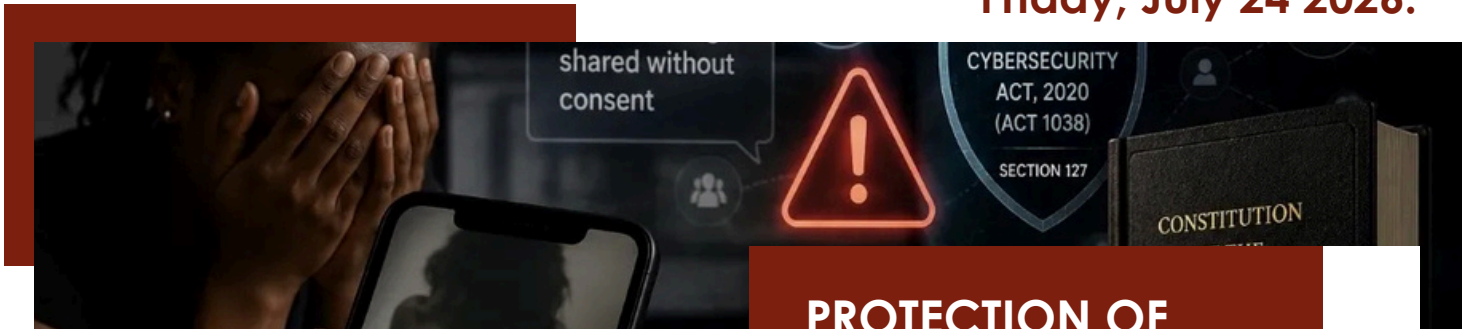


Friday, July 24 2026.



Introduction

Cybersecurity has become one of the most urgent legal and social issues in the digital age. The rapid growth of digital technology and social media has changed how people communicate in Ghana and all over the world. While these platforms have opened up new ways to connect and express ourselves, they have also led to new forms of harm and harassment. One of the most common issues is the non-consensual sharing of intimate images and videos, often known as revenge porn.

This practice involves distributing private sexual images or videos of someone without their permission, usually to humiliate, threaten, or cause emotional pain. It is a serious violation of human rights that attacks a person's privacy, dignity, and personal freedom.

PROTECTION OF PRIVACY AND DIGNITY UNDER GHANA'S CYBER SECURITY ACT, 2020 (ACT 1038):

THE OFFENSE OF SHARING INTIMATE IMAGES WITHOUT CONSENT.

Victims often endure severe psychological distress, social isolation, damage to their reputation, and, in many cases, face extortion and blackmail. In a society that emphasizes moral standards over mental health, the impact of revenge porn can be especially destructive.

This article looks at how the Cybersecurity Act, 2020 (Act 1038) addresses the non-consensual sharing of intimate images and videos in Ghana. It assesses how well the law protects victims and whether the current legal system is enough to keep up with the fast-changing digital world.

The Legal Framework

Ghana passed the Cybersecurity Act, 2020 (Act 1038) in response to the rising incidence of digital and cybercrime. This law aims to regulate the digital environment and provide real legal protection against digital abuse. The Act works both as a deterrent and as a way to address crimes carried out through electronic communication, intending to ensure safety and security for everyone online.

Notably, Act 1038 makes it a crime to share intimate images and videos without consent. It includes specific measures to protect individual rights, especially the rights to privacy and dignity in the digital space.

Section 67(1) of the Act states that it is a crime for a person to intentionally share an intimate image of someone else without that person's consent, especially if the person depicted had a reasonable expectation of privacy when the image was made. Importantly, the law clarifies that it does not matter when or how the image was originally created. Any further sharing without consent is a criminal act. A person found guilty under this section can face imprisonment for one to three years.



The Legal Framework

Section 66(3) defines an intimate image as any depiction where a person's genital or anal area is shown, either bare or covered only by underwear, or where the breast below the top of the areola is uncovered or visible through clothing.

Elements of the Offence

For someone to be held criminally responsible under Section 67 of Act 1038, the following elements must be established:

Nature of the image: The image must be intimate, meaning it relates to sexual or private matters and involves nudity or sexual activity.

Reasonable expectation of privacy: There must have been a reasonable belief that the images would remain private and not be shared publicly. Even if someone initially shared such images in a private setting, it does not mean they agreed to a wider distribution.

Consent must be absent at the time of sharing. Notably, agreeing to the creation of an intimate image does not imply agreement for it to be shared.

Intentionality: The act must be done on purpose. The offender must have shared the images with the intent to humiliate, cause emotional distress, or take revenge.



