(MIJ) 2021, Vol. No. 7, Jan-Dec **e-ISSN: 2454-924X; p-ISSN: 2454-8103**

AN IN DEPTH ANALYSIS OF THE RULE OF LAW IN CORRUPTION AND INTERNATIONAL LEGAL STANDARDS ON PRIVACY

Yashika Nagpal

Amity Law School, Delhi (Affiliated to Guru Gobind Singh Indraprastha University)

ABSTRACT

The Internet's and computer systems' importance in modern life cannot be overstated. Though the growth of networking and cyberspace has significantly benefitted the general public, there are others who take advantage of this progress in order to obtain illicit benefits. Recent social-networking site users have seen a variety of assault methods. Both impersonation scams involving the Internal Revenue Service (IRS) and those involving technical help are the most prevalent types of tactics attackers employ to steal money from their victims. In this study the focus is on Rule of Law and Technology, International Cybercrime and types Of Internet-Related Crimes. This study will give the detailed on Rule of Law in Corruption and International Legal Standards on Privacy.

KEYWORDS: *Rule of Law, Technology, International Cybercrime, Corruption, Privacy Law*

1. INTRODUCTION

Information and communication technology (ICT) crime law identifies acceptable online behaviour standards, establishes socio-legal sanctions for cybercrime, protects ICT users in general and mitigates or prevent harm to people, data, systems, services and infrastructure in particular; protects human rights; enables the investigation and prosecution of online crime (outside of traditional real-world settings); and facilitates cooperation between law enforcement agencies (UNODC, 2013, p. 52). For the use of the Internet, computers, and related digital technologies and the actions of government and private organisations, as well as rules of evidence and criminal procedure and other criminal justice matters in cyberspace, cybercrime law provides guidelines and standards of conduct and behaviour. It also regulates risk and/or mitigates harm to individuals, organisations, and infrastructure in the event of a cybercrime. Because of this, cybercrime legislation incorporates substantive, procedural, and preventative aspects. Cybercrime

Substantive law

Illegal activities require specific definitions and prohibitions under law. A person cannot be punished for an act that was not prohibited by law when it was performed, according to the moral concept of nullum crimen sans lege (Latin for "no crime without law") (UNODC, 2013, p. 53). Legal subjects, such as individuals, organisations, and governments, have rights and obligations defined by substantive law. Statutes and ordinances passed by local, state, and federal legislatures (statutory law), the constitutions of the United States and the states, and court decisions are all sources of substantive law.

Procedural law

Rule-making is governed by procedural law, which sets forth the norms for enforcing rulemaking. Criminal procedure is an important component of procedural law because it includes detailed rules and guidelines on how the criminal justice system and its agents should handle and process suspects, accused, and convicted individuals (Maras, forthcoming, 2020; for general information about criminal procedure, see LaFave et al., 2015; for information about international criminal procedure, see Boas, et al., 2011). Ultimately, procedural cybercrime law includes provisions on jurisdiction and investigative power, evidence and criminal procedure relating to data collection, wiretapping, search and seizure, data preservation and storage (which are discussed in greater detail in Cybercrime Module 4 on Introduction to Digital Forensics, Module 5 on Cybercrime Investigation, Module 6 on Practical Aspects of Cybercrime Investigations and Digital Forensics, and Cybercrime Module 10 on Privacy and Data Protection; see also UNODC, 2013, p. xxii-xxiii). With regard to process, cybercrime offers a number of unique problems, particularly in terms of jurisdiction, investigations and digital evidence.

Preventive law

Regulatory and risk-mitigation are the primary goals of preventive legislation. preventative law focuses on cybercrime to either prevent it or at least reduce the harm that results from a cybercrime being committed (UNODC, 2013, 55). Cybercrime Module 10 on Privacy and Data Protection covers data protection laws like EU General Data Protection Regulation 2016 and the African Union Convention on Cyber Security and Personal Data Protection of 2014, which aim to reduce the material harms from criminal breaches of private data if a cybercrime occurs and/or mitigate those harms. As a result, criminal justice agents are equipped with the instruments necessary to investigate and punish cybercrime. This includes equipment such as telecommunications and electronic communications service providers' infrastructure that allows wiretapping and data storage. According to 47 U.S.C. 1001-1010, the Communications Assistance for Law Enforcement Act (or CALEA) of 1994 mandated that telecommunications service providers and equipment manufacturers ensure that their services and products allow government agencies with legal authorization (i.e., the appropriate legal order) to access communication.

