

**Networked Intimate Image Abuse and Public Interest Remedies: MaskPark,
China's Enforcement Gap, and Canadian Comparative Lessons**

by

Yilin Wang

**A Practicum submitted to the
Faculty of Graduate and Postdoctoral Studies
of the University of Manitoba
in partial fulfilment of the requirements of the degree of**

Master of Human Rights

**Faculty of Law
University of Manitoba
Winnipeg**

Copyright © 2026 by Yilin Wang

Abstract

This paper examines intimate image abuse as a form of sexual wrongdoing through the lens of the MaskPark scandal in China, a large-scale online network that distributed non-consensual intimate images, covert recordings, and AI-generated sexual composites.

The MaskPark case discusses how digitally mediated sexual harms extend beyond individualized victimization and exposes the limits of traditional, post-hoc legal responses that rely primarily on individual criminal enforcement.

The paper argues that public interest considerations become especially important in intimate image abuse cases which are shaped by rapid circulation and replication, cross-platform persistence, scalable exposure, and difficulty in obtaining timely protection, and that such features call for legal responses capable of both early intervention and broader systemic effects. While China formally recognizes personality and privacy rights, the MaskPark scandal reveals significant enforcement gaps, including delays in investigation and content control, fragmented remedial pathways, and limited *victim agency*. These gaps highlight the inadequacy of individualized legal responses in addressing harms that are inherently collective, technologically amplified, and difficult to contain once they begin to spread.

Using a comparative approach, this study first examines the enforcement gap and related structural weaknesses in China and then draws on public interest considerations from Canadian law as a reference point for identifying alternative legal and institutional response architectures. It highlights civil and procedural tools that can support faster, more victim-centered remedies. By analyzing MaskPark against a public interest oriented remedial toolkit, the paper contributes to broader debates on how to achieve effective legal responses to intimate image abuse and other transnational digital harm in particular by contemplating harms and potential responses against the following tiered response structure: early-phase control and preservation; mid-phase access and procedural protection; later-phase adjudication and continuing enforcement.

Acknowledgements

This paper has taken several years to reach completion. Looking back on the past two years of my academic journey, I still find it remarkable how far this work has come.

First and foremost, I would like to express my deepest gratitude to my supervisor and Program Director, Professor Mary Shariff. Without her rigorous and thoughtful guidance, patience, profound insight into the field of human rights law, and consistently detailed and meticulous feedback, I could not have completed a paper involving the laws and legal systems of multiple jurisdictions.

My sincere thanks also go to the instructors and professors at Robson Hall from whom I have learned throughout this program. Their teaching and guidance have played an essential role in shaping my understanding of human rights law. I am also grateful to my examiner for taking the time to read and engage with this paper.

Special thanks are owed to Katrine Dilay, the exceptional supervisor with whom I worked during my practicum at the Public Interest Law Centre. Through her guidance and through my experience at the Centre, I gained invaluable insight into the practice of public interest law in Canada, which greatly informed and inspired this research.

I am deeply grateful to my parents. Without them, I would never have been able to undertake this educational journey thousands of kilometres from home. I also wish to thank all the friends I have met in Winnipeg, as well as my family doctor and pharmacist. Without your support and unfailingly timely assistance, I could not have continued working towards each of my goals through periods of loneliness and anxiety.

Finally, I would like to thank the women in China who have never ceased to resist, and everyone who has followed, documented, and spoken out about the MaskPark incident. Your courage and persistence gave this research both its foundation and its purpose.

Dedication

To the women of my homeland, and to my sisters across the earth, united by the destiny we share.

Table of Contents

Abstract.....	I
Acknowledgements.....	II
Dedication	III
1. Introduction.....	1
1.1 <i>A word on Research Design, Methodology, Scope and Limitations</i>	<i>6</i>
1.2 <i>A Note on Definitions</i>	<i>7</i>
2. China after MaskPark	8
2.1 <i>Timeline of Exposure and the Absence of Early Investigations</i>	<i>8</i>
2.2 <i>Personality rights, deep synthesis rules, and the enforcement gap.....</i>	<i>9</i>
2.3 <i>Platform Governance Failures and Cross-Platform Barriers</i>	<i>13</i>
2.4 <i>Remedial Gaps in Doctrine and Practice.....</i>	<i>15</i>
2.5 <i>Gendered Dynamics of Silence</i>	<i>17</i>
2.6 <i>Comparative Criteria.....</i>	<i>18</i>
3. Selected Comparative Responses: East Asian Contexts and Canadian Legal Pathways ...	19
3.1 <i>East Asian contextual comparators.....</i>	<i>19</i>
3.2 <i>Criminal touchpoints from Canadian law.....</i>	<i>21</i>
3.3 <i>Civil and statutory remedies from Canadian law</i>	<i>23</i>
Provincial Legislation	23
Common Law	28
Remedies.....	28
3.4 <i>Procedural and remedial features with public interest relevance</i>	<i>29</i>
3.5 <i>Access to justice architecture</i>	<i>31</i>
3.6 <i>Compact case study cluster</i>	<i>33</i>
4. Comparative Evaluation, Reform Directions, and Limits.....	36
4.1 <i>Revisiting MaskPark through Canadian Legal Mechanisms</i>	<i>36</i>

a) Early-phase response: rapid control, interim relief, and preservation	36
b) Mid-phase response: access, anonymity, and victim-centred navigation	37
c) Later-phase response: adjudication, durable control, and continuing enforcement ...	39
d) Systemic and cross-cutting considerations: prevention, accountability, and public confidence.....	40
4.2 <i>Reform directions: a tiered model</i>	42
a) Tier 1: rapid civil control	42
b) Tier 2: coordinated investigation and platform response	42
c) Tier 3: access architecture and public accountability	43
4.3 <i>Limits, transfer cautions, and future research</i>	43
5. Conclusion	44
<i>BIBLIOGRAPHY</i>	46

1. Introduction

Intimate image abuse is recognised in Canadian scholarship as a form of sexual wrongdoing raising not only individual harms but also broader societal and public policy concerns. It involves, for example, the sharing or threatened sharing of nude or sexual images without consent, and undermines a person's control over how their body and sexuality are exposed in both digital and offline spaces.¹ Canadian law has not been silent²³ and judicial and legislative developments increasingly reflect an understanding that intimate image abuse (IIA) can be especially damaging in digital environments,⁴ where harmful material may circulate quickly, widely, and sometimes anonymously,⁵ making timely and meaningful intervention especially important.

Studies describe IIA as a form of sexual violence and as an infringement of sexual autonomy, privacy, dignity, and equality, since the images are often created or circulated in circumstances where the person reasonably expected confidentiality, only to be later posted to sites or forums designed to humiliate, harass, or exploit.⁶⁷ Researchers also emphasise that women and girls are disproportionately targeted,⁸ that 2SLGBTQ+ people and people with disabilities face heightened risk,⁹ and that the online circulation makes the harm social as well as individual,¹⁰ affecting who feels able to participate safely in public and online life.¹¹

¹ Suzie Dunn, "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI" (2024) 69:4 McGill Law Journal 395.

² *Criminal Code*, RSC 1985, c C-46, s 162.1.

³ *Intimate Image Protection Act*, SM 2015, c 42, CCSM c I87, s 1(2).

⁴ *A.B. (Litigation Guardian of) v Bragg Communications Inc*, 2012 SCC 46 at paras 20, 22.

⁵ *R v NG et al*, 2015 MBCA 81 at para 33.

⁶ Dunn, *supra* note 1 at 395–416.

⁷ V Karasavva, "The Frequency, Nature, Impact, and Coping Strategies of Nonconsensual Intimate Image Dissemination Victimization: A Scoping Review" (October 2025) *Trauma, Violence, & Abuse*, online: SAGE Journals <<https://journals.sagepub.com/doi/epub/10.1177/15248380251383940>>.

⁸ Moira Aikenhead, "Non-Consensual Disclosure of Intimate Images as a Crime of Gender-Based Violence" (2018) 30:1 *Canadian Journal of Women and the Law* 117.

⁹ Rebecca Umbach, Nicola Henry & Gemma Beard, "Prevalence and Impacts of Image-Based Sexual Abuse Victimization: A Multinational Study" (March 2025), online: arXiv <<https://doi.org/10.48550/arXiv.2503.04988>>.

¹⁰ Kimberly J Mitchell, Lisa M Jones, Ateret Gewirtz-Meydan, Jennifer O'Brien & Deirdre Colburn, "Image-Based Sexual Abuse: Characteristics Linked to Different Reasons Why Youth Decide Not to Disclose" (2025) 26:8 *Prevention Science* 1157.

¹¹ A Wayne MacKay, "Law as an Ally or Enemy in the War on Cyberbullying: Exploring the Contested Terrain of Privacy and Other Legal Concepts in the Age of Technology and Social Media" (2015) 66 *University of New Brunswick Law Journal* 3.

Slow or non-investigative state responses can make these harms significantly worse. Canadian research on policing and prosecution of IIA, for example, notes that criminal provisions and civil tools often exist on paper, yet victims struggle to obtain prompt help, clear information about options, or rapid removal of images.¹² Empirical and doctrinal reviews point to delays in laying charges,¹³ uneven use of Canadian *Criminal Code* provisions¹⁴ such as section 162.1 (publication of intimate image without consent) and related offences, and a tendency among police to rely on informal measures that may spare perpetrators criminal records¹⁵ leaving survivors without firm protection or meaningful recognition of the harm they have suffered. Commentators further observe that while officials hesitate, images are copied, mirrored, and reposted across multiple platforms, so that each day of inaction increases the number of viewers and the difficulty of ever achieving full takedown.¹⁶

In short, the overall picture is of a legal response that too often arrives late and in the view of the author, improperly only focuses on the individual victim, rather than on rapid intervention to stop circulation and prevent secondary spread, which is why intimate image abuse must also be treated as a public interest problem rather than only a private dispute.

Recent Canadian reform efforts further show that expanding definitions and strengthening penalties remain important. Reform proposals are reflected at both the federal and provincial levels. At the federal level, Bill C-16 would expand the *Criminal Code* response to sexually explicit deepfakes and to threats to distribute intimate images.¹⁷ At the provincial level,

¹² Gabriel Rojas Hruška, “Updating Canadian Law to Address Online Hate and Gender-Based Violence” (2 December 2025), online: Canadian Centre for Policy Alternatives <<https://www.policyalternatives.ca/news-research/updating-canadian-law-to-address-online-hate-and-gender-based-violence/>>.

¹³ Moira Aikenhead, “Image-Based Abuse in Intimate Partnerships in Canada: Lessons from the Criminal Case Law” in Gian Marco Caletti & Kolis Summerer, eds, *Criminalizing Intimate Image Abuse: A Comparative Perspective* (Oxford: Oxford University Press, 2024) 320, online: <<https://doi.org/10.1093/oso/9780198877813.003.0016>>.

¹⁴ *Criminal Code*, *supra* note 2.

¹⁵ Canada, Department of Justice, “Non-Consensual Distribution of Intimate Images” in *Cyberbullying and the Non-Consensual Distribution of Intimate Images*, online: <<https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/p6.html>>.

¹⁶ Rebecca Katz, “Takedowns and Trade-Offs: Can Copyright Law Assist Canadian Victims of Non-Consensual Intimate Image Distribution?” (2020) 29:2 *Education Law Journal* 169.

¹⁷ Canada, Department of Justice, “Bill C-16: An Act to Amend Certain Acts in Relation to Criminal and Correctional Matters (Child Protection, Gender-Based Violence, Delays and Other Measures)” (tabled in the House of Commons, 27 February 2026), online: <https://www.justice.gc.ca/eng/csj-sjc/pl/charte-charte/c16_3.html>.

proposed amendments to Manitoba's *Non-Consensual Distribution of Intimate Images Act*¹⁸ for example would, among other things, expand individual tort liability.¹⁹ The proposed Manitoba provincial legislation is interesting, because it expressly contemplates two narrow circumstances in which distribution may be in the "public interest", namely for a law enforcement investigation or in the context of a court proceeding.²⁰ These exceptions remain largely centred on the individual, however, and do not amount to a broad public interest model.

For the purposes of this paper, "public interest" is used in a broad but not unlimited sense. It refers to harms and responses with public dimensions that extend beyond the immediate private interests of the victim and perpetrator, including wider effects on reporting, institutional trust, and the capacity of legal systems to respond to networked abuse. Put another way, a public interest analysis must go beyond consideration of perpetrator punishment or individual liability to ask how broader structural and systemic conditions enable image abuse, frustrate reporting, and weaken protection in practice. This is the context in which MaskPark becomes especially instructive.

The MaskPark scandal, a distinctly Chinese case, makes these structural and systemic weaknesses particularly visible. Much of what is known about MaskPark comes from investigative reporting. This reporting describes MaskPark as a large Chinese-language network on Telegram, composed of a main channel and multiple sub-groups with a combined membership exceeding one hundred thousand users.²¹ These groups shared covert recordings alongside intimate photographs uploaded without consent.²² Reports also documented the sale of disguised cameras inside the same network and the use of AI tools to generate sexualised composites.²³ Although the main channel was eventually removed, replacement groups rapidly

¹⁸ *The Non-Consensual Distribution of Intimate Images Act*, CCSM c N93, online: CanLII <<https://www.canlii.org/en/mb/laws/stat/ccsm-c-n93/latest/ccsm-c-n93.html>> formerly *The Intimate Image Protection Act*, SM 2015, c 42, online: CanLII <<https://www.canlii.org/en/mb/laws/astat/sm-2015-c-42/latest/sm-2015-c-42.html>>.

¹⁹ *Ibid.*

²⁰ Bill 2, *The Intimate Image Protection Amendment Act*, 3rd Sess, 43rd Leg, Manitoba, 2025, online: <<https://web2.gov.mb.ca/bills/43-3/b002e.php#exNote>> [Bill 2].

²¹ Hsieh Yi-hsuan, "Chinese Voyeurism Group of Over 100,000 People Suspected of Illegal Activity, Weibo Trending Topic Allegedly Suppressed" (26 July 2025), online: Central News Agency <<https://money.udn.com/money/story/5603/8898079>>.

²² Ling Li, "MaskPark and the Silence around China's Gender-Based Violence Online" (11 November 2025), online: Made in China Journal <<https://madeinchinajournal.com/2025/11/11/maskpark-and-the-silence-around-chinas-gender-based-violence-online/>>.

²³ *Ibid.*

appeared, and official responses from Chinese authorities remained slow and limited, highlighting difficulties in investigating encrypted, foreign-hosted platforms where users remain anonymous.²⁴

MaskPark is fundamentally a Chinese incident, involving Chinese users, Chinese victims, and Chinese social contexts. The case exposes a gap between China's formal legal protections for personality rights²⁵ and the limited enforcement. Reports indicate that public discussion was swiftly managed, yet broad and coordinated investigations did not follow.²⁶ This gap matters not only for individual victims, but also for public confidence in the legal system. Where rights are formally recognised but enforcement remains fragmented, slow, and heavily dependent on individual victims to initiate action, the problem cannot be understood as a series of private wrongs alone.²⁷ MaskPark therefore matters less because of technological novelty than for what it reveals: the limits of current Chinese remedies in responding to large-scale, networked intimate image abuse.

Even though Canadian law itself remains incomplete and uneven, it is useful because it demonstrates specific legal mechanisms for some of the weaknesses revealed by MaskPark. Its clearer recognition of the public policy significance of intimate image abuse in criminal, civil, and procedural responses suggests possible approaches to rapid control, coordinated intervention, victim protection, and remedies including interlocutory relief. The comparative value of Canadian materials therefore lies not in transplantation of Canadian law, but in the functional insight they offer into how law might better respond to the structural and public dimensions of networked intimate image abuse.

