CUHK LAW
THE CHINESE UNIVERSITY OF HONG KONG
香 港 中 文 大 學

2022 Professional Ethics Student Essay Competition

Postgraduate Entries - First Prize

KUM Sin Ue Zoe (PCLL)
&
GIN Christopher Hoey Kwun Wai (PCLL)

Acknowledgement
The 2022 Professional Ethics Student Essay Competition is sponsored by the MaMa Charitable Foundation Limited to promote the awareness of professional ethics among CUHK LAW students through research.

2022 Professional Ethics Student Essay Competition

"Professional ethical obligations and data protection – can lawyers ever fully safeguard the interests of their clients, particularly with regard to confidentiality?"

Introduction

The importance of confidentiality to the work of legal practitioners cannot be overstated. Clients trust their legal representatives with all forms of sensitive information from business strategies to guilty pleas, and the potential ramifications of data leaks can be disastrous. Fundamentally, the ability to trust in confidentiality is crucial for clients to communicate openly with their lawyers, and for lawyers to be able to effectively represent their clients[1].

In the bygone era, when information was stored physically, physical safeguards would have offered sufficient protection, but in the cyber-age where vast tracts of information are disseminated and stored electronically, new threats to confidentiality are constantly emerging, as Jones Day found to their detriment in the 2021 CLOP Ransomware cyberattack that saw gigabytes of private client information leaked on to the dark web[2]. Indeed, according to a 2021 study conducted by the United Kingdom's Solicitor Regulation Authority, a worrying 75% of firms surveyed said that they had been targeted by cyber attacks, resulting in more than £4 million worth of client money being stolen[3].

This essay explores the challenges faced and responses devised by law firms in safeguarding their clients' interests and confidentiality in the digital age. The central thesis is that the professional obligations placed on lawyers do not require absolute protection, but rather an obligation of best endeavours. This essay goes on to argue that there is no minimum standard

[1] Principle 8.01(2) of the Guide.
[2] Lee Mathews, 'Hackers Leak Gigabytes Of Data Stolen From International Law Firm Jones Day' (*Forbes*, 2021) <https://www.forbes.com/sites/leemathews/2021/02/18/hackers-leak-gigabytes-of-data-stolen-from-international-law-firm-jones-day/?sh=5d91e339ebba> accessed 13 April 2022.
[3] 'Cyber Security - Thematic Review' (*Solicitors Regulation Authority*, 2020) <https://www.sra.org.uk/sra/research-publications/cyber-security/> accessed 13 April 2022.

of conduct that can satisfy this best endeavours standard. Instead, firms must be ever vigilant of the rapidly developing cyber landscape and constantly keep themselves updated on new threats and protective measures.

The argument is developed in two parts:

In part A, we set out the guiding principles and obligations that currently exist in Hong Kong relevant to safeguarding confidentiality. We explore the content of a client's interest in confidentiality and whether it imposes an absolute obligation on lawyers to safeguard confidentiality. As well as the question of whether the current protection afforded to client confidentiality is adequate.

In part B, we set out the actual risks and experiences of law firms in protecting and responding to various forms of cyber attacks, and highlight good practices that firms should bear in mind when seeking to discharge their best endeavours obligations.

Part A: Obligations and Confidentiality

When answering the question of whether lawyers can safeguard the interests of their client's in terms of confidentiality, the starting point must be to ask, what is the extent of a "client's interest"? Clients and lawyers might give slightly different answers. The lay client expects there to be an absolute guarantee of confidentiality, and when it comes to breaches potentially originating from their lawyers that position must be correct. Difficulty arises when the breach originates from a third party: a lay client may still expect absolute confidentiality, but with law firms increasingly targeted by dedicated hacker groups over which they have no control, an absolute guarantee might be impossible. The question surrounding the issue of cyber-breaches is shifting from being one of "if", to one of "when"[4], and cyber-security is increasingly understood not as something that can be guaranteed, but rather as a risk that must be managed. In understanding what the obligation imposed actually is, the starting point must be to consider all relevant statutory and non-statutory guidance on data protection.

