Santa Clara Journal of International Law

Volume 20 | Issue 1 Article 2

12-2-2021

PAST AS PROLOGUE: INTERCEPT & SURVEILLANCE RULES UNDER HONG KONG'S NATIONAL SECURITY LAW

Hargreaves, Stuart

PAST AS PROLOGUE: INTERCEPT & SURVEILLANCE RULES UNDER HONG KONG'S NATIONAL SECURITY LAW

By Stuart Hargreaves[*]

Abstract

In response to civil unrest in 2019, in 2020 Beijing directly applied a new National Security Law to Hong Kong. Part of this law established a new system of rules for the authorisation of communications intercepts and covert surveillance in the context of certain national security offences. Interestingly, this new scheme looks in many ways like a prior system that was deemed unconstitutional by a Hong Kong court in 2006: it centralizes authorization authority in the executive branch and there is little external oversight of the process. This paper argues that the new system of rules regarding covert surveillance of national security suspects and the interception of their communications is more than just a mechanism to ease the detection of national security threats, however. The Central Authorities have recently stated the Chief Executive of Hong Kong holds a 'transcendent position' over the rest of the local government. This paper suggests the new scheme shows the purpose of this transcendence – the removal of the judicial branch from the process allows the Central Authorities to more effectively ensure the primacy of core state goals through the office of the Chief Executive.

[*] BA, JD, BCL, SJD. Associate Professor, Faculty of Law, the Chinese University of Hong Kong. I am immensely grateful to Simon Young for comments on an earlier draft.

Table of Contents

INTRODUCTION

Hong Kong was gripped by civil unrest for an extended period in 2019, with violent clashes between protestors and the police making headlines around the world.[1] Though wide-scale street protests ebbed following the emergence of COVID-19 in early 2020, it was apparent that the Chinese government perceived an ongoing, and unacceptable, challenge to its authority. In June 2020, Beijing directly applied a new National Security Law[2] ("NSL") to Hong Kong. That law outlines a series of offences against national security, establishes a number of new institutions related to them, and creates various procedural mechanisms that apply only to their prosecution, in effect setting them apart from the conventional legal order. This paper focuses on one particular element of the NSL, Art. 43. That provision details the creation of a new department within the Hong Kong Police Force tasked with investigating national security offences and provides them with wide-ranging powers related to the covert surveillance of suspects and the interception of their communications.

This provision is of interest because it essentially reverses a finding of unconstitutionality made in 2006.[3] Prior to that finding, Hong Kong's Chief Executive could order the interception of the communications of any individual in the name of public security or safety under the Telecommunications Ordinance[4] ("TO"). Subsequent to the 2006 case, the Hong Kong government adopted an entirely new law – the Interception of Communications and Surveillance Ordinance[5] ("ICSO") – that was more protective of the right to privacy. The ICSO required judicial authorization of both the interception of communications and particular forms of covert surveillance and created a mechanism of public oversight through an independent commissioner's office.

This paper shows that in the context of investigating national security offences the new scheme occasioned by the NSL returns Hong Kong to the pre-ICSO era: it centralizes authorization authority in the executive branch and reduces

[1] *See, e.g., Chaotic Scenes as HK Protests Turn Violent*, BBC, (June 12, 2019), https://www.bbc.com/news/live/world-asia-china-48455370.

[2] Law of the People's Republic of China on Safeguarding in the Hong Kong Special Administrative Region (promulgated by the Standing Comm. Nat'l People's Cong., June 30, 2020, effective June 30, 2020) [hereinafter *National Security Law*].

[3] *Leung Kwok Hung v. Chief Exec. of H.K.*, H.C.A.L. 107/2005 (C.F.I.) (Feb. 9, 2006). Though the substance of the finding of unconstitutionality was not appealed by the Government, the question of the appropriate remedy was, and this was considered by the Court of Appeal in *Leung Kwok Hung v. Chief Exec. Of H.K.*, CACV 72/2006 (C.A. May 10, 2006) and the Court of Final Appeal in *Leung Kwok Hung v. Chief Exec. Of H.K.* [2006] 9 H.K.S.F.A.R. 441, FACV12/2006 (C.F.A. July 12, 2006).

[4] Telecommunications Ordinance, (1963) Cap. 106, § 33 (H.K.).

[5] Interception of Communications & Surveillance Ordinance, (2006) Cap. 589 (H.K.).

external oversight of the process. This paper suggests, however, that the new scheme is more than just a mechanism to ease the detection of national security threats. It is an example of the Central Authorities' intent to exercise 'comprehensive jurisdiction' over Hong Kong through the office of the Chief Executive, who has recently been described as holding a 'transcendent' position over the three branches of Hong Kong's local government. By concentrating authorization authority in a transcendent Chief Executive with primary accountability to the Central Authorities, the new scheme ensures the primacy of the national interest even though decisions taken regarding intercepts and surveillance are still taken by local bodies. The complete removal of the judiciary from the process reflects a belief that the courts of Hong Kong should never be permitted to act as a check on state goals.

I. THE TELECOMMUNICATIONS ORDINANCE SCHEME & ITS DEMISE

A. The Telecommunications Ordinance in the Colonial Period

The origin of the regulatory framework surrounding the interception of the communications of criminal suspects dates to before the return of Hong Kong to Chinese sovereignty in 1997. The TO was enacted by the colonial government in 1962, and read in part:

> Whenever he considers that the public interest so requires, the Governor, or any public officer authorised in that behalf by the Governor either generally or for any particular occasion, may order that any message or any class of messages brought for transmission by telecommunication shall not be transmitted or that any message or any class of messages brought for transmission, or transmitted or received or being transmitted, by telecommunication, shall be intercepted or detained or disclosed to the Government or to the public officer specified in the order.[6]

While "the public interest" was undefined within the TO itself, the Secretary for Security declared in 1992 that it referred to "the prevention or detection of serious crime, including corruption, or in the interests of the security of Hong Kong."[7] Even so, the circumstances in which the Governor (or his designated subordinate) could order interception were clearly broad.[8] There was no apparent standard to meet other than a subjective belief in the necessity of the order, and no requirement to take into account any countervailing interests such as the

[6] Telecommunications Ordinance, s*upra* note 4.
[7] *Hong Kong Hansard*, Nov. 11, 1992, at 634, *cited in* H.L. Fu & Richard Cullen, Political Policing in Hong Kong, 33 H.K. L.J. 199, 219 (2003).
[8] Leah Angela Robis, *When Does Public Interest Justify Government Interference and Surveillance?* 15 ASIA-PAC. J. ON HUM. RTS. & L. 203, 213 (2014).

privacy of the target or third parties who might have had their communications exposed as a consequence.

Section 33 of the TO was modelled on the UK's Post Office Act, which effectively authorized the interception of communications provided it had been done "in obedience to a warrant under the hand of the Secretary of State."[9] In *Malone*[10] the European Court of Human Rights (ECtHR) found the untrammelled authority that this gave to the executive branch an unjustifiable restriction upon the right to respect for one's private life and correspondence.[11] The absence of a tailored scheme meant there was not "reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."[12] Though, of course, *Malone* had no direct application to the legal status of the TO in Hong Kong, the ECtHR's reasoning highlighted the conflict between unconstrained executive authority and the right to privacy and the problematic aspects of the law became more pressing following the introduction of the Hong Kong Bill of Rights Ordinance[13] ("BORO") in 1991. The BORO largely incorporated the International Covenant on Civil and Political Rights[14] ("ICCPR") into domestic law, creating a right to privacy and prohibiting unlawful interference with correspondence.

Questions about the consistency of § 33 of the TO with the quasi-constitutional[15] protections under the BORO were asked not only by a variety of public and professional organizations,[16] but eventually by the Governor himself.[17]

---

[9] The Post Office Act 1969, c. 45, sch. 5(1) (UK)– rather than directly 'authorizing' an intercept, this provision provided a defence to the offence of interfering with communications under section 45 of the Telegraph Act 1868. *See* Telegraph Act 1863, 26 & 27 Vict. ch. 112, § 45 (UK).

[10] *Malone v. the United Kingdom*, 89 Eur. Ct. H.R. (1984).

[11] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 (entered into force Sept. 3, 1953).

[12] Malone, *supra* note 10, at ¶ 79.

[13] Hong Kong Bill of Rights Ordinance (BORO), (1991) Cap. 383 (H.K.).

[14] *See generally* International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR]. I say "largely" because when the ICCPR was signed by the U.K. on behalf of Hong Kong in 1976 it also entered a reservation to the effect that it did not consider itself bound to apply the ICCPR's Art.25(b) commitment to free and open elections to the establishment of either an elected executive or legislative council in Hong Kong. Reference to this reservation was also incorporated into section 13 of the BORO and continued in effect after the transfer of sovereignty in 1997; *See, e.g.*, H.K. LEGIS. COUNCIL PANEL ON CONST. AFFS., REPORTS OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION IN THE LIGHT OF THE ICCPR, CB(2)602/17-18(04) (2018), https://www.legco.gov.hk/yr17-18/english/panels/ca/papers/ca20180104cb2-602-4-e.pdf.

[15] While the BORO was enacted as a conventional statute, § 3 required that all existing laws be construed consistently with it to the greatest extent possible. If existing laws could not be so construed, they were to be repealed to the extent of the inconsistency.

[16] *See* Fu, *supra* note 7, at 221.

[17] Fu, *supra* note 7, at 220.