²⁴ Wang Yi & Feng Xi, "Her Ex-Boyfriend Sold Her to One Hundred Thousand Men: Exposing the Dirty Cross-Border Hidden-Camera Trade" (24 July 2025), online: N Video <<https://archive.ph/20250724110043/https://www.nfnews.com/content/0oxwwNLN6L.html>>.

²⁵ "Personality rights" refers here to the Civil Code framework protecting privacy, reputation, image, and related personal interests. For Canadian readers, it is broadly comparable to a cluster of privacy-related interests. *Civil Code of the People's Republic of China*, Order No 45 of the President of the People's Republic of China, 28 May 2020, effective 1 January 2021, art 990, CLI.1.342411(EN), online: PKUlaw <https://www.pkulaw.com/en_ch1/aa00daeb5a4fe4ebdfb.html>.

²⁶ Hsieh Yi-hsuan, *supra* note 21.

²⁷ UN Women, Technology-Facilitated Gender-Based Violence: Developing a Shared Research Agenda (September 2024), online: <<https://www.unwomen.org/en/digital-library/publications/2024/09/technology-facilitated-gender-based-violence-developing-a-shared-research-agenda>>.

This paper therefore asks: with reference to Canadian law and policy, in what ways might China strengthen its structural responses to harms associated with deepfakes and non-consensual intimate images; what forms of functional learning can be drawn, and what requires further critical reflection and discernment?

In Part 2, the MaskPark case is examined not only as a narrative of large-scale intimate image abuse, but as a case study that exposes the gap between Chinese law on the books and law in action.²⁸ It considers the state, judicial, and platform responses to identify the structural dimensions of the problem and the practical weaknesses of existing Chinese remedies. Through this analysis, the author identifies six key criteria that will guide the rest of the analysis: *speed*, *accessibility*, *durability*, *victim agency*, *prevention*, and *accountability*. These criteria though not exhaustive, capture the relevant policy dimensions that emerge most clearly from MaskPark when the harms of intimate image abuse are understood as simultaneously individual, public, and structural.

Part 3 turns to other jurisdictions. It begins with a brief reference to other Asian jurisdictions, particularly South Korea and Japan, as supplementary comparators. This is important not only for a later cultural considerations, but also because the emergence and public framing of MaskPark is tied to earlier regional debates, particularly those shaped by the South Korean Nth Room scandal.²⁹ Part 3 then turns to Canada and examines selected criminal provisions, civil and statutory remedies, key jurisprudence, and procedural pathways. This chapter focuses selectively on those Canadian responses that appear most relevant to addressing the structural weaknesses identified through MaskPark and most useful in light of the six criteria developed in Part 2. Its purpose is not to exhaustively catalogue Canadian legal doctrine, but to isolate legal and policy mechanisms that can help illuminate possible directions for reform in China, especially where they respond to the criteria developed in Part 2 in ways not yet clearly reflected in Chinese law or practice. The selection is therefore guided by relevance, not completeness.

²⁸ Here, “law on the books” and “law in action” refer to the gap between formal legal protections and the extent to which those protections are actually implemented in practice. See Martha-Marie Kleinhans & Roderick A Macdonald, “What is a Critical Legal Pluralism?” (1997) 12:2 Canadian Journal of Law and Society 25.

²⁹ Park Eun-jee, “Rushed ‘Nth Room Law’ Unlikely to Actually Stop Criminals” (2 June 2020), online: Korea JoongAng Daily <<https://koreajoongangdaily.joins.com/2020/06/02/business/indepth/Nth-room-digital-crime-Naver/20200602195600193.html>>.

It is also important to note that this discussion does not address the federal-provincial allocation of legal authority in Canada in any detail, since the present analysis is concerned mainly with the substance of legal responses. Even within these limits, the comparison remains valuable as a necessary preliminary step in clarifying the structural and systemic problems and identifying possible directions for more effective responses to networked intimate image abuse in China.

Part 4 brings the analysis together by evaluating the six criteria developed in Part 2 against the response structure that emerges from the Part 3 comparative analysis. That structure includes early-phase control and preservation, mid-phase access and procedural protection, later-phase adjudication and continuing enforcement, as well as broader systemic considerations that cut across those stages.

It then makes recommendations for a tiered reform model for strengthening China's responses to non-consensual IIA. The chapter closes by identifying a set of limits and cautions that emerge from the six-criteria analysis, including documentation gaps, risks associated with over-removal, the limits of cross-jurisdictional transfer, and the unsettled role of emerging provenance and watermarking tools.

The paper concludes by returning to the central comparative insight: that the most effective responses to large-scale networked intimate image abuse must combine timely control, institutional coordination, and practical and accessible pathways to relief.

1.1 A word on Research Design, Methodology, Scope and Limitations

This study uses a comparative research method which is doctrinal and case-oriented rather than empirical. It interprets legal texts, decisions, and institutional practices in order to explore how different systems frame IIA, victims remedies, and how far those remedies respond to the individual, public, and systemic dimensions of the harm.

China serves as the primary site of inquiry, with MaskPark functioning as the central case study through which the paper examines large-scale networked intimate image abuse. As earlier described, the MaskPark case is used because it brings together many of the issues at the centre of this study, including encrypted circulation, cross-border platform use, limited investigation, and the resulting strain on legal protection and public trust. Chinese civil, criminal, and

regulatory materials are read against the available MaskPark record to assess how formally recognised rights operate in practice in China. This record is necessarily incomplete, since it is drawn mainly from journalistic, advocacy, and other publicly available accounts rather than from official investigative files or a body of publicly available court materials, which, at least at the time of writing, are essentially absent. Some factual details therefore remain difficult to verify with precision. This limitation does not defeat the purpose of the inquiry, however, because the paper does not rely on MaskPark as a fully closed evidentiary record, but as a well-documented case through which systemic issues can be easily identified and broader weaknesses in existing Chinese responses can be analysed.

Canada provides the main comparative reference point. The study examines Canadian criminal offences on voyeurism and non-consensual distribution of intimate images, certain civil and statutory remedies, tribunal and court practice, and commentary from clinics and advocacy organisations. As earlier mentioned, the goal is not to transplant Canadian law, but to draw out concrete mechanisms that could help inform Chinese reform.

1.2 A Note on Definitions

This paper uses “intimate image abuse” (IIA) as its principal term. I adopt this term because it provides the clearest umbrella for the forms of harm examined here, including covert image capture, non-consensual sharing, and related forms of sexualised image misuse. Other terms appear in the literature and in some of the sources discussed and/or referred to throughout this paper. “Non-consensual intimate image” distribution is a narrower term, referring more specifically to distribution-based wrongdoing. “Image-based sexual abuse” is often used to emphasise the sexual violence and gendered character of the harm. “Technology-facilitated gender-based violence”, and the related expression “technology-facilitated sexual violence”, are broader categories or terms that situate intimate image abuse within a wider field of digitally mediated abuse. These terms are therefore related, but not fully identical in scope.

Where different terminology appears below, it is used in the more limited sense reflected in the relevant source material or context. Unless otherwise indicated, however, this paper uses intimate image abuse as its main term because it best captures the paper’s combined concern with privacy, sexual autonomy, circulation, and the public and systemic dimensions of the harm.

2. China after MaskPark

2.1 Timeline of Exposure and the Absence of Early Investigations

MaskPark came to public attention in July 2025 as a large Chinese language network built around Telegram channels that catered almost entirely to a male Chinese user base. Reporting indicates that the “MaskPark tree hole forum” included a main channel and at least twenty sub groups that focused on sexual content.³⁰ Membership across these channels exceeded one hundred thousand users, and some individual groups reportedly attracted more than two hundred thousand subscribers.³¹ Within this ecosystem, users shared covert recordings of women in a wide range of everyday settings, including rental apartments, bathrooms, public transport, shopping areas, changing rooms, dormitories, and medical facilities, alongside intimate images of partners and family members posted without consent.³² They also used artificial intelligence deepfake technology,³³ namely AI-generated or AI-altered images or recordings manipulated to make a person appear to do or depict something that did not in fact occur, to turn secretly recorded footage into pornographic videos and photos.³⁴

Hong Kong and international journalistic coverage trace the forum’s origins back several years and describe how MaskPark grew into what many users and journalists called “China’s Nth Room,”³⁵ explicitly linking it to the earlier South Korean Telegram exploitation case.³⁶ In early July 2025, a post on Xiaohongshu warning a woman with a distinctive tattoo that hidden cameras had been discovered in her rental flat and bathroom drew widespread attention and helped connect scattered suspicions to the existence of MaskPark.³⁷ Soon after, hashtags about overseas

³⁰ Wang Yi & Feng Xi, *supra* note 24.

³¹ *Ibid.*

³² Hsieh Yi-hsuan, *supra* note 21; Ling Li, *supra* note 22; Wang Yi & Feng Xi, *supra* note 24.

³³ Chidera Okolie, “Artificial Intelligence-Altered Videos, Image-Based Sexual Abuse, and Data Privacy Concerns” (March 2023) 25:2 *Journal of International Women’s Studies*, art 11.

³⁴ Lianhe Zaobao, “MaskPark: More than 100,000 People in China’s ‘Nth Room’ Circulated Hidden-Camera Photos, and No Government Department Has Yet Responded or Taken Action” (31 July 2025), online: HK01 <<https://www.hk01.com/article/60262198>>.

³⁵ *Ibid.*

³⁶ Park Eun-jee, *supra* note 29.

³⁷ Li Hsuan-hsuan, “China’s Version of the ‘Nth Room’ Erupts: Private Images Allegedly Leaked as the ‘MaskPark Tree Hole’ Group Exposes One Hundred Thousand Members” (20 July 2025), online: Newtalk News <<https://gqr.sh/mvNc>>.

forums circulating large volumes of Chinese women’s private images began to trend on mainland social media, although discussion appeared to be quickly contained.³⁸

Against this background, and based on the author’s review, what is striking in the contemporaneous media coverage is how little visible state action was reported. As of the end of July 2025, Hong Kong media explicitly noted that no Chinese government department had issued a public statement or announced concrete investigative steps in response to the MaskPark revelations.³⁹ Civil society commentators also observed that MaskPark channels remained active for some time after the scandal broke, and contrasted this with the rapid investigative response and criminal trials that followed the Nth Room case in South Korea.⁴⁰ Taken together, these accounts depict a sequence in which public anger and media investigation escalated far more quickly than any documented move by Chinese authorities to open large numbers of cases against administrators or core participants.⁴¹

This in turn raises the next question for the present analysis: what aspects of existing Chinese law might potentially apply to conduct of this kind.

2.2 Personality rights, deep synthesis rules, and the enforcement gap

Conduct like that revealed in MaskPark appears to potentially fall within several existing Chinese legal regimes. Most immediately, it engages the separate Book on Personality Rights in the *Civil Code of the People’s Republic of China* (*Chinese Civil Code* or *Civil Code*), which is organised into six chapters and provides the main civil framework.⁴² Within this framework, the legal issues raised by MaskPark are especially connected to personality interests.

In short, personality rights are similar to Western concepts of privacy and security rights. The *Civil Code*’s personality rights chapter:

³⁸ Chen Zhengjia, “China’s Version of ‘Nth Room’: The ‘MaskPark Tree Hole’ Scandal Has Victimized 900,000 Women” (29 July 2025), online: Yahoo News <<https://gqr.sh/92gX>>.

³⁹ Lianhe Zaobao, *supra* note 34.

⁴⁰ Li Youzhen, “Fear of Secret Filming as an Everyday Reality: How ‘China’s Nth Room’ Ignited Women’s Anger” (4 August 2025), online: Deutsche Welle <<https://gqr.sh/79y7>>.

⁴¹ Lianhe Zaobao, *supra* note 34.

⁴² *Civil Code of the People’s Republic of China*, *supra* note 25, Book IV Personality Rights, chs 1–6.

- recognises privacy,⁴³ reputation,⁴⁴ and bodily integrity;⁴⁵
- describes privacy in terms of private life, private activities, private spaces, and private information;⁴⁶
- treats dwellings, hotel rooms, and comparable locations as spaces that may not be intruded into or monitored without consent.⁴⁷

Secretly installing cameras in bedrooms, rental flats, or dormitories and recording women's bodies in those spaces therefore sits squarely within this understanding of an unlawful invasion of privacy and an infringement of personality rights.^{48,49}

Alongside civil norms, the combination of public security law and selected criminal offences forms a second layer of regulation. Voyeuristic and secret recording is treated in practice as a violation of public security rules on “peeping, secret photography, secret recording or spreading the privacy of others,”⁵⁰ and is frequently punished with short administrative detention or fines rather than criminal penalties.⁵¹ Only a minority of cases escalate into criminal proceedings, typically by using offences such as illegal intrusion into dwellings,⁵² illegal use of special eavesdropping or secret-photography equipment,⁵³ extortion,⁵⁴ or producing and disseminating obscene material for profit.⁵⁵ This structure does indicate that covert recording is not regarded as a matter of purely private concern. At the same time, the public dimension is framed mainly through public order, security management, or regulated equipment,⁵⁶ rather than

⁴³ *Ibid*, Book IV Personality Rights, ch 6 Right to Privacy and Protection of Personal Information.

⁴⁴ *Ibid*, Book IV Personality Rights, ch 5 Right to Reputation and Right to Honour.

⁴⁵ *Ibid*, Book IV Personality Rights, ch 2 Right to Life, Right to Bodily Integrity and Right to Health.

⁴⁶ *Ibid*, Book IV Personality Rights, ch 6 Right to Privacy and Protection of Personal Information, art 1032.

⁴⁷ *Ibid*, art 1033.

⁴⁸ *Civil Code of the People's Republic of China*, *supra* note 25, Book IV Personality Rights, ch 1 art 990.

⁴⁹ *Ibid*, Book IV Personality Rights, ch 6 Privacy and Personal Information Protection, arts 1032–1033.

⁵⁰ *Law of the People's Republic of China on Public Security Administration Punishments* (2025 Revision), Order No 49 of the President of the People's Republic of China, 27 June 2025, effective 1 January 2026, art 50(6), CLI.1.5299183(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/4a0675f698316d0fbdfb.html>.

⁵¹ *Ibid*.

⁵² *Criminal Law of the People's Republic of China* (2023 Amendment PKULAW Version), 29 December 2023, effective 1 March 2024, art 245, CLI.1.5185739(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/3b70bb09d2971662bdfb.html>.

⁵³ *Ibid*, art 284.

⁵⁴ *Ibid*, art 274.

⁵⁵ *Ibid*, art 363.

⁵⁶ Hu Junyan, A Study on Criminal Regulation of Secret Photography, master's thesis, Southwest University of Political Science and Law, 2023.

through the protection of privacy or sexual autonomy as such. That framing makes it difficult to calibrate criminal sanctions to the actual harm of persistent or commercialised secret filming.⁵⁷

A similar pattern appears in relation to “private spaces within public places,” such as shopping-mall changing rooms and public washrooms. Regulatory measures restrict the installation of cameras in these areas and impose real-name management on certain devices,⁵⁸ yet there is still no dedicated criminal offence that directly targets covert recording that violates a person’s privacy and sexual dignity. In practice, police and prosecutors continue to rely on administrative sanctions and on general offences that were not drafted with image-based abuse in mind, which leaves the legal response fragmented and in the view of the author and other commentators, too lenient.⁵⁹

The overall result is a structural gap between civil and administrative norms that look robust on paper and the protection that victims actually receive. Personality rights under the *Civil Code* depend on individual victims recognising the violation, identifying a responsible party, collecting evidence and bringing a civil claim. In a case like MaskPark, many women had no idea cameras were present or only learned of the possibility when a stranger recognised them online, and even then the forum was hosted overseas and the uploader was often anonymous. The key point to be taken here is that the basic preconditions for civil litigation, including a known defendant and a stable evidentiary record, are missing.

