2 August 2017), online: <https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/>.

[4] Bennett Haselton, "Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE," The Citizen Lab (28 November 2013), online: <https://citizenlab.ca/2013/11/smartfilter-miscategorization-filtering-saudi-arabia-uae/>; The Citizen Lab, "O Pakistan We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime," Research Brief (June 2013), online: <https://citizenlab.ca/wp-content/uploads/2015/03/O-Pakistan-We-Stand-on-Guard-for-Three-An-Analysis-of-Canada-based-Netsweepers-Role-in-Pakistans-Censorship-Regime.pdf>.

[5] See for example: Gul Bukhari, "Technology Driven Violence Against Women," Country Report: Pakistan (August 2014), Bytes for All (B4A), in partnership with Association for Progressive Communications (APC), online: <http://content.bytesforall.pk/sites/default/files/ViolenceAgainstWomenPakistanCountryReport.Pdf>.

[6] EC, European Institute for Gender Equality, "Cyber Violence Against Women and Girls" (2017), online: <http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls>; UN Broadband Commission for Digital Development Working Group on Broadband and Gender, "Cyber Violence against Women and Girls: A Worldwide Wake-Up Call" (2015), online: <http://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf>; Linda Baker, Marcie Campbell, and Elsa Barreto, "Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences," Centre for Research & Education on Violence Against Women & Children, Learning Network Brief 6 (2013), online: <http://www.learningtoendabuse.ca/sites/default/files/Baker_Campbell_Barreto_Categories_Technology-Related_VAW_.pdf>; see also personal accounts detailed in Bytes for All (B4A), in partnership with Association for Progressive Communications (APC), online: <http://content.bytesforall.pk/sites/default/files/ViolenceAgainstWomenPakistanCountryReport.Pdf>.

[7] A recent Pew Research Center survey of American adults found that people who experienced online harassment were targeted most often due to their political views, physical appearance, gender, and/or race or ethnicity. Black people, Hispanic people, and women are disproportionately targeted. See Maeve Duggan, "Online Harassment 2017," Pew Research Center (11 July 2017), online: <http://www.pewinternet.org/2017/07/11/online-harassment-2017/>. In Canada, about half (52%) of police-reported hate crimes in 2011 were motivated by race or ethnicity. Another 25% were related to religion, and 18% to sexual orientation. See Mary Allen and Jillian Boyce, "Police-Reported Hate Crime in Canada, 2011," *Juristat* (11 July 2013), online: <http://www.statcan.gc.ca/pub/85-002-x/2013001/article/11822-eng.pdf>. See also: UN Women, "Beijing Declaration and Platform for Action, adopted at the Fourth World Conference on Women," (27 October 1995), UN Doc A/COF.177/20 (1995) and A/CONF.177/20/Add.1 (1995), endorsed by UN GA Resolution 50/203 (22 December 1995), online: <http://www.refworld.org/docid/3dde04324.html>; UN Committee on the Elimination of Discrimination against Women, "General Recommendation No 35 on Gender-Based Violence against Women, Updating General Recommendation No 19," UN Doc CEDAW/C/GC/35 (14 July 2017), see especially at para 12, online: <http://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf>; UN Human Rights Council, "Report of the Special Rapporteur on Violence against Women, its Causes and Consequences, Rashida Manjoo," 17th Sess, Agenda item 3, UN Doc A/HRC/17/26 (2 May 2011), see especially at para 14, online: <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A-HRC-17-26.pdf>; International Criminal Court, "Policy Paper on Sexual and Gender-Based Crimes," The Office of the Prosecutor (June 2014), online: <https://www.icc-cpi.int/iccdocs/otp/OTP-Policy-Paper-on-Sexual-and-Gender-Based-Crimes--June-2014.pdf>.

[8] See, for example: Human Rights Watch (2013), "Those who take us away: Abusive policing and failures in protection of Indigenous women and girls in Northern British Columbia," www.hrw.org/sites/default/ les/reports/canada0213webwcover.pdf; UN Human Rights Council, "Report of the Special Rapporteur on the rights of indigenous peoples, Victoria Tauli Corpuz," 30th Sess, Agenda item 3, UN Doc A/HRC/30/41 (6 August 2015), see especially paras 50, 77, and 79; Elizabeth Fast and Delphine Collin-Vézina, "Historical Trauma, Race-based Trauma and Resilience of Indigenous Peoples: A Literature Review" *First Peoples Child & Family Review* 5: 1 (2010) 126; Bronwyn Morrison, "Identifying and Responding to Bias in the Criminal Justice System: A Review of International and New Zealand Research," Research, Evaluation and Modelling Unit, New Zealand Ministry of Justice (November 2009), online: <https://www.justice.govt.nz/assets/Documents/Publications/Identifying-and-responding-to-bias-in-the-criminal-justice-system.pdf>; Harry Blagg, Neil Morgan, Chris Cunneen, and Anna Ferrante, "Systemic Racism as a Factor in the Over-Representation of Aboriginal People in the Victoria Criminal Justice System" (September 2005); Chris Cunneen and Juan Tauri, *Indigenous Criminology* (Bristol; Chicago, IL: Policy Press, 2016); Elena Marchetti and Thalia Anthony, "Sentencing Indigenous Offenders in Canada, Australia, and New Zealand" *University of Technology Sydney Law Research Series* 27 (2016), last updated May 16, 2017, online: <http://classic.austlii.edu.au/au/journals/UTSLRS/2016/27.html>; Amnesty International, "Indigenous Peoples' Long Struggle to Defend Their Rights in the Americas" (London, UK: Amnesty International Publications, 2014), see especially 21-24; UNICEF, UN Women, UNFPA, ILO, and OSRSG/VAC, "Breaking the Silence on Violence against Indigenous Girls, Adolescents and Young Women: A Call to Action Based on an Overview of Existing Evidence from Africa, Asia Pacific and Latin America" (May 2013), online: <https://www.unfpa.org/sites/default/files/resource-pdf/VAIWG_FINAL.pdf>; Rachel Sieder and Maria Teresa Sierra, "Indigenous Women's Access to Justice in Latin America," CMI Working Paper no 2 (2010), online: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1023.5720&rep=rep1&type=pdf>.

[9] See, for example: Yamikani Msosa and Erin Leigh, "Statement on Sexual Violence & Police Brutality in Case of Abdirahman Abdi," Ottawa Coalition to End Violence against Women (4 August 2016), online: <http://www.octevaw-cocvff.ca/statement-sexual-violence-police-bruatality-case-abdirahman-abdi>; Christa E. Noel and Dr. Olivia Perlow, "American Police Crimes Against African Women and Women of Color," Women's All Points Bulletin, Presented for the Review of the United States on the Adherence to the International Convention on the Elimination of All Forms of Racial Discrimination (2014), online: <http://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/USA/INT_CERD_NGO_USA_17744_E.pdf>; Andrea Ritchie, *Invisible No More: Police Violence Against Black Women and Women of Color* (Boston, Mass: Beacon Press, 2017); UN Committee on the Elimination of Racial Discrimination, "Report of the Day of Thematic Discussion on Racial Discrimination against People of African Descent," 78th Session (7 March 2011); Marcela Valente, "Full Access to Justice Elusive for Women in Latin America," *Inter Press Service News Agency* (6 April 2012), online: <http://www.ipsnews.net/2012/04/full-access-to-justice-elusive-for-women-in-latin-america/>; INCITE! "Dangerous Intersections: Women of Color Live in the Dangerous Intersections of Sexism, Racism and Other Oppressions" (2014), online: <http://www.incite-national.org/page/dangerous-intersections>; UK Judicial College, "Ethnicity, Inequality and Justice," in *Equal Treatment Bench Book* (November 2013), online: <https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/judicial-college/ETBB_Ethnicity__finalised_.pdf>.