Constitutional Foundations

The 1992 Constitution of Ghana lays the groundwork for privacy protection in the country. Article 18(2) guarantees every person the right to privacy, which includes their home, property, and communications. Any interference with this right must be based on law and defensible in a free and democratic society. The non-consensual sharing of intimate images directly intrudes on a person's private life and thus violates this constitutional right.

Article 15 also protects every person's dignity and prohibits treatment that degrades or humiliates them. The unauthorized sharing of intimate images often subjects victims to public shame, deep embarrassment, and long-term psychological harm, targeting a person's dignity.

Victims have enforceable rights under the law. Article 33(1) allows anyone whose fundamental rights have been violated to seek justice through the High Court, providing a viable legal remedy for those who have endured this harm. Together, these constitutional rights enhance the protections available to victims and affirm that privacy and dignity must be honored by everyone in the expanding digital space.



Challenges in Inforcement.

Despite the promising aspects of the Cybersecurity Act, 2020 (Act 1038), numerous practical challenges hinder effective enforcement of crimes involving the non-consensual sharing of intimate images. Having legislation on the books does not guarantee proper protection, especially where institutional, technological, and cultural barriers remain.

- **Underreporting Due to Stigma and Social Consequences**

A significant hurdle to enforcement is that victims often hesitate to report incidents. Victims of image-based sexual abuse frequently feel shame, fear public mockery, face victim-blaming, and worry about damage to their reputation. In the Ghanaian society, where cultural standards often place more blame on victims than on perpetrators, many victims may avoid legal action to escape further humiliation.

Research shows that victims of non-consensual intimate image distribution (“revenge pornography”) often deal with anxiety, depression, social isolation, damage to their reputation, and job-related issues. These problems, alongside fears of being blamed or having their images further circulated, can discourage many victims from coming forward (Citron & Franks, Criminalizing Revenge Porn, 49 Wake Forest Law Review 345 (2014)).

This issue also undermines the guarantees outlined in Article 33(1) of the 1992 Constitution, as rights enforcement relies heavily on victims taking legal action.



Challenges in Inforcement.

- **Difficulties in Identifying Perpetrators and Obtaining Digital Evidence**

Cybercrimes are often committed anonymously through fake accounts, encrypted messaging apps, temporary profiles, or foreign digital platforms. This makes it technically challenging to identify offenders.

Digital evidence is often fleeting and can be easily deleted. Images may be shared multiple times across various platforms before investigators can collect evidence. This creates challenges regarding authenticity, admissibility, and accountability.

- **Limited Technical Capacity of Investigative Institutions**

Prosecuting cyber offenses effectively requires specialized digital forensic skills. However, many law enforcement agencies in developing countries face resource shortages, weak cyber forensic infrastructure, and a lack of training.

Enforcing cybercrime laws in many places is hampered by a lack of technical skills and investigative resources. Without professionals who can trace IP addresses, recover deleted content, or analyze metadata, prosecutions become hard, even with laws in place.

As a result, many offenses may remain unresolved, reducing public trust in legal responses.



Challenges in Enforcement.

- **Jurisdictional and Cross-Border Enforcement Challenges**

Digital platforms operate beyond geographical borders. An intimate image shared in one country may be stored on servers in other locations and accessed worldwide in seconds. This raises questions about jurisdiction, extradition, and enforcement against offenders in other countries.

Although Ghanaian courts can handle cases impacting people within Ghana, enforcement becomes more complicated when offenders live outside the country. International legal cooperation often moves slowly and involves complex procedures.

- **Absence of Comprehensive Victim Support Systems**

Legal remedies by themselves rarely address the severe emotional and psychological damage that victims experience. Victims typically need counseling, legal help, immediate digital support, and ways to quickly remove intimate content from the internet.

Without institutional backing, victims might drop cases or choose not to pursue complaints at all. Protecting dignity under Article 15 of the Constitution likely requires more than just criminal penalties; it also needs practical steps for recovery and support.



Challenges in Enforcement

- **Absence of Comprehensive Victim Support Systems**

Legal remedies by themselves rarely address the severe emotional and psychological damage that victims experience. Victims typically need counseling, legal help, immediate digital support, and ways to quickly remove intimate content from the internet.

Without institutional backing, victims might drop cases or choose not to pursue complaints at all. Protecting dignity under Article 15 of the Constitution likely requires more than just criminal penalties; it also needs practical steps for recovery and support.