At the same time, the dominance of low-level administrative responses further weakens the expressive and deterrent functions of existing law. Empirical analyses of decided cases show that most secret-photography incidents in private spaces are seen as basic security or public order issues, resolved through public security penalties rather than criminal convictions, with only a small fraction entering the criminal courts, as already mentioned.⁶⁰ Scholars argue that treating voyeuristic recording primarily as a minor public order issue fails to recognise its character as a serious infringement of privacy and sexual integrity, particularly where images are stored, shared

⁵⁷ *Ibid.*

⁵⁸ *Regulation on the Administration of Public Security Video Image Information Systems*, Order No 799 of the State Council of the People’s Republic of China, 13 January 2025, effective 1 April 2025, art 8, CLI.2.5291008(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/2e489e43d96ae400bdfb.html>.

⁵⁹ *Law of the People’s Republic of China on Public Security Administration Punishments*, *supra* note 50, art 50(6).

⁶⁰ Hu Junyan, *supra* note 56.

or monetised.⁶¹ They call for a specific offence that would identify privacy or sexual dignity as the direct object of protection and would attach penalties that reflect the long-term harm associated with the creation and circulation of intimate images.⁶²

Debates on network-based sexual offending reinforce this diagnosis. Chinese commentary traces a shift from direct physical contact offences toward non-contact, image-based and platform-mediated abuse, and stresses that network sexual crimes are more concealed, more complex in structure and often more enduring in their impact on victims.⁶³ In China, traditional pornography and obscenity offences were designed with commercial distribution and public morality in mind, not with the protection of individuals whose intimate images are captured or shared without their consent. Scholars analysing cases inspired by the South Korean Nth Room scandal argue that large-scale distribution of non-consensual intimate images should be treated as a distinct form of sexual violence, yet they note that existing offence structures have not been systematically revised to incorporate this understanding.⁶⁴

Superimposed on this picture is the newer regime for deep synthesis and AI-generated content. Regulations on network audio-visual services and later generative-content rules require prominent labelling of synthetic audio-visual material⁶⁵ and impose preventive duties on providers and users of deep synthesis technology.⁶⁶ These measures create ex ante obligations aimed at marking and constraining certain uses of synthetic media, and some commentators suggest that criminal law might build upon them in serious cases. At the same time, commentators recognise that much deep synthesis draws on material that is already publicly available and that many abusive uses fall outside existing norms on unlawful collection of personal information, which limits the reach of these rules.⁶⁷

⁶¹ Li Jingying, Research on the Criminal Regulation of Secret Filming in Private Spaces, master's thesis, Yunnan University of Finance and Economics, 13 May 2024.

⁶² Hu Junyan, *supra* note 56.

⁶³ Wang Wenqi, Criminal Regulation of Online Sexual Offenses, master's thesis, University of International Business and Economics, 2021.

⁶⁴ *Ibid.*

⁶⁵ *Provisions on the Administration of Cyber Audio and Video Information Services*, 18 November 2019, effective 1 January 2020, art 11, online: <<https://gqr.sh/LvaL>>.

⁶⁶ *Ibid.*, arts 12–13.

⁶⁷ Liu Zishuo & Zhu Tonghui, “Criminal Regulation of the Abuse of ‘Deepfake’ Technology” (2025) 41:9 Journal of China People's Police University 58.

Research on deepfake evidence in criminal proceedings further highlights the difficulty of relying on these regulatory tools once abuse is coordinated through encrypted or foreign-hosted platforms. Analysts emphasise that legal norms have not kept pace with generative AI,⁶⁸ that domestic regulators have limited leverage over overseas services,⁶⁹ and that a governance model built mainly on technical detection tools leaves investigators and courts reacting after harmful content has already spread.⁷⁰ They call for a combined institutional and technological response, including specific legislation on deep synthesis risks and clearer obligations for service providers, precisely because current arrangements do not provide clear triggers for rapid state intervention when large volumes of manipulated or covertly recorded images begin to circulate.⁷¹

The MaskPark example makes the enforcement gap clear. Victims often cannot identify the person who installed the camera, uploaded the material, or could realistically be sued in China. Administrative penalties are too limited to address large-scale image trading. Criminal law remains fragmented and does not target non-consensual intimate image abuse as a distinct wrong. Deep synthesis rules were designed for labelled synthetic content on domestic platforms, not for ordinary-looking images circulating through encrypted overseas channels. As a result, privacy and personality rights are formally recognised, but there is no clear legal route to rapid, coordinated enforcement against the kind of cross-border, cross-platform abuse exposed by MaskPark.

2.3 Platform Governance Failures and Cross-Platform Barriers

MaskPark operated through a constellation of Chinese language Telegram channels that hosted voyeuristic recordings and non-consensual intimate images of Chinese women, alongside groups selling covert cameras and related tools. Investigative accounts describe a main forum linked to numerous subsidiary channels, with a large membership, where covert recordings from everyday settings were circulated alongside private photographs uploaded without consent, in some cases involving minors.⁷² These channels relied on an encrypted, foreign hosted service

⁶⁸ Pan Jingui & Yang Hongbin, “Technical Black Boxes and Rule Reconstruction: The Dilemma of Examining Deepfake Evidence in Criminal Procedure and Possible Paths Forward” (2025) 4 Journal of Liaoning Police and Justice Management Cadre Institute 69.

⁶⁹ *Ibid.*

⁷⁰ *Ibid.*

⁷¹ Liu Zishuo & Zhu Tonghui, *supra* note 67.

⁷² Li Youzhen, *supra* note 40.

officially blocked in China yet widely accessible through technical workarounds,⁷³ which placed the core of the abuse beyond the direct reach of Chinese regulatory structures.

When reporting and public advocacy pushed MaskPark into wider visibility, Telegram's responses were partial and uneven. Media and civil society accounts indicate that the main channel was eventually removed,⁷⁴ but adjacent groups with tens of thousands of members remained active, and new channels emerged to replicate established patterns of trading and sharing.⁷⁵ Some forums simply shifted from open access to invitation only status,⁷⁶ which limited external monitoring but offered no assurance to victims that their images had been permanently deleted. From a survivor's standpoint, takedown therefore appeared temporary and reversible, rather than a coordinated platform wide effort to dismantle a network organised around intimate image abuse.⁷⁷

Inside China, platform practices moved in the opposite direction. Instead of facilitating documentation or supporting calls for *accountability*, domestic social media companies constrained the visibility of the scandal itself. In the first days after exposure, hashtags linked to MaskPark and to Chinese language Telegram voyeurism groups drew enormous traffic as users circulated news stories and safety information.⁷⁸ Shortly afterward, searches for "MaskPark" produced notices that content could not be displayed under relevant regulations, and posts framing the incident as evidence of gender based violence or urging official inquiry were removed or buried.⁷⁹ Feminist accounts that attempted to coordinate information gathering were reportedly suspended or subjected to sharply reduced reach.⁸⁰ By late summer, the term had largely vanished from Chinese platforms, even as the underlying content remained active on Telegram.⁸¹

⁷³ *Ibid.*

⁷⁴ *Ibid.*

⁷⁵ *Ibid.*

⁷⁶ Lianhe Zaobao, *supra* note 34.

⁷⁷ A Mei, "Advocacy on the Maskpark Case: Stop Saying Telegram Cannot Be Investigated, the Real Question Is Whether Authorities Are Willing to Act" (31 July 2025), online: No More Chained (Substack) <<https://nomorechained.substack.com/p/maskparktelegram>>.

⁷⁸ *Ibid.*

⁷⁹ *Ibid.*

⁸⁰ *Ibid.*

⁸¹ Ling Li, *supra* note 22.

This interaction between an encrypted foreign platform and tightly moderated domestic services reveals the difficulty of developing any meaningful cross platform response. Women who feared their images might be on MaskPark typically encountered the issue through domestic apps, while the material itself circulated overseas in channels shielded by invitation links and opaque group rules. No institutional mechanism linked domestic platforms with Telegram, so survivors were forced to navigate separate reporting systems, repeating their accounts without any guarantee that action on one platform would trigger follow up elsewhere. The result was a fragmented governance environment in which no actor assumed responsibility for coordinating removal, supporting evidence preservation, or communicating outcomes.

Research from Canada and other jurisdictions underscores the structural limits of complaint-driven takedown systems when abuse is mobile and networked. Studies of reporting practices describe lengthy forms, minimal feedback, and patterns in which removed images reappear in altered formats or migrate to other sites, placing survivors in a cycle of monitoring and repeated takedown requests.⁸² Research on misogynistic online ecosystems likewise shows that even when platforms close specific channels, similar communities often regroup under new names, while transparency about enforcement remains limited.⁸³ These problems were amplified because Telegram was encrypted, foreign-based, and beyond any effective cross-platform enforcement framework.

2.4 Remedial Gaps in Doctrine and Practice

On paper, Chinese law offers an extensive set of remedies that appear capable of addressing the harms revealed by MaskPark. The *Civil Code*, for example, authorises courts to order the cessation of infringing conduct, to require the removal or blocking of unlawful content, to eliminate continuing negative effects, to restore reputation, to mandate public apologies, and to award compensation for both economic loss and emotional injury when privacy and related personality interests have been violated.⁸⁴ Procedural rules also contemplate evidence

⁸² Rebecca Katz, *supra* note 16.

⁸³ Cynthia Khoo, *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence* (Toronto: Women's Legal Education and Action Fund, 2021).

⁸⁴ Li Jingying, *supra* note 61.

preservation and conduct preservation,⁸⁵ which could in principle be used to secure digital traces of covert filming and to oblige intermediaries to restrict access to intimate images while proceedings are underway. Administrative⁸⁶ and criminal⁸⁷ frameworks allow public security organs and courts to impose fines, short terms of detention, criminal penalties, and confiscation of equipment used for secret recording.

In practice, however, the remedial picture is much narrower than the formal framework suggests. Three limits are central. Most secret-photography cases are still handled through modest administrative penalties rather than civil or criminal proceedings.⁸⁸ Courts have had little opportunity to develop a stable practice around injunctions, takedown orders, apologies, or other restorative relief. And civil personality rights claims depend on victims being able to identify a responsible actor, which is often impossible in a network built on hidden cameras, anonymous uploads, and encrypted foreign-hosted platforms.⁸⁹ In these conditions, much of the civil remedial framework remains theoretical for affected individuals.

Chinese scholarship on online sexual offending also highlights the near absence of structured survivor recovery mechanisms within existing remedial frameworks. Academic debate frequently focuses on offence classification, evidentiary standards, and sentencing, while issues central to victim recovery, such as psychological support, safety planning, and assistance with managing digital traces, receive limited sustained attention.⁹⁰ There is no coordinated scheme combining legal assistance, mental health services, and technical support for victims of image-based abuse, nor any institutional mechanism to track whether intimate images have been removed, whether they have resurfaced, or whether new uploads have emerged elsewhere.⁹¹ As a result, remedies such as apologies or damages function, when granted, as isolated outcomes in a

⁸⁵ *Civil Procedure Law of the People's Republic of China* (2023 Amendment), 1 September 2023, effective 1 January 2024, arts 84, 103, CLI.1.5175519(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/55ada7bc4fc9d8ccbd8fb.html>.

⁸⁶ *Law of the People's Republic of China on Public Security Administration Punishments*, *supra* note 50, art 50(6).

⁸⁷ *Criminal Law of the People's Republic of China*, *supra* note 52, art 284.

⁸⁸ Li Jingying, *supra* note 61.

⁸⁹ Jin Qianqian, "Research on the Legal Regulation of Secret Photography in Private Spaces of Public Places" (November 2023) *Journal of City University of Macau* 56.

⁹⁰ He Ye & Gao Jun, "Stigma and Psychological Recovery among Survivors of Sexual Assault" (2022) 30:3 *Chinese Journal of Clinical Psychology* 693.

⁹¹ See discussion in Xiao Shanshan & Wang Zerun, "From 'Direct Contact' to 'Non-Direct Contact': New Forms of Sexual Crimes Fostered by Online Media and Their Legal Regulation" (June 2022) 34:3 *Journal of Hunan Police Academy* 88.

small number of litigated cases⁹² rather than as components of a broader recovery response to continuing online harm.

2.5 Gendered Dynamics of Silence

The aftermath of MaskPark unfolded within a social environment where gendered power relations strongly shape who feels able to report harm. Media coverage of the scandal showed that many women first learned about the forum through warning posts circulating on social media, yet very few were willing to attach their identities when seeking help.⁹³ Research on gender-based violence in China provides insight into this pattern by documenting how women who disclose sexual harm are frequently treated as sources of trouble rather than as rights holders, and are subjected to moral judgment about their private lives.⁹⁴ When placed alongside the scale of MaskPark, these dynamics help explain why thousands of potential victims did not translate into a comparable number of formal complaints.

These pressures become particularly acute in the intimate and family contexts that MaskPark directly disrupted. The content shared in the forum included images taken in bedrooms, bathrooms and other private spaces, as well as photos originally exchanged within dating or marital relationships. Any attempt to seek redress required women to explain to parents, partners or relatives why such images existed or how hidden cameras could have captured their bodies.⁹⁵ Studies on survivors of sexual assault describe how families often prioritise concerns about reputation, marriage prospects and social standing over emotional support, and how partners may respond with suspicion or control rather than solidarity.⁹⁶ In the MaskPark context, these relational dynamics created additional risks that sit on top of the technological and legal barriers already faced by victims.

Online gender politics further intensified this chilling effect. Feminist analyses of digital debates around campus harassment show that when women speak publicly about sexual harm, reactions tend to polarise: some express support, while others cast doubt on victims' motives or

⁹² *Ibid.*

⁹³ Ling Li, *supra* note 22.

⁹⁴ See, for example, discussion in He Ye & Gao Jun, *supra* note 90.

⁹⁵ noise, "From 'China's Version of Room N' to Seeing How Fragile Our Digital Defenses Are" (9 August 2025), online: Commonwealth Opinion <<https://opinion.cw.com.tw/blog/profile/52/article/16441>>.

⁹⁶ He Ye & Gao Jun, *supra* note 90.

criticise them for not preventing the harm.⁹⁷ Reporting on MaskPark revealed similar patterns. Although many users voiced outrage and demanded investigation, others minimised the abuse, questioned why women had not “protected themselves,” or warned that speaking out would only attract further scrutiny.⁹⁸ For women who suspected that their images had circulated in MaskPark channels, these online reactions signalled that public disclosure might bring ridicule and moral judgment from strangers as well as from officials or family members.

Together, these gendered dynamics produced a pronounced barrier to formal reporting and shaped how the MaskPark aftermath unfolded. Many women limited their responses to anonymous posts, private requests for information or quiet attempts to remove content where possible. Engaging legal channels required navigating cross-platform evidence issues and jurisdictional limits, but also confronting the risk of social exposure in an environment where women’s sexuality is closely policed. As a result, MaskPark revealed not only gaps in Chinese legal and platform governance, but also a social order in which the costs of naming intimate image abuse fall disproportionately on victims, making silence appear safer than seeking state intervention.

2.6 Comparative Criteria

The foregoing points to six criteria for the comparative discussion that follows: *speed*, *accessibility*, *durability*, *victim agency*, *prevention*, and *accountability*. These criteria emerge from the weaknesses exposed by MaskPark, including delayed intervention, fragmented enforcement, unstable control over circulation, barriers to victim-led recourse, and the absence of a visible and coordinated response. They also show why the issues raised here are not reducible to private injury alone, but engage broader questions about effective protection, institutional response, and the conditions under which legal remedies become meaningful in practice.

⁹⁷ Liu Ting, A Comparative Study of Online Public Opinion on University Sexual Harassment Cases from a Feminist Perspective, master’s thesis, Harbin Institute of Technology, 2019.

⁹⁸ noise, *supra* note 95.