[10] See, for example: Luin Goldring, Carolina Berinstein, and Judith Bernhard, "Institutionalizing Precarious Immigration Status in Canada," CERIS Working Paper No 61 (December 2007); Canadian Council for Refugees, "Migrant Workers: Precarious and Unsupported: A Canada-Wide Study on Access to Services for Migrant Workers" (March 2016), online: <http://ccrweb.ca/sites/ccrweb.ca/files/migrant-workers-2016.pdf>; West Coast LEAF, "Position Paper on Violence against Women without Immigration Status" (May 2012), online: <http://www.westcoastleaf.org/wp-content/uploads/2014/10/2012-POSITION-STATEMENT-Women-without-Status-in-Canada.pdf>; Janet Mosher, "Grounding Access to Justice Theory and Practice in the Experiences of Women Abused by Their Intimate Partners," *Windsor Yearbook of Access to Justice* 32: 2 (2015) 149, online: <http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=3527&context=scholarly_works>; EC, Committee on Women's Rights and Gender Equality, *Report on Undocumented Women Migrants in the European Union* (2013/2115(INI)), online: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0001+0+DOC+PDF+V0//EN>; Platform for International Cooperation on Undocumented Migrants, "Undocumented Migrant Women's Lack of Access to Justice in Europe," Submission to the 54th Session of the Committee on the Elimination of Discrimination against Women, General Discussion on "Access to Justice" (18 February 2013, Geneva), online: <http://www.ohchr.org/Documents/HRBodies/CEDAW/AccesstoJustice/PlatformForInternationalCooperationOnUndocumentedMigrants.pdf>.

[11] See, for example: "Amnesty International Policy on State Obligations to Respect, Protect and Fulfil the Human Rights of Sex Workers," POL 30/4062/2016 (26 May 2016); Dana Phillips, "Public Interest Standing, Access to Justice, and Democracy under the Charter: *Canada (AG) v Downtown Eastside Sex Workers United Against Violence*," *Constitutional Forum* 22: 2 (2013) 21, online: <https://journals.library.ualberta.ca/constitutional_forum/index.php/constitutional_forum/article/viewFile/20970/15919>; Sex Workers' Rights Advocacy Network (SWAN), "Failures of Justice: State and Non-State Violence Against Sex Workers and the Search for Safety and Redress," A Community-Based Research Project of the Sex Workers' Rights Advocacy Network in Central and Eastern Europe and Central Asia (May 2015), online: <http://www.nswp.org/sites/nswp.org/files/Failures%20of%20Justice%20State%20and%20Non-State%20Violence%2C%20SWAN%20-%20September%202015.pdf>; Federation of Women Lawyers (FIDA) Kenya, "Documenting Human Rights Violations of Sex Workers in Kenya: A Study Conducted in Nairobi, Kisumu, Busia, Nanyuki, Mombasa and Malindi," Supported by a Grant from the Open Society Institute (2008), online: <https://www.opensocietyfoundations.org/sites/default/files/fida_20081201.pdf>.

[12] UN Broadband Commission, "Cyber Violence against Women and Girls," at 2.

[13] See, for example: Kashmir Hill, "Using craigslist to crowdsource revenge" (January 6, 2010) Forbes, online: <www.forbes.com/sites/kashmirhill/2010/06/01/using-craigslist-to-crowdsource-revenge/>; see also *Motherboard*'s 2017 series "When Spies Come Home," on commerical surveillance software, online: <https://motherboard.vice.com/en_us/topic/when-spies-come-home>.

[14] Bill C-30, *Protecting Children from Internet Predators Act*, 1st Sess, 41st Parl, 2012; Bill C-13, *Protecting Canadians from Online Crime Act*, 2nd Sess, 41st Parl, 2014.

[15] Bill C-13, *Protecting Canadians from Online Crime Act*, 2nd Sess, 41st Parl, 2014, at s 162.1.

[16] Jane Baiiley, "Time to Unpack the Juggernaut? Reflections on the Canadian Federal Parliamentary Debates on 'Cyberbullying'", (2014) 37(2) *Dalhousie L J* 661, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2448480>: "in the midst of Bullying Awareness Week, federal Justice Minister Peter MacKay tabled Bill C-13, the Protecting Canadians from Online Crime Act, describing it as the government's way of responding to the "horrible crime of cyberbullying". Bill C-13 would amend the Criminal Code to, among other things, prohibit non-consensual distribution of intimate images, extend the grounds covered by the criminal hate propaganda provisions, and amend prohibitions on false, indecent and harassing communications to specifically refer to use of telecommunications systems. However, the vast majority of Bill C-13's provisions are not directly connected to cyberbullying, but to expanded state surveillance powers writ large."; Jesse Kline, "A bigger surveillance state won't stop 'cyberbullying'" National Post (26 May 2014), online: <http://fullcomment.nationalpost.com/2014/05/26/jesse-kline-a-bigger-surveillance-state-wont-stop-cyberbullying/>.

[17] See, for example: The Canadian Press, "Rehtaeh Parsons-inspired cyber-safety act challenged in court" (25 August 2015), online: <http://www.huffingtonpost.ca/2015/08/25/rehtaeh-parsons-cyberbullying-law_n_8040494.html>; Josh Wingrove, "MacKay defends expanded surveillance powers in cyberbullying legislation" (26 May 2014), online: <https://beta.theglobeandmail.com/news/politics/mackay-defends-expanded-surveillance-powers-in-cyberbullying-legislation/article18861278/>; Jane Taber, "New cyberbullying laws should pass this spring, Justice Minister says" The Globe and Mail (9 January 2014), online: <https://beta.theglobeandmail.com/news/politics/mackay-defends-expanded-surveillance-powers-in-cyberbullying-legislation/article18861278/>; Melanie Patten, "Cyberbullying law allows victims in Nova Scotia to sue, seek protection order" The Canadian Press (7 August 2013), online: <http://www.huffingtonpost.ca/2013/08/07/cyberbullying-law_n_3719658.html>.

[18] Murray D Segal, "Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case", October 8, 2015, <http://novascotia.ca/segalreport/Parsons-Independent-Review.pdf>: "The investigator had grounds to believe that at least some of the boys either had the photograph–child pornography–on their phones or had transmitted it. Search warrants could have been obtained to seize those devices at the earliest opportunity."

[19] Jonathon W. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study," Internet Policy Review, 6(2). DOI: 10.14763/2017.2.692, but see discussion at p. 19 regarding the potential salutary or positive impact of hypothetical anti-cyberbullying legislation on sharing personally created content among women respondents

[20] See e.g., Christopher Parsons and Tamir Israel, "Canada's Quiet History Of Weakening Communications Encryption," The Citizen Lab (11 August 2015) <https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/>; Michael Geist, "Why Bill C-30 Gives the Govt the Power To Install Its Own Surveillance Equipment on ISP Networks," (29 Ocotber 2012) <http://www.michaelgeist.ca/2012/10/cacp-lawful-access/>.

[21] *Cyber-Safety Act*, SNS 2013, c 2; *Self v Baha'i*, 2015 NSSC 94, para 25; *Crouch v Snell*, 2015 NSSC 340; Jonathon W. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study," at 12.