2. THE RULE OF LAW AND TECHNOLOGY

Upholding the rule of law by encouraging innovation and technology means leveraging new technologies to provide equitable access to justice, eradicate prejudice, boost transparency and ensure a secure and just future for everyone - especially the most vulnerable and disadvantaged..

People's lives are being transformed all around the world as a result of new technology. They may simplify official contacts with government entities in the same way that they simplify ordinary chores, and they can bring new answers to a variety of rule of law issues. As yet, technological advancements hold enormous promise for enhancing the rule of law in the United States. As a result of technological advancement, more people will have access to justice, and prejudice will be eliminated.

Using the internet, people from all walks of life may access huge amounts of knowledge and resources, which can serve as a tremendous equaliser. Additionally, it may be utilised to guarantee public access to information about government procedures. Transparency is especially important in the public sector since it helps deter corruption. New information and communication technologies can assist in enforcing the rule of law by keeping institutions responsible. Numerous court systems have already begun implementing technological measures aimed at improving public knowledge. People can readily and inexpensively access court cases and other rulings by posting them online.

Efficiency is, without a doubt, a major benefit of innovation. In time-sensitive sectors like the administration of justice or violence against women and children, efficiency becomes a rule of law concern. Using technology, underserved people may locate the resources they need and ensure that the

public sector responds quickly enough to their cases to save their lives or better uphold their rights.

At the same time, new technology development, distribution, and usage must be subject to legal restrictions. Using technology incorrectly can put the rule of law at risk. For example, even though it increases efficiency, using computer algorithms to determine jail bail might aggravate prejudice. The right of individuals to privacy extends to protecting their personal data, which is why it is imperative to do so whenever new apps are developed. Asserting rule of law requires advancing technology while also ensuring that human rights are protected.

As new technologies become more critical to the rule of law, the problem of equal access becomes more pressing. Rule of law demands that the "digital divide" between nations and groups within countries be closed.

3. INTERNATIONAL CYBERCRIME

'Cybercrime,' as a term, has no universally accepted definition. It's a slang term for illicit operations carried out through worldwide electronic networks, such as those facilitated by the internet. When it comes to cybercrime, there are "no cyber-borders between countries," as the saying goes. Domestic and international laws, as well as law enforcement agencies' ability to combat transnational cybercrime is frequently put to the test. Cybercriminals increasingly utilise the Internet to commit crimes because traditional rules are too harsh or it is too difficult to find them, making it more appealing for them. Governments and businesses throughout the world, whether in developing or wealthy countries, have come to recognise the enormous dangers that cybercrime poses to national security, the economy, and the public good. Despite this, cybercrime has become increasingly difficult to combat because of the proliferation of many sorts and forms of the criminal activity. Combating cybercrime necessitates worldwide collaboration in this regard. There have already been collaborative regional and worldwide initiatives by a number of organisations and countries to develop global standards for legislation and law enforcement. Because China and the United States are the two nations that generate the most cybercrime, collaboration between the two has made a significant breakthrough recently.

Global standards-based interoperability and security are made possible in part by information and communication technology (ICT). Internet content restriction, public or private proxy and computer forensics are some of the general countermeasures used in the fight against cybercrime. Other countermeasures include legal and technological methods to trace down crimes committed over the network. We will concentrate on worldwide legislative and regulatory cooperation activities because of the diversity of national law enforcement and technology countermeasures.

International trends

A growing number of cybercriminals are aware of the substantial financial rewards that can be realised through cybercrime, and as a result, they are shifting their focus from general vandalism and adventure to more focused assaults on specific targets, such as computers, mobile devices, and the Cloud. Cybercrime is evolving at a rapid pace on a global scale.