3. Selected Comparative Responses: East Asian Contexts and Canadian Legal Pathways

3.1 East Asian contextual comparators

MaskPark did not enter public discussion in a regional vacuum. Its rapid identification as “China’s Nth Room” shows that Chinese commentators, journalists, and activists were already drawing on an East Asian vocabulary for understanding digitally mediated sexual abuse. South Korea is the most important reference point in this regard. Korea’s Nth Room scandal had already transformed the regional discussion by making it harder to treat non-consensual intimate images and platform-based sexual exploitation as isolated incidents or as merely obscene content.⁹⁹ In the Korean context, the issue came to be understood as a form of digital sexual violence with both individual and public significance.¹⁰⁰

The point is not to suggest that South Korea has solved the problem. The literature instead shows that the Nth Room scandal became a focal point within a broader climate of feminist mobilisation, public anger, and continuing contestation over sexual violence, censorship, and state response.¹⁰¹ In that setting, digital sexual abuse was more quickly named as a social and political problem rather than left at the level of private shame. Research comparing technology-facilitated gender-based violence across jurisdictions also treats South Korea as a legal and institutional environment that has developed a more robust response to this form of harm than many other states in Asia.¹⁰² Read against MaskPark, this offers a meaningful contrast. The Chinese case generated widespread online outrage, but the available record suggests that public discussion was managed more quickly than the abusive network itself. The Korean reference thus helps clarify what is missing in China: not simply stronger law in the abstract, but a more recognisable chain between exposure, investigation, public acknowledgement, and enforcement.

⁹⁹ Min Joo Lee, “Sexual Violence and Censorship in Contemporary Korea: Examining the Debate Surrounding the Digital Sexual Violence Prevention Law” (2025) 49:1 Korean Studies 14.

¹⁰⁰ *Ibid.*

¹⁰¹ See, e.g., Kim Joohee & Jamie Chang, “Nth Room Incident in the Age of Popular Feminism: A Big Data Analysis” (2021) 14 Azalea: Journal of Korean Literature & Culture 261.

¹⁰² Ishita Sharma, “Technology-Facilitated Gender-Based Violence in the Digital Age: A Comparative Analysis of India and South Korea” (August 2025) 24:2 Journal of Korean Law 359.

Japan is also a useful supplementary comparator because it shows that covert recording and intimate image abuse are not unique to China. Japanese scholarship on intimate image abuse and voyeuristic photography describes a legal landscape in which these harms are recognised, but not always directly or comprehensively addressed.¹⁰³ Earlier responses relied heavily on piecemeal provisions and local public nuisance frameworks, especially in relation to covert photography, before more specific legislative tools were developed.¹⁰⁴ Even then, the literature notes significant gaps, including the uneven treatment of non-consensual production, covert capture, and newer forms of image manipulation.¹⁰⁵ For present purposes, the value of the Japanese comparison is not that it offers a comprehensive model for reform, but that it confirms a wider regional pattern: technological change has outpaced legal categories, and image-based abuse often falls between privacy law, obscenity law, and criminal prohibitions that were not designed with these harms in mind.

Taken together, the South Korean and Japanese materials help position MaskPark within a broader East Asian problem structure. Across the region, technology-facilitated abuse has been linked to entrenched gender inequality, digital misogyny, and persistent barriers to reporting. Regional review literature also suggests that underreporting remains common, in part because victims face shame, uncertainty about available remedies, and doubt about whether authorities will act effectively.¹⁰⁶ These features resonate closely with what the Chinese record reveals. MaskPark was not simply a large Telegram forum; it was a case in which intimate image abuse, voyeuristic subcultures, platform opacity, and weak legal translation from rights to enforcement converged in a particularly visible form. The East Asian reference is therefore relevant not as a detour into regional sociology, but as a way of sharpening the Chinese question. South Korea demonstrates the significance of *speed*, public recognition, and coordinated enforcement. Japan demonstrates the persistence of legal fragmentation even where reform has begun. Together, they help show that China's difficulty lies neither in cultural exceptionalism nor in technological

¹⁰³ See discussion in Yoshifumi Okada, "Criminalization of Intimate Image Abuse in Japan" in Gian Marco Caletti & Kolis Summerer, eds, *Criminalizing Intimate Image Abuse: A Comparative Perspective* (2024) 238.

¹⁰⁴ Shimpei Kudo, Plinio Montagna, Ald Ron & Adrienne Harris, "Voyeuristic Photography (Tosatsu): Liberation in the Claustrium" in *Anxiety, Psychoanalysis and Law* (2026) 110.

¹⁰⁵ *Ibid.*

¹⁰⁶ Vaiddehi Bansal, Mayumi Rezwan, Mithila Iyer, Erin Leasure, Connor Roth, Poulomi Pal & Laura Hinson, "A Scoping Review of Technology-Facilitated Gender-Based Violence in Low- and Middle-Income Countries Across Asia" (January 2024) 25:1 *Trauma, Violence, & Abuse* 463.

novelty alone, but in how slowly and unevenly its legal and institutional responses have adjusted to forms of abuse that are networked, gendered, and highly scalable.

3.2 Criminal touchpoints from Canadian law

The *Criminal Code of Canada (Criminal Code)*¹⁰⁷ is a federal statute enacted by the Parliament of Canada that provides the principal framework for criminal offences across Canada. Within this framework, several provisions offer relevant points of contact for harms of the MaskPark kind, especially voyeurism,¹⁰⁸ non-consensual distribution of intimate images,¹⁰⁹ criminal harassment,¹¹⁰ and, in some circumstances, extortion,¹¹¹ and defamatory libel.¹¹²

Canadian *Criminal Code* offences do not form a unified response to intimate image abuse, but they do show how criminal law can treat certain forms of covert recording, circulation, and coercion as public wrongs that warrant state condemnation and, where appropriate, prosecution, rather than leaving them entirely to the realm of private grievance.¹¹³ In that sense, the criminal law matters not only because it punishes, but also because it marks these harms as matters of public concern implicating privacy, dignity, equality, and collective welfare interests when intimate images are created or shared without consent.¹¹⁴

That broader criminal law orientation can be seen more concretely in the specific *Criminal Code* provisions that address image capture, non-consensual distribution, and related forms of coercive conduct.

Voyeurism is the clearest criminal touchpoint at the moment of image capture. Under section 162 of the *Criminal Code*, voyeurism centres the idea of a reasonable expectation of

¹⁰⁷ *Criminal Code*, *supra* note 2.

¹⁰⁸ *Ibid*, s 162.

¹⁰⁹ *Ibid*, s 162.1(1).

¹¹⁰ *Ibid*, s 264(1).

¹¹¹ *Ibid*, s 346.

¹¹² *Ibid*, ss 298–300.

¹¹³ Lisa Kerr, “The Legitimate Scope of Criminal Law: A Question for Legal History?” (April 2017) 4:1 Critical Analysis of Law: An International & Interdisciplinary Law Review 11.

¹¹⁴ Richard Jochelson, David Ireland & Hannah Taylor, “Clearing Your History: A Review of Non-Consensual Distribution of Intimate Images in Canada and Future Responses” (September 2021) 54:3 University of British Columbia Law Review 763.

privacy,¹¹⁵ and the case *R v Jarvis*¹¹⁶ confirms that this must be assessed contextually, with attention to setting, relationship, purpose, and power rather than physical location alone.¹¹⁷ This creates a clearer nexus between the individual violation and the broader public dimensions of the harm than a framework focused primarily on recording in prohibited spaces.

The offence of non-consensual distribution of intimate images under section 162.1, addresses the next stage of the harm - circulation. This section is important because it expressly recognises that the unauthorised circulation of intimate images is itself a serious injury to autonomy, privacy, and sexual dignity.¹¹⁸ In practical terms, these provisions are strongest in denunciation, recognition of harm, and targeted deterrence.¹¹⁹

Their practical limits, however, are equally instructive. Canadian commentary consistently shows that criminal coverage remains fragmented, with different aspects of the harm falling under different offences, including harassment or extortion where threats, repeated contact, or coercive demands are involved.¹²⁰ No single offence fully addresses the broader life of intimate images once they move across platforms, are copied by multiple actors, or become embedded in ongoing abuse. Criminal law is also limited in terms of victim control. A prosecution may punish an offender and affirm the seriousness of the wrong, but it does not necessarily secure rapid takedown, prevent reposting, or give victims meaningful influence over the process.¹²¹ Its capacity for sustained systemic change is also weak, since its basic structure remains offender-focused and retrospective even where the underlying harm is networked and scalable.

For present purposes, the value of these criminal touchpoints lies in their selective utility. They provide examples of tools for *accountability* and deterrence and which operate at both the individual and broader public level. For individual victims, they recognise the wrong and impose punishment on identifiable offenders. More broadly, they mark covert recording, non-consensual

¹¹⁵ *Criminal Code*, *supra* note 2, s 162.

¹¹⁶ *R v Jarvis*, 2019 SCC 10, [2019] 1 SCR 488. In *Jarvis*, a teacher secretly recorded students at school using a pen camera. The Supreme Court of Canada held that the students had a reasonable expectation of privacy and restored the teacher's conviction for voyeurism.

¹¹⁷ Richard Jochelson, *supra* note 114.

¹¹⁸ *Criminal Code*, *supra* note 2.

¹¹⁹ Richard Jochelson, *supra* note 114.

¹²⁰ Cynthia Khoo, *supra* note 83.

¹²¹ Moira Aikenhead, *supra* note 13.

circulation, and related coercive conduct as matters of public concern rather than purely private grievance, thereby engaging wider interests in privacy, equality, and confidence in legal protection.¹²² At the same time, they do not offer a complete answer to the structural weaknesses identified in Part 2. The stronger public dimension of criminal law also does not make it sufficient on its own. Criminal prohibitions can denounce the wrong and affirm the wider social importance of privacy, equality, and sexual autonomy, but they are generally less capable of securing rapid control over ongoing circulation or providing victims with accessible, durable, and participatory forms of relief. In the terms developed through MaskPark, the criminal law touchpoints contribute most clearly to *accountability* and *prevention*, but much less to *speed*, *victim agency*, *durability*, or *accessibility*.

3.3 Civil and statutory remedies from Canadian law

If criminal law in Canada is strongest for denunciation and recognition, civil and statutory remedies are more significant for controlling ongoing harm as they are potentially directed more toward stopping circulation, protecting identity, and giving victims a clearer procedural route to seek relief.¹²³

*Provincial Legislation*¹²⁴

Canadian provincial legislation on intimate image abuse demonstrates how legal design can be oriented toward practical victim needs rather than toward criminal classification alone.

The provincial statutes are particularly useful because they isolate the wrong and attach remedies tailored to it. Rather than forcing claimants to proceed indirectly through older legal categories, these laws identify non-consensual intimate image distribution as a specific civil wrong and then provide targeted responses. The remedies commonly include declarations, injunctions, takedown obligations, damages, and, in some jurisdictions, anonymity protections or publication restrictions. Examples of provincial legislation include:

¹²² Richard Jochelson, *supra* note 114.

¹²³ Rebecca Katz, *supra* note 16.

¹²⁴ At the time of writing, Nunavut, the Northwest Territories, and Yukon appear to rely primarily on *Criminal Code* provisions and do not have statutory torts specifically addressing the non-consensual distribution of intimate images. See Nova Scotia, Department of Justice, Report on the Review of the *Intimate Images and Cyber-protection Act* (2022) at 14, online: <<https://novascotia.ca/intimate-images-and-cyber-protection-act-survey/documents/report-on-the-review-of-the-intimate-images-and-cyber-protection-act.pdf>>.

- British Columbia: *Intimate Images Protection Act*, SBC 2023, c 11 (*BC Act*, BC model)¹²⁵

British Columbia adopts a stand-alone statutory approach that identifies intimate image abuse as a distinct wrong. Its focus is practical and control-oriented: the *BC Act* defines intimate images broadly, extends protection to altered and non-identifiable images, addresses both distribution and threatened distribution, and builds relief around expedited orders, removal, de-indexing, damages, and publication protections. In comparative terms, the BC model stands out for the clarity with which it prioritises rapid control and procedural usability in digital settings.¹²⁶

- Alberta: *Protecting Victims of Non-Consensual Distribution of Intimate Images Act*, S.A. 2017, c. P-26.9 (*AB Act*, AB model)¹²⁷

Alberta adopts a narrower stand-alone statutory tort model. Like British Columbia, it treats non-consensual distribution as a distinct civil wrong actionable without proof of damage and preserves the claimant's reasonable expectation of privacy despite prior recording or sharing. Its focus, however, is more conventional and court-centred, emphasizing damages, accounting of profits, injunctions, and publication bans rather than the more elaborate expedited removal and de-indexing architecture found in British Columbia.¹²⁸

- Saskatchewan: *Privacy Act*, R.S.S. 1978, c. P-24, s. 7.3(1), (2); *Privacy Amendment Act*, 2018, SS 2018, c 28 (*SK Act*, SK model)¹²⁹

Saskatchewan occupies a middle position. Its scheme remains anchored in 1970s privacy legislation, but later 2018 amendments move it beyond a more conventional privacy model by expressly addressing threats, altered images, de-indexing, and orders directed to internet intermediaries. In this respect, it is not entirely dissimilar to the BC or Alberta models but still reflects a clear shift toward more tailored relief for intimate image abuse.

¹²⁵ *Intimate Images Protection Act*, SBC 2023, c 11, online: CanLII <<https://www.canlii.org/en/bc/laws/stat/sbc-2023-c-11/latest/sbc-2023-c-11.html>>.

¹²⁶ Jasmine Samra & Christopher Oates, "Navigating British Columbia's *Intimate Images Protection Act*" (26 February 2024), online: Gowling WLG <<https://gowlingwlg.com/en-ca/insights-resources/articles/2024/british-columbia-intimate-images-protection-act>>.

¹²⁷ *Protecting Victims of Non-consensual Distribution of Intimate Images Act*, SA 2017, c P-26.9, online: CanLII <<https://www.canlii.org/en/ab/laws/stat/sa-2017-c-p-26.9/latest/sa-2017-c-p-26.9.html>>.

¹²⁸ *Ibid.*

¹²⁹ *The Privacy Act*, RSS 1978, c P-24, s 7.3(1)–(2), online: CanLII <<https://www.canlii.org/en/sk/laws/stat/rss-1978-c-p-24/latest/rss-1978-c-p-24.html>>; *The Privacy Amendment Act*, 2018, SS 2018, c 28, online: CanLII <<https://www.canlii.org/en/sk/laws/astat/ss-2018-c-28/latest/ss-2018-c-28.html>>.

- Manitoba: *The Non-Consensual Distribution of Intimate Images Act* (MB Act, MB model)¹³⁰

Manitoba takes a somewhat different path. Rather than relying on a purely remedial model, it combines a civil cause of action with a support framework aimed at assisting persons whose intimate images have been distributed, or are at risk of distribution. Its more recent amendments also extend the scheme to fake intimate images. In comparative terms, Manitoba is less notable for its removal architecture than for linking civil relief with a more express victim-support structure.

- Ontario

Ontario also takes a different route. Rather than adopting a dedicated civil statute in this area, the Ontario model continues to rely primarily on common law development and equitable relief. The clearest illustration is the 2018 decision of the Ontario Superior Court (ONSC), *Jane Doe 72511 v Morgan*,¹³¹ where the ONSC treated the non-consensual online posting of an intimate video as giving rise to a civil remedy through the tort of public disclosure of private facts. In comparative terms, Ontario stands apart less for statutory design than for leaving this field to judge-made development.

- Quebec: *Act to counter non-consensual sharing of intimate images*, CQLR c P-9.0002 (*QC Act*, QC model)¹³²

Quebec broadly follows the stand-alone statutory pattern, but with a more expressly urgent and court-centred design. Its scheme is framed around a simple and rapid recourse to stop or prevent non-consensual sharing, with particular emphasis on restraint, destruction, de-indexing, and confidentiality.