[22] The Stop Enabling Sex Traffickers Act (SESTA) S.1693 — 115th Congress (2017-2018); see e.g., Sacramento Sex Workers Outreach Project, letter to Senator John Thune, Senator Bill Nelson, and members of the U.S. Senate Committee on Commerce, Science, and Transportation (18 September 2017) <https://www.eff.org/files/2017/09/18/sestahearing-sac-swop.pdf>; Freedom Network USA, "Freedom Network Urges Caution in Reforming the CDA," (18 September 2017) <https://www.eff.org/files/2017/09/18/sestahearing-freedomnetwork.pdf>; Sex Workers Outreach Project USA, "SWOP-USA stands in opposition of disguised internet censorship bill SESTA, S. 1963," (11 August 2017) <http://www.new.swopusa.org/2017/08/11/call-to-actionpress-release-swop-usa-stands-in-direct-opposition-of-disguised-internet-censorship-bill-sesta-s-1963-call-your-state-representatives-and-tell-them-to-fight/>; Elliot Harmon, "Sex Trafficking Experts Say SESTA Is the Wrong Solution," (3 October 2017) Electronic Frontier Foundation <https://www.eff.org/deeplinks/2017/10/sex-trafficking-experts-say-sesta-wrong-solution>.

[23] OpenNet Korea <http://www.opennetkorea.org/>.

[24] Cure53, <https://cure53.de>.

[25] Fabian Faessler, Geoffrey Alexander, Masashi Crete-Nishihata, Andrew Hilts, and Kelly Kim, "Safer Without: Korean Child Monitoring and Filtering Apps," (11 September, 2017) <https://citizenlab.ca/2017/09/safer-without-korean-child-monitoring-filtering-apps/>; Collin Anderson, Masashi Crete-Nishihata, Chris Dehghanpoor, Ron Deibert, Sarah McKune, Davi Ottenheimer, and John Scott-Railton, "Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application," The Citizen Lab, (20 September, 2015) <https://citizenlab.ca/2015/09/digital-risks-south-korea-smart-sheriff/>; Masashi Crete-Nishihata, Jakub Dalek, John Scott-Railton, and Collin Anderson, "The Kids Are Still At Risk: Update to Citizen Lab's "Are the Kids Alright?" Smart Sheriff report," The Citizen Lab, (1 November 2015) <https://citizenlab.ca/2015/11/smart-sheriff-update/>.

[26] Cure53 <https://cure53.de/>.

[27] *Id.*

[28] See e.g., Vassilis Prevelakis and Diomidis Spinellis, (2007). "The Athens Affair," IEEE Spectrum, June 29 2007, <http://spectrum.ieee.org/telecom/security/the-athens-affair>.

[29] See e.g., Lucy Clarke-Billings, "North Wales detective caught in office 'love square' used police systems to spy on ex-girlfriend," *The Telegraph,* (20 August, 2015) <http://www.telegraph.co.uk/news/uknews/law-and-order/11814591/North-Wales-detective-caught-in-office-love-square-used-police-systems-to-spy-on-ex-girlfriend.html>; Michael Purvis, "Officer pleads guilty to misconduct in cellphone spyware case, to be demoted," *Saultstar* (27 June 2013) <http://www.saultstar.com/2013/06/27/officer-pleads-guilty-to-misconduct-in-cellphone-spyware-case-to-be-demoted>; Hugo Gye and Sophie Jane Evans, "Police officers caught spying on their ex-wives, uploading illicit videos on YouTube and snooping on Liverpool captain Steven Gerrard," *The Daily Mail*, (11 February 2014) <http://www.dailymail.co.uk/news/article-2556906/Police-officers-caught-spying-ex-wives-uploading-illicit-videos-YouTube-discussing-cases-social-media.html>.

[30] See e.g., Alina Selyukh, "NSA staff used spy tools on spouses, ex-lovers: watchdog," *Reuters* (27 September, 2013) <https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927>; Letter from Dr. George Ellard (Inspector General, National Security Agency Central Security Service) to Senator Charles E. Grassley, 11 September 2013 <https://www.nsa.gov/news-features/press-room/statements/assets/files/grassley-letter.pdf>.

[31] See David Kaye, A/HRC/29/32; Professor Joseph Cannataci, "Report of the Special Rapporteur on the right to privacy," (24 November 2016) A/HRC/31/64 <undocs.org/a/hrc/31/64>.

[32] Necessary & Proportionate Coalition, "International Principles on the Application of Human Rights Law to Communications Surveillance," Final Version, May 2014, online: <https://necessaryandproportionate.org/principles>. See also: Electronic Frontiers Foundation & Article 19, Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance: Background and Supporting International Legal Analysis", May 2014, https://cippic.ca/uploads/IPAHRCS-legal_analysis.pdf.

[33] Fabiola Carrion, "Surveillance and Human Rights Principles are launched at 24th Session of the Human Rights Council," Access Now Blog, September 22, 2013, online: <https://www.accessnow.org/surveillance-and-human-rights-principles-are-launched-at-the-24th-hrc/>. See also: UN General Assembly, "Written statement submitted by Reporters Without Borders International, a non-governmental organization in special consultative status," UN Doc A/HRC/24/NGO/31, Human Rights Council 24th Sess, Agenda item 2, online: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/167/33/pdf/G1316733.pdf?OpenElement>.

[34] The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," December 12, 2013, online: <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>. United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", June 30, 2014, A/HRC/27/27, <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>; David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", May 22, 2015, A/HRC/29/32, <https://undocs.org/A/HRC/29/32>; Dr Catalina Botero, "Annual Report of the Inter-American Commission on Human Rights 2013", Volume II, December 21, 2013, OEA/Ser.L/V/II, <http://www.oas.org/en/iachr/docs/annual/2013/informes/LE2013-eng.pdf>; *Szabo and Vissy v Hungary*, Application No 37138/14, January 12, 2016, (ECHR 4th Section), concurring opinion of Judge Pinto de Albuquerque.

[35] Christopher Parsons, (2016). "Transparency in Surveillance: Role of various intermediaries in facilitating state surveillance transparency," Centre for Law and Democracy. <http://responsible-tech.org/wp-content/uploads/2016/06/Parsons.pdf>; Christopher Parsons, (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," <http://www.telecomtransparency.org/release-the-governance-of-telecommunications-surveillance/>.

[36] Canada. *Criminal Code,* RSC, 1985, c C-46, Part VI, s 183.

[37] *Id*, s 195(2)(i), see e.g., Public Safety Canada, "Annual report on the use of electronic surveillance," (2015) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2015/index-en.aspx>.

[38] Canada. *Criminal Code,* RSC, 1985, c C-46, at ss 492.1, 492.2; 487.015, 487.016 and 487.017.

[39] West Coast LEAF, "#CyberMisogyny: Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online" (June 2014), online: <http://www.westcoastleaf.org/wp-content/uploads/2014/10/2014-REPORT-CyberMisogyny.pdf>, at 12.

[40] *Id.*

[41] Canada. *Bill C-51, An Act to amend the Criminal Code and the Department of Justice Act and to make consequential amendments to another Act,* 1st Sess, 42nd Parl, (Tabled in the House of Commons, June 6, 2017) <http://www.parl.ca/DocumentViewer/en/42-1/bill/C-51/first-reading>: Amending Section 276 of the *Criminal Code* by adding the following after subsection (3): "(4) For the purpose of this section, sexual activity includes any communication made for a sexual purpose or whose content is of a sexual nature."

[42] Canada. *Criminal Code,* RSC, 1985, c C-46, s. 276; R v Darrach, [2000] 2 SCR 443.