- **Platform switch**: The battleground for cybercrime is shifting from Windows-system PCs to mobile phones, tablets, and VoIP. Because the level of vulnerability has risen significantly. Faster updates, fixes, and warnings for possible vulnerabilities are all features that PC makers are implementing into their devices. Mobile devices—from smart phones to tablet PCs—will access the Internet in greater numbers than desktop computers by 2013, increasing the number of targets for cybercrime. Mobile versions of Zeus, the wildly popular banking Trojan, are already under development. To get beyond the SMS-based two-factor authentication most banks employ to authenticate online cash transfers by clients, cyber criminals utilise smishing, which is also known as SMS phishing. Smishing works by tricking users into downloading malicious software onto their mobile devices. Vishing

(telephone-based phishing) techniques are more popular, and VoIP technologies are being utilised to assist them.

- **Social engineering scams:** If you're talking about a non-technical type of infiltration, it's one that uses e-mail or social networking discussions to trick potential victims into installing malware or revealing personal information. Social engineering, on the other hand, is a very successful attack method for exploiting confidence in well-protected computer systems. The use of social media by cyber criminals to recruit money mules for their money laundering activities throughout the world is becoming increasingly essential. Instead of using real social networking messages, spammers are creating fake ones to trick their victims into clicking on links in their emails. They're also using the confidence that users have in their social networking contacts to find new victims.
- **Highly targeted**: Malware designed to damage industrial systems, such as the Stuxnet network worm, leverages zero-day vulnerabilities in Microsoft as the newest twist in "hypertargeting." The worm's first known host was found in a German plant. After then, there was a global pandemic caused by a different strain.
- **Dissemination and use of malware**: These types of malicious software are known as viruses, worms, Trojan horses, and spyware. China ranked second (17.2 percent) and Spain ranked third (with 51.4% of virus connections to host Web sites registered there) (15.7 percent). Email is a common vector for the spread of malware. It has a genuinely global reach.
- **Intellectual property theft (IP theft)**: The global trade in counterfeit goods exceeds $600 billion a year, with as much as 90% of the software, DVDs, and CDs marketed in some countries being fakes. Theft of intellectual property costs American firms $250 billion a year and 750,000 jobs.

Types of internet-related crimes

Cybercrime and cyberattacks have no agreed-upon definition at the global level. For the most part, crimes fall into one of four categories: I offences against computer data confidentiality, integrity and availability; ii) computer-related offences; ii3) content-related offences; and, lastly, iv) offences against copyright and associated rights.

In general, cybercrime may be divided into three categories: cyber-dependent crimes, cyber-enabled crimes, and online child sexual exploitation and abuse, which is a distinct sort of crime.

- Malware, ransomware, and attacks on critical national infrastructure (such as the cyber-takeover of a power plant by an organised crime group) are all examples of cyber-dependent crime that rely on an ICT infrastructure. Another example would be overloading a website with data in order to take it offline (a DDOS attack).
- Criminal activity that may take place both offline and online is known as cyber-enabled crime. Online scams, drug transactions, and money laundering are all examples of this.
- Sextortion is the exploitation of self-created images by extortion, and it's becoming increasingly common on the open internet and darknet forums.

4. RULE OF LAW IN CORRUPTION

Corruption has a well-deserved reputation as one of society's most pernicious ills. Persons who belong to underrepresented or oppressed groups such as minorities, people with disabilities, refugees, migrants, and convicts are disproportionately affected by the erosion of confidence in governmental institutions and the impediment of economic progress as a result. Affecting women, children and the poor most, it prevents them from accessing essential social entitlements including health care, housing, and education.

Shocking figures show that every year, tens of billions of euros are paid out in corrupt payments, and that bribery costs developing nations $1.26 trillion in lost revenue due to graft and bribery. This is enough to keep the 1.4 billion people living on less than $1.25 a day out of poverty for at least six years. Transparency International's 2019 study, The Ignored Pandemic, shows that corruption has a terrible effect on our lives, with almost 7% of healthcare expenditures wasted as a result. The article cites a research that looked at data from 178 countries and found that corruption is responsible for more than 140 000 child deaths per year.

- **Strong anti-corruption standards**

GRECO, the Council of Europe's specialist body against corruption, has been tasked with overseeing the implementation of these standards through an active process of mutual evaluation and peer pressure to identify shortcomings in national anti-corruption policies and prompt legislative, institutional, and practical reforms as needed. The Criminal Law Convention on Corruption (as well as the 2003 Additional Protocol) and the Civil Law Convention on Corruption (both created in 1999) are the most significant instruments in the fight against corruption. These agreements are supported by other important legislative documents, such as the Committee of Ministers' Resolution (97), which lays out twenty guiding principles for the fight against corruption.