- New Brunswick: *Intimate Images Unlawful Distribution Act*, SNB 2022, c 1 (*NB Act*, NB model)¹³³

¹³⁰ *The Non-Consensual Distribution of Intimate Images Act*, *supra* note 18.

¹³¹ *Jane Doe 72511 v Morgan*, 2018 ONSC 6607, 143 OR (3d) 277.

¹³² *Act to Counter Non-Consensual Sharing of Intimate Images*, CQLR c P-9.0002, online: CanLII <<https://www.canlii.org/en/qc/laws/stat/cqlr-c-p-9.0002/latest/cqlr-c-p-9.0002.html>>.

¹³³ *Intimate Images Unlawful Distribution Act*, SNB 2022, c 1, online: CanLII <<https://www.canlii.org/en/nb/laws/stat/snb-2022-c1/latest/snb-2022-c1.html>>.

New Brunswick structures the issue through a two-track scheme. One track is directed to expedited court-ordered relief aimed at stopping or limiting circulation. The other supports a fuller damages claim. The statute also extends to threatened distribution and builds in publication-ban protection. Its significance lies less in any sharp departure from other provinces than in the comparatively clear separation between urgent control and longer-form civil recovery.

- Nova Scotia: *Intimate Images and Cyber-protection Act*, S.N.S. 2017, c.7, (*NS Act*, NS model)¹³⁴

Nova Scotia adopts a broader and more flexible remedial structure. The *NS Act* legislation is notable for the range of orders available, including interim and final relief, access restrictions, disclosure measures aimed at identifying responsible actors, and a damages framework that is not limited to straightforward compensatory loss. In comparative terms, its distinctiveness lies in the breadth of its remedial design rather than in a fundamentally different model.

- PEI: *Intimate Images Protection Act*, SPEI 2020, c 55, (*PEI Act*, PEI model)¹³⁵

Prince Edward Island takes a comparatively structured approach. Its model separates applications for declaratory and injunctive relief from damages claims, while also extending to threats, altered images, de-indexing, and revocation of consent. In comparative terms, what stands out is less the overall model than the relative clarity with which different forms of relief are organized within the statute.

- Newfoundland and Labrador: *Intimate Images Protection Act*, RSNL 2018, c I-22, (*NL Act*, NL model)¹³⁶

Newfoundland and Labrador remains close to the more conventional statutory tort pattern. The *NL Act* centres a direct civil action for non-consensual distribution without proof of damage, preserves privacy despite prior recording or sharing, and provides the familiar

¹³⁴ *Intimate Images and Cyber-protection Act*, SNS 2017, c 7, online: CanLII <<https://www.canlii.org/en/ns/laws/stat/sns-2017-c-7/latest/sns-2017-c-7.html>>.

¹³⁵ *Intimate Images Protection Act*, SPEI 2020, c 55, online: CanLII <<https://www.canlii.org/en/pe/laws/astat/spei-2020-c-55/210231/spei-2020-c-55.html>>.

¹³⁶ *Intimate Images Protection Act*, RSNL 2018, c I-22, online: CanLII <<https://www.canlii.org/en/nl/laws/stat/rsnl-2018-c-i-22/latest/rsnl-2018-c-i-22.html>>.

combination of damages, injunctive relief, and publication protection. In comparative terms, it adds little by way of structural innovation, but confirms the wider provincial tendency to treat intimate image distribution as a distinct civil wrong rather than leaving it to general private law alone.

Viewed together, these provincial measures fall into a few related patterns rather than a single uniform model. Most treat non-consensual intimate image distribution as a distinct civil wrong and are organised around practical relief, but they differ in structure and emphasis. Some proceed through stand-alone statutes built around direct applications, injunctions, damages, and control-oriented orders. Others remain anchored in broader privacy legislation or, in Ontario, in common law development. The main differences lie in the degree of procedural urgency, the breadth of available orders, the extent to which threats, altered or fake images, and internet intermediaries are expressly addressed, and whether the scheme is confined to civil liability or also incorporates a more explicit support framework. What links them is a common shift away from indirect reliance on older legal categories and toward more tailored responses to a form of harm that is fast-moving, cumulative, and difficult to contain once circulation begins.

That shared orientation also helps clarify the public dimension, if any, of the civil approach. It lies less in denunciation than in the attempt to make relief more reachable and more responsive to the realities of digital circulation.¹³⁷ In that sense, these schemes do more than provide individualized compensation. By creating more direct routes to injunctions, takedown-oriented orders, anonymity protections, and, in some instances, support services and financial compensation, they can reduce some of the practical barriers that would otherwise leave victims without any meaningful recourse. At the same time, their limits remain evident. The burden still falls largely on the depicted person to trigger the process, seek relief, and navigate enforcement.¹³⁸¹³⁹ For that reason, the civil model may respond more effectively to access and immediate control than to the broader structural and collective conditions that allow this form of harm to persist. Read through the six criteria developed in Part 2, the civil models' strongest

¹³⁷ Technology Safety Canada, "Preserving Digital Evidence Example: Sexual Images Shared Online", online: Tech Safety <<https://techsafety.ca/resources/toolkits/preserving-digital-evidence-example-sexual-images-shared-online>>; *Lawrence v Bassett*, 2015 ONSC 3707.

¹³⁸ Rebecca Katz, *supra* note 16.

¹³⁹ See, e.g., *Intimate Images Protection Act*, *supra* note 125; *The Non-Consensual Distribution of Intimate Images Act*, *supra* note 18.

contributions lie in *accessibility*, *victim agency*, and *speed*, with some support for durability where ongoing orders or continuing restraints are available. Their weaker contribution lies in *prevention* and *accountability* at the systemic level, since civil relief remains largely claimant-driven and does not by itself ensure visible institutional response or broader deterrence

Common Law

Common law and equitable routes remain important alongside criminal and civil statutes. For example, privacy torts, breach of confidence, intrusion upon seclusion, and intentional infliction of mental suffering continue to offer pathways where no dedicated statute applies or where plaintiffs seek a fuller account of the harm.¹⁴⁰ Common law tort significance to this issue lies in its flexibility. It can allow courts to recognise a privacy injury even where the loss is not easily expressed in economic terms, and can provide a vocabulary for harms that may begin with surveillance, deepen through circulation, and persist through the threat of renewed exposure.¹⁴¹ In a technological environment shaped by remote observation and easy image capture and circulation, flexibility matters. It allows civil law to respond to layered privacy injury rather than treating publication as the only legally meaningful moment.

Remedies

Within these provincial civil and statutory responses, in the view of the author, the remedies that matter most in practice are injunctions, takedown-oriented orders, and damages. Canadian case law shows that courts are capable of granting swift control-oriented relief, tailored orders, and substantial damages in intimate image and related cyber abuse cases.¹⁴²

For present purposes, the precise facts of the leading Canadian cases on IIA matter less than the remedial orientation they demonstrate. From a policy and remedy perspective, their value is complementary rather than substitutive. Criminal law speaks most directly to *prevention*, *denunciation*, and *accountability*. Civil and statutory remedies, by contrast, are often more responsive to *speed*, *durability*, *accessibility*, and *victim agency* because they can target the continued presence of the image, support ongoing injunctions or preservation mechanisms, and

¹⁴⁰ Kristen Thomasen, *Private Law & Public Space: The Canadian Privacy Torts in an Era of Personal Remote-Surveillance Technology*, doctoral thesis, University of Ottawa, 29 June 2022.

¹⁴¹ Richard Jochelson, *supra* note 114.

¹⁴² *Jones v Tsige*, 2012 ONCA 32; *Jane Doe 464533 v N.D.*, 2016 ONSC 541.

allow claimants to shape the relief sought more directly than in a criminal process controlled by the state.¹⁴³

This does not mean that civil or statutory remedies fully resolve the problem. Canadian commentary notes that takedown orders cannot guarantee complete disappearance once images have been copied, saved, or reposted across platforms.¹⁴⁴ Cost, legal literacy, emotional burden, and the difficulty of identifying the right defendant also remain serious constraints. Even so, these remedies are significant because they recognise privacy harm, exposure, humiliation, and continuing vulnerability in terms more closely aligned with effective relief than a framework centred only on punishment.¹⁴⁵ For this paper, their relevance lies in what they suggest for contexts such as MaskPark, where rights may already exist in principle, but the pathways for turning those rights into meaningful protection remain too slow, indirect, or difficult to access in practice.

3.4 Procedural and remedial features with public interest relevance

The significance of Canadian procedural mechanisms lies in a simple point: substantive rights are of limited value if victims cannot use them in time, in safety, or against an identifiable defendant. In image-based abuse cases, this problem is acute.¹⁴⁶ Harm often unfolds quickly, evidence is easily lost, and the legal process itself may expose victims to renewed injury.¹⁴⁷ For that reason, procedural features such as anonymity orders, publication bans, disclosure mechanisms, and preservation tools are not merely technical devices. They bear most directly on *accessibility*, because they help make relief practically available in time and with less risk of renewed exposure. They also support *victim agency*, and in some contexts speed and durability, by enabling claimants to proceed more safely, identify defendants, and preserve the evidentiary basis for continuing control.

Anonymity orders and publication bans are especially important where the process of seeking relief may deepen the harm. The 2012 Supreme Court of Canada case *A.B. v Bragg*

¹⁴³ Eric Turcotte, “Non-Consensual Distribution of Intimate Images: Diverging Approaches to Remedies in the Prairie Provinces” (March 2024) 87:1 Saskatchewan Law Review 51.

¹⁴⁴ Cynthia Khoo, *supra* note 83.

¹⁴⁵ Moira Aikenhead, *supra* note 13.

¹⁴⁶ *Bragg*, *supra* note 4.

¹⁴⁷ Cynthia Khoo, *supra* note 83.

*Communications Inc.*¹⁴⁸ shows that courts may protect a claimant's identity where public exposure would deter them from proceeding and would compound the injury at issue. Later decisions confirm that initials and publication restrictions can serve the same function where online dissemination and reputational harm threaten to reproduce the damage through litigation itself.¹⁴⁹ Their relevance is therefore practical rather than symbolic. They reduce one of the main barriers to entry and make it more realistic for victims to seek a remedy at all.¹⁵⁰

Disclosure and preservation mechanisms address a different obstacle. In online abuse cases, the victim may know that the harm occurred but still have no way to identify the wrongdoer or preserve the evidence before it disappears. "Norwich orders" are an exceptional form of pre-action or pre-trial disclosure directed to third parties who are not alleged wrongdoers themselves but who hold information needed to identify an otherwise unknown actor, assess whether a viable claim exists, or preserve evidence before it is lost.¹⁵¹ Put simply, their function is to compel third parties holding relevant information to disclose the identity of an otherwise unknown actor.¹⁵² Guidance on preserving digital evidence similarly stresses that screenshots, links, metadata, and contextual records often need to be captured immediately if later proceedings are to be viable.¹⁵³ These tools matter because they help convert anonymous and fast-moving online harm into something legally actionable.

Interim restraints are also relevant where immediate control is necessary. In 2015 *Ontario decision of Lawrence v Bassett*,¹⁵⁴ for example, the court accepted that threatened online exposure of intimate information could justify prompt restraint, recognising that digital dissemination may cause serious non-physical harm and may also destabilise the conditions for fair litigation. This logic is particularly important in a case such as MaskPark, where the central

¹⁴⁸ *Bragg, supra* note 4.

¹⁴⁹ *Ibid.*

¹⁵⁰ *A.T. v V.S.*, 2020 ONSC 4198.

¹⁵¹ Kay Scorer, "The Norwich Order: The Lesser-Known Sibling of the Mareva and Anton Piller" (24 March 2025), online: Commercial Litigation <<https://www.commerciallitigationblog.com/the-norwich-order-the-lesser-known-sibling-of-the-mareva-and-anton-pillar/>>.

¹⁵² Milosevic & Associates, "Norwich Orders and Claims of Defamation Online" (22 October 2025), online: Milosevic & Associates <<https://www.mlflitigation.com/media/norwich-orders-and-claims-of-defamation-online/>>.

¹⁵³ *Ibid.*

¹⁵⁴ *Lawrence v Bassett, supra* note 137.

problem is not only the original intrusion, but the risk of continued circulation before formal adjudication can catch up.

Anti-SLAPP protections and cost rules are less central, but still relevant at the margins. Canadian analysis of anti-SLAPP legislation shows that procedure can itself be used either to protect or to burden participation in matters of public importance. Access to justice literature likewise makes clear that legal rights are shaped by representation, advocacy support, and the practical costs of entering the system.¹⁵⁵ In that sense, procedural design matters not only for efficiency, but for whether privacy harms can realistically be brought before courts at all.

Taken together, these mechanisms are relevant because they demonstrate ways to strengthen *accessibility*, support *victim agency*, and improve the practical *durability* of relief. They also help secure meaningful access to remedy in a way that is consistent with broader concerns about privacy, equality, and effective protection, without requiring a separate human rights framework. For the purposes of this paper, their value lies in showing how formal rights can be made more usable in practice, which is precisely one of the weaknesses exposed by MaskPark.

Additionally, their relevance is not only private or procedural. By reducing the practical barriers that often prevent online abuse from ever reaching a legal forum, they also serve a limited but important public function: they make it more likely that serious privacy harms can be identified, documented, and acted upon rather than disappearing into anonymity, delay, or repeated circulation. That point also helps explain why the next issue is not only what remedies exist on paper, but what kinds of legal and institutional architecture make those remedies realistically accessible in practice.

3.5 Access to justice architecture

Access to justice is best understood here as a question of whether legal rights can be made real through a process that is fair, reachable, and practically usable, rather than merely available in principle.¹⁵⁶ Read in this way, it is not separate from the remedies discussed above,

¹⁵⁵ Hilary Young, “Canadian Anti-SLAPP Laws in Action” (January 2022) 100:2 Canadian Bar Review 186.

¹⁵⁶ Brandi Chartier, Access to Justice: Legal Aid and Other Forms of Advocacy, MHR thesis, University of Manitoba, 28 March 2021.

but asks whether those remedies can actually be mobilised by the people they are meant to protect.

In the context of IIA, that question is especially acute. The issue is not simply whether the law recognises a wrong, but whether a person facing fast-moving and often anonymous digital harm can obtain timely advice, preserve evidence, understand available routes, and move between legal, technical, and support systems without being overwhelmed.¹⁵⁷ Canadian materials on legal aid, advocacy, and practical guidance make clear that formal entitlement does not by itself produce meaningful relief.¹⁵⁸ What matters is whether the surrounding institutional structure makes remedies usable in practice.

Accessibility in this context includes usability. Image-based abuse often unfolds faster than victims can assess what has happened, so affected persons must be able to identify, understand, and act on remedies in time.¹⁵⁹ Canadian materials suggest that support may come through overlapping routes, including legal aid, advocacy pathways, clinic-style assistance, guidance on digital evidence preservation, and trauma-informed support that helps victims move between reporting, platform contact, and potential litigation.¹⁶⁰ For adult IIA, Canadian law does not appear to rely on a broad mandatory reporting model;¹⁶¹ the more relevant issue is whether reporting, application, takedown, and support pathways are clear and usable in practice. Access, trust, and *accountability* reinforce one another: a system that complainants cannot enter will struggle to produce meaningful *accountability*.

The same is true of trauma-informed practice. Canadian work on image-based abuse, particularly in intimate relationships, shows that victims may be dealing not only with exposure, but also with coercion, shame, fear, and ongoing control.¹⁶² A system that assumes confident,

¹⁵⁷ Nicolas Suzor, Molly Dragiewicz, Bridget Harris, Rosalie Gillett, Jean Burgess & Tess Van Geelen, “Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online” (March 2019) 11:1 Policy and Internet 84.

¹⁵⁸ Technology Safety Canada, “Legal Remedies for Image-Based Abuse”, online: Tech Safety <<https://techsafety.ca/resources/toolkits/legal-remedies-for-image-based-abuse>>.