At the same time, there were allegations that the Independent Commission Against Corruption[18] ("ICAC") was using the broad authority granted to it under the TO to target opponents of the Government.[19] In 1996, the Law Reform Commission ("LRC") recommended amending § 33 of the TO on grounds that paralleled the concerns raised by the ECtHR in *Malone* vis-à-vis the Post Office Act.[20] The LRC argued that the law as it stood was not "sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which interceptions may be authorised."[21]

The Hong Kong Government issued a White Paper on proposed reform in February 1997[22] but did not introduce a bill into the Legislative Council in order to implement it. A private member's bill dealing with the same matter was, however, introduced in April 1997.[23] If adopted, that bill would have become the Interception of Communications Ordinance ("IOCO").[24] The would-be IOCO significantly circumscribed the Governor's power to order intercepts, imbuing it instead in the court, which would act upon applications from identified senior officers in various departments.[25] It was passed by the Legislative Council on June 27, 1997 — four days before the transfer of sovereignty over Hong Kong from the United Kingdom to China — and signed by the Governor.[26] However, the law was never brought into force by the new Special Administrative Region ("SAR") government, with the first Chief Executive arguing that it was unbalanced and its adoption would unduly hamper law enforcement in the detection and investigation of serious criminal activity.[27] The result was that the TO continued on as the scheme for interception as of July 1, 1997, with the Chief Executive replacing the Governor as the relevant authority.[28]

---

[18] The Independent Commission Against Corruption was established in 1974 as part of an effort to eliminate widespread corruption in the civil service. Its existence is now constitutionally guaranteed. *See* XIANGGANG JIBEN FA Art. 57, § 1 (H.K.).

[19] Fu, *supra* note 7, at 219.

[20] *See* Law Reform Comm'n of Hong Kong, Privacy: Regulating the Interception of Communications , (1996), https://www.hkreform.gov.hk/en/docs/rintercept-e.pdf [hereinafter the 1996 Report]; *see also* Fu, *supra* note 7, at 222.

[21] *Id*. at 41.

[22] *See* Law Reform Comm'n of Hong Kong, Privacy: Regulating the Interception of Communications , CB(2)971/05-06(01) (2006), https://www.legco.gov.hk/yr05-06/english/panels/se/papers/se0207cb2-971-01e.pdf.

[23] Alana Maurushat, *Hong Kong Anti-Terrorism Ordinance and the Surveillance Society: Privacy and Free Expression Implications*, 12 ASIA PAC. MEDIA EDUCATOR 26, 37 (2002).

[24] Interception of Communications Ordinance, No. 109 (1997).

[25] *See id.* at s.5(1-2).

[26] Graham Greenleaf & Robin McLeish, *The Rule of Law and Surveillance in Hong Kong*, 11 PRIVACY LAW AND POLICY REPORTER 227, para. 4 (2006).

[27] *Leung Kwok Hung & Anor v. Chief Executive of Hong Kong*, [2006] H.K.C. 230, 86.

[28] Greenleaf & McLeish, *supra* note 27, para. 1

B. The Telecommunications Ordinance in the SAR-era

The quasi-constitution of the Hong Kong SAR, the Basic Law,[29] served to reinforce the privacy rights of Hong Kong residents, concerns about the law did not abate with the arrival of the new sovereign. In addition to mandating that the ICCPR continue to be implemented through domestic law,[30] the Basic Law created a separate constitutional guarantee of communications privacy in Art. 30:

> The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.[31]

Concerns were raised as to whether the virtually unrestricted power of the Chief Executive to order interception met the threshold of "in accordance with legal procedures."[32] This mattered greatly because the newly established Court of Final Appeal had held it not only had the power to declare government legislation inconsistent with the provisions of the quasi-constitution, but also to declare legislation to be invalid to the extent of any found unconstitutionality.[33]

In 2004, the Legislative Council's Panel on Security published a comparative report on the governance of the interception of communications as it occurred in other jurisdictions as part of the Panel's review of the (failed) 1997 IOCO and what future legislative efforts in this area ought to look like instead.[34] The report concluded that allowing the head of government or their designate to directly authorize interception was an outlier. The other three jurisdictions chosen for comparison — the United Kingdom, the United States, and Australia — all relied on a more complicated application process for the issuance of interception

[29] The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China, Adopted on 4 April 1990 by the Seventh National People's Congress of the People's Republic of China at its Third Session. XIANGGANG JIBEN FA.

[30] XIANGGANG JIBEN FA, *supra* note 18, at art. 39, § 1. This continued to be done in the form of the BORO.

[31] XIANGGANG JIBEN FA, *supra* note 18, at art. 30,

[32] *See, e.g.*, Won Hah Ng, *Remedies Against Telephone Tapping by the Government*, 33 H.K.L.J. 543 (2003).

[33] *See Ng Ka Ling v. Director of Immigration*, [1999] 2 H.K.C.F.A.R.

[34] Research and Library Services Division – Legislative Council Secretariat, *Regulation of Interception of Communications in Selected Jurisdictions*, (Feb. 2, 2005) RP02/04-05, https://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf.

warrants.[35] The report further suggested that the TO's lack of time limits for authorizations once issued, lack of internal safeguards, and lack of some form of oversight were all inconsistent with international practice.[36]

In the same time period, the courts of Hong Kong were confronted with related issues in light of the new constitutional structure. In 2005 the lower courts twice[37] considered the impact of the Art. 30 privacy right in the context of covert surveillance leading to the capture of conversations.[38] *Li Man-tak*[39] dealt with an allegation of bribery, the prosecution of which turned in part on covert audio and video surveillance made by the ICAC that captured incriminating conversations between the defendant and others.[40] The defence argued in part that this surveillance resulted in recordings of private conversations and ought to be inadmissible as evidence of an infringement of the Art. 30 right to privacy.[41] The court noted that while Art. 30 contemplates that authorities may inspect communications "in accordance with legal procedures," no relevant framework had been introduced by the government that detailed these procedures.[42] Instead, all that existed were internally-developed "Standing Orders" by the ICAC, which simply required an investigator to request approval from a senior officer before the installation of a surveillance device.[43] The court concluded that the opacity and informality of this process meant that "the only protection the citizen has [against] unfettered and unsupervised power is the goodwill of the principal investigator."[44]

The court went on to consider *Malone*, suggesting the meaning of "in accordance with legal procedures" was analogous to that of "in accordance with law" per Art. 8 of the European Convention on Human Rights.[45] The court ultimately concluded that the ICAC's "Standing Orders" failed to meet the standard of "in accordance with legal procedures" and there was, in essence, a legislative

[35] *Id*. at 5.2.4. In the UK, warrants would be issued by the executive branch; in the US, by judges; in Australia, by either the executive branch or by judges depending on the context.
[36] *Id.* at 5.2.6-5.2.27.
[37] *See* Simon NM Young, *The Executive Order on Covert Surveillance: Legality Undercover?* 35 H.K.L.J. 265, 271-273 (2005).
[38] This is distinct from a communications intercept as it does not capture conversations while in transit within a telecommunications system.
[39] *See Hong Kong v. Li Man Tak,* [2005] H.K.E.C. 1308.
[40] *Id.* at 8.
[41] *Id.* at 13.
[42] *Id*. at 18.
[43] *Id*. at 19.
[44] *Id*. at 22.
[45]*See Hong Kong v. Li Man Tak*, [2005] H.K.E.C. 1308.

lacuna.[46] While the court nonetheless found that the unconstitutionally-obtained evidence could be admitted under the exclusionary rule,[47] it warned that

> Now that a Hong Kong court has made a ruling that the installation of covert surveillance devices is in breach of the Basic Law without proper legal procedures in place, and unless and until this ruling is overturned, it may well be held in future criminal trials that the ICAC are acting mala fide if they continue this practice without some legislative basis.[48]

In *HKSAR v Shum Chui*,[49] an individual arrested by the ICAC subsequently served as an undercover informant in exchange for immunity from prosecution. Activities undertaken as an informant included, *inter alia*, wearing covert recording devices in an attempt to gather evidence on multiple defendants.[50] The recorded material included conversations between the informant and one defendant in the presence of their solicitor.[51] Some of that material was introduced as evidence. That defendant argued that the covert nature of the recording was an infringement on their fundamental rights and the proceedings should thus be stayed.[52]

The court concluded that the ICAC knew that the solicitors would be present at the meeting in question, and thus intentionally recorded and listened to material that would be *prima facie* privileged.[53] Yet the authorisation of the surveillance approved by a principal investigator made no mention of the fact that solicitors would be present at the meeting, which the court considered a "serious flaw" in the authorisation process.[54] This "cynical and flagrant infringement [of the] right to legal professional privilege"[55] of the defendant meant the Government needed to "introduce the regulations required for lawful covert surveillance as was originally

[46] *Id*. at 54-55.
[47] *Id*. at 65.
[48] *Id.* at 67. Interestingly, it was revealed during trial that the ICAC had relied on authorization under s. 33 of the TO to conduct telephone intercepts, which in turn led to the justification for the audio and video surveillance leading to the capture of the conversations. After ordering a *voir dire*, Sweeney J. accepted the legitimacy of these intercepts and no constitutional arguments against the TO were raised by the defence. *See HKSAR v. Li Man Tak & Ors*, [2005] H.K.E.C. 1309.
[49] *HKSAR v. Shum Chiu*, DCCC687/2004 (July 5, 2005), https://www.legco.gov.hk/yr04-05/english/panels/se/papers/secb2-2280-1e.pdf.
[50] *Id.* at 8.
[51] *Id.*
[52] *Id.* at 10-11.
[53] *Id.* at 17.
[54] *Id.* at 20.
[55] *HKSAR v. Shum Chiu*, DCCC687/2004 (July 5, 2005), at 33, https://www.legco.gov.hk/yr04-05/english/panels/se/papers/secb2-2280-1e.pdf.

envisaged under the Basic Law. They should do so with all due haste, so that the guarding of the guards is not just left to the [j]udiciary."[56]

