PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 4 Number 3 June 2025

Thinking of Harm, Surveillance and Corporate Responsibility in Digital Criminology

Jiachen Xu[1]

[1] The University of Sydney Law School, Sydney, Australia
Correspondence: Jiachen Xu, The University of Sydney Law School, Sydney, Australia.

doi:10.56397/SLJ.2025.06.06

Abstract

This paper explores how harm, control, and responsibility appear in the digital age, using the 2023 Latitude Financial data breach and technology-facilitated abuse cases as examples. The study applies digital criminology and surveillance theory to understand the hidden and complex nature of modern cybercrime. First, it discusses how hackers use technical methods to attack companies indirectly, and how poor communication after a breach can increase the harm to users. Then, it shows how surveillance tools are also used in private settings, such as domestic violence, to control victims. The paper finds that harm in the digital world is often invisible, long-term, and hard to prevent. It argues that current laws are not enough to deal with these new types of crime. Stronger regulation, better cross-border cooperation, and more attention to surveillance misuse are needed to protect people in digital environments.

Keywords: digital criminology, surveillance theory, data breach, invisible harm, corporate responsibility, technology-facilitated abuse

1. Introduction

As digital technologies continue to reshape society, new forms of crime and harm have emerged that challenge traditional legal and criminological frameworks. One example is the 2023 cyberattack on Latitude Financial, which exposed the personal data of millions of customers and raised public concerns about corporate responsibility, data governance, and regulatory failure. [1]At the same time, the misuse of surveillance technologies in private settings—such as domestic violence involving spyware—shows how harm can also occur in interpersonal contexts through digital means. This paper explores these issues using the frameworks of digital criminology and surveillance theory. It argues that digital harm is often hidden, delayed, and extended, requiring new approaches to regulation, punishment, and prevention. The study focuses on two core cases: the Latitude Financial data breach and the use of technology in intimate partner abuse. By analyzing both institutional and personal examples of digital harm, the paper aims to rethink how power, control, and responsibility operate in a digital society, and to suggest ways

[1] ABC News, (2023). Latitude Financial Customers Frustrated by Lack of Communication after Cyberattack. 28 March 2023. https://www.abc.net.au/news/2023-03-28/latitude-financial-customers-frustrated-lack-of-communication/102151166 accessed 12 October 2024.

the law might better address these challenges.

2. Summaries of News Reports and Their Relevance to Digital Criminology

In 2023, the cyberattack on Latitude Financial led to the hole of amounts of individual data, increasing customer concerns over the company's data protection methods and inadequate communication. Numerous sensitive customer data were revealed as a result of the cyberattack. Customers who were affected feel dissatisfied with Latitude. They think the company did not communicate enough and kept data for too long. They also see problems in how Latitude manages data security. These customers believe that the company has not done enough to fix these issues. The event is strongly related to digital criminal behavior, digital enforcement, and digital punishment. Firstly, this incident reflects digital criminal behavior. Hackers gained access to Latitude's third-party systems, demonstrating that the company's supply chain has spaces in terms of security gaps. This is similar to the computer attack in the Medibank event, where hackers exploited vendor vulnerabilities to gain access to sensitive data, revealing the trend of using external partner vulnerabilities for system intrusion in modern digital crimes. Next, the event reflects the problem with digital regulation in Australia. The Latitude event exposed the companies' and related institutions' inadequacies in data retention and supervision. When information is no longer needed, companies are required to eliminate or encrypt it according to the Australian Privacy Principles. However, Latitude's long-term retention of historical customer data indicates the need to strengthen supervision of enterprise data management. Finally, news reports reflect that there is some space for reform in Australia's digital punishment. A discussion about corporate responsibility and punishment mechanisms has arisen as a result of Latitude's decision to remain silent in its reaction to the data breach.

3. Selected Theoretical Framework: Digital Criminology

With the development of technology, digital criminology is also constantly evolving, and the rapid development of digital technology has had an impact on criminal behavior, law enforcement, and criminal justice systems. Social actions, business methods, and criminal behavior have all gone through big changes. These changes happened because digital technology has spread widely. The advancement of technology and the improvement of usability have driven the widespread application of digital media, affecting various aspects of social life.[1] In addition, digital criminology attempts to explain how the understanding, execution, and tackling of legal actions are profoundly affected by the digital lifestyle. It also focuses on cybercrime, such as hacking, identity theft. Digital technology is not only a means of preventing and combating crime, but also a tool for crime. Digital technology has been integrated into People's Daily Lives in modern society. Every aspect of contemporary society, including work, social relationships, media usage, and more, is influenced by electronic devices and the Internet.[2] In the digital society, criminal act is becoming more and more complex, and traditional criminological theory can no longer fully reveal emerging forms of crime such as data leakage and privacy invasion. Digital criminology completes this vacuum and offers a fresh perspective on how to interpret and respond to digital crime.

4. The Theory of Digital Criminology Embodied in the News

4.1 Digital Criminal Behavior

First of all, it reflects the variety and complexity of attack methods under modern digital criminal behavior. The cyber attack at Latitude Financial highlights the range and technical complexity of the methods of committing current online crimes. Hackers break through security protection by exploiting vulnerabilities, demonstrating the high-tech nature of contemporary hacker attacks. The risk of cyberattacks and incursions grows as the use of modern technologies grows. Detecting these attacks has become challenging, not only because the attack methods are becoming increasingly complex, but also because the current IT infrastructure is large and complex in scale.[3] Usually, these problems are carried out through a series of meticulously planned steps rather than a single technology means. These

[1] Gavin J D Smith, Lyria Bennett Moses and Janet Chan. (2017). The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach. *British Journal of Criminology, 57*, 259, 265.

[2] Deborah Lupton. (2015). *Digital Sociology*, 1-6, Routledge.