The European Court of Human Rights is progressively addressing corruption in its caselaw, demonstrating the numerous connections between corruption and human rights abuses. In the case of Kövesi v. Romania, the European Court of Human Rights found violations of Article 6 (right to a fair trial) and Article 10 (freedom of expression) of the Convention in relation to the removal of the head of the national anticorruption prosecutor's office before the end of her second term, following her criticism of legislative reforms in the corruption area. When considering the applicant's office, the Court noted that it was particularly important because "those functions and duties included expressing her opinion on legislative reforms which were likely to have an impact on the judiciary and its independence and more specifically, on the fight against corruption conducted by her department."

- **Corruption - a serious threat to the administration of justice and human rights**

Corruption has a particularly negative impact on the court and law enforcement. As a result, governments in a number of Council of Europe member nations have implemented hasty judicial changes that reinforce executive power by eroding judicial independence, decreasing judicial monitoring of the executive branch, and weakening the capacity to fight corruption. According to GRECO, ensuring judges' independence is essential to preventing political influence on the court, which might result in unfair, corrupt decisions that benefit special interests rather than the general interest.

It's especially hazardous when corruption in law enforcement has an influence on the safety of individuals and their ability to seek justice in situations of political corruption and police wrongdoing. Several high-profile investigations in Ukraine, notably the murder of anti-corruption campaigner Kateryna Handzyuk, appear to have been slowed down by corruption. With regard to the ongoing GRECO evaluation on anti-corruption and integrity promotion in law enforcement, one interesting aspect has been the publication of several recommendations aimed at increasing the representation and integration of women in higher police posts and at all levels of law enforcement agencies, particularly to avoid group-think that increases corruption risks. Police in Estonia, Denmark, and Spain were among those targeted by such recommendations.

- **Importance of the protection of freedom of expression and transparency**

When it comes to the battle against corruption, investigative journalists and whistleblowers are critical. Two recent murders, one in Malta and one in Slovakia, illustrate the dangers journalists face when they go after corrupt politicians and the money they accept from organised crime. Since then, three years

have passed since Daphne was brutally murdered, and no one has been able to determine who or what ordered it or why. In September 2020, two and a half years after the deaths of Jan Kuciak and his fiancée Matina Kunrová, the killers were found guilty; however, those who organised the crimes were not found guilty. As a result of a court ruling, I believe that justice must be ensured and impunity must be avoided in Slovakia. Attempts were made on the life of Montenegrin journalist Olivera Laki in 2018, and the perpetrators of this crime have yet to be apprehended; she is well-known for her investigations into political corruption in her daily, Vijesti. Crime and corruption reporting network KRIK has received death threats and been the focus of smear efforts since the violent beating of Serbian investigative journalist Ivan Nini in 2015. Investigative journalist Khadija Ismayilova, who was jailed for criticising government officials and their families over allegations of corruption and illicit business operations, is another illustrative instance. While the European Court identified many violations of the Convention in her case — including a violation of Article 18 — it concluded it was done in order to punish and silence the journalist for her work as a journalist.

The so-called Strategic Lawsuits against Public Participation pose another danger to journalists investigating wrongdoing (SLAPPs). These are frivolous lawsuits initiated by wealthy persons or corporations in an attempt to frighten journalists into giving up on their investigations and refraining from using the judicial system. So, for example, before she was killed, Daphne Caruana Galizia was already the target of over 40 civil and criminal defamation actions in Malta, some of which have been brought against her family even after she died.

- **Fight against corruption must remain a priority**

Despite the strict anti-corruption standards in place, and GRECO's efficient monitoring of member states' adherence to those standards, corruption remains a major threat to the rule of law and human rights throughout the Council of Europe area..

To successfully combat corruption, member states of the Council of Europe should adhere to all Council of Europe and international norms relating to the prevention of corruption and the promotion of integrity, as well as speed up the implementation of GRECO's recommendations.

Corruption can appear in many forms other than bribery, such as conflicts of interest, thus perception and reality do not always match completely. Even countries with a high degree of confidence in their public institutions, according to GRECO, should implement anti-corruption measures in areas where a potential gap has been discovered, regardless of where they are ranked on perception indices.