These judicial criticisms led the Chief Executive to issue, apparently as an interim measure while fuller legislation was drafted,[57] an executive order (hereafter referred to as "the Order") that purported to create a scheme of authorization that would more tightly regulate certain forms of covert surveillance.[58] The Government stated that no new powers were created by the Order; rather, it merely "clarified" what law enforcement bodies could do.[59] The Order stated — with an important exception, *infra* — that any covert surveillance that would lead to the obtaining of private information about the subject had to be authorized under its terms. Authorization would only be granted if the relevant authorizing officer deemed it to be for the purpose of crime prevention or public safety, and if the intrusive measures were proportionate to the need.[60] While Departments were required to issue guidelines to staff on how the new scheme would operate, the Order explicitly noted that failure to follow those guidelines would not affect the validity of any authorization.[61] No penalties for failure to comply with the Order were established, and no judicial oversight was contemplated.[62]

The Order did not distinguish between covert surveillance and the interception of communications in the way that later legislation would. "Covert surveillance" was defined as the systematic surveillance of an individual, carried out in circumstances where a person was entitled to a reasonable expectation of privacy, which would likely result in the capture of private information.[63] Though this broad definition may have meant it could apply to communications intercepts as a particular species of covert surveillance, the point was never tested in Court. In any event, the Order specifically excluded from its ambit any surveillance that was otherwise legally authorised,[64] suggesting it would not apply to the Chief Executive exercising their intercept power under § 33. The Order thus seemed aimed at only the excesses of law enforcement agencies acting on their own

[56] *Id.* at 53.
[57] Legislative Council Panel on Security, *Law Enforcement (Covert Surveillance Procedures) Order*, LC Paper No. CB(2)2419/04-05(01) at 4, 13, (Aug. 5, 2005), https://www.legco.gov.hk/yr04-05/english/panels/se/papers/se0815cb2-2419-1e.pdf.
[58] *The Law Enforcement (Covert Surveillance Procedures) Order*, Executive Order No. 1 of 2005, S.S. No. 5 to Gazette No. 31/2005, https://www.gld.gov.hk/egazette/pdf/20050931/es5200509312.pdf.
[59] Hong Kong Government, *CE speaks on Law Enforcement (Covert Surveillance Procedures) Order* (Aug. 6, 2005), https://www.info.gov.hk/gia/general/200508/06/08060147.htm.
[60] *See supra* note 58, at s. 3.
[61] *See supra* note 58, at s. 17.
[62] Young, *supra* note 37, at 266.
[63] *See supra* note 58, at s. 2(1).
[64] *See supra* note 58, at s. 2(1).

recognizance as represented in the aforementioned cases, which were cited by the Legislative Council Panel on Security when introducing the Order.[65]

Despite the apparent plan for the Order to be temporary in nature, it was quickly subject to judicial review. Two applicants – both political activists who believed they were subject to government monitoring in various forms – sought to challenge the "legislative and administrative framework authorising and regulating secret surveillance in all its forms."[66] As a result, the court considered the constitutionality of not only the Order but also § 33 of the TO.[67] The essential claim against the Order was that, since it was not legislation, it could not constitute "legal procedures" within the meaning of Art. 30 of the Basic Law.[68] The applicants then argued that the entire framework of the TO regarding executive authorization for intercepts was not substantively compatible with Art. 30.[69] Handing down his decision in February 2006, Judge Hartmann of the Court of First Instance agreed with the substance of these two arguments.[70] He found that while the Chief Executive was free to issue executive orders containing administrative procedures governing the behaviour of public servants, including staff of the ICAC, they could not be classed as "legal procedures" for the purposes of restricting a constitutional right guaranteed by the Basic Law.[71] To do so would substantially derogate from the protection a right was supposed to offer.[72]

Further, Judge Hartmann stated that while the Art. 30 communications privacy right was not absolute, any restriction had to meet the standard of "legal certainty" or precision such that individuals could accurately govern their behaviour under the law.

> Section 33 has not been formulated with sufficient precision to enable Hong Kong residents, with legal advice if necessary, to foresee to a degree that is reasonable in the circumstances the consequences of any telecommunication intercourse they may have with others even if those consequences may not be foreseeable with absolute certainty.[73]

---

[65] Legislative Council Panel on Security, *Law Enforcement (Covert Surveillance Procedures) Order*, LC Paper No. CB(2)2419/04-05(01) (Aug 5. 2005) at 3, https://www.legco.gov.hk/yr04-05/english/panels/se/papers/se0815cb2-2419-1e.pdf.

[66] *See Leung Kwok Hung & Anor v Chief Executive of the HKSAR*, [2006] H.K.C.F.I. 123, 3.

[67] *See Id.*

[68] *Id.* at 12-20.

[69] *Id.* at 21-26.

[70] He rejected a third argument, however, that the Chief Executive was legally obliged to bring into effect the IOCO. *Id.* at 35.

[71] *Id*. at 149.

[72] *Leung Kwok Hung & Anor v. Chief Executive of the HKSAR*, [2006] HKCU 230.

[73] *Id.* at 133-134.

As a result, the intercept regime created by § 33 of the TO failed to meet constitutional muster.[74] Recognizing the harm that could befall Hong Kong should there be *no* ability for law enforcement agencies to conduct covert surveillance, however, Hartmann J. ordered that the existing scheme be granted a "temporary validity" period of six months, to allow the Government to bring in more comprehensive legislation.[75]

In March 2006, one month after this finding, the LRC issued its second report on covert surveillance which proposed to regulate activities by both state and non-state actors.[76] Shortly thereafter the Court of Appeal in May 2006[77] and Court of Final Appeal (CFA) in July 2006[78] dealt with various appeals and cross-appeals regarding the meaning of "legal procedures" and the appropriateness of the so-called "temporary validity order" as a remedy,[79] but there was no appeal of the central holding regarding the unconstitutionality of § 33. At the CFA, Justice Bokhary made clear that covert surveillance and the interception of communications was not inherently unconstitutional, but that an adequate balance needed to be struck between the needs of law enforcement and other societal interests:

> By its nature covert surveillance involving the interception of communications impacts upon the privacy of the communications which are intercepted. And the knock-on effect of that is an impact upon freedom of communication, too. For it is only natural that even law-abiding persons will sometimes feel inhibited in communicating at all if they cannot do so with privacy. Nevertheless covert surveillance is an important tool in the detection and prevention of crime and threats to public security i.e., the

[74] *Id.* at 127.
[75] *Id.* at 185-186.
[76] Law Reform Comm'n of H.K., *Privacy: The Regulation of Covert Surveillance* (2006) https://www.hkreform.gov.hk/en/docs/rsurveillance-e.pdf ("The 2006 Report"). This report did not consider the issue of the interception of communications, other than to note that the LRC had previously issued "final recommendations" in its 1996 Report on the subject, *infra (missing note and page information)*, including a requirement for judicial authorization. The 2006 Report was ambitious, proposing to regulate surveillance activities by both state and non-state actors. It sought to criminalize activities by private citizens that could be interpreted as placing others under covert surveillance as well as create a constitutionally acceptable regulatory framework governing covert surveillance by law enforcement. This framework required the issuance of judicial warrants or departmental authorisation, depending on context; proposed detailed rules regarding the admissibility of evidence gathered by such surveillance; suggested the creation of an independent supervisory authority; and outlined a requirement for annual public report on covert surveillance activities undertaken.
[77] *Leung Kwok Hung & Anor v. Chief Executive of the HKSAR*, [2006] H.K.E.C. 816.
[78] *Koo Sze Yiu & Anor v. Chief Executive of the HKSAR*, [2006] H.K.L.R.D. 455.
[79] *See generally* Johannes Chan, *Some Reflections on Remedies in Administrative Law* 39 H.K.L.J. 321, 3-5 (2009).

> safety that the public is entitled to enjoy in a free and well-ordered society. The position reached upon a proper balance of the rival considerations is that covert surveillance is not to be prohibited but is to be controlled.[80]

This meant that the government would have to develop new legislation governing the interception of communications and surveillance with sufficiently precise and clear legal procedures for the authorization in order for the law to be consistent with the Art. 30 right. The result was the introduction in August 2006[81] of the Interception of Communications and Surveillance Ordinance ("ICSO").[82]

II. THE INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE SCHEME

The ICSO separates the interception of communications and covert surveillance as distinct activities and divides the latter into two forms.[83] "Interception" is defined as the inspection of the "content" of communications "in the course" of transmission.[84] "Type 2" covert surveillance is that carried out through optical or listening devices on someone whom the target might reasonably expect to be able to hear or see them. For example, the use of a wire to record a conversation between a target and an informant would be "type 2" covert surveillance.[85] Type 2 can also involve the use of tracking devices providing there is no entry into private premises without permission or interference with any object —for example, a GPS tracker attached to a car. "Type 1" is any other form of covert surveillance, such as the placing of a recording device inside someone's home, or the installation of a backdoor allowing remote access into a target's computer.[86]

---

[80] *See supra* note 78, at 3.

[81] The urgency with which the Legislative Council adopted the new law is notable – there was clearly a concern that law enforcement agencies would be dramatically weakened if the government failed to act within the six-month window granted to them by the courts.

[82] ICSO, *supra* note 5.

[83] ICSO, *supra* note 5, at § 2.

[84] ICSO, *supra* note 5. "In the course" refers to activities such as monitoring real-time telephone conversations or opening postal documents in transit. Once the transmission has ceased (that is, the information has reached its destination), then conventional search and seizure rules apply. The Court of Appeal has held that the warrantless search of the content of mobile phones seized incidental to arrest may be acceptable in limited scenarios, such as where it is immediately necessary to preserve information related to the arrest or to protect those at the scene; outside such scenarios, a warrant is required to obtain information off an electronic device *See Sham Wing Kan v. Commissioner of Police*, [2020] H.K.C.A., at 186.

[85] *See* ICSO, *supra* note 5.

[86] *See* ICSO, *supra* note 5.