[3] Mariya Ouaissa et al (eds). (2022). *Big Data Analytics and Computational Intelligence for Cybersecurity*, Springer.

include phishing emails, exploiting weaknesses in corporate networks, and an in-depth analysis of the digital ecosystem of enterprises to determine the best way of incursion.[1] Hackers gained access to the systems of third-party vendors in the Latitude Financial event, exhibiting the potential security risks of technology dependence and information sharing between businesses and external vendors. Because hacker does not immediately attack Latitude Financial systems, but attacks a third-party vendors, it is difficult to spot this striking. Network defense becomes more difficult as a result of this indirect attack, and standard firewalls and intrusion detection systems struggle to identify the cause of the threat first. Faced with the growth and complexity of such means, the defense strategy of enterprises faces enormous challenges. In contrast, hackers frequently take advantage of emerging technologies to quickly bypass detection. Business defense capabilities must not only have a high level of agility but also develop a multi-level security system at the technical and management levels to avoid potential risks, due to the complexity and variety of these attack methods.[2]

Second, digital criminal behavior's high level of concealment is a distinguishing quality in comparison to traditional crimes. Hackers typically enter a user's system through complex technological means and collect enough data. Hackers are able to get around company protection system. They can cause serious harm to important company data. At the same time, they can avoid being noticed for a short period. In response to such secret attacks, businesses are frequently on the defensive in the face of digital crime. In the Latitude Financial incident, hackers not only successfully infiltrated the system, but also were able to perform a series of operations after the initial intrusion to exacerbate the impact of the harm. After a period of time following the data breach, the company realized that the scale of the breach could be even larger, highlighting the covert nature of the digital crime implementation process. The invisible character of digital crime is also illustrated by the Equifax breach of 2017. The attacker infiltrated the Equifax system for about two months, exploiting vulnerabilities to obtain a large amount of users' personal information. In the end, 147 million customers' sensitive data was ultimately compromised, leaving Equifax with serious legal and financial repercussions.[3]

The transnational nature of digital crime is another quality. People, businesses, or governments in many nations can be directly or indirectly affected by digital crimes that cross national borders and are committed on a worldwide level. Attacker can attack without having to physically approach their goals because digital crime is frequently carried out using the global platform of the Internet. Medibank, another business involved in the story, was the victim of a cyberattack that exposed a lot of consumer information. According to the Australian government's confirmation, the intrusion into Medibank to steal data was carried out by Russian hackers. According to limitations on Judicial Jurisdiction, this transnational crime presents a significant challenge for nations that deal with digital crime. Attackers may use tools like virtual private networks (VPNs) and proxy servers, adding complexity to crime tracking. Due to the transnational nature of digital crime, according to Sofaer and Goodman, traditional legal frameworks are inadequate because a country's regulations and enforcement measures typically only apply to specific regional boundaries, while Internet crimes can spread across multiple national borders.[4] To address this challenge, international cooperation has become particularly important. By joining international law enforcement organizations like Interpol, signing a cyber security cooperation agreement, and achieving consensus at international events, many nations are functioning to better fight transnational digital crime. The European Union has strict rules for data that moves across borders and for keeping data private. These rules are in the General Data Protection Regulation (GDPR). This regulation was created

[1] Md Abu Imran Mallick and Rishab Nath. (2024). Navigating the Cybersecurity Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News, 190*(1), 1, 39.

[2] Maria Fernanda Pires. (2024). AI and Machine Learning: Revolutionizing Supply Chain Security. *Advances in Computer Sciences*, *7*, 1, 3–5.

[3] Stephen Smiley. (2017). Equifax: Australians' Sensitive Financial Information at Risk in Data Breach of US Company. ABC News, online, 8 September 2017. https://www.abc.net.au/news/2017-09-08/smiley-credit-check-australians-financial-information-at-risk/8887198.

[4] Abraham D. Sofaer and Seymour E. Goodman. (2001). *Cyber Crime and Security: The Transnational Dimension*, 1–2, Hoover Institution Press.

in recent years. It applies to countries that are members of the EU. It also applies to companies from other countries that do business with the European Union.[1] The implementation of such international norms will help establish unified digital crime response standards on a global scale, and reduce the risks posed by transnational digital crimes. But cross-border cooperation also faces several challenges in practice. On the one hand, the laws of various nations differ in how they determine and handle crime and data security, which causes contradictions in law enforcement and extradition. On the other hand, conflicts of interest between nations, may influence the efficiency of Cross border Tracking. For instance, in the case of Medibank, even if Australia has identified the origin of the intruders, if Russia has not agreed to surrender the hackers involved, effective accountability for criminals will face great difficulties. Thus, it is important to keep working on promoting legal coordination of transnational digital crimes. This legal harmonization will help countries work together more easily in the future. It is needed to make sure they can fight against criminal actions in the global digital space.

4.2 Digital Law Enforcement and Regulation

Within the wake of the data breach at Latitude Financial, Australia's controller, the OAIC, can examine to decide whether the company's data protection measures are input. This indicates that the government plays an important regulatory role in the digital society. In today's digital society, information leakage and privacy protection have become issues that cannot be ignored. These are issues that need close attention. With the increase of cyber attacks and data theft incidents, global governments and regulatory agencies are facing a huge challenge of how to effectively protect personal information and ensure that businesses comply with information protection security standards. Cybercrime is different from traditional criminal act, driven by the quick advancement of Web innovation, cybercriminals typically possess a high level of education and professional skills. Hackers can utilize complex coding procedures to attack, which reflect the continuous improvement of digital security measures and the importance of cooperation among various institutions.[2] Digital criminology explores the response measures of legal and regulatory agencies and points out that effective digital regulation is important to decreasing the information breaches. Specifically, the objective of digital regulation is to constrain companies to take effective data protection measures to guarantee the security of user's data through legislation and enforcement. In Australia, a fundamental system for privacy protection for citizens has been set up through the Australian Privacy Principles and the OAIC has been set up to supervise data management compliance for businesses.

In the case of Latitude Financial, the OAIC started an investigation into the company after the incident. This investigation was to check if the company follows the rules of the Australian Privacy Principles. This event highlights the important role of the OAIC in cases of information breaches. OAIC reviews enterprise data governance measures to ensure that enterprises fulfill their corresponding legal responsibilities in information protection. Australian Privacy Principles require businesses to eliminate or hide of data identification information.[3] But Latitude Financial has saved unnecessary information for up to 18 years, raising questions about its information administration practices. The OAIC's duty not only included posting evaluation of corporate responsibility but also investigated whether there was systemic negligence in data management.