¹⁵⁹ Eric Turcotte, *supra* note 143.

¹⁶⁰ Rebecca Umbach, *supra* note 9.

¹⁶¹ Canada has a statutory reporting regime for Internet child sexual abuse and exploitation material, but not a comparable general regime for adult IIA. See *An Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service*, SC 2011, c 4, ss 2, 3, online: Justice Laws Website <<https://laws-lois.justice.gc.ca/eng/acts/I-20.7/FullText.html>>.

¹⁶² Moira Aikenhead, *supra* note 13.

informed, and well-resourced claimants will exclude many of those most affected. Trauma-informed and coordinated support matters because it shapes whether victims can seek help, remain engaged, and exercise meaningful agency in choosing among available remedies.¹⁶³

This is also the point at which privacy, equality, and effective remedy concerns come into focus most concretely. When access depends on time, literacy, emotional capacity, and institutional support, remedies are not equally available to all victims. In that sense, access to justice is not separate from the substance of the harm. It forms part of whether privacy is treated seriously, whether gendered burdens are reproduced, and whether relief is meaningful in practice.¹⁶⁴ For the purposes of this paper, that insight is especially important because MaskPark exposed not only gaps in formal law, but also the absence of realistic pathways through which victims could turn recognised rights into usable protection.

Access to justice therefore also carries public significance in this field. When timely guidance, evidence preservation, and workable routes to relief are missing, the law does not merely fail isolated claimants. It leaves a form of sexualized abuse to circulate with wider consequences for safety, participation, and institutional credibility in digital and public life.

3.6 Compact case study cluster

A small group of Canadian cases makes the preceding discussion more concrete. Rather than providing a full map of Canadian law on IIA, privacy, or cyber abuse, these cases have been selected to illustrate how criminal, civil, and procedural tools might address weaknesses exposed by MaskPark. Together, they show potential responses to the six criteria developed in Part 2, while also revealing persistent gaps.

The 2019 SCC decision *R v Jarvis* concerned a teacher who secretly recorded female students at school using a pen camera.¹⁶⁵ The Supreme Court held that the students had a reasonable expectation of privacy in those circumstances and entered a conviction for voyeurism.¹⁶⁶ The case is important because it confirms that covert recording may be legally wrongful at the point of capture, even outside traditionally private spaces, when the surrounding

¹⁶³ *Ibid.*

¹⁶⁴ Cynthia Khoo, *supra* note 83.

¹⁶⁵ *R v Jarvis*, *supra* note 116.

¹⁶⁶ *Ibid.*

context, including relationship, purpose, and power, gives rise to a reasonable expectation of privacy. The Supreme Court treated reasonable expectation of privacy as a contextual question shaped by setting, relationship, purpose, and power, even within a school environment that was not wholly private in the ordinary sense. This helps the understanding of when secret filming becomes legally cognisable harm. In comparative terms, *Jarvis* is most useful for *accountability* and *prevention*. It shows how law can recognise the wrong at the point of capture rather than waiting until later circulation.¹⁶⁷

The 2012 SCC decision *A.B. v Bragg Communications Inc.*¹⁶⁸ concerned a 15-year-old girl who sought disclosure of the identity behind a fake Facebook profile that used her image and made sexualized comments. The Supreme Court allowed her to proceed anonymously in pursuing that order. Its significance lies in the recognition that procedural protection may be necessary to make access to justice real, especially when identifying a victim would deepen the harm, deter her from proceeding, and undermine the victim-centred use of legal process.¹⁶⁹ *Bragg* illustrates how victim protection can be built into process itself, and why *accessibility* can include shielding claimants from the exposure that litigation might otherwise reproduce.¹⁷⁰ It therefore speaks most directly to *accessibility*, *victim agency*, and harm *prevention*.

The 2012 Ontario Court of Appeal decision *Jones v Tsige*¹⁷¹ arose after a bank employee repeatedly accessed another woman's personal banking records, without authorization, over a period of several years. The Court of Appeal recognized intrusion upon seclusion as a distinct common law tort and awarded modest damages for the deliberate invasion of the plaintiff's private affairs.¹⁷² That recognition gave Canadian courts a clearer private-law route for addressing privacy invasion even where criminal law was not invoked and economic loss was

¹⁶⁷ "Privacy Rights vs Technological Advances: A Case Comment on *R v Jarvis* and What It Means for the Future of Privacy", online: Saskatchewan Law Review (Law Society of Saskatchewan) <<https://www.lawsociety.sk.ca/saskatchewan-law-review-articles/privacy-rights-vs-technological-advances-a-case-comment-on-r-v-jarvis-and-what-it-means-for-the-future-of-privacy/>>.

¹⁶⁸ *Bragg*, *supra* note 4.

¹⁶⁹ *Bragg*, *supra* note 4 at paras 9, 10 and 14.

¹⁷⁰ "Bullying and Balancing Rights in *A.B. v Bragg Communications*" (16 November 2012), online: IP Osgoode (Osgoode Hall Law School) <<https://www.yorku.ca/osgoode/iposgoode/2012/11/16/bullying-and-balancing-rights-in-ab-v-bragg-communications/>>.

¹⁷¹ *Jones v Tsige*, *supra* note 142.

¹⁷² *Ibid* at paras 12-13.

not the central issue.¹⁷³ *Jones* shows that privacy harm can be recognised as a legal injury in its own right, without depending on criminal liability. It therefore helps explain why civil avenues may be especially important where victims need acknowledgement, control, and a more direct route to remedies than the criminal process is able to provide.

The Ontario Superior Court decision in *Yenovkian v Gulian* (2019)¹⁷⁴ arose out of a prolonged pattern of cyber abuse in a family law dispute, including repeated online harassment of the mother, the posting of images and videos of the children, and ongoing breaches of court orders prohibiting such conduct. The Ontario Superior Court decision in *Doe 464533 v N.D.* (2016)¹⁷⁵ involved a young woman whose former boyfriend posted an intimate video she had sent him on a pornography website without her knowledge or consent. These decisions are especially useful on the remedial side. The first illustrates that courts can respond to sustained cyber abuse with substantial damages and carefully tailored orders, while the second is widely treated as an important example of recognizing non-consensual distribution as actionable and of supporting rapid injunctive logic. Their comparative value lies less in doctrinal novelty than in what they show about remedial design.¹⁷⁶ They point toward flexibility, immediate control, and continuing protection across a range of related activity, including non-consensual distribution, repeated circulation, and associated forms of cyber abuse. That breadth matters because intimate image harm often does not end with first publication. In the terms used throughout this chapter, these two cases are especially instructive on *speed*, *durability*, and *victim agency*.

Taken together, Part 3 yields a somewhat narrow but nonetheless coherent comparative lesson for purposes of unpacking MaskPark. The criminal materials show that law can identify covert recording and non-consensual circulation as serious public wrongs while also revealing the limits of criminal law as a remedial framework. The provincial legislation points to more tailored and control-oriented responses, though with important differences in urgency, available orders, support structures, and the scope of activity captured. The disclosure, preservation, and access to justice materials add a further point: rights matter only if they can be identified,

¹⁷³ Stephen Aylward, “The Idea of Privacy Law: *Jones v Tsige* and the Limits of the Common Law” (2013) 71:1 University of Toronto Faculty of Law Review 61.

¹⁷⁴ *Yenovkian v Gulian*, 2019 ONSC 7279.

¹⁷⁵ *Jane Doe 464533 v N.D.*, *supra* note 142.

¹⁷⁶ Evan Rankin, “Assessing Damages for the Public Disclosure of Private Facts: The Case of *Jane Doe 464533 v N.D.*” (2017) 42:2 Queen’s Law Journal 135.

invoked, and used in time. The cases show how these different strands can be translated into victim-centred relief through injunctions, anonymity protections, damages, and other tailored orders, and how the relevant conduct can be contextualised as part of a broader pattern of privacy invasion, exposure, and continuing vulnerability. Read together, these materials clarify that the Canadian response is most useful not as a complete model, but as a set of mechanisms that respond to different aspects of the structural weaknesses exposed by MaskPark, especially delay, fragmented control, and the difficulty of turning formal rights into practical protection. The next section develops this point more directly by evaluating those mechanisms through the criteria set out in Part 2.

4. Comparative Evaluation, Reform Directions, and Limits

4.1 Revisiting MaskPark through Canadian Legal Mechanisms

This section does not revisit the six criteria (*speed*, *accessibility*, *durability*, *victim agency*, *prevention*, and *accountability*) as wholly separate headings. Instead, it reorganises the comparative analysis around the stages at which different Canadian legal mechanisms become most significant once IIA is already in motion: early-phase control and preservation; mid-phase access and procedural protection; later-phase adjudication and continuing enforcement; and broader systemic considerations that cut across those stages. The six criteria remain the evaluative lens throughout, but are applied through the practical sequence in which harm unfolds and legal response becomes possible.

a) Early-phase response: rapid control, interim relief, and preservation

This is the point at which legal intervention can limit further spread. MaskPark exposed a central weakness of *speed*: harm continued to spread, adapt, and intensify faster than legal and institutional responses could intervene.¹⁷⁷ In a case of this kind, slow response time is not a neutral feature of process - it is part of the harm itself, because each period of inaction increases the likelihood of copying, reposting, and wider exposure.

¹⁷⁷ Li Youzhen, *supra* note 40.

The most relevant Canadian mechanisms are those capable of acting at the early stage of dissemination. Interlocutory relief (e.g. injunctions) matters because it can achieve immediate restraint. Early preservation measures matter because digital evidence can disappear before a claimant is ready to proceed.¹⁷⁸ Rapid civil control over circulation is important for the same reason: once intimate material begins to move across platforms, a remedy that arrives only after final adjudication may recognise the wrong but fail to limit its spread. Practical guidance on preserving digital evidence and Canadian commentary on takedown-oriented remedies both reinforce the same point, namely that early action often determines whether later legal relief remains meaningful.¹⁷⁹

This is where the distinction between punishment and control becomes especially important. Criminal law may denounce and deter, but it usually operates after the fact. The more urgent question in a MaskPark-type case is which legal tools can interrupt ongoing dissemination before it becomes unmanageable. Current Chinese personality rights law may support civil claims, but it does not clearly provide the expedited takedown, preservation, identification, and coordinated enforcement tools needed for networked dissemination. On that issue, civil and procedural mechanisms have a comparative advantage, even if they remain imperfect. They do not guarantee complete removal, and Canadian experience also shows the limits of site-by-site takedown once content has spread. Even so, they respond more directly to the temporality of the harm.¹⁸⁰ The South Korean contrast briefly reinforces this point: the legacy of the Nth Room scandal shows that investigative tempo and coordinated early response are themselves part of legal effectiveness.¹⁸¹

b) Mid-phase response: access, anonymity, and victim-centred navigation

Once some form of early control becomes possible, the next question is whether the available remedies can in fact be used by those harmed. The Canadian materials discussed in Part 3 show that legal routes to relief are meaningful only where victims can enter the process without incurring new forms of exposure, can understand the available options, and can remain engaged long enough to obtain an outcome. *Accessibility* therefore depends not only on the formal

¹⁷⁸ Technology Safety Canada, *supra* note 137.

¹⁷⁹ Rebecca Katz, *supra* note 16.

¹⁸⁰ *Ibid.*

¹⁸¹ Kim Joohee & Jamie Chang, *supra* note 101.

availability of a cause of action or other legal redress, but also on anonymity protections, publication controls, practical guidance, advocacy support, and manageable procedural burden.

Anonymity protections and publication bans are especially important because image-based abuse creates a distinctive procedural risk: the act of seeking relief may intensify the very harm the claimant is trying to stop. The Canadian cases¹⁸² show that identity protection can be necessary to make access real rather than theoretical. This matters directly to *victim agency*. A complainant who must choose between abandoning the claim and becoming more publicly exposed does not meaningfully control the process. By contrast, where anonymity is available, victims are in a stronger position to decide whether, when, and how to proceed.

Access also depends on whether the system is navigable. Practical toolkits and advocacy-oriented resources make clear that victims often need early guidance on preserving evidence, choosing between civil and criminal routes, and understanding what each form of relief can realistically achieve.¹⁸³ Legal aid, clinic-style support, and other advocacy pathways matter for the same reason. They reduce the gap between rights on paper and rights in use. Without that support, complexity, cost, and uncertainty can turn formally available remedies into inaccessible ones.¹⁸⁴

Affordability and emotional burden are equally significant. Canadian work on IIA, especially in coercive relational settings, shows that victims may face stigma, fear, confusion, and continuing pressure from those who harmed them.¹⁸⁵ A system built on the assumption that claimants are well informed, emotionally detached, and financially able to pursue litigation will predictably fail many of those most affected. This is why trauma-informed practice belongs within the analysis of access rather than outside it. It shapes who can remain in process, who can instruct counsel, and who can make meaningful decisions about timing and remedy.¹⁸⁶

This is also where privacy, equality, and effective remedy concerns come into view most concretely. If remedies are unevenly usable because of cost, complexity, stigma, or exposure,

¹⁸² Bragg, *supra* note 4; *A.T. v V.S.*, *supra* note 150.

¹⁸³ Technology Safety Canada, *supra* note 137.

¹⁸⁴ Brandi Chartier, *supra* note 156.

¹⁸⁵ Moira Aikenhead, *supra* note 13.

¹⁸⁶ Canada, Public Health Agency of Canada, “Trauma and Violence-Informed Approaches to Policy and Practice” (2018), online: Government of Canada <<https://www.canada.ca/en/public-health/services/publications/health-risks-safety/trauma-violence-informed-approaches-policy-practice.html>>.

then privacy is not fully protected in practice, equality burdens are reproduced, and effective remedy remains incomplete.¹⁸⁷ For present purposes, that insight matters because although Chinese personality rights law may recognise the underlying privacy harm, MaskPark exposed the need for clearer pathways to practical assistance, evidence preservation, timely removal, and usable protection.

c) Later-phase response: adjudication, durable control, and continuing enforcement

Durability should be treated as distinct from *speed*. A response may arrive quickly and still fail to hold over time. That distinction is central here because the harm exposed by MaskPark was cumulative and ongoing, not confined to a single act of publication. Once images began moving through interconnected groups, the injury no longer depended on one uploader or one post. It depended on repetition, storage, transfer, and renewed exposure across time.¹⁸⁸ The relevant question is therefore not only whether the law can interrupt circulation, but whether it can preserve control after dissemination has already begun.

Some of the strongest Canadian responses are significant precisely because they are framed in continuing rather than purely retrospective terms. Injunctions, takedown-oriented orders, and comparable statutory remedies matter because they are capable of imposing obligations that persist beyond the first judicial finding of wrongdoing.¹⁸⁹ The most useful examples are those in which courts or statutes aim not merely to recognise a past violation, but to restrain further sharing, maintain limits on access, and support continuing compliance over time.¹⁹⁰ In that sense, these mechanisms are more responsive to *durability* than remedies that focus mainly on punishment or compensation after the fact.

At the same time, the Canadian materials also show that durable control remains difficult in digital environments. Removing content from one location does not guarantee that it has disappeared in any meaningful sense. Reposting, mirroring, cross-platform transfer, and private storage all weaken the effect of site-by-site removal.¹⁹¹ A legal order may therefore produce

¹⁸⁷ Eric Turcotte, *supra* note 143.

¹⁸⁸ Zheng Ning, “China’s ‘N Room’: Overseas Groups with Over 100,000 Members Spread Voyeuristic and AI-Generated Images, Victims Recount Their Experiences” (27 July 2025), online: HK01 <<https://gqr.sh/n7Fm>>.

¹⁸⁹ *Intimate Images and Cyber-protection Act*, *supra* note 134.

¹⁹⁰ Evan Rankin, *supra* note 176.