Any type 2 surveillance that is likely to result in the acquisition of legally privileged material is automatically re-classed as type 1.[87]

The ICSO treats the interception of communications and type 1 surveillance as more serious intrusions, and so requires judicial authorization for them.[88] An application may be made for authorization to one of a specific list of judges ("panel judges"), drawn from the Court of First Instance and appointed for a period of three years by the Chief Executive on the recommendation of the Chief Justice.[89] The application for authorization must include an affidavit stating the purpose of the interception or surveillance, the method, the proposed duration, the likely benefits, an assessment of the impact upon third parties, and the reason the purpose cannot be reasonably furthered by less intrusive means.[90] A judge shall not approve an application for authorization unless they are satisfied the purpose is for the prevention or detection of serious crime or protecting public security, that there is a reasonable suspicion that the target is connected to those matters, and that the interception or surveillance is proportionate.[91] The introduction of the judicial authorization component is perhaps the most significant aspect of the ICSO and, as will later be shown, one of the key points of divergence from the new scheme introduced under the NSL. Judicial authorization for communications intercepts or covert surveillance serves the same principle as a judicial warrant in cases of search and seizure: a bulwark against overly intrusive state action, even though said action furthers a legitimate aim.[92]

Type 2 surveillance is treated under the ICSO as less serious, and so requires only "executive authorization" for approval.[93] Such authorization requires the provision of the same information as required for a judicial authorization but is made not by a judge but by a departmental "authorizing officer".[94] The head of the

[87] *See* ICSO, *supra* note 5. The Law Reform Commission recommended in its 2006 Report (*supra* note 75) that judicial warrants be mandatory for any surveillance operation regardless of form where confidential journalistic material or highly sensitive personal data was likely to be acquired. The ICSO does not do the same but does require that the probability that journalistic material will be acquired be identified in the application for either a judicial warrant or executive authorization. The Code of Practice (*infra* p. 15 and note 98) further requires law enforcement agencies to report to the Commissioner any situation in which they do happen to come across such material.
[88] ICSO, *supra* note 5.
[89] ICSO, *supra* note 5, at § 6.
[90] ICSO, *supra* note 5, at Schedule 3.
[91] ICSO, *supra* note 5, at § 3, 9(2)
[92] *Attorney General of Jamaica v. Williams*, [1998] AC 351, 358F-G, per Hoffman LJ (cited in *Keen Lloyd Holdings Ltd & Ors v. Commissioner of Customs & Excise & Anor* [2016] H.K.C.A. 150, 74.
[93] ICSO, *supra* note 5, at § 14.
[94] ICSO, *supra* note 5, at § 14-15.

department can assign that role to any officer of rank equivalent to or higher than a senior superintendent of police.[95] The authorizing officer is only to approve the request if they are satisfied the same proportionality requirements described above are established.[96] Authorizing officers may also entertain "emergency" applications for type 1 surveillance or interception of communications where there is an immediate need, such as to prevent a serious harm to person, damage to property, threat to public security, or loss of vital evidence, and it is not reasonably practicable to apply for judicial authorization.[97] Application for judicial authorization must still be made within 48 hours of an emergency authorization being granted and repeat emergency authorizations are not allowed.[98] The Secretary of Security has issued a Code of Practice ("CoP") for officers in law enforcement agencies tasked with following these rules,[99]however, any failure to follow that Code does not affect the validity of a prescribed authorization.[100]

The ICSO also created the office of the Commissioner on Interception of Communications and Surveillance.[101] The Commissioner is to be appointed for a term of three years by the Chief Executive on the recommendation of the Chief Justice and drawn from either the current or former members of the Court of First Instance or the Court of Appeal, or former members of the Court of Final Appeal.[102] The Commissioner is to review the operation of the ICSO generally and compliance by departments as they consider necessary; this includes reviewing all applications made for emergency authorizations, renewed authorizations, and any reports received from departments regarding potential non-compliance by their officers.[103] The CoP requires that departments offer assistance to the Commissioner in performing their oversight duties. This practice currently involves submitting weekly reports on all requested and ongoing prescribed authorizations.[104]

The Commissioner is to produce an Annual Report to the Chief Executive detailing statistics of all applications and authorizations, any instances of non-compliance by departments, and any instances in which disciplinary action was

[95] ICSO, *supra* note 5, at § 7.
[96] ICSO, *supra* note 5, at § 3, 15(2).
[97] ICSO, *supra* note 5, at § 20.
[98] ICSO, *supra* note 5, at 23(3).
[99] ICSO, *supra* note 5, at § 63. *See generally* Code of Practice Issued Pursuant to Section 63 of the Interception of Communications and Surveillance Ordinance, (2016) Cap. 589 (H.K.), https://www.sb.gov.hk/eng/special/sciocs/2016/ICSOCoP-June2016E.pdf. [hereinafter CoP].
[100] ICSO, *supra* note 5, at § 63(5).
[101] ICSO, *supra* note 5, at § 39.
[102] ICSO, *supra* note 5, at § 40.
[103] ICSO, *supra* note 5, at § 41.
[104] CoP § 147; A.R. Suffiad, OFF. OF THE COMM'R ON INTERCEPTION OF COMMC'N AND SURVEILLANCE, ANN. REP. 2019 TO THE CHIEF EXEC. 11-12 (2020), https://www.sciocs.gov.hk/en/pdf/Annual_Report_2019.pdf.

taken for such non-compliance.[105] These reports are publicly available.[106] In the reports, the Commissioner may also make recommendations to the Secretary of Security on updating the CoP[107] and make recommendations to individual departments on ways to improve compliance.[108] The Commissioner may also hear public complaints from individuals who believe they have been placed under covert surveillance or had their communications intercepted in a way inconsistent with the ICSO and may make awards of compensation if they believe the terms of the law have been breached.[109]

Without doubt, the ICSO provides for more robust regulation of the interception of communications and covert surveillance than § 33 of the TO and the Order. In addition to establishing clear standards that must be met for authorization of relevant intercept and surveillance activities, the ICSO creates a system of meaningful oversight to which the public has access. At the same time, the ICSO is imperfect and has been criticized on a number of grounds. In particular, it seeks only to regulate the behaviour of public actors.[110]

The narrowness of the law goes beyond those subject to its terms, however. As noted, the interception provisions apply only to "content" of a message in "the course of transmission."[111] This has at least two consequences. First, it completely excludes metadata from the ambit of the law, meaning law enforcement agencies are free to try and build out a picture of communication networks between contacts

[105] ICSO, *supra* note 5, at § 49

[106] All such reports produced since the inception of the ICSO are available at "Annual Reports", Secretariat of the Commissioner on Interception of Communications and Surveillance, https://www.sciocs.gov.hk/en/reports.htm.

[107] ICSO, *supra* note 5, at § 51.

[108] ICSO, *supra* note 5, at § 52.

[109] ICSO, *supra* note 5, at § 44.

[110] The Security Bureau argued at the time of the ISCO's introduction that while criminal offences for the interception of communications by private individuals were necessary (in line with the LRC's recommendations in the 2006 Report), they were better left to separate legislation – but no such legislation has ever been introduced. As a result, the ICSO does nothing to regulate the private behaviour of Hong Kong residents in terms of cybercrime, hacking, or doxing. (*See* Urania Chiu, *12 Years On: Implications of the Interception of Communications and Surveillance Ordinance on Fundamental Rights and Freedoms in Hong Kong*, 49 H.K. LAW J. 487, 493-494 (2019). The Hong Kong Bar Association has also criticized the ICSO's focus only on public officers (*see generally* H. K. BAR ASS'N, COMMENTS OF THE BAR ASS'N ON THE INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE, CAP. 589 (2011), available online at: https://www.hkba.org/sites/default/files/20110909.pdf. Kellogg has also criticized the ICSO for not applying to Mainland law enforcement agencies (*see generally* Thomas E. Kellogg, *A Flawed Effort? Legislating on Surveillance in Hong Kong*, H.K.J. (2007)), but it seems implausible that the Government would have drafted a law to apply to Mainland agents that (at least in 2006) would not legally have been operating within Hong Kong.

[111] ICSO, *supra* note 5, at § 2.

with no oversight whatsoever. Second, it means that once a message has been "delivered," a law enforcement agency does not need to seek authorization under the ICSO to obtain it. The Service-Based Operator License that internet and mobile phone service providers must obtain states that they may disclose the information of customers for the prevention or detection of crime.[112] It appears as though they regularly agree to provide such information on request from the police, meaning the ICSO's interception provisions are likely of reduced relevance in the context of instantaneous digital communications.[113] Indeed, the Secretary for Security has avoided directly explaining whether law enforcement agencies should seek authorization under ICSO in order to access delivered communications such as emails or instant messages.[114]

The ICSO has also been criticized by several scholars as being predisposed to granting authorizations requests. Kellogg, for example, criticizes the panel judge system as insufficiently distant from the executive branch.[115] But while the appointment power of the Chief Executive regarding the panel judges may raise questions about the separation of powers, those judges are still drawn from the membership of the Court of First Instance and are only appointed upon the recommendation of the Chief Justice.[116] They are not unknown figures plucked out of obscurity by the Chief Executive who might owe some personal loyalty. While one could obviously conceive of a system of judicial appointment further removed from the possible influence of the executive branch, the model established under the ICSO does not appear unduly problematic.