The Latitude Financial incident shows a central and sensitive issue in digital regulation, how to ensure that companies actively meet their notification obligations after a data breach occurs and promptly notify affected users. Companies, especially listed ones, may choose to hide for fear of hurting their share prices. In digital society, data breaches are inevitable, but how to notify victims quickly and accurately has become one of the important criteria to measure the effectiveness of digital regulation. In this incident, Latitude Financial was questioned for failing to communicate with customers in a

[1] European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art 3.

[2] Naeem AllahRakha. (2024). Transformation of Crimes (Cybercrimes) in Digital Age. *International Journal of Law and Policy*, *2*(2), 1, 8.

[3] Office of the Australian Information Commissioner. (January 2014). Australian Privacy Principles. APP 11.

timely manner, many of whom only learned of the severity and scope of the incident through media reports. This lack of transparency not only adversely affects customers and the public interest, but also makes it difficult for regulators to fully understand the nature and scale of incidents at an early stage, thereby impeding timely and effective responses. Transparency is not only a symbol of corporate responsibility, but also a foundation of public trust in a digital society. For victimized customers, information opacity directly affects their ability to prevent personal risks and protect data. If customers do not have timely access to relevant information, it is difficult to take effective action, resulting in greater financial and privacy losses. From the perspective of digital criminology, information transparency is a key element of effective digital regulation. The speed and transparency of a company's response to a data breach is critical to protecting the rights of victims. Lack of information transparency not only weakens corporate compliance, but also affects the health of the digital society as a whole. The requirement for information transparency is not only to make the company take responsibility, but also to reduce the overall impact of data breaches on the public. In the international data protection framework, information transparency has become a key concern for national regulators. For example, the GDPR clearly states that companies must notify affected customers and relevant regulators within 72 hours of a data breach.[1] This strict requirement for information transparency aims to enable customers to understand their situation and take protective measures in the shortest possible time. There are comparative arrangements within the United States, the California Civil Code states that any person or commerce substance that incorporates a data breach must inform the influenced person and certain government organizations.[2] Laws in different regions illustrate that Information transparency is central to worldwide digital regulation. The handling of the Latitude Financial incident highlights the need for Australia to strengthen its regulations and enforcement in this area.

Although OAIC has played a certain role in digital regulation, its regulatory capabilities still have significant limitations. Firstly, OAIC's regulatory measures mainly focus on investigating and punishing incidents after they occur, and there are insufficient preventive measures in advance. OAIC lacks of comprehensive review and risk monitoring capabilities for enterprises. This lack of ability makes it hard for the OAIC to find possible dangers in data management ahead of time. As a result, many data breaches are only handled after serious consequences have already happened. The Latitude Financial occurrence is a typical example. After the hacker effectively invaded and stole a large number of client information, the company did not inform the client at the early of the occurrence, and OAIC's investigation only intervened after the incident occurred, which did not successfully avoid the risk of information breaches. The limitations of post regulatory measures are particularly inadequate in the face of modern digital crimes. With the continuous development of technology, increasingly criminals utilize emerging technologies to hide attack, making data breach detection more difficult.

4.3 Digital Punishment

The punishment in such incidents not only applies to the attacker, but also includes the punishment of the enterprise. For failed to protect customer information, Latitude Financial may experience severe fines and legal action. In the digital society, enterprises bear the heavy responsibility of protecting customer information. Once there is dereliction of duty in data management, they should bear corresponding responsibilities and punishments. latitude financial incident exposed the shortcomings of data protection and risk management, and hackers successfully invaded and stole a large amount of sensitive information. As a restraint measure against businesses that violate their obligations to defend privacy, digital punishment is also used as a response to non-compliance with data breaches. Firms must adhere to high standards of security to avoid data breaches. Enterprises that violate this commitment should bear corresponding legal and economic responsibilities. The purpose of digital punishment is to compensate for the client in the event as well as provide a warning to other businesses. This deterrent effect prompts

[1] European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art 33.

[2] California Civil Code § 1798.82.

companies to invest more tools in data protection, improve personal security methods and risk management mechanisms, thereby reducing the occurrence of future data breaches. By the Australia Privacy Act Amendments passed in 2022, the Privacy Act 1988 was amended and came into effect in 2023. This clause stipulates more severe punishments for serious or repeated violations of privacy and strengthens OAIC's authority to handle data breaches and hold companies accountable for their actions.[1] Other areas, such as the European Union, have comparable regulations in place. GDPR provides provisions for companies to be fined for data protection breaches, up to 4% of the company's global annual revenue or 20 million euros.[2]

However, companies now face civil liability and administrative penalties for data protection vulnerabilities in Australia, but usually do not include criminal liability. Under the provisions of the Privacy Act 1988 and its later amendments, the OAIC may impose large fines for critical or repeated breaches of privacy, but laws in Australia does not directly provide for criminal liability for data protection breaches. Simple civil and administrative liability may not be sufficient to deter data breaches. Although high fines pose a certain deterrent to enterprises, the personal accountability of management is relatively limited. Serious breaches or errors by principal responsible person about data protection that do not contain fraud or harm are often do not need to bear criminal responsibility. This legal framework is difficult to establish sufficient sense of responsibility among individual management when dealing with major data breaches caused by internal negligence within the company. The lack of criminal liability in Australia's data protection laws should be brought up in light of the rise in data breaches and the risk of data privacy vulnerabilities. Especially in the wake of major data breaches quite as Medibank and Latitude Financial in recent years, public and legislative institution should be aware that administrative and civil penalties may not be enough to handle data security threats. The data protection program needs to be made even stronger. This can be done by adding criminal responsibility measures. These measures would ensure that management is held personally responsible in cases of major data breaches. It could also expand the types of individual accountability. In other jurisdictions, for instance, China has formulated the refusal to fulfill information network security management obligations, when a network service provider violates regulations and refusing to right after being ordered by the governmental department to take corrective measures, fines may be imposed on the unit in accordance with the law, and criminal responsibility shall be pursued against its directly responsible supervisors and other directly responsible personnel.[3] These laws may make businesses more responsible in handling customer information and minimize the losses after they occur. This has certain reference significance for Australia.