[4] 'Cyber Security Breaches: It's Not If, But When | BAE Systems' (*BAE Systems | Cyber Security & Intelligence*, 2022) <https://www.baesystems.com/en/cybersecurity/cyber-security-breaches-its-not-if-but-when> accessed 13 April 2022.

Legislation

There is no stand-alone legislative regime specifically on cybersecurity in Hong Kong. But there is the Personal Data (Privacy) Ordinance (Cap. 486) ("**the PDPO**"), which is the main legislation that protects individuals' personal data and regulates the collection, holding, processing or use of such personal data and applies to private information kept in all forms, electronic or otherwise. Schedule 1 of the PDPO sets out the six principles of data protection, namely the purpose and manner of collection, accuracy and duration of retention, use, security, access, and information that are generally available. s.26 of the PDPO stipulates that all practicable steps must be taken to erase personal data held by the data user when such data is no longer required. This applies to law firms who may habitually keep clients' data to build a strong database, without paying heed to the risks of exposure.

Non-statutory guidance

In addition to the PDPO, the professional obligations imposed by the Solicitors' Guide to Professional Conduct ("**the Guide**") and the Hong Kong Bar Association's Code of Conduct ("**the Code**"), are also relevant as they jointly set out the minimum standards expected of all legal practitioners in our jurisdiction.

The Guide

Chapter 8 of the Guide imposes a duty of confidentiality on all solicitors in Hong Kong. Lawyers owe a duty of confidentiality to every client without exception, and such duty continues indefinitely even when the lawyers cease working for the client[5]. It goes without saying that lawyers are forbidden from revealing information of any client unless express consent is given[6]. Lawyers must take reasonable and prudent steps to preserve clients' information, as well as enlist extra precautions in accordance with the degree of sensitivity of the information[7].

[5] Principle 8.01 of the Guide.
[6] Principle 8.01(1) of the Guide.
[7] Drew Simshaw, 'Ethical Implications Of Electronic Communication And Storage Of Client Information' (2016) 33 The Computer & Internet Lawyer.

The Guide also explicitly extends the duty of confidentiality to cyber-communications at commentary 31 of Principle 8.01, and makes reference to Principle 1.07, which imposes an obligation on solicitors to endeavour to ensure that their use of information communication technology does not breach other principles of the Code, bearing in mind available technology, information and knowledge. The commentary to Principle 1.07 further refers to the work of the International Organisation for Standardisation ("**ISO**") as suggested best practice[8].

Beyond the explicit references to confidentiality, it is also trite that the first and foremost duty of a lawyer is to provide competent representation for clients[9]. Commentary 4 of Principle 6.01 of the Guide explains that this duty requires more than an understanding of the legal principles, but also an adequate knowledge of the practice and procedures by which legal principles can be effectively applied to practical effect[10]. In other jurisdictions the duty to provide competent representations is understood to encompass understanding the benefits and risks posed by technology to a lawyers legal practice[11].

The Code

Under para. 7.13, the Code similarly imposes a duty on barristers in Hong Kong to at all times take all reasonable steps to ensure the confidentiality of client information. It sets out specific obligations as to the handling of computers, portable storage devices and cloud computing services[12]. Para. 7.3(c) also imposes an obligation on heads of chambers to ensure that appropriate systems and measures are in place to secure handling, storage, preservation and disposal of privileged or confidential papers. Other members of the chambers must also use their best endeavours to assist or co-operate. Para. 10(18) of the Code further provides that a barrister must treat all papers in any brief or instructions as property of the client and preserve the confidentiality of clients' affairs. Such duty of confidentiality continues even after termination of relation[13].

[8] Referring to Circular 04-604, ISO/IEC 17799:2005 and ISO/IEC 27001:2005.
[9] Chapter 6 of the Guide.
[10] Principle 6.01(4) of the Guide.
[11] Drew Simshaw, 'Ethical Implications Of Electronic Communication And Storage Of Client Information' (2016) 33 The Computer & Internet Lawyer.
[12] At para. 7.13(c)(iii), 7.13(c)(v) and 7.13(c)(vi) of the Code respectively.
[13] At 10.18(b) of the Code.