Tsui argues that the ICSO's judicial authorization process itself is inadequate, calling it a "rubber stamp process."[117] He points to statistics that suggest the overwhelming majority of requests made under the ICSO are approved and questions whether making law enforcement agencies jump through procedural hoops makes any practical difference.[118] Certainly, the most recent Annual Reports could be read in a way that lend credence to Tsui's concerns. In 2019, a total of

---

[112] *See generally* Telecommunications Ordinance § 7; *See, e.g.*, Telecommunications Ordinance Sample Unified Carrier Licence, Cap. 106, 4 § 7.1 (H.K.), https://www.coms-auth.hk/filemanager/common/licensing/sample_ucl_licence.pdf.
[113] *See e.g.*, Lokman Tsui, *The coming colonization of Hong Kong cyberspace: government responses to the use of new technologies by the umbrella movement*, 8 CHINESE J. OF COMMC'N 1 447, 450 (2015); Stuart Hargreaves, *Online Monitoring of 'Localists' in Hong Kong: A Return to Political Policing?* 15 SURVEILLANCE AND SOC'Y 425, 427 (2017); Chiu, *supra* note 110, at 502.
[114] Legislative Council Press Release LCQ15, A question by the Hon Kenneth Leung and a written reply by the Secretary for Security, Mr. Lai Tung-kwok, in the Legislative Council (Apr. 29, 2015 HKT 15:23), http://www.info.gov.hk/gia/general/201504/29/P201504290534.htm.
[115] Kellogg, *supra* note 110, at 4.
[116] ICSO, *supra* note 5, at § 6.
[117] Tsui, *supra* note 113, at 450.
[118] Tsui, *supra* note 113, at 450.

1335 prescribed authorizations were issued: 1,310 for interception, 22 for type 1, and three for type 2.[119] Only four applications (0.3%) were refused, all for interception.[120] In 2018, a total of 1,378 prescribed authorizations were issued: 1,337 for interception, 41 for type 1, and none for type 2. Only six applications (0.4%) were refused, all for interception.[121] On the one hand, these kinds of statistics might indeed mean that obtaining a judicial authorization is a relatively straightforward process for law enforcement.

However, they could also be interpreted in a different light. For example, they might represent improved knowledge on the part of law enforcement agencies as to what kind of applications are likely to be approved and the form in which they must be presented. After all, in the law's first year of operation, 2006, 11% of applications were refused, but that number quickly dropped.[122] It seems more plausible that law enforcement agencies changed their approach after failure to obtain authorizations than that panel judges all suddenly decided to lower their standards. The Annual Reports also do not reveal to what extent panel judges or those involved in the initial drafting of authorization requests push back on the demands of law enforcement agencies. It seems reasonable to assume that panel judges take the proportionality question seriously as it is a well understood principle in Hong Kong law. While it is fair to note that the judiciary seems on the whole to be relatively deferential to government interests as compared to their counterparts in other jurisdictions,[123] it would be strange to think panel judges simply accept any law enforcement request with which they are presented, without seriously considering its implications. While acknowledging much of this is speculative, it does seem probable that the presence of the panel judges means authorization requests are drafted in narrower terms than would otherwise be the case.[124]

Chiu critiques the oversight process from a different angle, contending that the supervision of law enforcement agencies in terms of their compliance with the ICSO remains lax. She argues that where complaints are brought to the Commissioner the result is typically that failures to comply with the procedures are

[119] Suffiad, *supra* note 104, at 6.
[120] Suffiad, *supra* note 104, at 6.
[121] Suffiad, *supra* note 104, at 6.
[122] For comparison, in the law's first year of operation (2006) 11% of applications were refused, but that number quickly dropped (1.8% in 2007, 1.4% in 2008, etc). *See* Suffiad, *supra* note 104, at 6.
[123] *See, e.g.*, Rehan Abeyratne, *More Structure, More Deference: Proportionality in Hong Kong* PROPORTIONALITY IN ASIA Po Jen Yap ed., (2020).
[124] Young shows the Reports have described attempts by law enforcement to minimize scrutiny from the Commissioner and opposition to orders from the panel judges, again suggesting that both serve to constrain the wishes of law enforcement agencies; *see* Simon NM Young, Prosecuting Bribery in Hong Kong's Human Rights Environment, 272, MODERN BRIBERY LAW: COMPARATIVE PERSPECTIVES (Jeremy Horder J and Peter Alldridge eds., 2013).

considered to be "honest mistakes."[125] Chiu is right that a more confrontational approach from the Commissioner might improve departmental level compliance at a procedural level, but in my view the most valuable aspect of the Commissioner's oversight role comes in the publication of the Annual Reports. While not always providing a complete picture, those reports mean the public and the media have *some* window into law enforcement intercept or covert surveillance operations that they otherwise would simply not have. This is an important form of oversight that exists beyond bare procedural compliance. Young notes, for example, that in the context of the operations of the ICAC, the Commissioner's Annual Reports helped increase public awareness and generate pressure on the ICAC to reform some of its practices.[126]

Greenleaf generally sees the ICSO in a positive light, concluding it has resulted in "a relatively high degree of accountability and transparency" in the conduct of covert surveillance and interception operations by law enforcement.[127] The courts seem to take the same view and have treated the basic approach to authorization under the law with approval. The Court of Appeal, for instance, has found that the executive authorization scheme for type 2 surveillance is a constitutionally justifiable limitation on the Art. 30 privacy right:

> When the justification for the measure is taken together with the after-the-event judicial supervision safeguards that are in place and regard is also had to the fact that the executive authorization only permits low levels of intrusiveness into the privacy rights of others, we are of the view that the measure of executive authorization is one that cannot be said to be manifestly without reasonable foundation. The use of executive authorizations for Type 2 surveillance is, therefore, constitutional.[128]

In addition, though it has not heard a direct challenge to the ICSO's authorization scheme for more intrusive type 1 surveillance or interception, the CFA has spoken in a general sense about the validity of the overall framework, arguing it "provides the machinery and framework for striking [the] balance" between law enforcement interests and the privacy of communications.[129] On the heels of ongoing and often violent civil unrest on the streets of Hong Kong in 2019,

---

[125] Chiu, *supra* note 110, at 496.
[126] Young, *supra* note 124, at 269-272.
[127] *See* Graham Greenleaf, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in Light of Technological Developments: Country Study B.3 – Hong Kong*, European Commission Directorate-General Justice, Freedom, and Security (May 2010).
[128] *HKSAR v. Yu Lik Wai William & Anor*, [2019] H.K.C.A. 135, 286.
[129] *Ho Man Kong v. Superintendent of Lai Chi Kok Reception Centre*, [2014] H.E.C. 424, 7 (per Ribeiro PJ). The cited passage is obiter; in *Ho Man Kong* the CFA concluded that Art. 30 of the Basic Law did not render intercepts of communications obtained in foreign jurisdictions inadmissible as evidence in extradition proceedings in Hong Kong.

a spanner was thrown into this machinery in the form of the National Security Law (NSL).

III. THE NATIONAL SECURITY LAW SCHEME

On May 28, 2020, the National People's Congress ("NPC") authorized its Standing Committee ("NPCSC") to draft and pass a law for Hong Kong aimed at preventing a range of acts it considered harmful to China's national security and/or territorial integrity.[130] The resulting law, the NSL, was adopted on June 30, 2020, and inserted into Annex III of the Basic Law, coming into force in Hong Kong immediately after promulgation by the Chief Executive. The substance of the law has been well considered elsewhere,[131] and this article focuses only on a single element: Art. 43. which deals with the powers of a newly established Department for Safeguarding National Security within the Hong Kong police force.[132] It provides that in addition to all pre-existing powers law enforcement bodies have, this Department may take further measures when investigating matters of national security, including "upon approval of the Chief Executive, carrying out interception of communications and conducting covert surveillance on a person who is suspected, on reasonable grounds, of having [been] involved in the commission of an offence endangering national security."[133]

Art. 43 further gives the Chief Executive, working in conjunction with a new National Security Committee,[134] the authority to make procedural rules that explain in more detail how such interception or surveillance will be approved. Relevant rules came into force on July 7, 2020.[135] In the following discussion, I will explain the key elements of the new scheme and note in particular where it diverges from the ISCO. The two most significant changes are the removal of the

---

[130] Decision on Establishing and Improving the Legal System and Enforcement Mechanisms for the Hong Kong Special Administrative Region to Safeguard National Security, Adopted at the Third Session of the Thirteenth National People's Congress (May 28, 2020), https://www.elegislation.gov.hk/hk/A215.

[131] *See, e.g.,* Cora Chan, *Can Hong Kong remain a liberal enclave within China? Analysis of the Hong Kong National Security Law*, PUBLIC LAW 271 (Mar. 15, 2021)); Simon NM Young, *The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region* 60 INTERNATIONAL LEGAL MATERIALS 1 (2021); Han Zhu, *The Hong Kong National Security Law: The Shifted Groundnorm of Hong Kong's Legal Order and Its Implications,* University of Hong Kong Faculty of Law Research Paper, (2021), https://ssrn.com/abstract=3812146.

[132] This department is established by virtue of Art. 16 of the NSL.

[133] *National Security Law*, at Art. 43(6), at 20.

[134] This committee is established by virtue of Art. 12 of the NSL.

[135] Comm. For Safeguarding Nat'l Sec. of the H.K. Special Admin. [HKSAR], Implementation Rules for Article 43 of the Law of the People's Republic of China, A406A (July 7, 2020), https://www.elegislation.gov.hk/hk/A406A!en.

judicial authorization scheme and the reduction in mechanisms of external oversight.