5. Limitations and Reform Proposals of Digital Criminology

5.1 Conflicts Between Data Privacy Requirements and Regulations

With the rise in digital crimes and the complexity of means, data privacy has become increasingly important, and the dependence on digital evidence is gradually increasing. Businesses and law enforcement organizations must gather, business, and evaluate user data in large quantities during investigations, which poses a danger to personal privacy. Law enforcement may need to look through social media, geolocation records, communications files, and other sources. But large scale data collection not only violates individual privacy rights, but also simply leads to the phenomenon of excessive data collection. Overcollection of data exposes the core contradiction between law enforcement and privacy protection. To deal with complex digital crimes, law enforcement agencies must rely on data analysis, reasonable surveillance and privacy infringement, which could lead to power abuse and even threaten personal freedom. Under strict rules and transparency, boundary issues in data collection and uncontrolled data collection gradually infringe upon specific privacy rights. These are all questions that should be considered. The selection range should be limited to ensure that

[1] Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022.

[2] European Parliament and Council, Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), art 83.

[3] Criminal Law of the People's Republic of China (2023 Amendment), art 286-1.

only directly relevant data is collected. This helps to balance the needs of law enforcement with the need to protect privacy. At the same time, a clear system for data reporting should be created. Regularly share information on data collection and usage with the public. An independent oversight institution should be set up to check the data practices of law enforcement agencies. This will help to increase public trust and improve data protection compliance. These steps may improve the relationship between privacy protection and data usage.

5.2 Strengthen Cross-Border Supervision

Coordinating the fight against digital crime on a global scale is challenging because digital crime frequently involves multinational operations. Although the theory of digital criminology can point out the global characteristics of digital crime, further exploration is needed on how to coordinate policies and laws to combat crime on a global scale. The transnational nature of digital crimes and the complexity of technology pose new demands for cross-border cooperation. [1] Due to the fact that the source, target, and transfer of criminal proceeds of cyber attacks may involve multiple countries, so law enforcement agencies from different countries need to collaborate in tracking and responding. This requires countries to establish a cooperative relationship of mutual trust and coordinate in legislation and enforcement procedures. To combat cybercrime, harmonize international legal frameworks, optimize legitimate processes, strengthen cooperation between the public and private sectors, and strike a balance between privacy protection and law responses to tackle evolving digital threats. [2] The existing international mechanisms have significant shortcomings in law enforcement and punishment of transnational crimes, it relies on the judicial systems of various countries makes it difficult to promote law enforcement. Despite convention on Transnational Crime, extradition procedures and legal frameworks frequently prevent successful trials, and some offenders do not get the punishment they deserve. The impact of law enforcement is affected by this complicated transnational crime pattern, which includes various legal procedures for investigations, collection of evidence, extradition, and other such things. [3] The challenges of working together across borders come from differences in each country's legal system. There are also differences in data privacy rules, cyber security practices, and the focus of law enforcement in different nations. Data privacy is protected in the European Union, but some other nations' law enforcement does have broader authority to track criminal suspects.

In addition, political issues often become a major barrier to working together on cross-border digital crime control. This is especially in dealing with hacker attacks that cross borders. The political relationships between the countries involved can directly impact how well and quickly law enforcement agencies can cooperate. The teamwork between Australia and Russia to fight the Medibank data breach has been significantly hampered by the fact that the attackers are from Russia. Substantial sanctions against Russian hackers are difficult to achieve because of the strained relationship between Australia and Russia right now. If Australia imposes more sanctions on Russia, it will make the already tense relationship between the two countries even worse. This will also reduce any possible willingness for the two nations to work together in law enforcement. In the case of Medibank, if the diplomatic situation between Australia and Russia deteriorates more, Australia will be more difficult to ask Russia to provide legal support or extradite the network suspect, which will lead to a vicious circle. Cross-border digital crime cases show how hard it is to coordinate effectively within current international frameworks. This is especially true when handling sensitive national information or political issues. Therefore, it is necessary to rethinking the current global cooperation model, assess its functional effects and practical application, and explore more legally binding and valid cooperation mechanisms. Cross border "mandatory cooperation" clauses can be introduced in this regard, and it is suggested to include "mandatory cooperation" clauses in relevant cybercrime conventions. In specific

[1] Stéphane Leman-Langlois (ed). (2013). *Technocrime, Policing and Surveillance, 71,* Routledge.

[2] Enver Buçaj and Kenan Idrizaj. (2025). The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. *Multidisciplinary Review*, *8*, e2025024, 8–9.

[3] Idorenyin Akabom Eyo and Glory Charles Okebugwu. (2024). Analysis of Fundamental Challenges in the Combat of Transnational Crimes. *International Journal of Research and Innovation in Social Science*, 8, 1297, 1305.

major transnational events, countries should provide necessary law enforcement support and data sharing, unless there is a clear national security threat. Without compromising the sovereignty of each country, this would enhance cooperation among countries in transnational digital crime cases.

5.3 Adapt to Technological Update and Strengthen Supervision

The field of digital criminology is always changing as technology develops quickly. This is especially true with the wide use of new technologies like big data and blockchain. Criminal patterns are becoming more complex and varied.[1] The fragmented and private nature of blockchain technology makes it more easily for criminals to carry out illegal transactions and money laundering. However, existing tracking methods are difficult to effectively regulate these anonymous transactions. [2] Digital crime has become more complex as a result of the widespread application of big data evaluation, and criminals gather and analyze significant amounts of user data to carry out detailed fraud or attacks, increasing the success rate. These difficulties highlight the limits of contemporary digital criminology in addressing emerging technologies, that is the existing theories and practices often lag behind technological development and cannot effectively curb crime. To handle the challenges posed by these technology, the field of digital criminology needs to incorporate emerging technologies into its research. Law enforcement agencies should invest in advanced technology for as blockchain monitoring technology to improve their ability to detect hidden acts. Although blockchain technology is used for digital crimes, it can also be used to combat such crimes. The integration of blockchain in investigations provides new tools and methods to address emerging challenges.[3]