[43] R v Darrach, [2000] 2 SCR 443.

[44] Canada. *Bill C-51, An Act to amend the Criminal Code and the Department of Justice Act and to make consequential amendments to another Act*; However, note that certain other elements of Bill C-51 may raise concerns regarding the right of the accused to make full answer and defence, and this Bill has not yet been studied in Committee.

[45] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", May 22, 2015, A/HRC/29/32, <https://undocs.org/A/HRC/29/32>.

[46] See e.g., David Kaye, A/HRC/29/32; Wolfgang Schulz & Joris van Hoboken, "Human Rights and Encryption" (2016) UNESCO Series on Internet Freedom, <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>; House Judiciary Committee and House Energy and Commerce Committee Encryption Working Group, "Encryption Working Group Year-End Report" (December 20, 2016) <https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf>.

[47] The Tor Project, <https://www.torproject.org/>.

[48] The Tor Project, "Tor Hidden Service Protocol" (now "onion services") <https://www.torproject.org/docs/hidden-services.html.en>.

[49] Keith Bradsher, "China Blocks WhatsApp, Broadening Oline Censorship", Sept 25, 2017, *New York Times*, <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html>.

[50] David Kaye, A/HRC/29/32 at para 12.

[51] *Id.* at paras 14-26; see also Jon Penney, "Internet Access Rights: A Brief History and Intellectual Origins," William Mitchell Law Review (2011) 38:1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2029087> for discussion on the history of the right to "seek, receive, and impart information."

[52] *id.* at para 56.

[53] United Nations Human Rights Office of the High Commissioner, "Apple-FBI case could have serious global ramifications for human rights: Zeid," (Geneva: 4 March 2016) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E>.

[54] See e.g, James Comey, "Encryption, Public Safety, and "Going Dark," July 6, 2015, <http://www.lawfareblog.com/encryption-public-safety-and-going-dark>; Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence, IACP Summit Report (February 2015) <http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf> at 4-12.

[55] Press conference with the Prime Minister, Attorney-General, Senator, the Hon. George Brandis QC and the Acting Commissioner of the Australian Federal Police, Mr. Michael Phelan APM, AFP Headquarters, Sydney, 14 July 2017 <http://www.pm.gov.au/media/2017-07-14/press-conference-attorney-general-senator-hon-george-brandis-qc-and-acting>; Timothy Revell, "Theresa May's repeated calls to ban encryption still won't work," New Scientist, (June 5, 2017) <https://www.newscientist.com/article/2133644-theresa-mays-repeated-calls-to-ban-encryption-still-wont-work/>; Rob Price, "UK home secretary Amber Rudd says 'real people' don't need end-to-end encryption," (August 1 2017) Tech Insider <http://www.businessinsider.com/home-secretary-amber-rudd-real-people-dont-need-end-to-end-encryption-terrorists-2017-8>.

[56] Cory Doctorow, "The FBI wants a backdoor only it can use – but wanting it doesn't make it possible," (24 February 2016) *The Guardian* <https://www.theguardian.com/technology/2016/feb/24/the-fbi-wants-a-backdoor-only-it-can-use-but-wanting-it-doesnt-make-it-possible>; and see genderally Daniel J. Weitzner, "Warning Signs: A Checklist for Recognizing Flaws of Proposed "Exceptional Access" Systems," (11 May 2016) Lawfare <https://www.lawfareblog.com/warning-signs-checklist-recognizing-flaws-proposed-exceptional-access-systems>; eredith Whittaker and Ben Laurie (Association for Computing Machinery), "Wanting It Bad Enough Won't Make It Work: Why Adding Backdoors and Weakening Encryption Threatens the Internet," (9 December 2016) HuffPost <http://www.huffingtonpost.com/acm-the-association-for-computing-machinery/wanting-it-bad-enough-won_b_8762322.html>; Harold Abelson et. al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," (2015) <https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf>.

[57] *Id.* See also: See also: Ellen Nakashima & Craig Timberg, "NSA Officials Worried About the Day its Potent Hacking Tool Would Get Out. Then it Did", May 16, 2017, *The Washington Post*, <https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html>; Vassilis Prevelakis & Diomidis Spinellis, "The Athens Affair,"June 29 2007, *IEEE Spectrum*, <http://spectrum.ieee.org/telecom/security/the-athens-affair>.

[58] See Matt Olsen, Bruce Schneier, Jonathan Zittrain et. al., "Don't Panic! Making Progress on the "Going Dark" Debate," (2016) Berkman Klein Center for Internet and Society at 12-15 <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf>; Peter Swire & Kenesa Ahmad, "'Going Dark' Versus a 'Golden age for Surveillance," Center for Democracy and Technology (November 8 2011) <https://cdt.org/blog/'going-dark'-versus-a-'golden-age-for-surveillance'/>.

[59] *Id.*

[60] The Tor Project, "Who Uses Tor?" online: <https://www.torproject.org/about/torusers.html>.

[61] Open Whisper Systems, Signal, online: <https://signal.org/>; note also that the use of Tor increased following the release of the Snowden revelations: Tim Sampson, "Tor usage doubles after Snowden's surveillance revelations," *The Daily Dot* (23 August, 2013) < https://www.dailydot.com/layer8/tor-usage-doubles-snowden-nsa-prism/>.

[62] Signal, "Disappearing Messages," online: <https://signal.org/blog/disappearing-messages/>; Tom Warren, "WhatsApp now lets you delete and revoke messages you sent by mistake," *The Verge* (30 October 2017), online: <https://www.theverge.com/2017/10/30/16556838/whatsapp-delete-revoke-feature>.

[63] Russell Brandom, "Domestic violence survivors turn to Tor to escape abusers," *The Verge* (9 May, 2014) <https://www.theverge.com/2014/5/9/5699600/domestic-violence-survivors-turn-to-tor-to-escape-abusers>.
George LeVines, "As domestic abuse goes digital, shelters turn to counter-surveillance with Tor," *The Boston Globe* (5 July, 2014) <http://www.betaboston.com/news/2014/05/07/as-domestic-abuse-goes-digital-shelters-turn-to-counter-surveillance-with-tor/?Src=longreads>.

[64] See e.g., Project Callisto: Tech to combat sexual assault, <https://www.projectcallisto.org/>.

[65] Freedom of the Press Foundation, Secure Drop <https://securedrop.org/>.

[66] Official SecureDrop Directory, <https://securedrop.org/directory>, including *The New York Times, The Guardian, Associated Press, The Washington Post,* and others.

[67] See also GlobalLeaks, <https://www.globaleaks.org/>.

[68] Tactical Technology Collective, "Women's Bodies on the Digital Battlefield: Information exchange and networks of support and solidarity of pro-choice activists in Latin America," <https://tacticaltech.org/media/Womensbodies.pdf> at 12.

[69] The Need for Democratization of Digital Security Solutions to Ensure the Right of Freedom of Expression, Joint submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) and Collin Anderson to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. David Kaye (10 February 2015) <https://citizenlab.ca/wp-content/uploads/2015/02/SR-FOE-submission.pdf>.

[70] Wolfgang Schulz & Joris van Hoboken, "Human Rights and Encryption" (2016) UNESCO Series on Internet Freedom, <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf> at 13.