¹⁹¹ Richard Jochelson, *supra* note 114.

interruption without producing lasting control. This is why the *durability* inquiry cannot stop at the availability of injunctions or takedown mechanisms in the abstract. It must also ask whether compliance can be monitored, whether renewed circulation can be traced, and whether later enforcement remains possible once content begins to fragment across different channels.

Preservation logic remains important for the same reason. Durable control depends not only on what a court is willing to order, but also on whether the records needed to support later enforcement have been secured early enough. If links, screenshots, metadata, and contextual evidence are not preserved at the outset, later efforts to prove reposting, identify breaches, or seek renewed relief become substantially weaker.¹⁹² Preservation, in that sense, is not only an early procedural step. It is part of what makes continuing protection possible.

For present purposes, then, the remedies with the greatest comparative value are those capable of producing more than temporary interruption. Current Chinese personality rights law may recognise the underlying violation, but MaskPark shows the need for continuing takedown, preservation, and enforcement mechanisms where content is reposted or redistributed. Where harm is structurally repetitive, control must also persist across time. Otherwise, the law may intervene, but it does not truly contain the injury.

d) Systemic and cross-cutting considerations: prevention, accountability, and public confidence

But even durable control remains incomplete if it is not connected to a wider structure of *prevention and accountability*. *Prevention* and *accountability* are best read together because both ask whether legal response can do more than arrive after the harm is already entrenched. In the MaskPark context, the central weakness was not simply that intimate image abuse occurred, but that public discussion was rapidly managed while no comparably visible, broad, and coordinated structure of investigation and enforcement appeared to follow. Where circulation continues, reporting pathways remain unclear or victim-dependent, and institutional response remains difficult to see, legal recognition on paper does little to build either deterrence or trust in practice.¹⁹³

¹⁹² Technology Safety Canada, *supra* note 137.

¹⁹³ Ling Li, *supra* note 22.

At the level of individual liability, criminal law still matters, including because it reflects a public interest in denunciation and *accountability*. It can identify covert recording and non-consensual distribution as public wrongs rather than private embarrassment, and it can communicate a denunciatory signal to identifiable perpetrators.¹⁹⁴ That function is important, but it is limited. Criminal law is strongest when a defendant can be charged and punished after the fact. It is weaker where abuse is diffuse, repeated, digitally networked, or sustained by multiple actors. In those conditions, punishment may acknowledge wrongdoing without significantly reducing the likelihood of recurrence.¹⁹⁵

This is why *accountability* cannot stop with the individual offender. *Prevention* also depends on whether platforms cooperate, whether institutions respond in a coordinated way, and whether enforcement is visible enough to signal that the system is actually functioning. These features also reveal the public interest dimensions of intimate image abuse: the issue is not only whether one victim can obtain relief against one perpetrator, but whether the wider system can reduce repetition, clarify institutional responsibility, and maintain public trust in legal protection. Current reform discussions in Canada move in that direction by linking user protection to platform duties, transparency, and institutional oversight, while policy commentary continues to stress that existing protections remain incomplete and uneven. A system that punishes some perpetrators but leaves platform responsibility opaque will struggle to generate either structural deterrence or sustained public confidence.¹⁹⁶ Current Chinese personality rights law may recognise the underlying privacy and personality rights violation, but MaskPark shows the need for reform that more clearly links those rights to platform cooperation, evidence preservation, takedown duties, and coordinated enforcement.

The wider lesson, then, is that *prevention* requires *accountability* that is distributed across more than one institutional site. Responses that are fragmented, private, or largely symbolic may recognise harm without making recurrence less likely. What carries the greatest preventive value

¹⁹⁴ *Criminal Code*, *supra* note 2, ss 162, 162.1.

¹⁹⁵ Moira Aikenhead, *supra* note 13.

¹⁹⁶ Canada, Department of Justice, “Charter Statement – Bill C-63: An Act to Enact the *Online Harms Act*, to Amend the *Criminal Code*, the Canadian Human Rights Act and Related Acts” (4 June 2024), online: <<https://www.justice.gc.ca/eng/csj-sjc/pl/charte-charte/c63.html>>; Michelle Abel, “Canada Lags Behind US in Protecting Victims of ‘Deepfakes’ and Other Image-Based Abuse” (27 August 2025), online: Inside Policy <<https://macdonaldlaurier.ca/canada-lags-behind-us-in-protecting-victims-of-deepfakes-and-other-image-based-abuse-michelle-abel-for-inside-policy/>>.

is a structure in which perpetrators can be identified, platforms are pressed to cooperate,¹⁹⁷ institutions are seen to act, and enforcement is visible enough to reassure victims and deter repetition. That is the point at which *accountability* begins to do preventive work rather than merely expressive work.

4.2 Reform directions: a tiered model

a) Tier 1: rapid civil control

The first tier should prioritise rapid civil control as the initial response to image-based harm. The immediate objective is not final liability, but stabilisation. A useful first layer is one that can be activated before full adjudication and is directed to interruption rather than retrospective judgment. A clear and auditable notice-and-action process, immediate evidence preservation from the outset, and a fast-track route to interlocutory relief would address the period in which harm expands faster than ordinary litigation can move.¹⁹⁸ Early judicial authority to order takedown, blocking, or restraint of further circulation is especially important because later remedies may recognise the wrong while failing to control its spread.¹⁹⁹ This tier responds most directly to *speed*, *durability*, and *victim agency*, because it creates a practical route to seek control at the point when control still matters most.

b) Tier 2: coordinated investigation and platform response

A second tier is necessary because private action alone cannot manage large-scale, networked abuse, fragmented across institutions, platforms, and enforcement bodies.²⁰⁰ A more effective structure would define clear triggers for digital forensic action, require preservation and retention of relevant data, and establish more consistent obligations on platforms to cooperate once serious image-based abuse is identified. It should also create more structured pathways for identifying anonymous actors and for linking investigative bodies with platform-facing response mechanisms, so that evidence, account information, and removal efforts do not remain scattered

¹⁹⁷ Associated Press, “Telegram CEO Pavel Durov Arrested in France over Alleged Criminal Activity on the Platform” (25 August 2024), online: Associated Press <<https://apnews.com/article/france-telegram-pavel-durov-arrest-6e213d227458f330ed16e7fe221a696c>>.

¹⁹⁸ Dou Naimai, “MaskPark ‘Tree Hole’: An Overview of China’s ‘N Room’ Scandal Involving the Public Disclosure of Intimate Images and up to 900,000 Victims” (29 July 2025), online: HK01 <<https://gqr.sh/xu9h>>.

¹⁹⁹ Rebecca Katz, *supra* note 16.

²⁰⁰ Ling Li, *supra* note 22.

across separate systems.²⁰¹ This tier speaks most clearly to *prevention* and *accountability*, while also reinforcing *speed*. Its function is to reduce the gap between private complaint and public enforcement, and to make response visible enough to support deterrence and trust.

c) Tier 3: access architecture and public accountability

A third tier should address the fact that rights remain weak if victims cannot realistically mobilise them. Even the strongest remedy is of limited value if ordinary complainants cannot understand it, afford it, or remain in process long enough to use it. This tier should therefore strengthen clinic and advocacy pathways, provide limited public funding for technical or expert assistance where digital evidence or tracing is required, and embed trauma-informed support within the response structure. It should also integrate legal, practical, and platform-facing assistance more clearly, so that victims are not forced to navigate evidence preservation, reporting, and legal strategy as separate and confusing tasks.²⁰² Transparent public reporting on enforcement and outcomes belongs to the same architecture. This tier responds most directly to *accessibility*, *victim agency*, and *accountability*, while also giving practical force to privacy, equality, and effective remedy concerns.

These three tiers are not offered as a complete legislative blueprint. They are better understood as structured reform directions drawn from the weaknesses identified through MaskPark and from the selective comparative material examined earlier. The aim is functional learning: how to build faster control, stronger coordination, and more usable access in a setting where rights may already exist in principle but remain too slow, too fragmented, or too difficult to activate in practice.

4.3 Limits, transfer cautions, and future research

Several limits should remain in view. The available record is incomplete, and much of the accessible material comes from journalism, advocacy writing, and publicly circulating accounts rather than from full official files or disclosed investigative records. Underreporting is also likely. Even so, that limitation does not remove MaskPark’s analytical value. Its significance lies in the

²⁰¹ Women’s Legal Education and Action Fund (LEAF), “Unacceptable: Responding to Technology-Facilitated Gender-Based Violence” (2021), online: <<https://www.leaf.ca/factsheet/unacceptable-responding-to-technology-facilitated-gender-based-violence/>>.

²⁰² Technology Safety Canada, *supra* note 158.

fact that it provides a documented example of how large-scale, networked intimate image abuse can expose the distance between formally recognised rights and practical response.

A second caution concerns removal itself. Faster takedown procedures and stronger platform response may improve control, but they may also create risks of over-removal, especially where low-threshold or automated systems are relied upon. A further limit concerns knowledge or model transfer. The comparative material examined here is used selectively rather than as a transplant model, and the institutional setting, legal culture, platform environment, and implementation structure differ in important ways.²⁰³ The argument of this paper is therefore functional and comparative, not based on any assumption that one jurisdiction's legal framework can simply be reproduced in another.

A final point concerns emerging authenticity and provenance tools. Watermarking, metadata-based provenance systems, and related verification mechanisms may become increasingly relevant to the regulation of synthetic and manipulated images. At the same time, these technologies remain unsettled in both technical and institutional terms, particularly with respect to robustness, interoperability, standardisation, and resistance to tampering.²⁰⁴ For that reason, they are better treated here as an important direction for future research than as settled solutions. Despite these limits, the comparative exercise remains useful because it clarifies which kinds of legal and institutional responses are most likely to matter in large-scale, networked intimate image abuse cases such as MaskPark.

5. Conclusion

This paper began with a focused question: when large-scale intimate image abuse is already in motion, what kinds of legal responses are capable not only of recognising the wrong, but of limiting its spread, supporting victims, and restoring public confidence in the legal system? MaskPark shows that the central problem is not simply the presence of harmful content,

²⁰³ Eric Turcotte, *supra* note 143.

²⁰⁴ Ayushi Singh, *The Two Faced Lie: Regulation of Generative AI and Watermarking*, working paper, O P Jindal Global University, Jindal Global Law School, 23 February 2024 (posted 18 July 2025), online: SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5347736>.

nor even the formal inadequacy of any single legal rule. It is the failure to translate recognised rights into timely, coordinated, and usable protection once networked abuse begins to expand.

The comparative contribution of this paper lies in its selective method. Rather than treating Canadian law as a complete, transferable model, the analysis isolates a set of legal and procedural responses that illuminate and respond to the particular weaknesses exposed by MaskPark. Read through the six criteria of *speed*, *accessibility*, *durability*, *victim agency*, *prevention*, and *accountability*, the comparison clarifies that the most useful lessons do not come from any single doctrine. They emerge from the combined operation of rapid civil control, procedural protection, coordinated investigation, and practical access pathways.

The central functional insight is therefore straightforward. In cases of large-scale, digitally networked intimate image abuse, the most effective legal response is not the one that punishes most severely after the fact. It is the one that can act early, hold control over time, distribute responsibility across perpetrators, platforms, and institutions, and remain realistically usable to those harmed. That is the lesson MaskPark makes urgent, and it is the lesson that should shape future reform.

BIBLIOGRAPHY

LEGISLATION: CANADA

Act to Counter Non-Consensual Sharing of Intimate Images, CQLR c P-9.0002, online: CanLII <<https://www.canlii.org/en/qc/laws/stat/cqlr-c-p-9.0002/latest/cqlr-c-p-9.0002.html>>.

An Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service, SC 2011, c 4, online: Justice Laws Website <<https://laws-lois.justice.gc.ca/eng/acts/I-20.7/FullText.html>>.

Bill 2, *The Intimate Image Protection Amendment Act*, 3rd Sess, 43rd Leg, Manitoba, 2025, online: <<https://web2.gov.mb.ca/bills/43-3/b002e.php#exNote>>.

Criminal Code, RSC 1985, c C-46.

Intimate Image Protection Act, SM 2015, c 42, CCSM c I87, online: CanLII <<https://www.canlii.org/en/mb/laws/astat/sm-2015-c-42/latest/sm-2015-c-42.html>>.

Intimate Images and Cyber-protection Act, SNS 2017, c 7, online: CanLII <<https://www.canlii.org/en/ns/laws/stat/sns-2017-c-7/latest/sns-2017-c-7.html>>.

Intimate Images Protection Act, RSNL 2018, c I-22, online: CanLII <<https://www.canlii.org/en/nl/laws/stat/rsnl-2018-c-i-22/latest/rsnl-2018-c-i-22.html>>.

Intimate Images Protection Act, SBC 2023, c 11, online: CanLII <<https://www.canlii.org/en/bc/laws/stat/sbc-2023-c-11/latest/sbc-2023-c-11.html>>.

Intimate Images Protection Act, SPEI 2020, c 55, online: CanLII <<https://www.canlii.org/en/pe/laws/astat/spei-2020-c-55/210231/spei-2020-c-55.html>>.

Intimate Images Unlawful Distribution Act, SNB 2022, c 1, online: CanLII <<https://www.canlii.org/en/nb/laws/stat/snb-2022-c1/latest/snb-2022-c1.html>>.

The Non-Consensual Distribution of Intimate Images Act, CCSM c N93, online: CanLII <<https://www.canlii.org/en/mb/laws/stat/ccsm-c-n93/latest/ccsm-c-n93.html>>.

The Privacy Act, RSS 1978, c P-24, online: CanLII <<https://www.canlii.org/en/sk/laws/stat/rss-1978-c-p-24/latest/rss-1978-c-p-24.html>>.

The Privacy Amendment Act, 2018, SS 2018, c 28, online: CanLII <<https://www.canlii.org/en/sk/laws/astat/ss-2018-c-28/latest/ss-2018-c-28.html>>.

Protecting Victims of Non-consensual Distribution of Intimate Images Act, SA 2017, c P-26.9, online: CanLII <<https://www.canlii.org/en/ab/laws/stat/sa-2017-c-p-26.9/latest/sa-2017-c-p-26.9.html>>.

LEGISLATION: PEOPLE'S REPUBLIC OF CHINA

Civil Code of the People's Republic of China, Order No 45 of the President of the People's Republic of China, 28 May 2020, effective 1 January 2021, CLI.1.342411(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/aa00daaeb5a4fe4ebdfb.html>.

Civil Procedure Law of the People's Republic of China (2023 Amendment), 1 September 2023, effective 1 January 2024, CLI.1.5175519(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/55ada7bc4fc9d8ccbdffb.html>.

Criminal Law of the People's Republic of China (2023 Amendment PKULAW Version), 29 December 2023, effective 1 March 2024, CLI.1.5185739(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/3b70bb09d2971662bdffb.html>.

Law of the People's Republic of China on Public Security Administration Punishments (2025 Revision), Order No 49 of the President of the People's Republic of China, 27 June 2025, effective 1 January 2026, CLI.1.5299183(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/4a0675f698316d0fbdfb.html>.

Provisions on the Administration of Cyber Audio and Video Information Services, Guoxinban Tongzi [2019] No 3, 18 November 2019, effective 1 January 2020, online: <<https://gqr.sh/LvaL>>.

Regulation on the Administration of Public Security Video Image Information Systems, Order No 799 of the State Council of the People's Republic of China, 13 January 2025, effective 1 April 2025, CLI.2.5291008(EN), online: PKUlaw <https://www.pkulaw.com/en_chl/2e489e43d96ae400bdffb.html>.

JURISPRUDENCE: CANADA

A.B. (Litigation Guardian of) v Bragg Communications Inc, 2012 SCC 46, [2012] 2 SCR 567.

A.T. v V.S., 2020 ONSC 4198.

Jane Doe 464533 v N.D., 2016 ONSC 541.

Jane Doe 72511 v Morgan, 2018 ONSC 6607, 143 OR (3d) 277.