6. From Data Breaches to Digital Surveillance

The Latitude Financial data breach not only shows the company's weak data management and the lack of strong regulations, but also raises a deeper question: how harm works in a digital society. In traditional criminology, harm usually means physical injury, property loss, or damage to reputation. But in today's world, where we rely heavily on technology, harm often happens in more hidden, delayed, and long-lasting ways. For example, a person may not notice that their data was stolen at first, but later may suffer from identity theft, financial loss, or emotional stress. This kind of digital harm is not only caused by one person, but often by systems, platform design, company actions, and weak laws working together. More importantly, digital harm is not only found in big companies or public systems. In private life, technology is also used to control and hurt others. For example, in domestic violence, abusers use spy software, smart devices, or cloud accounts to track the victim all the time. This takes away their freedom and causes fear and anxiety. It also shows how new forms of digital abuse are difficult for the law to see or stop. The law often has no clear rules to deal with these kinds of problems. Because of these changes, we need to use theories like digital criminology and surveillance theory to better understand how harm, control, and power now work in a digital world. The next part of this paper will explain these ideas and show how people can become victims even when they are just using normal digital tools in everyday life. It also looks at how laws and rules should change to protect people from these new kinds of harm.

7. Understanding of Digital Criminology Theory

7.1 The Definition of Digital Criminology

In traditional criminology, criminal behavior is usually seen as an individual acting against social rules. It focuses on analyzing the social reasons behind these behaviors and the legal ways to deal with them. However, with the rapid development of digital technology, the forms and meanings of crime are also undergoing significant changes. Digital criminology is an interdisciplinary field that has emerged to address these changes. Digital criminology studies how digital technology affects criminal behavior, the justice system, and society's response. The core of digital criminology is to understand crime in the "digital society." This digital society not only refers to the widespread use of technology, it

[1] Naeem AllahRakha. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–29.

[2] Shreya Sangal. (2024). Gaurav Duggal and Achint Nigam, 'Blockchain's Double-Edged Sword: Thematic Review of Illegal Activities Using Blockchain. *Journal of Information, Communication and Ethics in Society*, *22*(1), 58, 64–66.

[3] Amit Kumar Tyagi et al. (2024). Role of Blockchain in Digital Forensics. *Role of Blockchain in Digital Forensics*, IGI Global, 208.

also includes how technology deeply affects social relationships, legal systems, and social norms.[1] For example, cyberbullying and online hate speech are not just expressions of personal malice, but also reflect the role of social media platforms in amplifying these behaviors and the helplessness of the law in protecting victims. In the case of Police v Ravshan Usmanov, the defendant acted out of revenge after a breakup, he posted private photos of his ex-girlfriend on Facebook. However, the judge stated that New South Wales lacks clear precedents to hold someone accountable for such crimes. As a result, the defendant was only sentenced to six months in jail.[2] From the perspective of digital criminology, criminal behavior is no longer simply a personal issue. Instead, it is the result of the interaction between technology, society, and law. What must be focused on is, how digital technology has shaped the creation, spread, consequences of criminal behavior and how the law can effectively respond to these changes in this new social context. In addition, digital criminology also requires a re-examination of the boundaries of the law. Traditional law is often based on territorial boundaries, while digital crime has cross-border and cross-space characteristics and this makes existing laws face significant challenges in combating related crimes. These issues need to be considered within a new theoretical framework. Finally, digital criminology not only covers traditional cybercrimes like hacking, identity theft, and cyberbullying, but also involves the impact of digital technology on crime in areas like surveillance, law enforcement, and evidence collection.

7.2 The Importance of "Harm" in the Study of Digital Criminology

The central role of "harm" in the study of digital criminology. In traditional law, "harm" is usually understood as direct damage to a person's body, property, or reputation. However, in the digital society, forms of harm are more diverse and hidden. Compared to traditional physical harm, the harm caused by digital crimes includes not only physical harm to people and property, but also causes emotional harm to the victims. Compared to the limited nature of traditional harm and due to the convenience of information spreading in the digital society, the harm, especially from online defamation, such as damage to the victim's reputation caused by cybercrime can significantly increase the scope and severity of the harm suffered by the victim. In issues related to digital criminology, technology becomes an important medium for causing harm in this process. The emergence of digital technology has changed traditional forms of crime and created new forms of harm. Especially through the spread of digital media and online platforms, the harm has been amplified and prolonged. For example, the online spread of sexual assault images keeps the victim in a state of ongoing trauma, the harm in these digital spaces is endless.[3] And this complex and ever-changing new technology requires a deeper understanding of harm. Digital criminology should rethink the effectiveness of the law in addressing digital harm. Current laws, when dealing with cross-border and highly anonymous digital crimes, it often struggles to hold offenders accountable or protect victims effectively. For example, when personal privacy information is leaked on the internet, even if the victim turns to the law, it is difficult to completely stop or delete the spread of the information. This limitation of legal responses urges us to consider the new risks and challenges brought by technological advancements when making laws and policies. Therefore, the concept of harm becomes especially important in the study of digital criminology.

8. Surveillance Theory

The core of surveillance theory is the use of invisible power to restrain and control individuals. With the advancement of technology, especially the widespread use of information technology, the surveillance capabilities of governments, corporations, and individuals have greatly increased. This not only changed how people interact with each other but also had a deep impact on how surveillance is conducted. In modern society, surveillance has expanded from physical spaces to the digital area. Through data collection and algorithm analysis, control is further achieved. This is not just about how technology extends power and

[1] Anastasia Powell. (2018). *Gregory Stratton and Robin Cameron, Digital Criminology: Crime and Justice in Digital Society*, 3, Routledge.

[2] Police v Ravshan Usmanov [2011] NSWLC 40.