[71] See e.g., Una Lee and Dann Toliver, "Building Consentful Tech," designed by And Also Too (24 October 2017), online: <http://ripplemap.io/zine.pdf>; Gender and Tech Resources, "Zen and the Art of Making Tech Work for You," <https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual>; Violet Blue, *Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online* (No Starch Press: 2015); Take Back the Tech, "Safety Toolkit" <https://www.takebackthetech.net/be-safe/safety-toolkit>; Tactical Technology Collective, "Holistic Security" (Guide) <https://tacticaltech.org/themes/digital-security/holistic-security/> and "Security in a Box," <https://tacticaltech.org/projects/security-in-a-box-key-project />.

[72] David Kaye, A/HRC/29/32 at para 57.

[73] *A.B. v. Bragg Communications Inc.,* 2012 SCC 46.

[74] Canadian Newspapers Co. v. Canada (Attorney General), [1988] 2 SCR 122.

[75] See Section 3 of this report for a more complete account of the harms that can flow from online and technology-facilitated violence, abuse, and harassment.

[76] Swedish National Council for Crime Prevention, "Polisanmälda hot och kränkningar mot enskilda personer via internet: Rapport 2015:6", (Brottsförebyggande rådet 2015), <https://www.bra.se/download/18.5e2a4a6b14ab166759985c/1422612591546/2015_6_Polisanm>, p 25: "In one third (33 percent) of the cases examined, the perpetrator of the threat or abuse has either been anonymous or is someone whose identity is unknown to the complainant (although the complainants in some cases report having a fairly good idea as to whom the perpetrator is likely to be). Cases involving an anonymous or unknown perpetrator are most common among the incidents reported by girls (44 percent), but cases of this kind are also found to a greater or lesser extent among the complaints filed by boys, men and women."

[77] See e.g., in the mobile device context: Citizen Lab, "The Many Identifiers in our Pockets: A Primer on Mobile Privacy & Security", May 21, 2015: <https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/>.

[78] The criminal or potentially criminal nature of anonymous content or activity can often be assessed facially, as the content or activity itself constitutes the basis of the complaint. Tamir Israel & Christopher Parsons, "Canada's National Security Consultation I: Digital Anonymity & Subscriber Identification Revisited… Yet Again", *Canadian Internet Policy & Public Interest Clinic (CIPPIC) & Citizen Lab*, October 5, 2016, <https://cippic.ca/news/national_security_consultation_revisiting_online_anonymity_yet_again>, documenting the limited impediment posed to Canadian law enforcement's ability to identify those accused of anonymous online criminal conduct by the imposition of a grounds-based warrant obligation. Similarly, most of the instances involving anonymous online violence, harassment or abuse against women examined in a Swedish study included instances where the offensive nature of the content is facially evident, or involved instances of account hijacking, which equally provide sufficient grounds to trigger merits-based police search and seizure powers. The report further notes that identification-based evidence gathering challenges were largely due to cross-border challenges, not to a lack of sufficent grounds, and notes that "online offences...may in certain cases be easier to prove than offline offences, since there is often some kind of digital record showing what has been written or published." Swedish National Council for Crime Prevention, "Polisanmälda hot och kränkningar mot enskilda personer via internet: Rapport 2015:6", (Brottsförebyggande rådet 2015), <https://www.bra.se/download/18.5e2a4a6b14ab166759985c/1422612591546/2015_6_Polisanm>, pp 25-27.

[79] Murray D Segal, "Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case", October 8, 2015, <http://novascotia.ca/segalreport/Parsons-Independent-Review.pdf>, p v.

[80] *R v Spencer*, 2014 SCC 43 (Supreme Court of Canada); David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and <expression", May 22, 2015, A/HRC/29/32, https://undocs.org/A/HRC/29/32>.

[81] See for example: *Warman v Grosvenor*, [2008] 92 OR (3d) 663 (ONSC); *Doe 464533 v ND*, 2016 ONSC 541; *Giller v Procopets*, [2008] VSCA 236, *Crouch v Snell*, 2015 NSSC 340. But see also for ongoing challenges: Jane Bailey & Carissima Mathen, "Technology-facilitated Violence Against Women & Girls: If Criminal Law *Can* Respond, *Should* it?, DISCUSSION DRAFT, (2017) *Ottawa F of Law WP No 2017-44*, <https://ssrn.com/abstract=3043506>, and *US v Elonis*, 575 US __ (SCOTUS, 2015).

[82] See: Department of Justice, Tasmanian Government, Australia, Submission to the Consultation on Civil Penalties Regime for Non-Consensual Sharing of Intimate Images", May 2017, <https://www.communications.gov.au/sites/g/files/net301/f/submissions/tasmanian_government.pdf> for an analysis of the potential for overlapping civil and criminal remedies in relation to some types of online and technologically facilitated violence, harassment or abuse, namely the non-consensual sharing of intimiate images. See also: Swedish National Council for Crime Prevention, "Polisanmälda hot och kränkningar mot enskilda personer via internet: Rapport 2015:6", (Brottsförebyggande rådet 2015), <https://www.bra.se/download/18.5e2a4a6b14ab166759985c/1422612591546/2015_6_Polisanm>, 27, for the overlap between defamation and Swedish criminal prohibitions.

[83] Murray D Segal, "Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case", October 8, 2015, <http://novascotia.ca/segalreport/Parsons-Independent-Review.pdf>, p v: "While the police did not have at its disposal many new tools now available to them and other authorities to address cyberbullying, certain actions could have been taken to address this urgent problem. The investigator had grounds to believe that at least some of the boys either had the photograph – child pornography – on their phones or had transmitted it. Search warrants could have been obtained to seize those devices at the earliest opportunity." See also: Danielle Keats-Citron, "Expand harassment laws to protect victims from online abuse", March 21, 2015, *Aljazeera.com*, http://america.aljazeera.com/opinions/2015/3/expand-harassment-laws-to-protect-victims-of-online-abuse.html. Swedish National Council for Crime Prevention, "Polisanmälda hot och kränkningar mot enskilda personer via internet: Rapport 2015:6", (Brottsförebyggande rådet 2015), <https://www.bra.se/download/18.5e2a4a6b14ab166759985c/1422612591546/2015_6_Polisanm>.

[84] Department of Justice, Tasmanian Government, Australia, Submission to the Consultation on Civil Penalties Regime for Non-Consensual Sharing of Intimate Images", May 2017, <https://www.communications.gov.au/sites/g/files/net301/f/submissions/tasmanian_government.pdf>.

[85] *AB v Bragg Communications Inc*, 2012 SCC 46. As identification-based discovery powers become available at the earliest stages of a civil cause of action filed against an anonymous defendant, the costs entailed at this early stage are relatively low. Indeed, the costs are so low that caution must be exercised to ensure that this identification power is not abused in the absence of a legitimate cause of action or where extra-judicial remedies are the ultimate objective of the civil process.

[86] *BMG Canada Inc v Doe*, 2005 FCA 193; *Dendrite Int'l Inc v Doe No 3*, 775 A.2d 756 (NJ S Ct, App Div, 2001); *Doe No 1 v Cahil*, 884 A.2d 451 (Del, 2005)

[87] Notably, the plaintiff is able to provide a court with any context necessary to assess the merits of the anonymous online conduct alleged to have infringed her rights, rendering merits-based court orders highly feasible as a vehicle for identification: *Warman v Wllkins-Fournier*, 2010 ONSC 2126 (ON Div Ct), (rev'd on other grounds: *1654776 Ontario Ltd v Stewart*, 2013 ONCA 184), para 41: "Because the present proceeding is a defamation action, that concern does not arise. Unlike BMG, the respondent knows the details of precisely what was done by each of the unknown alleged wrongdoers."