The Art. 43 Implementation Rules (the "Implementation Rules") state that an authorization for the interception of communications or covert surveillance made under Art. 43 will only be granted for the purpose of preventing or detecting offences endangering national security or protecting national security. This means for non-national security crimes the ICSO remains the relevant law. For an authorization to be granted under Art. 43, the Implementation Rules hold that there must be a reasonable suspicion the target is involved in those offences or an activity that may constitute a threat to national security and the interception or surveillance must be necessary and proportionate in terms of the balance between the purpose and its intrusiveness, both in terms of intrusiveness on the target and third parties.[136] The language here largely mirrors that found in the ISCO, with alterations to refer to national security rather than serious crime or public security.[137] The definitions of interception and covert surveillance, including the difference between type 1 and type 2, bear the same meanings in the Implementation Rules as they do in the ICSO.[138] The Implementation Rules stipulate that a set of Operating Guidelines are to be issued to the police regarding matters that fall under the NSL.[139] This parallels the requirement in the ICSO for the Secretary for Security to develop a Code of Practice for implementation.[140] As with the Code, while officers must comply with the Operating Guidelines a failure to do so will not affect the validity of any authorization and no criminal or civil liability will be incurred as a result.[141]

The Implementation Rules also define two modes of authorization, but there are significant differences in their substance in comparison to those under the ICSO. Under the first mode, an officer within the National Security Department of the police may apply in writing to the Chief Executive for the authorization of interception, type 1, or type 2 surveillance.[142] This essentially replaces the judicial authorization process established under the ICSO, which was limited to interception and type 1 surveillance. The application must contain a description of

[136] *Id.* at Schedule 6 § 2.
[137] ICSO, *supra* note 5, at § 3.
[138] ICSO, *supra* note 5, at § 2; *See* the Implementation Rules, *supra* note 135, at Schedule 6 § 27.
[139] *See* The Implementation Rules, *supra* note 135, at Schedule 6 § 20. An initial set of Guidelines were issued in July 2020. Secretary for Sec., Operating Principles and Guidelines for Application for Authorization to Conduct Interception and Covert Surveillance Issued Pursuant to Section 20 of Schedule 6 of the Implementation Rules for Article 43 of the of the People's Republic of China for on Safeguarding National Security in the Hong Kong Special Administrative Region, G.N. (E.) 74 (July 6, 2020) https://www.gld.gov.hk/egazette/pdf/20202450e/egn2020245074.pdf ["The Operating Guidelines"].
[140] *See* ICSO, *supra* note 5, at § 63, 65.
[141] *See* the Implementation Rules, *supra* note 135, at Schedule 6 §§ 20(3), 21.
[142] The Implementation Rules, *supra* note 135, at Schedule 6 §§ 3, 4(1).

the form of interception or surveillance, its purpose, the likely benefits, the proposed duration, the likelihood of privileged or journalistic material being obtained, and other similar information.[143] This mirrors the content of similar applications made under the ICSO,[144] though of course, the identity of the ultimate decision-maker is different as it is the Chief Executive rather than a panel judge.

Under the Implementation Rules, a second mode of authorization replaces the "executive authorization" scheme found in the ICSO. The Chief Executive may designate a "directorate officer" to review applications for and authorize type 2 surveillance.[145] This appears to create a slightly higher threshold, since a directorate officer is defined in the Implementation Rules as a police officer "not below the rank of chief superintendent of police."[146] In contrast, an authorizing officer under the ICSO need only be of a rank equivalent to that of a senior superintendent, which is one rank below that of a chief superintendent.[147] The content of the necessary written application is otherwise similar to that found in the ICSO, dealing with purpose, proposed duration, proportionality, etc.[148] The Operating Guidelines indicate that notwithstanding the form of surveillance being type 2, if there is a likelihood that journalistic material will be obtained as a result then the application ought to be made to the Chief Executive rather than the directorate officer.[149]

The requirements for renewing authorizations are the same under both the ICSO and the Implementation Rules, including stating whether there has been any significant change to information previously supplied, why a renewal is necessary, and the value of information obtained so far.[150] However, while both initial and renewed authorizations made under the Implementation Rules can last a maximum of six months,[151] under the ICSO they can only last for three months.[152] On the other hand, since both frameworks allow for indefinite repeated renewals the practical difference may be minimal.

A further similarity deals with emergency applications. Under the Implementation Rules, emergency applications for communication intercepts and

---

[143] *See* the Implementation Rules, *supra* note 135, at Schedule 6 §§ 23, 24.
[144] ICSO, *supra* note 5, at Schedule 3, Part 1 and 2.
[145] The Implementation Rules, *supra* note 135, at Schedule 6, § 5.
[146] The Implementation Rules, *supra* note 135, at Schedule 6, § 27.
[147] ICSO, *supra* note 5, at § 7; *See also Organization Structure: Organization Chart of HKPF*, HONG KONG POLICE FORCE, https://www.police.gov.hk/ppp_en/01_about_us/os_chart.html.
[148] *See* The Implementation Rules, *supra* note 135, at Schedule 6 §§ 5(2), 24; *See also* ICSO, *supra* note 5, at § 14(1), Schedule 3 Part 3.
[149] *See* The Operating Guidelines, *supra* note 139, at § 12.
[150] *See* The Implementation Rules, *supra* note 135, at §§ 6, 7; *See also* ICSO, *supra* note 5, at §§ 11, 17.
[151] *See* The Implementation Rules, *supra* note 135, at §§ 6(4), 7(4).
[152] ICSO, *supra* note 5, at §§ 13, 19.

type 1 surveillance may be made to the Commissioner of Police instead of the Chief Executive[153] on the same grounds that an emergency application may be made under the ICSO to a department head instead of to a panel judge.[154] Both specify a 48-hour time limit for any emergency authorization that is granted, both provide that it cannot be renewed by the same emergency process,[155] and both require a written follow-up application within 48 hours to the proper authorizing figure.[156] The Operating Guidelines indicate that failure to make a written application within the 48-hour period must be reported to the National Security Committee, whereas a similar failure under the ICSO would be reported to the Commissioner.[157]

The Implementation Rules and the ICSO are identical in terms of the specific matters that a Chief Executive or panel judge can authorize, such as the forced entry into premises to install devices.[158] They are also broadly similar in describing specific matters that cannot be authorized. Both, for instance, state that authorization to intercept the communications of a lawyer or place their offices under covert surveillance will not be granted unless "exceptional circumstances" exist.[159] The Operating Guidelines make clear that if legally protected products are likely to be obtained by proposed surveillance, then authorization must be personally obtained from the Chief Executive even if the form of covert surveillance to be undertaken is type 2.[160] While only a guideline rather than part of the Implementation Rules directly, this mirrors the principle found in the ICSO.[161] There is, however, one curious difference between the two schemes in matters that cannot be authorized. The ICSO explicitly states that "for the avoidance of doubt, a prescribed authorization does not authorize any device to be implanted in, or administered to" a person without the consent of that person.[162] The Implementation Rules contain no such prohibition.

---

[153] *See* The Implementation Rules, *supra* note 135, at § 9.
[154] ICSO, *supra* note 5, at § 20.
[155] *See* The Implementation Rules, *supra* note 135, at § 9(3)-(4); *See also* ICSO, *supra* note 5, at § 22(1)-(2).
[156] *See* The Implementation Rules, *supra* note 135, at § 10(1)*; See also* ICSO, *supra* note 5, at § 23(1).
[157] *See* The Operating Guidelines, *supra* note 139, at § 21*; See also* CoP, *supra* note 98, at § 2.
[158] *See* The Implementation Rules, *supra* note 135, at Schedule 6 § 8; *See also* ICSO, *supra* note 5, at § 30.
[159] *See* The Implementation Rules, *supra* note 135, at Schedule 6 § 13; *See also* ICSO, *supra* note 5, at § 31. Such circumstances under the Implementation Rules are reasonable grounds to believe the lawyer in question is a party to an activity that constitutes a national security offence or other threat to national security; under ICSO they are that the lawyer is a party to any activity that constitutes a serious crime or threat to public safety. These are essentially parallel grounds, given the nature of the offences that the two schemes are aimed at detecting, disrupting, or prosecuting.
[160] *See* The Operating Guidelines, *supra* note 139, at § 24.
[161] ICSO, *supra* note 5, at § 2(3).
[162] ISCO, *supra* note 5, at § 31(3).

Some relatively similar *post facto* protections for intercept products exist across the schemes. Under the ICSO, it is the responsibility of the head of department to ensure minimum disclosure of any protected product, protection against its unauthorized access or processing, and procedures for its ultimate destruction.[163] Under the Implementation Rules, these same responsibilities fall to the Commissioner of Police.[164] Both the Implementation Rules and the ICSO treat interception products as inadmissible as evidence other than to prove a relevant offence has been committed.[165] Any such product "must not," per the Implementation Rules, or "shall not," per the ICSO, be made available to any party to proceedings, other than proceedings instituted for the relevant offence.[166]

However, unlike the ICSO the Implementation Rules does not place a duty upon law enforcement agencies to disclose information obtained through a prescribed authorization that may undermine the case for the prosecution to the prosecution, nor a duty upon the prosecution to disclose that information to the judge.[167] Interestingly, though still contained in the text of the ICSO, this provision was found unconstitutional in *Yu Lik Wai William* on the grounds that it was a disproportionate restriction on the right to a fair trial, as it allowed the police to decide if the information should be disclosed or not.[168] The Court chose to offer a remedial interpretation of the relevant provision such that *any* information obtained pursuant to a prescribed authorization must be provided to the prosecution, and in turn the prosecution is obliged to disclose the information to a judge in an *ex parte* hearing should they believe it might reasonably be considered capable of undermining the prosecution or assisting the defence.[169] The Implementation Rules do not adopt this language, nor do they create a disclosure regime of any kind. This suggests it will be up to the National Security Department of the police to determine when to reveal intercept products to the prosecution. Presumably, if such a decision is taken, then the common law disclosure principle will continue to apply to the prosecution. In other words, if the prosecution receives intercept products they reasonably believe may undermine their case, they must disclose them to the court.[170]

---

[163] ICSO, *supra* note 5, at § 59.
[164] *See* The Implementation Rules, *supra* note 135, at Schedule 6 § 16.
[165] *See* The Implementation Rules, *supra* note 135, at § 17(1); *See also* ISCO, *supra* note 5, at § 61(1).
[166] *See* The Implementation Rules, *supra* note 135, at § 17(2); *See also* ICSO, *supra* note 5, § 61(2). The Implementation Rules specifically identify the prosecution as a party, unlike the ICSO.
[167] ICSO, *supra* note 5, at § 61(4).
[168] *HKSAR v. Yu Lik Wai William* [2019] 1 H.K.L.R.D. 1149, 231 (C.A.).
[169] *Id.* at 233, 237-238.
[170] Darryl K. Brown et al., *Evidence Discovery and Disclosure in Common Law Jurisdictions*, in THE OXFORD HANDBOOK OF CRIMINAL PROCESS (Darryl K. Brown et al. eds., 2019).