Analysing the texts of the PDPO, the Code and the Guide

When taken together, it is clear that the obligations imposed with respect to protecting client confidentiality in cyberspace is one of "best endeavours". The Code makes it quite clear on its face, since it uses the term "best endeavours". The position for solicitors is more opaque. However, if one reads principle 8.13 and 1.07 together, as commentary 31 to principle 8.13 instructs one to do, the obligation imposed on solicitors in an information communication technology context is to "endeavour" to ensure that the principle of confidentiality are not breached. This conclusion is buttressed by the observation that bearing in mind available technology, information and knowledge indicates a constantly evolving standard that lawyers must endeavour to keep level with. As for the PDPO and the obligation it imposes on data users with respect to deleting information (as replicated in the Guide at commentary 32 to principle 8.13), the wording is also one of "all practicable steps". Given that "best endeavours" and "all practicable steps" are congruent concepts[14], the contention that the interest of clients with respect to the confidentiality of their data is one of "best endeavours" on the part of their lawyers is consistent with a textual analysis of the Guide. This would explain why in the context of breaches originating from the lawyer himself there is an absolute requirement of confidentiality (outside of the usual legal exceptions): because a lawyer would have failed to exercise best endeavours to safeguard client confidentiality if he is the source of the breach, but why there is also a degree of flexibility available when the source of breach is an external third party.

Part B: Measures and Good Practices against Cyberattacks

On one hand it seems that firms have failed dismally at discharging this obligation. Cyberattacks are not an alien concept to most law firms in the world. The cyber infrastructure of DLA Piper was crippled by a ransomware attack in 2017 which costed it 15,000 hours of IT overtime to contain[15]. 2.6 Terabytes of data were taken from law firm Mossack Fonseca that became known as the "Panama Papers"[16]. It leads to the question of why law firms are

[14] *Sheffield Dist. Ry. Co. v. Great Cent. Ry. Co.* (1911) 27 TLR 451.
[15] Ry Crozier, 'DLA Piper Paid 15,000 Hours Of IT Overtime After Notpetya Attack' (*iTnews*, 2018) <https://www.itnews.com.au/news/dla-piper-paid-15000-hours-of-it-overtime-after-notpetya-attack-490495> accessed 13 April 2022.
[16] Michael S. Schmidt and Steven Lee Myers, 'Panama Law Firm's Leaked Files Detail Offshore Accounts Tied To World Leaders' (*The New York Times*, 2016) <https://www.nytimes.com/2016/04/04/us/politics/leaked-documents-offshore-accounts-putin.html> accessed 13 April 2022.

especially susceptible to cyber attacks, when seemingly the topic of cybersecurity has been on the table for quite some time.

Why Law firms are especially prone to cyber attacks

Under the status quo, law firms are valuable and easy targets which render them tempting to cyber criminals. They are typically seen as having lower cyber-security capabilities and training than their clients, being less cognizant of the risks posed by a lax cyber-security environment, whilst having access to the very same sensitive information that their clients try so hard to protect. Their ability and willingness to pay an enormous amount of ransom to recover hacked data is equally appealing. Law firms have therefore been described as the "weakest link", ripe for hackers to exploit[17].

How cyber-attackers gain access to systems

Weak cybersecurity is an invitation that hackers are all too happy to accept. There are many ways in which hackers can gain access into a law firm's computer systems, but there are a few approaches that seem to occur with increasing regularity. One of which is the use of "phishing" attempts, by which hackers send emails to law firms purporting to be a counterparty to trick law firm staff into divulging sensitive data and/or downloading malware. It was the case in the "Trojan Banker" virus cases in Toronto[18] where hackers managed to trick law firm personnel into downloading a file that opened up a backdoor to the firm's accounting systems. Hackers then diverted fund deposits and other forms of social engineering aimed at gaining access to a firm's cyber-infrastructure, resulting in over a six-figure amount of monetary loss. The firm only discovered the hack three days later. This shows how cyber attacks may be discreet and oftentimes law firms fail to take prompt and effective counteractions.