[88] *BMG Canada Inc v Doe*, 2005 FCA 193, para 37, "Pursuant to [the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5], ISPs are not entitled to 'voluntarily' disclose personal information such as the identities requested except with the customer's consent or pursuant to a court order."

[89] PIPEDA Case Summary #2005-315, August 9, 2005, (Privacy Commissioner of Canada), <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-315/>.

[90] Alyse Dickson, "'Revenge Porn': A Victim Focused Response", (2016) 2 *UniSA Student Law Review* 42, <https://www.ojs.unisa.edu.au/index.php/uslr/article/download/1357/899> [PDF]. Swedish National Council for Crime Prevention, "Polisanmälda hot och kränkningar mot enskilda personer via internet: Rapport 2015:6", (Brottsförebyggande rådet 2015), <https://www.bra.se/download/18.5e2a4a6b14ab166759985c/1422612591546/2015_6_Polisanm>.

[91] *Crouch v Snell*, 2015 NSSC 340.

[92] Manila Principles on Intermediary Liability, accessed October 31, 2017, <https://www.manilaprinciples.org/>, and Manila Principles Steering Committee, "The Manila Principles on Intermediary Liability: Background Paper", ver 1.0, May 30, 2105, https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf.

[93] Ahlert, C., Marsden, C. and Yung, C., 2004, How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation, <http://pcmlp.socleg.ox.ac.uk/liberty.pdf>. By analogy, see *Crookes v Newton*, 2011 SCC 47, paras 28-29 and 36: (in the context of hyperlinks and defamation, the Canadian Supreme Court held that potential 'chill' that can arise from imposing liability on those who merely facilitate access to defamatory material published by another but did not participate in its creation "could be devastating").

[94] Jennifer M Urban, Joe karaganis & Brianna L Schofield, "Notice and Takedown in Everyday Practice", Ver2, *UC Berkeley Public Law Research Paper No 2755628*, CC-BY 4.0 International, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628>, p 10-11; The US Digital Millennium Copyright Act, for example, premises its liability safe-harbor on the timely removal of content *alleged* to have infringed copyright. A recent examination of 108 million DMCA requests automatically removed by Google Web Search found that 31% (33.5 million) were 'questionable', and 4.5 million of these were fundamentally flawed (4.2% of all examined requests).

[95] Categorization—leading to subsequent blocking or even account suspension—is premised on the mere mention of broad terms such as country or organizational names: see: Parent of a sixth grader's account suspended for a month due to donations made to refugees (Aaron Hutchins, "Donations to Charities for Syrian Refugees are Hitting a PayPal Wall", January 6, 2016, *MacLean's*, <http://www.macleans.ca/news/canada/donations-to-charities-for-syrian-refugees-are-hitting-a-paypal-wall/>, Clint Lalonde, "PayPal No Pal of Mine", January 21, 2016, *ClingLalonde.net*, <http://clintlalonde.net/2016/01/21/paypal-no-pal-of-mine/>); any purchases made by individuals living on several streets along the Isis River, in the United Kingdom (BBC News, "Thames Isis Addresses Spark PayPal Confusion", May 26, 2016, <http://www.bbc.com/news/uk-england-oxfordshire-36387158>, Simon Usborne, "Why Living on Isis Close Might Affect Your Post -- But Not Your House Price", May 25, 2016, *The Guardian*, https://www.theguardian.com/uk-news/shortcuts/2016/may/25/why-living-on-isis-close-might-affect-your-post-but-not-your-house-price); account suspensions for online vendors selling history books about Egypt or Cuba (Shane Dingman, "PayPal's Pay Wall, How a Crackdown on Crime is Frustrating Some Customers", August 29, 2016, *The Globe and Mail*, https://beta.theglobeandmail.com/technology/use-of-sensitive-keywords-can-result-in-paypal-rejecting-benign-orders/article31600185/, Mark Frauenfelder, "Paypal Halted a Transaction Because it Contained the Word 'Cuba'", August 17, 2016, *BoingBoing.net*, <https://boingboing.net/2016/08/17/paypal-halted-a-transaction-be.html>); and anyone who jokingly refers to a flagged 'watch word' (Ben Guarino, "I Wrote 'ISIS Beer Funds!!!' in a Venmo Memo and the Feds Detained my $42", April 18, 2016, *ArsTechnica*, <https://arstechnica.com/tech-policy/2016/04/i-wrote-isis-beer-funds-in-a-venmo-memo-and-the-feds-detained-my-42/>).

[96] Anil Dash, "The Immortal Myths About Online Abuse", May 27, 2016, *Medium.com*, https://medium.com/humane-tech/the-immortal-myths-about-online-abuse-a156e3370aee; Ruth Lewis, Michael Rowe & Clare Wiper, "Online Abuse of Feminists as an Emerging Form of Violence Against Women and Girls", (2017) 57(6) *Brit J of Crim* 1462, https://doi.org/10.1093/bjc/azw073, "...flaming is varied, contextual and relational, distinguishes it from other forms of harassment and hate speech, and provides a platform for understanding sexualized and misogynistic abuse." O'Sullivan & Flanagin, "Reconceptualizing 'Flaming' and Other Problematic Messages", (2003) 5(1) *New Media & Soc* 69, http://journals.sagepub.com/doi/pdf/10.1177/1461444803005001908, "However, such operational definitions often fail to consider a crucial question: whose message interpretation determines the message label? In research on flaming, the determination of whether a message is considered a flame is often based upon an outside observer's perspective – that of the commentator, the researcher, or a coder. A third party's interpretation, however, might be very different from that of the interactants. What an outside observer might perceive as hostile language could be perceived by one or both interactants as a routine reminder, an attempt at humor, a deserved reprimand, a poorly-worded but well-intended suggestion, or an intentional use of non-normative language for specific interactional goals. Differences in interpretation could be due to observers' lack of access to the wide array of contextual factors that are key to interactants' message interpretation. It is precisely this context that interactants draw upon to achieve some degree of shared understanding."; Jane Bailey & Carissima Mathen, "Technology-facilitated Violence Against Women & Girls: If Criminal Law *Can* Respond, *Should* it?, DISCUSSION DRAFT, (2017) *Ottawa F of Law WP No 2017-44*, <https://ssrn.com/abstract=3043506>, p 29-30 (on the importance of considering the full context and circumstances when assessing the impact of technology assisted violence on women).

[97] Rima Athar, "End Violence: Women's Rights and Safety Online", March 2015, *Association for Progressive Communications (APC)*, https://www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf, p 21.

[98] *Scarlet Extended SA v Société belge des belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Case C-70/10, November 24, 2011 (CJEU, Third Chamber); *Société belge des belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog NV*, Case C-360/10, February 16, 2012 (CJEU, Third Chamber).

[99] See for example: *Warman v Grosvenor*, [2008] 92 OR (3d) 663 (ONSC); *Doe 464533 v ND*, 2016 ONSC 541; *Giller v Procopets*, [2008] VSCA 236, *Crouch v Snell*, 2015 NSSC 340. But see also for ongoing challenges: Jane Bailey & Carissima Mathen, "Technology-facilitated Violence Against Women & Girls: If Criminal Law *Can* Respond, *Should* it?, DISCUSSION DRAFT, (2017) *Ottawa F of Law WP No 2017-44*, <https://ssrn.com/abstract=3043506>.

[100] See: Jane Bailey & Carissima Mathen, "Technology-facilitated Violence Against Women & Girls: If Criminal Law *Can* Respond, *Should* it?, DISCUSSION DRAFT, (2017) *Ottawa F of Law WP No 2017-44*, <https://ssrn.com/abstract=3043506> and *US v Elonis*, 575 US __ (SCOTUS, 2015).