[3] Anastasia Powell. (2018). Gregory Stratton, and Robin Cameron. *Digital Criminology: Crime and Justice in Digital Society*, 97–98, Routledge.

social control,[1] the destruction of privacy and freedom. This technology can not only serve as a tool for crime prevention, it can also serve as a means of social discipline and control. It not only affects individual behavior but also shapes social structures and power relationships.[2] This theory can be specifically reflected in the following characteristics:

First is the characteristic of power and control. Surveillance is not just a way to gather information, it is also a means of exercising power. Through continuous and hidden surveillance, power institutions can effectively monitor people's behavior to achieve the goal of social control. In this news, the domestic violence perpetrator used technological means, like spyware, to exert complete control over the victim, Abigail. Through these surveillance methods, the perpetrator can keep track of her whereabouts, communications, and daily details at any time, they can even interfere with her daily plans, such as deleting her schedule.[3] These technologies allow the perpetrator to dominate both physically and psychologically and through continuous surveillance, they reinforce their power over the victim. This situation shows that, in private relationships, surveillance can also become a powerful tool for control.

Second is the characteristic of concealment. This characteristic is reflected in the effectiveness of surveillance, which comes from its concealment and the uncertainty of those being monitored. Even if people do not know exactly when and where they are being monitored, their behavior will adjust itself out of fear of possibly being observed. This self-discipline does not come from actual surveillance, but from the worry of possibly being monitored at any time. In the news, Abigail mentioned that her mouse moved for no reason and her email account was accessed by someone else. This made her realize that she might be under surveillance. Even though she is not clear about the exact methods and timing of the surveillance, her behavior has already been influenced by the knowledge of being monitored. Especially after the perpetrator learned about her conversations with her therapist, this increased her feelings of anxiety. This uncertainty has caused her behavior to be subject to "self-discipline." She started to stay highly alert in her daily life, constantly worrying about whether she was still being monitored.[4]This fear of surveillance is a reflection of how "invisible power" operates in surveillance theory. Under this characteristic, traditional theories suggest that this practice can deter criminal behavior by increasing the perceived risk of punishment for offenders. However, this view is not entirely accurate. Even under obvious surveillance cameras, professional thieves will still continue to commit crimes. In addition, police officers often engage in serious misconduct even in front of their own vehicle cameras.[5] The "concealment" feature discussed in surveillance theory can also be seen in the Latitude Financial data breach. In this case, the attack was done by external hackers. Their method was highly hidden and indirect. Instead of attacking Latitude's main system directly, they went through a third-party service provider. This way, the company did not notice the attack for a long time. After discovering the problem, the company also delayed telling the public. Many users only learned their information was leaked much later. This delay and lack of communication show a typical type of "invisible harm" in the digital world. The damage does not appear immediately, but becomes serious over time and is often hard to fix. This kind of situation, whether in family relationships or in company data systems, shows how digital crime can be hidden and hard to detect.

The third important characteristic is the diversity of actors. With the widespread use of digital technology, information collection and processing have become much easier. This means that the exercise of power is no longer limited to a single authority. States, businesses, and even individuals can monitor others through technology. This decentralization of power breaks traditional power structures and brings new challenges. In the news report, the

[1] Deborah Lupton. (2015). *Digital Sociology*, 33, Routledge.

[2] M. R. McGuire and Thomas J. Holt (eds). (2017). *The Routledge Handbook of Technology, Crime and Justice*, 21, Routledge.

[3] Grace Atta. (2024). Tech Companies Should Build Products with Domestic Violence Victims in Mind, Expert Says. ABC News. 11 February 2024 https://www.abc.net.au/news/2024-02-11/domestic-violence-perpetrators-misusing-apps-to-cyberstalk/103410954

[4] Atta, above 28.

[5] Stéphane Leman-Langlois. (2013). The Virtual Surveillance Lab: The Creation of a Simulated Experimental Environment. In Stéphane Leman-Langlois (ed), *Technocrime, Policing and Surveillance*, 48-49, Routledge.

perpetrator is described as an ordinary person, they installed surveillance software on common household devices like phones and laptops, gaining access to various private information about the victim.[1] This shows that the misuse of technology is not limited to surveillance at the state level, individuals can also collect information and conduct surveillance using simple technological means. This "diversity of actors" in technology gives ordinary people, and even perpetrators, significant power, this allows them to abuse technology for control in personal relationships. According to a survey by The Office of the Australian Information Commissioner (OAIC), citizens reported that many organizations and businesses collect personal information beyond what is necessary and they feel uneasy about how it is being used. Especially social media platforms and large companies, they believe that these companies excessively collect, store, and share personal data without explicit consent.[2]

Another important characteristic is the normalization and widespread use of surveillance technology. Surveillance is gradually becoming a normal part of society. Whether it is in the workplace, public spaces, or the online world, people are all under different levels of surveillance. This normalized surveillance blurs the boundary between private space and public space. As mentioned in media reports, the technologies used by abusers, such as parental control software and spyware. [3] Although these are legal and common tools in daily life, originally used for family management or safety purposes, when misused, these surveillance technologies have deeply invaded the victim's most private daily life. A report shows that GPS tracking apps and video surveillance devices are widely used, these technologies are used to continuously track and monitor the victims and the use of GPS tracking apps among abusers has increased significantly. Victims are often forced to enable these features, or they will be suspected of improper behavior.[4]

Lastly, there is the digitization of social behavior, this means that with the advancement of surveillance technology, surveillance is no longer limited to physical spaces, actions, communications, transactions, and even emotions can be monitored and analyzed through digital means. This digital surveillance strengthens the full control over social behavior. Abigail's ex-husband not only physically tracked her movements but also interfered with her work and life through digital platforms like email and calendars. [5] This shows that surveillance happens not only in physical spaces but is also everywhere in the virtual world. Abusers use digital methods to gain full control over the victim's life. This behavior shows the application of "digitized social behavior" in surveillance theory. Technology allows the monitoring of people's behavior and information to be seamlessly carried out through the virtual world.

9. Gender and Digital Violence: How Technology Is Used to Control People in Close Relationships

With the wide use of smart devices, social media, and remote control technology, domestic violence has become more connected to technology. This is called "technology-facilitated abuse in family, domestic and sexual violence." These kinds of abuse often use legal or grey-area tools to monitor, follow, control, or harass others. Most victims are women, which shows a clear gender pattern. In the case of Abigail, her ex-husband used spy apps and remote access tools to secretly control her phone, laptop, and email for a long time. He could see her location, daily activities, and even messages about her mental health. This use of technology allowed him to control her even after they were not living together.[6] This kind of behavior is a form of coercive control and is one of the most hidden and underestimated types of domestic violence.