Jones v Tsige, 2012 ONCA 32, 108 OR (3d) 241.

Lawrence v Bassett, 2015 ONSC 3707.

R v Jarvis, 2019 SCC 10, [2019] 1 SCR 488.

R v NG et al, 2015 MBCA 81.

Yenovkian v Gulian, 2019 ONSC 7279.

SECONDARY MATERIAL: BOOKS AND BOOK CHAPTERS

Aikenhead, Moira, "Image-Based Abuse in Intimate Partnerships in Canada: Lessons from the Criminal Case Law" in Gian Marco Caletti & Kolis Summerer, eds, *Criminalizing Intimate Image Abuse: A Comparative Perspective* (Oxford: Oxford University Press, 2024) 320, online: <<https://doi.org/10.1093/oso/9780198877813.003.0016>>.

Kudo, Shimpei et al, "Voyeuristic Photography (Tosatsu): Liberation in the Claustum" in *Anxiety, Psychoanalysis and Law* (2026) 110.

Okada, Yoshifumi, "Criminalization of Intimate Image Abuse in Japan" in Gian Marco Caletti & Kolis Summerer, eds, *Criminalizing Intimate Image Abuse: A Comparative Perspective* (Oxford: Oxford University Press, 2024) 238.

SECONDARY MATERIAL: ARTICLES

Aikenhead, Moira, "Non-Consensual Disclosure of Intimate Images as a Crime of Gender-Based Violence" (2018) 30:1 *Canadian Journal of Women and the Law* 117.

Aylward, Stephen, "The Idea of Privacy Law: *Jones v Tsige* and the Limits of the Common Law" (2013) 71:1 *University of Toronto Faculty of Law Review* 61.

Bansal, Vaiddehi et al, "A Scoping Review of Technology-Facilitated Gender-Based Violence in Low- and Middle-Income Countries Across Asia" (January 2024) 25:1 *Trauma, Violence, & Abuse* 463.

Dunn, Suzie, "Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI" (2024) 69:4 *McGill Law Journal* 395.

He Ye & Gao Jun, "Stigma and Psychological Recovery among Survivors of Sexual Assault" (2022) 30:3 *Chinese Journal of Clinical Psychology* 693.

Jin Qianqian, "Research on the Legal Regulation of Secret Photography in Private Spaces of Public Places" (November 2023) No 199 *Journal of City University of Macau* 56.

Jochelson, Richard, David Ireland & Hannah Taylor, "Clearing Your History: A Review of Non-Consensual Distribution of Intimate Images in Canada and Future Responses" (September 2021) 54:3 *University of British Columbia Law Review* 763.

Karasavva, V, "The Frequency, Nature, Impact, and Coping Strategies of Nonconsensual Intimate Image Dissemination Victimization: A Scoping Review" (October 2025) *Trauma, Violence, & Abuse* [advance online publication], online: SAGE Journals <<https://journals.sagepub.com/doi/epub/10.1177/15248380251383940>>.

Katz, Rebecca, "Takedowns and Trade-Offs: Can Copyright Law Assist Canadian Victims of Non-Consensual Intimate Image Distribution?" (2020) 29:2 *Education Law Journal* 169.

Kerr, Lisa, "The Legitimate Scope of Criminal Law: A Question for Legal History?" (April 2017) 4:1 *Critical Analysis of Law: An International & Interdisciplinary Law Review* 11.

Kim Joohee & Jamie Chang, "Nth Room Incident in the Age of Popular Feminism: A Big Data Analysis" (2021) 14 *Azalea: Journal of Korean Literature & Culture* 261.

Kleinhans, Martha-Marie & Roderick A Macdonald, "What is a Critical Legal Pluralism?" (1997) 12:2 *Canadian Journal of Law and Society* 25.

Lee, Min Joo, "Sexual Violence and Censorship in Contemporary Korea: Examining the Debate Surrounding the Digital Sexual Violence Prevention Law" (2025) 49:1 *Korean Studies* 14.

Liu Zishuo & Zhu Tonghui, "Criminal Regulation of the Abuse of 'Deepfake' Technology" (2025) 41:9 *Journal of China People's Police University* 58.

- MacKay, A Wayne, “Law as an Ally or Enemy in the War on Cyberbullying: Exploring the Contested Terrain of Privacy and Other Legal Concepts in the Age of Technology and Social Media” (2015) 66 *University of New Brunswick Law Journal* 3.
- Mitchell, Kimberly J et al, “Image-Based Sexual Abuse: Characteristics Linked to Different Reasons Why Youth Decide Not to Disclose” (2025) 26:8 *Prevention Science* 1157.
- Okolie, Chidera, “Artificial Intelligence-Altered Videos, Image-Based Sexual Abuse, and Data Privacy Concerns” (March 2023) 25:2 *Journal of International Women’s Studies*, art 11.
- Pan Jingui & Yang Hongbin, “Technical Black Boxes and Rule Reconstruction: The Dilemma of Examining Deepfake Evidence in Criminal Procedure and Possible Paths Forward” (2025) 4 *Journal of Liaoning Police and Justice Management Cadre Institute* 69.
- Rankin, Evan, “Assessing Damages for the Public Disclosure of Private Facts: The Case of *Jane Doe 464533 v N.D.*” (2017) 42:2 *Queen’s Law Journal* 135.
- Sharma, Ishita, “Technology-Facilitated Gender-Based Violence in the Digital Age: A Comparative Analysis of India and South Korea” (August 2025) 24:2 *Journal of Korean Law* 359.
- Suzor, Nicolas et al, “Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online” (March 2019) 11:1 *Policy and Internet* 84.
- Turcotte, Eric, “Non-Consensual Distribution of Intimate Images: Diverging Approaches to Remedies in the Prairie Provinces” (March 2024) 87:1 *Saskatchewan Law Review* 51.
- Xiao Shanshan & Wang Zerun, “From ‘Direct Contact’ to ‘Non-Direct Contact’: New Forms of Sexual Crimes Fostered by Online Media and Their Legal Regulation” (June 2022) 34:3 *Journal of Hunan Police Academy* 88.
- Young, Hilary, “Canadian Anti-SLAPP Laws in Action” (January 2022) 100:2 *Canadian Bar Review* 186.

SECONDARY MATERIAL: GOVERNMENT AND INSTITUTIONAL MATERIALS

- Canada, Department of Justice, “Bill C-16: An Act to Amend Certain Acts in Relation to Criminal and Correctional Matters (Child Protection, Gender-Based Violence, Delays and Other Measures)” (tabled in the House of Commons, 27 February 2026), online: <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c16_3.html>.
- Canada, Department of Justice, “Charter Statement – Bill C-63: An Act to Enact the Online Harms Act, to Amend the *Criminal Code*, the Canadian Human Rights Act and Related Acts” (4 June 2024), online: <<https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c63.html>>.
- Canada, Department of Justice, “Non-Consensual Distribution of Intimate Images” in *Cyberbullying and the Non-consensual Distribution of Intimate Images*, online: <<https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/p6.html>>.
- Canada, Public Health Agency of Canada, “Trauma and Violence-Informed Approaches to Policy and Practice” (2018), online: Government of Canada <<https://www.canada.ca/en/public->

health/services/publications/health-risks-safety/trauma-violence-informed-approaches-policy-practice.html>.

Khoo, Cynthia, *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence* (Toronto: Women's Legal Education and Action Fund, 2021).

Nova Scotia, Department of Justice, *Report on the Review of the Intimate Images and Cyber-protection Act* (2022), online: <<https://novascotia.ca/intimate-images-and-cyber-protection-act-survey/documents/report-on-the-review-of-the-intimate-images-and-cyber-protection-act.pdf>>.

Technology Safety Canada, "Legal Remedies for Image-Based Abuse", online: Tech Safety <<https://techsafety.ca/resources/toolkits/legal-remedies-for-image-based-abuse>>.

Technology Safety Canada, "Preserving Digital Evidence Example: Sexual Images Shared Online", online: Tech Safety <<https://techsafety.ca/resources/toolkits/preserving-digital-evidence-example-sexual-images-shared-online>>.

UN Women, *Technology-Facilitated Gender-Based Violence: Developing a Shared Research Agenda* (September 2024), online: <<https://www.unwomen.org/en/digital-library/publications/2024/09/technology-facilitated-gender-based-violence-developing-a-shared-research-agenda>>.

Women's Legal Education and Action Fund (LEAF), "Unacceptable: Responding to Technology-Facilitated Gender-Based Violence" (2021), online: <<https://www.leaf.ca/factsheet/unacceptable-responding-to-technology-facilitated-gender-based-violence/>>.

SECONDARY MATERIAL: THESES, DISSERTATIONS, WORKING PAPERS AND CONFERENCE PROCEEDINGS

Chartier, Brandi, *Access to Justice: Legal Aid and Other Forms of Advocacy*, MHR thesis, University of Manitoba, 28 March 2021.

Hu Junyan, *A Study on Criminal Regulation of Secret Photography*, master's thesis, Southwest University of Political Science and Law, 2023.

Li Jingying, *Research on the Criminal Regulation of Secret Filming in Private Spaces*, master's thesis, Yunnan University of Finance and Economics, 13 May 2024.

Liu Ting, *A Comparative Study of Online Public Opinion on University Sexual Harassment Cases from a Feminist Perspective*, master's thesis, Harbin Institute of Technology, 2019.

Singh, Ayushi, *The Two Faced Lie: Regulation of Generative AI and Watermarking*, working paper, O P Jindal Global University, Jindal Global Law School, 23 February 2024 (posted 18 July 2025), online: SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5347736>.

Thomassen, Kristen, *Private Law & Public Space: The Canadian Privacy Torts in an Era of Personal Remote-Surveillance Technology*, doctoral thesis, University of Ottawa, 29 June 2022.

Umbach, Rebecca et al, “Prevalence and Impacts of Image-Based Sexual Abuse Victimization: A Multinational Study” (March 2025), online: arXiv <<https://doi.org/10.48550/arXiv.2503.04988>>.

Wang Wenqi, *Criminal Regulation of Online Sexual Offenses*, master’s thesis, University of International Business and Economics, 2021.

SECONDARY MATERIAL: NEWS AND ONLINE COMMENTARY

A Mei, “Advocacy on the Maskpark Case: Stop Saying Telegram Cannot Be Investigated, the Real Question Is Whether Authorities Are Willing to Act” (31 July 2025), online: *No More Chained* (Substack) <<https://nomorechained.substack.com/p/maskparktelegram>>.

Abel, Michelle, “Canada Lags Behind US in Protecting Victims of ‘Deepfakes’ and Other Image-Based Abuse” (27 August 2025), online: *Inside Policy* <<https://macdonaldlaurier.ca/canada-lags-behind-us-in-protecting-victims-of-deepfakes-and-other-image-based-abuse-michelle-abel-for-inside-policy/>>.

Associated Press, “Telegram CEO Pavel Durov Arrested in France over Alleged Criminal Activity on the Platform” (25 August 2024), online: *Associated Press* <<https://apnews.com/article/france-telegram-pavel-durov-arrest-6e213d227458f330ed16e7fe221a696c>>.

“Bullying and Balancing Rights in *A.B. v Bragg Communications*” (16 November 2012), online: *IP Osgoode* (Osgoode Hall Law School) <<https://www.yorku.ca/osgoode/iposgoode/2012/11/16/bullying-and-balancing-rights-in-ab-v-bragg-communications/>>.

Chen Zhengjia, “China’s Version of ‘Nth Room’: The ‘MaskPark Tree Hole’ Scandal Has Victimized 900,000 Women” (29 July 2025), online: *Yahoo News* <<https://gqr.sh/92gX>>.

Dou Naimai, “MaskPark ‘Tree Hole’: An Overview of China’s ‘N Room’ Scandal Involving the Public Disclosure of Intimate Images and up to 900,000 Victims” (29 July 2025), online: *HK01* <<https://gqr.sh/xu9h>>.

Hsieh Yi-hsuan, “Chinese Voyeurism Group of Over 100,000 People Suspected of Illegal Activity, Weibo Trending Topic Allegedly Suppressed” (26 July 2025), online: *Central News Agency* <<https://money.udn.com/money/story/5603/8898079>>.

Li Hsuan-hsuan, “China’s Version of the ‘Nth Room’ Erupts: Private Images Allegedly Leaked as the ‘MaskPark Tree Hole’ Group Exposes One Hundred Thousand Members” (20 July 2025), online: *Newtalk News* <<https://gqr.sh/mvNc>>.

Li, Ling, “MaskPark and the Silence around China’s Gender-Based Violence Online” (11 November 2025), online: *Made in China Journal* <<https://madeinchinajournal.com/2025/11/11/maskpark-and-the-silence-around-chinas-gender-based-violence-online/>>.

Li Youzhen, “Fear of Secret Filming as an Everyday Reality: How ‘China’s Nth Room’ Ignited Women’s Anger” (4 August 2025), online: *Deutsche Welle* <<https://gqr.sh/79y7>>.

- Lianhe Zaobao, “MaskPark: More than 100,000 People in China’s ‘Nth Room’ Circulated Hidden-Camera Photos, and No Government Department Has Yet Responded or Taken Action” (31 July 2025), online: *HK01* <<https://www.hk01.com/article/60262198>>.
- Milosevic & Associates, “Norwich Orders and Claims of Defamation Online” (22 October 2025), online: *Milosevic & Associates* <<https://www.mlflitigation.com/media/norwich-orders-and-claims-of-defamation-online/>>.
- noise, “From ‘China’s Version of Room N’ to Seeing How Fragile Our Digital Defenses Are” (9 August 2025), online: *CommonWealth Opinion* <<https://opinion.cw.com.tw/blog/profile/52/article/16441>>.
- Park Eun-jee, “Rushed ‘Nth Room Law’ Unlikely to Actually Stop Criminals” (2 June 2020), online: *Korea JoongAng Daily* <<https://koreajoongangdaily.joins.com/2020/06/02/business/indepth/Nth-room-digital-crime-Naver/20200602195600193.html>>.
- “Privacy Rights vs Technological Advances: A Case Comment on *R v Jarvis* and What It Means for the Future of Privacy”, online: *Saskatchewan Law Review (Law Society of Saskatchewan)* <<https://www.lawsociety.sk.ca/saskatchewan-law-review-articles/privacy-rights-vs-technological-advances-a-case-comment-on-r-v-jarvis-and-what-it-means-for-the-future-of-privacy/>>.
- Rojas Hruška, Gabriel, “Updating Canadian Law to Address Online Hate and Gender-Based Violence” (2 December 2025), online: *Canadian Centre for Policy Alternatives* <<https://www.policyalternatives.ca/news-research/updating-canadian-law-to-address-online-hate-and-gender-based-violence/>>.
- Samra, Jasmine & Christopher Oates, “Navigating British Columbia’s *Intimate Images Protection Act*” (26 February 2024), online: *Gowling WLG* <<https://gowlingwlg.com/en-ca/insights-resources/articles/2024/british-columbia-intimate-images-protection-act>>.
- Scorer, Kay, “The Norwich Order: The Lesser-Known Sibling of the Mareva and Anton Pillar” (24 March 2025), online: *Commercial Litigation* <<https://www.commerciallitigationblog.com/the-norwich-order-the-lesser-known-sibling-of-the-mareva-and-anton-pillar/>>.
- Wang Yi & Feng Xi, “Her Ex-Boyfriend Sold Her to One Hundred Thousand Men: Exposing the Dirty Cross-Border Hidden-Camera Trade” (24 July 2025), online: *N Video*, archived at <<https://archive.ph/20250724110043/https://www.nfnews.com/content/0oxwwNLN6L.html>>.
- Zheng Ning, “China’s ‘N Room’: Overseas Groups with Over 100,000 Members Spread Voyeuristic and AI-Generated Images, Victims Recount Their Experiences” (27 July 2025), online: *HK01* <<https://gqr.sh/n7Fm>>.