Discharging the duty of best endeavours and effectively safeguarding the interests of clients

[17] Anurag Bana and David Hertzberg, 'Data Security And The Legal Profession: Risks, Unique Challenges And Practical Considerations' (2015) 16 Business Law International; J. Ames, 'Cyber Security: Lawyers Are The Weakest Link' (*The Lawyer*, 2013) <https://www.thelawyer.com/cyber-security-lawyers-are-the-weakest-link/?adfesuccess=1> accessed 13 April 2022.
[18] Yamri Taddese, 'Law Firm'S Trust Account Hacked, 'Large Six Figure' Taken' (*Lawtimesnews.com*, 2013)<https://www.lawtimesnews.com/news/general/law-firms-trust-account-hacked-large-six-figure-taken/259808> accessed 13 April 2022.

Having seen that the interest of a client with respect to confidentiality corresponds to an imposed duty on lawyers of best endeavours and how firms have fallen short in discharging that obligation. the next question is what lawyers must do to discharge that duty and therefore effectively safeguard the interests of their clients with respect to data protection and confidentiality. The short answer is that lawyers must be proactive in engaging with the evolving cyber landscape, but that breaks down into a few guiding principles, that are set out as follows:

1. *Staying informed*

In order to ensure that lawyers' measures are in line with the technology, information and knowledge of the time, a lawyer must keep oneself up to date with emerging cyber-threats and protective/reactive measures. Just as lawyers would be expected to keep themselves up to date with the law, it should be the case that lawyers feel obligated to keep themselves up to date with cyber-security/data protection issues. In Hong Kong, basic resources are readily accessible in the form of the quarterly reports of the Hong Kong Computer Emergency Response Team Coordination Centre and the Cyber Security Information Portal, to make no mention of the variety of blogs on cybersecurity available online. These would be sufficient for any lawyer to get a basic understanding of the nature of the threats faced by him and what to think about when devising systems.

2. *Developing appropriate systems*

Developing appropriate systems must occur concurrently with keeping abreast with technological development, indeed the two must inform one another: a lawyer is seeking to stay informed about any newly discovered vulnerabilities in the software and systems he employs, and should constantly be on the lookout for ways to further buttress the level of protection his systems can offer. In terms of the actual systems themselves, a lawyer should have systems in place to (1) protect against cyber-attacks: such as regular penetration tests/cyber-audits, policies regarding encryption, email discipline (not opening unknown emails, having isolated sandboxes in which email attachments can be opened without affecting other files/scanning before opening emails etc) and staff training, (2) to mitigate the harms if cyber-attacks occur: through policies such as data backups stored in isolated systems, (3) to respond to cyber-attacks if they occur by: having crisis response/role allocation plans, keeping

clients informed, having dedicated in-house or independent IT specialists[19] who firms can rely on in the event of an actual attack.

In addition to these systems, a lawyer should also have policies in place to minimise the risk posed by personal device usage and the storage of sensitive client information on such devices, and have policies in place to ensure copies of client information on private devices are retained and originals wiped when lawyers change firms. There should also be policies in place to destroy client data when retention is no longer necessary.

At all times a lawyer should understand what information they have in their possession, where it is stored, how it is accessed/segregated, what forms of technical, physical and administrative protections exist to protect information in hand and the limitations of those protections.

Lingering risks, and what the industry can do about them

Certainly, there are still limits to what an individual lawyer, or even an individual firm can do to safeguard client confidentiality even if they discharge the best endeavours duty above, and a hacker is unable to find purchase in their systems, a gapping lacunae in schemes around the world is that there are no obligations owed parties who are not actually a client of the firm. A lot of sensitive information changes hands during transactions and litigation, even if one firm is diligent in its practices, it cannot guarantee the same level of cyber-security in the systems of other party's lawyers who might also gain access to the same sensitive information through discovery or best endeavours processes. So long as there is no clear guidance, or minimum standards imposed on the industry as a whole, legal practitioners are unable to guarantee client confidentiality.