A 2023 report from Australia's eSafety agency says that in many studies and real-life cases, most victims of technology-based abuse are

[1] Atta, above 28.

[2] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey 2020' (Web Page, 2020) https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020 accessed 5 October 2024.

[3] Atta, above 28.

[4] Delanie Woodlock et al. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia* WESNET, 24.

[5] Atta, above 28.

[6] Atta, above 28.

women.[1] Digital forms of intimate partner violence include: forcing someone to share passwords and accounts, checking their messages and calls, using child tracking apps to follow the woman's location, controlling smart home devices to create fear, and sharing or threatening to share private photos or videos. This kind of tech abuse often comes with a pattern called "coercive control." It is not just one event, but part of a cycle of violence. The goal is to take away the victim's freedom, choices, and connection to others. Also, technology-based abuse often happens across many devices and platforms, which makes it harder to stop. On one hand, abusers often know how to use many devices and platforms, so they can control the victim in different ways. On the other hand, social media and online platforms do not respond quickly. It is hard to report abuse, and the steps to give proof are complex. These problems make it harder for victims to get help, and the harm becomes more hidden and more serious over time.

Australia's current laws do not fully deal with this new type of abuse. Although the Criminal code and Privacy act cover some actions like spying, threats, and misuse of information, most court decisions still focus on physical violence and harm that happens right away. It is hard to measure mental harm or digital control that shows up later, and there are no clear legal rules for these cases. Right now, there is a gap between most family violence laws in Australia and new technology. This mismatch is called a "systemic misalignment." Special laws and technical solutions are needed to close this gap. To protect victims of tech abuse, the law should clearly ban the use of spy or tracking software in private relationships. This kind of abuse should be included in the legal definition of family violence. On the platform side, companies should use "safety by design" when building apps. This means showing clear warnings about sharing access, and making it easy to report or block abuse. In the justice system, judges and police need special training to learn how to find and understand tech-based gender abuse and collect the right evidence.

10. The Application of Surveillance Theory in Digital Society and Digital Criminal Justice

10.1 Digital Surveillance and Crime Prevention

In the digital society, surveillance technology is widely used to fight crime. Technologies like video surveillance, data mining, and social media analysis have become important tools in the modern criminal justice system. These technologies can monitor and identify potential threats in real time and improve the efficiency of public safety. Take video surveillance as an example. Over time, CCTV systems have become smaller, more affordable, and more powerful, this is a direct result of technological advancements, meaning that the use and application of CCTV systems are gradually expanding.[2] In the case of Bayley v The Queen, CCTV recorded the last moments of the victim walking on the streets of Melbourne and interacting with Bayley.[3] This is crucial for identifying Bayley as the suspect and speeding up the investigation of the case.

10.2 Cybercrime and Digital Tracking

In digital criminology, surveillance technology is widely used to track and investigate cybercrime activities. By using big data, social media platforms, and communication records, law enforcement agencies can track and investigate criminal activities. This digital tracking increases the crime-solving rate and makes it possible to predict criminal behavior. As pointed out in a study, the investigation of cybercrime is different from traditional crime. The investigation process requires the use of advanced cyber detection technologies, including intrusion detection systems (IDS) to track and detect suspicious activities in real time. It also highlights the importance of online tracking through IP addresses and network accounts. This ensures the ability to quickly locate suspects and take action.[4] But on the other hand, although surveillance technology and digital tracking have improved law enforcement efficiency, it has also brought issues like privacy invasion, risk of wrongful judgments, and misuse. Massive data collection may excessively invade personal privacy. Especially in cybercrime investigations, real-time tracking and data analysis may cause

[1] eSafety Commissioner (Cth). (2023). Technology-Facilitated Abuse in Family, Domestic and Sexual Violence: A Literature Sca.

[2] M. R. McGuire and Thomas J. Holt (eds). (2017). *The Routledge Handbook of Technology, Crime and Justice*, 436, 438, Routledge.

[3] The Queen v Bayley [2013] VSC 313(19 June 2013).

[4] Yanbo Wu et al. (2019). Research on Investigation and Evidence Collection of Cybercrime Cases. *Journal of Physics: Conference Series*, *1176*, 042064, 3-4.

improper interference with innocent people. Moreover, reliance on technology may lead law enforcement agencies to depend too much on algorithms and neglect the strict verification of evidence, this creates the risk of unfair law enforcement.

10.3 Personal Privacy and Technology Misuse

As surveillance technology becomes more widespread, personal privacy faces increasing threats. For example, in domestic violence cases, abusers use legal surveillance technology to track and control victims, they even continue to digitally monitor them after the divorce. This phenomenon highlights the violation of personal privacy and security when surveillance technology is misused. A survey shows that, potential offenders can easily access various technological tools through search engines like Google, these tools include surveillance apps, spyware, GPS tracking devices, and more. The search engine's predictive feature will recommend similar queries based on the user's search habits and popular search trends. This suggests that when potential abusers conduct similar searches, they are likely to come across suggestions or tools related to technology misuse, further increasing their ability to carry out tech-based abuse.[1] Therefore, it becomes very necessary to limit this kind of behavior, strengthening legal regulation is needed. Limit the misuse of technology and provide more protection measures for victims, such as safe technology education. And require search engines to optimize algorithms to avoid recommending abusive tools, while pushing tech companies to enhance their reviews for illegal usage.

10.4 The Risks and Ethical Reflections of Digital Surveillance

Although digital surveillance technology helps prevent crime and improve public safety, its misuse also brings serious ethical risks and problems for society.