Recommendations

- **Public education and digital literacy programs should be established.**

Public awareness should go beyond occasional campaigns and become a long-term national initiative involving schools, universities, workplaces, religious organizations, and the media. Education must highlight that consent to create an intimate image does not mean consent to share it. Topics like digital citizenship, online ethics, privacy rights, and responsible social media use should be part of educational programs.

Long-term awareness efforts can help change victim-blaming attitudes and promote social recognition that sharing images without consent is abuse, not misconduct by the victims. Preventive education ultimately increases compliance with the law before violations happen.

- **Strengthen specialised cybercrime investigative capacity.**

The effectiveness of Cybersecurity Act 1038 depends substantially on the ability of investigators to identify offenders and preserve digital evidence. Government investment should therefore prioritise specialised cybercrime units equipped with digital forensic tools, software, and continuous professional training. Police officers, and prosecutors, should receive periodic training on electronic evidence, cyber investigations, privacy rights, and image-based sexual abuse.

The mandate and technical capabilities of bodies such as the Cyber Security Authority should continue to be expanded to support coordinated enforcement.



Recommendations

Develop accessible victim support and reporting mechanisms.

Victims require support that extends beyond criminal prosecution. Dedicated reporting channels, confidential complaint systems, legal aid services, emergency digital assistance, and psychosocial counselling should be established.

Accessible support structures may increase reporting rates by reducing fear and secondary victimisation. Survivors who receive emotional and legal support are more likely to pursue justice and cooperate throughout investigations.

Support mechanisms also reflect Ghana's constitutional commitment to protecting dignity under Article 15 of the constitution.

Enhance cooperation with technology companies and social media platforms.

Government agencies should strengthen partnerships with digital platforms to facilitate rapid removal of non-consensual intimate images once complaints are verified. Delayed removal often compounds harm because harmful content can spread rapidly.

Protocols for expedited takedown requests, evidence preservation, and disclosure of information to law enforcement subject to due process protections would significantly improve enforcement outcomes.



Recommendations

Consider introducing civil remedies alongside criminal sanctions.

Although criminal punishment serves deterrent purposes, victims may also require compensation for psychological harm, reputational damage, or financial loss. Expanding access to civil remedies could enable victims to seek damages independently of criminal proceedings.

Civil liability may further deter offenders and provide more comprehensive redress consistent with constitutional protections for dignity and privacy.



Conclusion

Is Privacy Shared Privacy Lost?

The Cybersecurity Act, 2020, represents a significant step in Ghana's commitment to protecting privacy and dignity in the digital age by criminalising the non-consensual sharing of intimate images and threats to distribute such images. Through these provisions, the law recognises the serious social, emotional, psychological, and reputational harm caused by such conduct and provides a legal framework for holding perpetrators accountable. However, as this article has demonstrated, the existence of legal protections alone is insufficient to effectively combat non-consensual intimate image sharing.

The persistence of these offences suggests that the law's deterrent effect is limited where public awareness, digital literacy, and education remain inadequate. Many individuals are unaware that such conduct constitutes a criminal offence or fail to appreciate the devastating consequences it has for victims. Consequently, Ghana's response must extend beyond criminalisation to include sustained public education, awareness campaigns, and digital initiatives that promote respect for privacy, consent, and online responsibility. Only by complementing legal enforcement with education and preventive measures can the objectives of the Cybersecurity Act, 2020, be fully realised and meaningful protection afforded to victims.



Bibliography

Legislation.

Constitution of the Republic of
Ghana, 1992.

Cybersecurity Act, 2020 (Act
1038) (Ghana).

Journal Articles

Citron DK and Franks MA, 'Criminalizing Revenge Porn'
(2014) 49 Wake Forest Law Review 345.





MERTON POLICY INSIGHTS

JULY 2026



Author:

**Victoria Araba
Michael**

Legal Fellow
Merton & Everett LLP

At Merton & Everett LLP, our Policy Research practice is dedicated to providing in-depth, evidence-based insights that guide effective decision-making for governments, organizations, and stakeholders. We combine legal expertise with strategic research methodologies to deliver actionable solutions that shape public policy and drive systemic change.

Victoria Michael is a law student with an LL.B. from Wisconsin International University College, currently building her Legal Career with keen interest in criminal law, cyber law, human rights, and the protection of vulnerable persons. She is particularly interested in how the law is responding or struggling to respond to new digital realities.

At Merton&Everett LLP, she works across legal research, administration, and litigation support. Writing, for her, is a way to make legal issues make sense to people outside the profession, to keep the conversation going on where Ghana's legal system is headed, and to push for a better access to justice and stronger protections for individual rights.