A key divergence between the Implementation Rules and ICSO regards oversight. Though the Implementation Rules conceive of an "independent person" being appointed by the Chief Executive to "assist" the National Security Committee in its overall supervisory role under Art. 43, who that may be or what the particulars of the role will be is as yet unknown.[171] It appears not to be the Commissioner on Interception of Communications and Surveillance, who goes unmentioned in both the Implementation Rules and the Guidelines. While it is conceivable that the Commissioner might still at least receive an initial complaint from an individual who believes they have been placed under covert surveillance or had their communications intercepted on national security grounds, their involvement seems to end if there is in fact evidence a national security offence is at issue. This means that the Commissioner's formal role in reporting and reviewing surveillance practices appears confined to applications for authorizations made under the ICSO, and they will not be involved in any kind of review of applications made under the Implementation Rules.

This supposition is strengthened by the Operating Guidelines, which indicate that a system to review authorizations and compliance by officers with the overall framework is to be made by the Commissioner of Police,[172] and that system is to be run by an individual of rank not below Assistant Commissioner of Police.[173] There is no requirement that the results of those reviews be revealed to the public. The only system for monitoring compliance of officers is self-reporting by the police of instances of non-compliance to the National Security Committee.[174] Combined with the absence of a robust freedom of information law in Hong Kong,[175] there appears little prospect for even statistical scrutiny of national security related intercepts or surveillance activities by the public or the press.

In sum, while the Implementation Rules share many procedural elements with the ICSO, there is a clear intention to remove non-executive branch bodies from the process of investigating national security offences. This is shown most clearly through the removal of the judicial component of the authorization scheme and the reduction of external oversight. Though applying only to matters related to national security offences, this means the new system appears in part like a return to the pre-ICSO period, creating a detailed procedural system governing

"Presumably", however, because the operation of the NSL makes this uncertain until tested in the courts.

[171] *See* The Implementation Rules, *supra* note 135, at Schedule 6 § 19.

[172] *See* The Operating Guidelines, *supra* note 139, at § 30.

[173] *See* The Operating Guidelines, *supra* note 139, at § 30.

[174] *See* The Operating Guidelines, *supra* note 139, at § 31.

[175] Tim Chi Hang Yu, *Constitutionality on the Code on Access to Information*, 43 HKLJ 189 (2013).

authorizations whilst concentrating ultimate decision-making power over those authorizations in the executive branch.

V. THE NEW SCHEME AS AN EXAMPLE OF THE "TRANSCENDENT" CHIEF EXECUTIVE

While the pre-ICSO scheme was, as noted, ultimately deemed unconstitutional, it is important to be clear on what the courts of Hong Kong have and have not said about it. While the overall framework for interception and surveillance occasioned by § 33 of the TO and the Order was found wanting, the Order itself fell only because as an executive order it could not function as "legal procedures" for the purposes of limiting the Basic Law's guarantee of privacy.[176] No particular analysis of the substance of the Order as a scheme for authorization was made at first instance or on either appeal.[177] The content of the Order itself was therefore never subject to a robust constitutional analysis —only the form of its enactment. While the CFA acknowledged that in a general sense an intercept regime "must sufficiently protect… fundamental rights and freedoms"[178] it was never asked nor did it state whether judicial authorization was necessary to do so.[179] In the ICSO-era, while the Court of Appeal did say in *Yu Lik Wai William* that the ICSO's executive authorization scheme for type 2 surveillance was constitutionally valid, it did not consider whether the same was true for a scheme that provided such authorization for intercepts or type 1 surveillance.[180]

Of course, the new legal order occasioned by the NSL means questions about the constitutionality of the authorization scheme detailed in the Implementation Rules will not be brought before the courts. The NSL excludes the Hong Kong courts from its interpretation,[181] and the CFA conceded in *Lai Chee Ying* that the NSL cannot be reviewed for compatibility with the Basic Law.[182] Since the Implementation Rules derive their authority directly from the NSL and

[176] *Leung Kwok Hung & Anor v HKSAR*, [2006] H.K.C. 123, 132 (C.F.I.).
[177] Hartmann J. did accept that it was "of value as an administrative tool in regulating the internal conduct of law enforcement agencies." *See id.*, at 151.
[178] *Koo Sze Yiu & Another v Chief Executive of the HKSAR*, [2006] 3 H.K.L.R.D. 455, 3 (C.F.A.).
[179] In the context of search and seizure of a home or other premises, the Court of Appeal has found that warrantless searches are only constitutionally permissible in exigent circumstances. *Keen Lloyd Holdings Ltd and others v. Comm'r of Customs and Excise and Another*, [2016] H.K.C.A. 150 (C.A.).
[180] Given the Court of Appeal's focus on the relatively "low level" of intrusiveness occasioned by type 2 surveillance, the implication was that it would not be. *HKSAR v Yu Lik Wai William & Another*, [2019] H.K.C.A. 135, 286 (C.A.).
[181] "The power of interpretation of this Law shall be vested in the Standing Committee of the National People's Congress." NSL, art. 65.
[182] *HKSAR v Lai Chee Ying*, [2021] H.K.C. 3, 35 (C.F.A.).

are "made by the Chief Executive in conjunction with the Committee for Safeguarding National Security,"[183] then it stands to reason that they are not reviewable by the courts either.[184] Nonetheless, it is still worth considering the purpose of the concentration in the executive branch of intercept and covert surveillance authorization power in matters of national security.

The notion of separation of powers in Hong Kong has long been debated.[185] While Deng Xiaoping argued in the 1980s that the doctrine could not apply to Hong Kong's relationship with the rest of China,[186] after the transition of sovereignty it nonetheless seemed that at a sub-national level Hong Kong governance reflected the idea. The Court of Final Appeal stated in key cases that the Basic Law enshrines the concept,[187] that the courts hold the role of being a constitutional check on the government,[188] and the courts have indeed declared various laws to be inconsistent with the Basic Law and therefore invalid since 1997.[189] As recently as 2014, the then-Chief Justice publicly stated that the Basic Law "clearly" sets out the principle of the separation of powers.[190]

As political tensions have risen, there has been increasing pushback against the idea that the doctrine has any application within Hong Kong and the debate has re-emerged as one of popular salience rather than purely academic interest. In particular, there appears to have been significant concern from establishment interests about what the doctrine may imply for Hong Kong's exercise of independent judicial power, which is guaranteed under the Basic Law.[191] In 2014, six months after the Chief Justice's statement referred to above, the State Council issued a White Paper stating that under the "one country, two systems" model, the Central Authorities maintain "overall jurisdiction" and that, in addition to

[183] *See* The Implementation Rules, *supra* note 139, at Preamble.
[184] At least, not reviewable on constitutional grounds. The emerging jurisprudence around the NSL suggests that there may still be some narrow scope for reviewing the application of the law on conventional administrative law grounds; *see Tong Ying Kit v Secretary of Justice* [2021] H.K.C.A. 912 (C.A.), (concluding that prosecutorial decisions in an NSL-related case could theoretically be reviewed, albeit on very narrow grounds).
[185] *See, e.g.*, Danny Gittings, *One Country, Two Stances on Separation of Powers: Tensions over Lack of Parallelism Between the National and Subnational Levels*, 26-27 (2017) http://repository.hku.hk/bitstream/10722/254858/1/Content.pdf.
[186] Deng Xiaoping, *Speech at a Meeting with the Members of the Committee for Drafting the Basic Law of the Hong Kong Special Administrative Region* in DENG XIAOPING ON THE QUESTION OF HONG KONG, 55 (trans., Foreign Language Press 1993).
[187] *Leung Kwok Hung* [2014] H.K.C. 27, 28 & 74 (C.F.A.).
[188] *Ng Ka Ling* [1999] 2 H.K.C.F.A.R. 4 (C.F.A.).
[189] *See, e.g.*, Po Jen Yap, *Constitutional Review under the Basic Law: The Rise, Retreat and Resurgence of Judicial Power in Hong Kong*, 37 HKLJ 44 (2007).
[190] Geoffrey Ma Tao-li, C.J. of the Ct. of Final Appeal, Chief Justice's Speech at the Ceremonial Opening of the Legal Year 2014, (Jan. 13, 2014).
[191] XIANGGANG JIBEN FA, art. 2 & 19 (H.K.).

government administrators, "judges" and "other judicial personnel" had to be "patriots" who must "ensur[e] the long-term stability and prosperity of Hong Kong."[192]

In 2015, the head of the Central Authorities Liaison office in Hong Kong stated that the "non-implementation of the separation of powers" was a "guiding principle" in the drafting of the Basic Law.[193] In 2019, in response to increasing conflict between protestors and the police, the Government relied upon a colonial-era law to declare a situation of "public danger" and enact what became popularly known as the "anti-mask law."[194] In a politically unwelcome finding, the Court of First Instance found that portions of the law were unconstitutional.[195] Despite the fact that the local courts have repeatedly declared legislation to be invalid as a result of an inconsistency with the Basic Law, in response an NPC spokesperson stated that only its Standing Committee had the right to determine the constitutionality of local laws.[196] In 2020 the phrase "separation of powers" was deleted from secondary school textbooks.[197] An Education Bureau webpage that contained a judicially-authored PowerPoint presentation with the phrase was removed.[198] Both the Chief Executive and Central Authorities reiterated that it did not apply in Hong