First, too much surveillance can take away personal freedom. When people know they might be watched at any time, they often change how they speak and act. They may not feel safe to express their true thoughts. Even if no one is forcing them, this kind of unclear situation can make people feel nervous for a long time and affect their privacy and mental health. Second, we cannot ignore problems like algorithm bias and data discrimination. Many digital surveillance systems use artificial intelligence and big data, but these systems are often trained with unbalanced data. Because of this, they may not work the same for everyone. For example, a study by Buolamwini and Gebru showed that many gender recognition systems are much more accurate for male faces than for female faces. This kind of unfair result makes the system less trustworthy and may harm people from minority groups.[2]

Also, there are no clear rules about how long personal data can be kept, who can see it, or how people can delete it. When people do not have control over their own data, it can lead to mistrust and misuse. To solve this, the government and other organizations should make better laws to clearly say how surveillance data can be used and where the limits are. Independent groups should check the use of this technology regularly. Only by protecting both safety and personal privacy can we build a fair and sustainable digital society.

11. Conclusion

As digital society keeps growing, traditional ideas about harm, control, and responsibility are being challenged. This paper looked at the Latitude Financial data breach and tech abuse in close relationships. It showed that digital harm is often hidden, happens later, and comes from many causes working together. These include poor company decisions, bad platform design, and weak law enforcement. Because digital crimes often involve high technology, cross-border actions, and hidden identities, they are hard to stop and hard to punish under old legal systems. Digital criminology and surveillance theory help us better understand these new problems. These theories show that power today often comes from technology, not just from people or rules. They also teach us that harm is not always physical—it can be emotional or social, caused by digital tools. The law must change to deal with this. In the future, privacy laws, criminal laws, and domestic violence laws should include rules about technology misuse. Tech companies should design safer apps, and the idea of "safety by

[1] Lisa Sugiura et al. (2024). The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses. *Criminology & Criminal Justice*, 1, 6–8.

[2] Joy Buolamwini and Timnit Gebru. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*, 1, 8.

design" should be required. Countries must also work together better to stop global digital crimes. Legal research should go beyond old ideas. It should pay more attention to how fast technology changes and how it affects people. Only when law, technology, and ethics work together can we really protect people in the digital world and build a fair and safe digital society.

References

ABC News. (2023). Latitude Financial Customers Frustrated by Lack of Communication after Cyberattack. 28 March 2023 https://www.abc.net.au/news/2023-03-28/latitude-financial-customers-frustrated-lack-of-communication/102151166 accessed 12 October 2024.

Abraham D. Sofaer and Seymour E. Goodman. (2001). *Cyber Crime and Security: The Transnational Dimension.* Hoover Institution Press.

Amit Kumar Tyagi et al. (2024). Role of Blockchain in Digital Forensics. *Role of Blockchain in Digital Forensics* (IGI Global).

Anastasia Powell. (2018). Gregory Stratton and Robin Cameron, *Digital Criminology: Crime and Justice in Digital Societ,* Routledge.

California Civil Code

Criminal Law of the People's Republic of China (2023 Amendment)

Deborah Lupton. (2015). *Digital Sociology.* Routledge.

Delanie Woodlock et al. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia*. WESNET.

Enver Buçaj and Kenan Idrizaj. (2025). The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention. *Multidisciplinary Review, 8*, e2025024.

eSafety Commissioner (Cth). (2023). *Technology-Facilitated Abuse in Family, Domestic and Sexual Violence: A Literature Scan*.

European Parliament and Council. (2016). Regulation (EU) 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation).

Gavin J D Smith, Lyria Bennett Moses and Janet Chan. (2017). The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach. *British Journal of Criminology,* 57, 259.

Grace Atta. (2024). Tech Companies Should Build Products with Domestic Violence Victims in Mind, Expert Says. ABC News, 11 February 2024. https://www.abc.net.au/news/2024-02-11/domestic-violence-perpetrators-misusing-apps-to-cyberstalk/103410954

Idorenyin Akabom Eyo and Glory Charles Okebugwu. (2024). Analysis of Fundamental Challenges in the Combat of Transnational Crimes. *International Journal of Research and Innovation in Social Science, 8*, 1297.

Joy Buolamwini and Timnit Gebru. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, *81*, 1.

Lisa Sugiura et al. (2024). The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses. *Criminology & Criminal Justice, 1*.

Maria Fernanda Pires. (2024). AI and Machine Learning: Revolutionizing Supply Chain Security. *Advances in Computer Sciences*, 7, 1.

Mariya Ouaissa et al (eds). (2022). *Big Data Analytics and Computational Intelligence for Cybersecurity.* Springer.

Md Abu Imran Mallick and Rishab Nath. (2024). Navigating the Cybersecurity Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News, 190*(1) 1.

Naeem AllahRakha. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy, 2*(5), 28.

Naeem AllahRakha. (2024). Transformation of Crimes (Cybercrimes) in Digital Age. *International Journal of Law and Policy*, 2(2), 1, 8.

Office of the Australian Information Commissioner. (2020). Australian Community Attitudes to Privacy Survey 2020.

https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020 accessed 5 October 2024.

Office of the Australian Information Commissioner. (January 2014). *Australian Privacy Principles*, APP 11.

Police v Ravshan Usmanov [2011] NSWLC 40

Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022

M. R. McGuire and Thomas J. Holt (eds). (2017). *The Routledge Handbook of Technology, Crime and Justice,* Routledge.

Shreya Sangal, Gaurav Duggal and Achint Nigam. (2024). Blockchain's Double-Edged Sword: Thematic Review of Illegal Activities Using Blockchain. *Journal of Information, Communication and Ethics in Society*, *22*(1), 58.

Stéphane Leman-Langlois (ed), (2013). *Technocrime, Policing and Surveillance, 71,* Routledge.

Stéphane Leman-Langlois. (2013). The Virtual Surveillance Lab: The Creation of a Simulated Experimental Environment. In Stéphane Leman-Langlois (ed), *Technocrime, Policing and Surveillance.* Routledge.

Stephen Smiley. (2017). Equifax: Australians' Sensitive Financial Information at Risk in Data Breach of US Company. *ABC News* (online, 8 September 2017) https://www.abc.net.au/news/2017-09-08/smiley-credit-check-australians-financial-information-at-risk/8887198.

The Queen v Bayley [2013] VSC 313(19 June 2013)

Yanbo Wu et al. (2019). Research on Investigation and Evidence Collection of Cybercrime Cases. *Journal of Physics: Conference Serie*s, 1176, 042064.