[101] Manila Principles on Intermediary Liability, accessed October 31, 2017, <https://www.manilaprinciples.org/>, principle 2.

[102] Centre for Law and Democracy, "Stand Up for Digital Rights: Recommendations for Responsible Tech", *Responsible-Tech.org*, <http://www.law-democracy.org/live/wp-content/uploads/2016/06/Final-Recommendations.pdf>.

[103] For example, prior to its leak to the Guardian, Facebook's content moderation guidelines would train content moderators to remove threats directed at important public figures who are placed in protective categories ("someone shoot Trump") but to ignore specific threats directed at women in general ("To snap a b****'s neck, make sure to apply all your pressure to the middle of her throat" or "I hope someone kills you") as such threats are deemed to be non-credible: Nick Hopkins, "Revealed: Facebook's Internal Rulebook on Sex, Terrorism and Violence", May 21, 2017, *The Guardian*, <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence>.

[104] Manila Principles on Intermediary Liability, accessed October 31, 2017, <https://www.manilaprinciples.org/>, Principle 6 Clause c; Centre for Law and Democracy, "Stand Up for Digital Rights: Recommendations for Responsible Tech", *Responsible-Tech.org*, <http://www.law-democracy.org/live/wp-content/uploads/2016/06/Final-Recommendations.pdf>, p 3.

[105] Many models for effective and procedurally sound complaints handling processes exist. For one examples, see: Commission for Complaints for Telecom-Television Services, "Complaints Process Explained", accessed November 1, 2017, <https://www.ccts-cprst.ca/for-consumers/complaints/complaints-process-explained/>.

[106] Anil Dash, "The Immortal Myths About Online Abuse", May 27, 2016, *Medium.com*, https://medium.com/humane-tech/the-immortal-myths-about-online-abuse-a156e3370aee, ("... most users will only report an action if it's extremely egregious, part of an ongoing or large-scale campaign, or presents a particularly urgent danger. Despite how reluctant targets are to actually report abuse, the reaction when they do so is often skepticism or denial from people who aren't the target of online abuse. These skeptics see the other, less-harmful messages that are merely critical or insulting and think that the targeted person is overreacting to messages that are merely annoying. This is especially true because social platforms will hide a potentially threatening or harmful message while they investigate reports of abuse. … This is especially true because many of the worst abusers online know how to shift from one medium to another, meaning a campaign that starts on one platform can lead to abuse on a different platform, making the full context of the abuse hard to recognize."); Jane Bailey & Carissima Mathen, "Technology-facilitated Violence Against Women & Girls: If Criminal Law *Can* Respond, *Should* it?, DISCUSSION DRAFT, (2017) *Ottawa F of Law WP No 2017-44*, <https://ssrn.com/abstract=3043506>, p 31: "Threats that may appear subtle, benign or neutral to an outsider, can quite reasonably carry very real and Intended meaning to the person they are targeted at."

[107] Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", May 16, 2011, A/HRC/17/27, <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>, p 12: "Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences."

[108] As noted above: "For example, prior to its leak to the Guardian, Facebook's content moderation guidelines would train content moderators to remove threats directed at important public figures who are placed in protective categories ("someone shoot Trump") but to ignore specific threats directed at women in general ("To snap a b****'s neck, make sure to apply all your pressure to the middle of her throat" or "I hope someone kills you") as such threats are deemed to be non-credible: Nick Hopkins, "Revealed: Facebook's Internal Rulebook on Sex, Terrorism and Violence", May 21, 2017, *The Guardian*, <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence>.

[109] Note: some of the underlying offences often linked with technology facilitated violence, harassment and abuse are already prohibited in international instruments.

[110] *X v Twitter Inc*, [2017] NSWSC 1300. See also: *Yahoo! Inc v LICRA*, 433 F.3d 1199 (US, 9th Circ, 2006); Michael Geist, "Google Files Suit in US Court to Block Enforcement of Canadian Global Takedown Order", July 25, 2017, *MichaelGeist.ca*, <http://www.michaelgeist.ca/2017/07/google-files-suit-u-s-court-block-enforcement-canadian-global-takedown-order/>.

[111] Katitza Rodriguez, "The Cybercrime Convention's New Protocol Needs to Uphold Human Rights", September 18, 2017, *Eff.org*, <https://www.eff.org/deeplinks/2017/09/cybercrime-conventions-new-protocol-needs-uphold-human-rights>.

[112] Max Cherney, "Inside the Booming Commercial Surveillance Industry," *Motherboard* (24 February, 2017) <https://motherboard.vice.com/en_us/article/kbz8mw/inside-the-booming-commercial-surveillance-industry>.

[113] Sarah McKune and Ron Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," The Citizen Lab, Munk School of Global Affairs, University of Toronto (2 March 2017) <https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf> at 2.

[114] Hacking Team, <http://www.hackingteam.it/>; see past Citizen Lab research related to Hacking Team here <https://citizenlab.ca/tag/hacking-team/>.

[115] FinFisher, <http://www.finfisher.com/>; see past Citizen Lab research related to FinFisher here <https://citizenlab.ca/tag/finfisher/>.

[116] See Citizen Lab's 7-part series on the abuse of NSO Group's spyware, Part 1 (and links to subsequent Parts) here: Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (24 August 2016), online: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>.

[117] *Id.*

[118] *Id.* Parts 2 to 7, "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links," "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware, "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware," "Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware," "Part 7: Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware."

[119] Bill Marczak, John Scott-Railton, and Sarah McKune, "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware," The Citizen Lab (9 March 2015) <https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/>.

[120] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware," The Citizen Lab, (2 August 2017) <https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/>.

[121] *Id.*

[122] United Nations Human Rights Office of the High Commissioner, "Mexico: UN experts call for an independent and impartial investigation into use of spyware against rights defenders and journalists," (Geneva: 19 July, 2017) <http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=E>; The list of experts included Mr. Michel Forst, Special Rapporteur on the situation of human rights defenders; Ms. Houria Es-Slami, Chairperson-Rapporteur of the Working Group on Enforced or Involuntary Disappearances; Mr. David Kaye, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and Mr. Joseph Cannataci, Special Rapporteur on the right to privacy.

[123] Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (24 August 2016), online: <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>; Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *The New York Times* (26 May, 2017) <https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/>.

[124] John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links," The Citizen Lab (11 February 2017), online: <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>.

[125] Privacy International (with European Center for Constitutional and Human Rights, Reporters Without Borders, Bahrain Center for Human Rights, Bahrain Watch), "OECD Complaint against Gamma International for possible Violations of the OECD Guidelines for Multinational Enterprises," (1 February 2013) < https://www.privacyinternational.org/sites/default/files/jr_bundle_part_2_of_2_0.pdf>; UK National Contact Point for the OECD Guidelines for Multinational Enterprises, "Privacy International & Gamma International & Gamma International UK Ltd. Final Statement After Examination of Complaint (December 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf>.

[126] Nate Cardozo and Sophia Cope, "Cisco's Latest Attempt to Dodge Responsibility for Facilitating Human Rights Abuses: Export Rules," Electronic Frontier Foundation (18 April 2016) <https://www.eff.org/deeplinks/2016/04/ciscos-latest-attempt-dodge-responsibility-facilitating-human-rights-abuses-export>; Doe I v. Cisco Systems Inc., Second Amended Complaint, Case No. 5:11-cv-02449-EJD-PSGx <https://www.eff.org/files/2016/01/12/113_second_amended_complaint_does_v._cisco_9.18.13.pdf>.