In order to protect the public against corruption, public officials must operate honestly and avoid any activities that might create a conflict of interest.

It's also critical to have a solid system in place to keep an eye out for instances of police misbehaviour, as well as to teach officers on matters of integrity and ethics on a regular basis.

In nations with weak governance, public health care spending is extremely wasteful. Member states must provide strong and effective governance as a vital instrument for the optimal operation of national health care systems and the prevention of catastrophes, such as pandemics, in order to avoid corruption in this sector.

5. PRIVACY LAW

Specifically, Privacy Law is the set of law that governs how personally identifiable information, healthcare information, and financial data about persons are acquired by governments, non-profits, and other individuals and is stored, accessed, and used. Trade secrets and directors', officers' and employees' responsibility when handling sensitive information are examples of things to which this rule also applies in the commercial sector.

A person's right to privacy, or a reasonable expectation of private, is taken into consideration while enacting privacy legislation. Everyone has the right to privacy, according to the United Nations

Declaration of Human Rights. Depending on where you live, these rights may not be interpreted the same way.

International legal standards on privacy

- **Asia-Pacific Economic Cooperation (APEC)**

In an effort to promote general information privacy and cross-border information flow, APEC developed a voluntary Privacy Framework in 2004 that was approved by all 21 member nations. Preventing damage, notifying, limiting the collection, using, and disclosing personal information are all part of the Framework's nine Privacy Principles. These principles serve as basic requirements for privacy protection.

To balance "the movement of information and data across borders...essential to trust and confidence in the internet economy," APEC developed the APEC Cross Border Privacy Rules System in 2011. System regulations include self-assessment, compliance evaluation, recognition/acceptance, and dispute resolution and enforcement based on the APEC Privacy Framework.

- **Council of Europe**

"Everyone has the right to respect for his private and family life, his home, and his correspondence." That's what Article 8 says in the 1950 European Convention on Human Rights, which covers the whole continent of Europe except for Belarus and Kosovo. A genuine right to privacy has been established for everyone thanks to the European Court of Human Rights in Strasbourg and its extensive caselaw.

When it came to Internet privacy protection in 1998, Council of Europe published "Draft Guidelines for Individuals' Protection with Regard to Collection and Processing of Personal Data on the Information Highway, which may be included in or annexed to Code of Conduct" as part of its Convention for the Protection of Individuals Against Automatic Processing Of Personal Data in 1981. They were prepared by the Council and the European Commission and accepted in 1999 by the European Union as policy guidelines.

- **European Union (EU)**

Directive 95/46/EC, which came into effect in 1995, established the jurisdiction of national data protection agencies and obliged all Member States to conform to uniform criteria for personal data protection and privacy protection. States must enact rigorous privacy legislation that does not stray from the directive's guidelines. The Directive also stipulates that non-EU nations must enact privacy legislation with the same level of limitation as EU countries before personal data can be exchanged between the two. Firms in non-EU nations must also comply with EU Directive privacy requirements of at least equivalent restraint in order to conduct business with EU firms. As a result, the Directive has had an impact on privacy legislation in nations outside of Europe. It also adds to European Union privacy legislation to propose an ePrivacy Regulation to replace the 2002 Privacy and Electronic Communications Directive (PECD).

Data Protection Directive 1995 was superseded on May 25, 2018, by the General Data Protection Regulation (GDPR). For example, the General Data Protection Regulation acknowledges that people have the right to be forgotten, which means that anybody gathering data on people is required to remove that person's records if they ask for them to be erased on their behalf. The European Convention on Human Rights, as previously noted, had an impact on the Regulation.

- **Organization for Economic Co-operation and Development (OECD)**

Due to rising concerns about privacy and data protection in an increasingly modern and connected society, the OECD released the optional OECD Guidelines on Privacy Protection and Transborder Flows of Personal Data in 1980. It was the OECD Guidelines that helped to establish a global standard for privacy law by defining the word "personal data" and establishing the fair information practise

principles (FIPPs) that other nations have embraced in their national privacy regulations.

Recommendation on Cross-border Coordination in the Enforcement of Privacy Laws was approved by the OECD in 2007. With this model framework, member nations will be more likely to enforce privacy rules as it is based on OECD guidelines. In addition, the phrase "Privacy Enforcement Authority" was coined in the Recommendation.