[192] Info. Off. Of the State Council, the Practice of One Country, Two Systems Policy in the Hong Kong Special Administrative Region, § V (2014). http://english.www.gov.cn/archive/white_paper/2014/08/23/content_281474982986578.htm.
[193] Staff, *Zhang Xiaming's Controversial Speech on Hong Kong Governance: The Full Text*, (S. CHINA MORNING POST, (Sept. 6, 2015) https://www.scmp.com/news/hong-kong/politics/article/1858484/zhang-xiaomings-controversial-speech-hong-kong-governance.
[194] Prohibition on Face Covering Regulation, Cap 241 § 2 (Oct. 5, 2019) (the regulation prohibited the wearing of masks or disguises that could prevent identification at a wide range of public order events, including lawful and peaceful protests).
[195] *Leung Kwok Hung and Sec. for Just. and Chief Exec. in Council*, [2019] H.K.C.F.I. 2820 (Court of First Instance 2019) (the Court of First Instance struck down large parts of the law and also found that the Government's reliance on the colonial-era law for its enactment was itself unconstitutional given the circumstances). .
[196] Huaxia, *NPC spokesperson expresses deep concern over HK court ruling*, XINHUA NET NEWS, (Nov. 19, 2019), http://www.xinhuanet.com/english/2019-11/19/c_138566373.htm. It should be noted however that when the Court of Appeal subsequently upheld the Court of First Instance's decision in part ([2020] HKCA 192), no similar statements were made. It may be that the statement was intended to simply be a reminder that the Standing Committee has the *final* say over interpretation over the meaning of the Basic Law, a well-accepted principle: *see* Basic Law, art. 158 (H.K); *see also Lau Kong Yung v Dir. of Immigr.* FACV No. 10 and 11, 57-58 (1999).
[197] *HK has no separation of powers: education chief*, RTHK ENGLISH NEWS (Aug. 31, 2020), https://news.rthk.hk/rthk/en/component/k2/1547075-20200831.htm.
[198] Kelly Ho, *Hong Kong Education Bureau removes website slide on separation of powers as part of update*, H.K. FREE PRESS, (Sept. 2, 2020), https://hongkongfp.com/2020/09/02/hong-kong-education-bureau-justifies-removal-of-top-judges-slide-on-the-separation-of-powers-as-an-update/.

Kong, arguing that the government is instead "executive-led".[199] The Secretary of Justice said attempts to latch onto the label without understanding it properly were "pathetic" and that the concept had "no place" in Hong Kong's political structure.[200]

That such public statements regarding the non-existence of the doctrine in Hong Kong have suddenly emerged is of course not a random event —they must be understood in the context of the anti-government protests which Beijing ultimately interpreted as a threat to one of its "red lines." For instance, the Hong Kong and Macau Affairs Office, a central body that helps oversee local affairs of the two SARs, stated that those who advocated for the principle of separation of powers were seeking to "undermine the authority of the chief executive and the Hong Kong Special Administrative Region, reject Beijing's comprehensive jurisdiction over Hong Kong… and turn Hong Kong into an independent political entity."[201] The Central Authorities appear concerned that the doctrine cannot be confined to sub-national matters, and that if unopposed could imply that the Hong Kong judiciary has the power to check the actions of the Chinese state itself.[202] Thus, the notion that Hong Kong is an "executive-led" government has been re-asserted.

Certainly, both before and after 1997, Hong Kong's government has been dominated by the executive branch. But what the phrase "executive-led" means is not entirely clear, and it is not obvious that a government cannot simultaneously be "executive-led" and nonetheless reflect the doctrine of separation of powers in certain ways.[203] Intriguingly, the Director of the Liaison Office has advanced one particular understanding that does seem hard to reconcile with a traditional understanding of the separation of powers. He noted that the Basic Law defines the

---

[199] Tony Cheung & Chris Lau, *Hong Kong leader Carrie Lam sides with education chief on no 'separation of powers' in city, defends move to delete phrase from textbook*, S. CHINA MORNING POST, (Sept. 1, 2020), https://www.scmp.com/news/hong-kong/education/article/3099729/hong-kong-leader-carrie-lam-insists-there-no-separation; Ng Kang-chung, *No 'separation of powers' in Hong Kong, Beijing agencies say, adding Deng Xiaoping spelled out stance in 1987*, S. CHINA MORNING POST, (Sept. 8, 2020), https://www.scmp.com/news/hong-kong/politics/article/3100590/no-separation-powers-hong-kong-beijing-agencies-say-adding.

[200] Teresa Cheng, *Why separation of powers has no place in Hong Kong's political structure*, S. CHINA MORNING POST, (Sept. 9, 2020), https://www.scmp.com/comment/opinion/article/3100695/why-separation-powers-has-no-place-hong-kongs-political-structure.

[201] Kang-chung, *supra* note 199.

[202] The Court of Final Appeal has elided this question, noting only that it "cannot question the authority of the National People's Congress or the Standing Committee to do any act which is in accordance with the provisions of the Basic Law and the procedure therein"; *see Ng Ka Ling and Another v Dir. of Immigr.*, [1999] H.K.F.C.A. 81 (C.F.A.).

[203] *See e.g.*, Pui-yin Lo & Albert Chen, *The Judicial Perspective of "Separation of Powers" in the Hong Kong Special Administrative Region of the People's Republic of China*, 5(2) J. OF INT'L & COMPAR. LAW 337 (2018).

Chief Executive as having a dual role as both head of the HKSAR government and as the individual accountable to the Central Authorities.[204] Therefore, he argued, the Chief Executive "transcends" the three branches.[205] The full constitutional implications of this argument are beyond the scope of this paper, but the new intercept and surveillance authorization scheme under the Implementation Rules is likely an early concrete example of what it means in practice. "Transcendence" appears to be a mechanism for more directly asserting central control through local institutions when considered necessary for the advancement of core state interests.

Offences under the NSL by definition deal with matters of national interest, but those matters are still primarily investigated and prosecuted by local bodies: the National Security Department of the Hong Kong police and the Department of Justice.[206] However, given the dual role of the Chief Executive, locating the authorization power in the executive branch rather than the judicial ensures that national interests are prioritized despite this local implementation. While the Implementation Rules still require that the Chief Executive or directorate officer take into account proportionality, the totality of the system seems to greatly favour investigative needs. Under the NSL, the Chief Executive, Commissioner of Police, and head of the police's National Security Department will all be members of the newly-created National Security Committee.[207] It will feature an advisor (who will sit in on all meetings) appointed directly by the Central People's Government (CPG).[208] This Committee will be responsible for, *inter alia*, coordinating operations regarding national security in Hong Kong.[209] Decisions made by this Committee are not subject to any form of judicial review; [210] the Committee is accountable only to the CPG.[211]

Together, these factors suggest a system significantly more predisposed to approve broad requests for intercepts or surveillance in cases that touch on national security concerns than would be the case under the ICSO. As I have suggested, the very existence of the judicial authorization aspect of the ICSO likely results in more narrowly tailored applications, limiting either the targets or the extent of the

[204] XIANGGFANG JIBEN FA, at art. 43.
[205] Staff, *Zhang Xiaoming's controversial speech on Hong Kong governance: full text*, S. CHINA MORNING POST, (Sept. 16, 2015), https://www.scmp.com/news/hong-kong/politics/article/1858484/zhang-xiaomings-controversial-speech-hong-kong-governance.
[206] Simon N.M. Young, *The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region*, 60 INT'L LEGAL MATERIALS, 1 (2021). Articles 55-58 provide that in certain instances cases may be transferred to the Mainland for prosecution, under Mainland law before Mainland courts.
[207] *National Security Law*, at art. 13.
[208] *National Security Law*, at art. 15.
[209] *National Security Law*, at art. 14.
[210] *National Security Law*, at art. 14.
[211] *National Security Law*, at art. 15.

surveillance they are put under. In contrast, the centralization of authorization authority and the accountability of the Chief Executive to the CPG under the concept of transcendence suggests that investigative needs are likely to take significant priority over the privacy rights of either targets or third parties. This tendency will only be magnified thanks to the reduction in mechanisms of external oversight. The public will have no idea as to the extent of surveillance, let alone a say in whether the balance between legitimate concerns about national security and individual privacy is being struck.

CONCLUSION: TIME IS A FLAT CIRCLE

From nearly untrammelled powers for the Governor in the colonial period, to the refusal to adopt the IOCO in 1997, to the failed attempt to introduce some departmental-level controls in 2005, to the ICSO in 2006, and now to Art. 43 of the NSL, the past echoes through the various permutations of the law relating to intercepts and surveillance in Hong Kong. While the relatively detailed provisions contained in the Implementation Rules means that the new regime appears *prima facie* more restrictive than the essentially free hand given to the Governor and later Chief Executive under § 33 of the TO, this paper has suggested the practical difference may not in fact be that significant. In short, the residents of Hong Kong must, to paraphrase the court in *Li Man-tak*, largely depend on the goodwill of the Chief Executive to properly apply the requirements under the Implementation Rules, including proportionality.[212]

While the return to something resembling the pre-2006 model occasioned by the NSL and its Implementation Rules will indeed ease the process of authorizing intercepts and covert surveillance when dealing with matters of national security, that is likely not the only purpose. The new system is also about asserting that regardless of "one country, two systems" and the promise of judicial independence, the dominance of state organs over the local judiciary is unquestioned. It is obviously not a coincidence that the return (in part) to an intercept and surveillance authorization process controlled by the executive branch has come on the heels of the political unrest of recent years. Part of the CPG's response to that unrest has been its assertion of "comprehensive jurisdiction" over Hong Kong. Thanks to its concentration of authorizing authority over interceptions and surveillance in a transcendent Chief Executive with primary accountability to the CPG, the new scheme created by the Implementation Rules serves this jurisdiction. It ensures the primacy of the national interest in authorizations, even though they and the investigations they relate to are still carried out by local bodies. The removal of judicial oversight in the context of authorizations related to national security offences ensures that core state interests are unhampered. This is as much

[212] *HKSAR v. Li Man Tak and Others*, [2005] H.K.E.C. 1308, (C.A.).

as a message to the local judiciary as it is a practical tool that will make authorizations for communications intercepts and the placement of suspects under covert surveillance easier to obtain.