Despite all this, some law firms are still circumspect about sharing cyber-security information[20], citing operational risks of sharing system vulnerabilities and allowing those to become more widely known as well as the reputational risk that comes with admitting to these

[19] Such as through the use of Master-Service agreements: Julie Sobowale, 'Managing Cyber Risk' (2017) 103 ABA Journal.
[20] *Data Security: Risks, Unique Challenges and Practical Considerations*, Anurag Bana and David Hertzberg, 2015 Business Law International Vol 16 No 3, at pg. 255.

vulnerabilities in the first place. These concerns are misplaced: consider the response of DLA Piper to the 2017 Pretya attack, where the firm immediately notified its clients and made a post on its website about the ongoing cyber attack. Its openness with regards to the cyberattack and the measures being taken by the firm to deal with the threat were widely lauded, and no doubt helped the firm retain most of its clientele and emerge with a reputation for honest-dealing. In fact, if industry wide cooperation is essential to safeguard client confidentiality, failure to proactively take part in this form of resource sharing may be antithetical to the duties owed by lawyers to use their best endeavours to protect clients information. Regulatory bodies can also help address these concerns by setting up industry-level anonymised sharing platforms for firms to pool their knowledge and experience regarding cyber security.

Despite the Guide and the Code endeavouring to safeguard clients' interests in the course of legal service in Hong Kong, they may still be inadequate and lagging behind. Most lawyers nowadays still fail to recognize the multitude of risks that follow even when precautions are taken and rules abided by. Often it is the blurred distinction between a lawyer's personal and professional life that increases the risks of leaking clients' confidential information[21]. For instance, young lawyers who are keen users of social media (e.g. Facebook, Twitter, Instagram) may inadvertently leak clients' data in the most unexpected ways. It could simply be a snapshot of an office's view and through the reflection of the glass window third parties gain insights into the work that they do.

Another risk is the skyrocketing use of instant messaging. In comparison to using smartphones for emails and voice calls, employers are more inclined to use instant messaging to carry out business[22]. Law firms are no exception in this regard. Lawyers may find it convenient to discuss with a colleague, a client or a third party matters that may be privileged. Though most instant messaging applications would brand themselves as having end-to-end encryption (i.e. only the sender and receiver can read the message), there is still no guarantee

[21] Drew Simshaw, 'Ethical Implications Of Electronic Communication And Storage Of Client Information' (2016) 33 The Computer & Internet Lawyer.
[22] Carmen Wong, 'What'S Wrong With Lawyers Using Instant Messaging? | Hong Kong Lawyer' (*Hk-lawyer.org*, 2019) <http://www.hk-lawyer.org/content/what%E2%80%99s-wrong-lawyers-using-instant-messaging> accessed 13 April 2022.

how strong these safeguards are, let alone the fact that certain platforms do not provide encryption at all[23].

Conclusion

Although professional ethical obligations are placed on lawyers to safeguard their clients' interests and confidentiality, this essay contends that such obligations require lawyers to use their best endeavours rather than offer absolute protection. The specific measures and safeguards discussed herein are only groundwork for maximising protection of clients' interests, in particular clients' confidentiality. Beyond these precautions, lawyers must take wider approaches with regard to cybersecurity through developing a network to cooperate with other lawyers or law firms openly, diligently and vigilantly.

Even if the obligation imposed on lawyers is not absolute, the duty to use best endeavours to protect client confidentiality is not a hollow one. Beyond any questions of liability on the part of a lawyer, potential clients are increasingly insistent on regular cyber-audits[24] and/or a minimum level of cyber-security accreditation[25] before they would consider engaging the services of a law firm. Increasingly, proper cyber-security protection is becoming a prerequisite for a firm to have any business in the first place. In this rapidly changing sphere, lawyers must rise to the challenge and learn to be well-versed in not just the letter of the law, but also the digital language of the 21st century.

[23] Carmen Wong, 'What'S Wrong With Lawyers Using Instant Messaging? | Hong Kong Lawyer' (*Hk-lawyer.org*, 2019) <http://www.hk-lawyer.org/content/what%E2%80%99s-wrong-lawyers-using-instant-messaging> accessed 13 April 2022.
[24] David G. Ries, '2021 Cybersecurity' (*Americanbar.org*, 2021) <https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/> accessed 13 April 2022.
[25] *Data Security: Risks, Unique Challenges and Practical Considerations*, Anurag Bana and David Hertzberg, 2015 Business Law International Vol 16 No 3, at pg. 263.