- **United Nations (UN)**

Private information is also protected by the United Nations' International Covenant on Civil and Political Rights, adopted in 1966, under Article 17 "A person's personal space, family, home, and correspondence shall not be invaded arbitrarily or unlawfully, nor shall anyone be subjected to unlawful attacks on his honour and reputation. The right to be protected by the law is a fundamental human right for everyone."

68/167, the United Nations General Assembly's resolution on digital age privacy rights, was approved on December 18, 2013. Referencing the Universal Declaration of Human Rights, the resolution states that privacy is a basic human right that should be upheld.

On the 11th of October, the United Nations System issued its Principles on the Protection of Individuals' Personal Data and Privacy.

6. CONCLUSION

For the use of the Internet, computers, and related digital technologies and the actions of government and private organisations, as well as rules of evidence and criminal procedure and other criminal justice matters in cyberspace, cybercrime law provides guidelines and standards of conduct and behaviour. It also regulates risk and/or mitigates harm to individuals, organisations, and infrastructure in the event of a cybercrime. Because of this, cybercrime legislation incorporates substantive, procedural, and preventative aspects. Cybercrime A person's right to privacy, or a reasonable expectation of private, is taken into consideration while enacting privacy legislation. It is possible to have as much privacy as you want with today's technical capabilities, and these technologies can enable a growing number of contractual procedures. Regulatory and risk-mitigation are the primary goals of preventive legislation. When it comes to cybercrime, prevention law aims to make it harder for criminals to commit crimes or, at the very least, reduce the harm they do.

REFERENCES

1. Oliver Diggelmann, Maria Nicole Cleis (7 July 2014). "How the Right to Privacy Became a Human Right". Human Rights Law Review. 14 (3): 441–458. doi:10.1093/hrlr/ngu014.
2. "Introduction: Privacy and Surveillance in Transatlantic Perspective", Surveillance, Privacy and Transatlantic Relations, Hart Publishing, 2017, doi:10.5040/9781509905447.ch-001, ISBN 978-1-5099-0541-6, retrieved 10 October 2020
3. Jump up to:a b Greenleaf, Graham (2009). "Five years of the APEC Privacy Framework: Failure or promise?". Computer Law & Security Report. 25: 28–43. doi:10.1016/j.clsr.2008.12.002. S2CID 62198335. SSRN 2022907.
4. Jump up to:a b c Marvin, Lynn M.; et al. (2015). "Conducting U.S. Discovery in Asia: An Overview of E-Discovery and Asian Data Privacy Laws". Richmond Journal of Law & Technology. 21 – via HeinOnline.
5. Jump up to:a b c d Reidenberg, Joel R. (2000). "Resolving Conflicting International Data Privacy Rules in Cyberspace". Stanford Law Review. 52 (5): 1315–1371. doi:10.2307/1229516. JSTOR 1229516.
6. Jump up to:a b Victor, Jacob M. (November 2013). "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy". The Yale Law Journal. 123 (2): 513–528. JSTOR 23744289.

7. Jump up to:a b Tene, Omar (2013). "Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws". Ohio State Law Journal. 74 – via HeinOnline.
8. "OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy - OECD". www.oecd.org. Retrieved 21 March 2018.
9. Greenleaf, Graham (2012). "Independence of data privacy authorities (Part 1): International standards". Computer Law & Security Review. 28: 3–13. doi:10.1016/j.clsr.2011.12.001.
10. "III.V.7 UNITED NATIONS GENERAL ASSEMBLY RESOLUTION 68/167 (ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE)". International Law & World Order: Weston's & Carlson's Basic Documents. doi:10.1163/2211-4394_rwilwo_com_033375.
11. "The UN Principles on Personal Data Protection and Privacy". 4 January 2019.
12. Grosse v Purvis [2003] QDC 151, District Court (Qld, Australia).
13. Jump up to:a b Giller v Procopets [2008] VSCA 236 (10 December 2008), Court of Appeal (Vic, Australia).
14. Jane Doe v. Australian Broadcasting Corporation [2007] VCC 281, County Court of Victoria
15. "Invasion of privacy: penalties and remedies: review of the law of privacy: stage 3" (2009) (Issues paper 14), New Zealand Law Commission, ISBN 978-1-877316-67-8, 2009 NZIP 14 accessed 27 August 2011