[127] See e.g., Jason Koebler, "'I See You': A Domestic Violence Survivor Talks About Being Surveilled By Her Ex," *Motherboard* (17 March 2017) <https://motherboard.vice.com/en_us/article/bmbpvv/i-see-you-a-domestic-violence-survivor-talks-about-being-surveilled-by-her-ex>; Joseph Cox, "How to Protect Yourself from Creepy, Phone Snooping Spyware," *Motherboard* (27 February 2017) <https://motherboard.vice.com/en_us/article/xymngz/how-to-protect-yourself-from-creepy-phone-snooping-spyware>; Lorenzo Franceschi-Bicchierai and Joseph Cox, "Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones," (18 April 2017) <https://motherboard.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x>.

[128] For documentation related to what has been reported as "the first-ever criminal conviction concerning the advertisement and sale of a mobile device spyware app" See U.S. Department of Justice, "Man Pleads Guilty for Selling 'StealthGenie' Spyware App and Ordered to Pay $500,000 Fine," (25 November, 2014) <https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine>; U.S. v. Akbar, Civil No. 1:14-cv-1273 (E.D. Va. September 26, 2014), <https://cdn.arstechnica.net/wpcontent/uploads/2014/09/akbar.pdf>; U.S. v. Akbar, Criminal No. 1:14-cr-276 (E.D. Va. August 7, 2014) <http://www.wired.com/wp-content/uploads/2014/09/Akbar_indictment.pdf>.

[129] Aarti Shahani, "Smartphones Are Used To Stalk, Control Domestic Abuse Victims," *National Public Radio* (15 September 2014) <http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>.

[130] Joseph Cox, "The Dirty Hackers Who Steal Passwords for Jealous Lovers," *Motherboard* (7 June 2017) <https://motherboard.vice.com/en_us/article/vbgbvm/the-dirty-hackers-who-steal-passwords-for-jealous-lovers>.

[131] Joseph Cox, "Paranoid Spouses Can Spy on Partners' iOS 10 Devices with iCloud Backups," *Motherboard* (27 February 2017) <https://motherboard.vice.com/en_us/article/4xpgnj/paranoid-spouses-can-spy-on-partners-ios-10-devices-with-icloud-backups>.

[132] Joseph Cox, "Meet FlexiSpy, The Company Getting Rich Selling 'Stalkerware' to Jealous Lovers," *Motherboard* (21 April 2017) <https://motherboard.vice.com/en_us/article/aemeae/meet-flexispy-the-company-getting-rich-selling-stalkerware-to-jealous-lovers>

[133] In 2015, Citizen Lab research revealed that this tool appeared to be covertly in use by government entities in 32 countries: See Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," (15 October 2015) <https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation>/; Joseph Cox, "Meet FlexiSpy, The Company Getting Rich Selling 'Stalkerware' to Jealous Lovers," *Motherboard* (21 April 2017) <https://motherboard.vice.com/en_us/article/aemeae/meet-flexispy-the-company-getting-rich-selling-stalkerware-to-jealous-lovers>; See also, Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "For Their Eyes Only: The Commercialization of Digital Spying," April 30, 2013, <https://citizenlab.ca/2013/04/for-their-eyes-only-2/>.

[134] Sarah McKune and Ron Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," at 3.

[135] United Nations Human Rights Office of the High Commissioner, "Guiding Principles on Businesses and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework," (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

[136] Sarah McKune and Ron Deibert, "Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking," at 4.

[137] *Id.* at 9.

[138] *Id.* at 6-9.

[139] *Id.* at 17-19.

[140] *Id.* at 19-21.

[141] *Id.* at 23-26.

[142] Sandra Laville, "Online abuse: 'existing laws too fragmented and don't serve victims,'" *The Guardian* (4 March 2016) <https://www.theguardian.com/uk-news/2016/mar/04/online-abuse-existing-laws-too-fragmented-and-dont-serve-victims-says-police-chief>.

[143] The Citizen Lab, "The Many Identifiers in Our Pockets: A Primer on Mobile Privacy and Security," May 21, 2015, <https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/>.

[144] Open Effect, the Citizen Lab at the Munk School of Global Affairs, and Professor Jedidiah Crandall, "Net Alert" (2017) <https://netalert.me/>.

[145] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton, "For Their Eyes Only: The Commercialization of Digital Spying," April 30, 2013, <https://citizenlab.ca/2013/04/for-their-eyes-only-2/>.

[146] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, "Every Step You Fake: Final Report Released," April 5, 2016, <https://citizenlab.ca/2016/04/every-step-you-fake-final-report/>.

[147] Fraser et al, "The New Age of Stalking: Technological Implications for Stalking," *Juvenile and Family Court Journal* 61(4), 2010, 39-55.

[148] Examples from the United States include 'The Use of Technology to Stalk' Online Training, developed by the Stalking Resource Center of the National Center for Victims of Crime, US Department of Justice; The International Association of Privacy Professionals (IAPP) privacy certification programs designed for professionals who manage, handle and access data; 2016 course taught by the Founder and President of Total Digital Security, Brad Deflin, on Cyber Security for Lawyers, which counted for two general credits toward Continuing Legal Education (CLE) for members of the Florida Bar; August 2017 digital security training for lawyers and advocates hosted by the Tech Institute, ACLU-DC, and DC Legal Hackers, which took place at Georgetown Law and was titled "Protecting Yourself and Your Clients: Data Security Information You Need to Know." Additionally, Martin Shelton hosts a "meta-guide" of current digital security resources on Medium (last updated October 2, 2017), including a list of current resources for lawyers and one for "dangerous situations," including domestic violence.

[149] West Coast LEAF, "#CyberMisogyny: Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online" at 66 ("Recommendation 29").

[150] Fraser et al, "The New Age of Stalking: Technological Implications for Stalking," Juvenile and Family Court Journal 61(4), 2010, at 51; Murray D Segal, "Independent Review of the Police and Prosecution Response to the Rehtaeh Parsons Case", October 8, 2015, <http://novascotia.ca/segalreport/Parsons-Independent-Review.pdf>.

[151] *Id.*

[152] Fraser et al, "The New Age of Stalking: Technological Implications for Stalking," Juvenile and Family Court Journal 61(4), 2010, at 51-52.

[153] *Id.* at 52.

[154] One example of an effective training program for frontline workers was the Technology Safety Project of the Washington State Coalition Against Domestic Violence. The Project was designed to increase awareness and knowledge of technology safety issues for domestic violence victims, survivors, and advocacy staff. The goals of the program were threefold: (1) increase safe computer and Internet access for domestic violence survivors in Washington; (2) reduce the risk posed by abusers by educating survivors about technology safety and privacy; and (3) increase the ability of survivors to help themselves and their children through information technology. An evaluation of the Project confirmed that many women who are victims of domestic violence are being stalked using technological means, and are particularly affected by email monitoring, cyberstalking, and identity theft. The results also suggested that the program was useful and effective, and that participants found training about technology safety to be empowering. See Finn and Atkinson, "Promoting the safe and strategic use of technology for victims of IPV: Evaluation of the technology safety project," *Journal of Family Violence* 24 (2009): 53-59.

[155] Southworth et al, "IPV, Technology, and Stalking," *Violence Against Women* 13(8): 842-856, August 2007.

[156] Canadian Internet Policy and Public Interest Clinic, <https://cippic.ca/>.