12 Years On: Implications of the Interception of Communications and Surveillance Ordinance on Fundamental Rights and Freedoms in Hong Kong

Urania Chiu*

This article broadly reviews the Interception of Communications and Surveillance Ordinance (ICSO) and judicial decisions on interception and covert surveillance in Hong Kong both before and after the passage of the ICSO, discussing in particular their implications on the right to privacy and the right to fair trial. The author questions whether the ICSO has fulfilled its role as a piece of corrective legislation to the pre-2006 lack of legislative framework for government surveillance activities and addresses concerns about whether further reform is required to better protect fundamental rights and freedoms in the 'digital age'.

1. Introduction

In 2005, controversies regarding the practice of covert surveillance by law enforcement agencies (LEAs) in Hong Kong came to public attention in the form of court cases challenging the lawfulness and admissibility of prosecution evidence obtained by such surveillance or interception of private communications. Concerns about the legality of such evidence led to the issuance of an Executive Order providing for procedures for such practices by the Chief Executive (CE). Subsequently, in *Leung Kwok Hung v Chief Executive of the HKSAR*, the applicants successfully challenged the constitutionality of the existing administrative and legislative framework,[1] and the Interception of Communications and Surveillance Ordinance (ICSO) was enacted by the Government in response in 2006. However, academic commentary about the ICSO and the state of the law after its enactment, especially from a human rights perspective, has been scarce.

* LLB (LSE), LLM in Human Rights (HKU).

[1] *Leung Kwok Hung and another v Chief Executive of the HKSAR* [2006] HKEC 239.

In this paper, I aim to fill that gap in the literature. After setting out the historical background of the regulation of interception and surveillance and the current state of the law in Hong Kong, I look at the implications of the ICSO on fundamental rights and freedoms, in particular the right to privacy and the right to fair trial, highlighting two significant aspects of the law which have been the focus of legislative, public, and judicial discussions, namely the possibility of criminalising unauthorised interception and covert surveillance activities and the admissibility of evidence obtained by means of interception and covert surveillance. Before I conclude, I take note of some challenges presented by today's "digital age" in constraining state surveillance and protecting human rights online and comment on whether and how the ICSO may be able to tackle them.

2. The regulation of interception and surveillance in Hong Kong: a brief history

The first significant piece of legislation pertaining to the interception of communications in Hong Kong was the Interception of Communications Ordinance (ICO), which was passed in June 1997, prompted by the case of *Malone v United Kingdom* [2] and the resulting legislative reform in the area of interception of communications by authorities in the United Kingdom. [3] Intended to be a legal framework for the judicial authorisations of interceptions carried out by law enforcement agents for purposes of the prevention or detection of serious crime or in the interests of security, the ICO was however never put into effect by the executive.

[2] *Malone v the United Kingdom* [1984] ECHR 10.
[3] H. L. Fu and Richard Cullen, "Political Policing in Hong Kong" (2003) 33 HKLJ 199.

As a result, authorities had relied on section 33 of the Telecommunications Ordinance over the next decade for operations requiring the interception of telecommunications. Section 33, as originally enacted, stated that the CE might order the interception of any message or class of messages transmitted via telecommunication whenever they considered the public interest so required. As Hartmann J commented in the *Leung Kwok Hung* case, it was an "open-ended power" not subject to any restrictions or independent oversight.[4] In 2005, two cases challenged the lawfulness of prosecution evidence obtained by the Independent Commission Against Corruption (ICAC) by means of the secret recording of private communications. The first of these was *HKSAR v Li Man Tak and Others*.[5] In this case, although the evidence obtained by covert surveillance was admitted, the judge found that the ICAC's practice of covert surveillance was not in accordance with legal procedures and was thus in breach of article 30 of the Basic Law, which protects the freedom and privacy of communication of Hong Kong residents. He held that the lack of a legislative framework in Hong Kong to regulate covert surveillance meant that "the minimum degree of legal protection to which citizens of Hong Kong are entitled under article 30 of the Basic Law is lacking, i.e. there is a legislative lacuna".[6] Furthermore, the judge warned that if the practice of covert surveillance was continued without any legislative basis, such evidence might not be admitted in the future.[7] In the second case, *HKSAR v Shum Chiu and Others*, the judge stayed the prosecution on the ground that that the ICAC's deliberate secret recording of the conversation between the defendant and his solicitors was a "cynical and flagrant infringement of [his] right

[4] *Leung Kwok Hung* (n 1 above), para 23.
[5] *HKSAR v Li Man Tak and Others* [2005] HKEC 1308.
[6] *ibid*, para 54.
[7] *ibid*, para 67.

to legal professional privilege" and an "affront to the public conscience with severe consequences for public confidence in the administration of justice".[8]

In response to the criticisms targeted at such investigative practices, the CE, pursuant to his powers under article 48 of the Basic Law, published the Law Enforcement (Covert Surveillance Procedure) Order ("the Order") as an interim measure in August 2005, laying down a procedural scheme for law enforcement agents to obtain authorisations from senior officers for covert surveillance, which had to be for a specified purpose and proportionate to that purpose. The safeguards provided by the Order included periodic review by superior officers and internal guidelines specific to the LEA.[9]

Although the executive was adamant that the Order was not law, official statements also asserted that the Order provided the necessary legal procedures for restricting rights under article 30 of the Basic Law. This was questioned by legal scholars such as Young, who argued that the Order could not constitute "legal procedures" under article 30, and that article 30 itself did not confer a power on law enforcement to conduct covert surveillance but instead imposed a requirement for any restriction on the rights guaranteed to be "in accordance with legal procedures".[10] The legality of the Order was successfully challenged in *Leung Kwok Hung v CE*, a case that has been mentioned above. It was held at first instance that, firstly, section 33 of the Telecommunications Ordinance was not sufficiently precise to attain the level of legal certainty required to comply with the "in accordance with legal procedures"

[8] *HKSAR v Shum Chiu and Others* (2005) DCCC 687/2004, paras 33, 36.
[9] Simon N. M. Young, 'The Executive Order on Covert Surveillance: Legality Undercover?' 35 HKLJ 265.
[10] *ibid*.

requirement under article 30 or the "prescribed by law" requirement under article 39 to restrict constitutional rights.[11] Secondly, although the court accepted that the Order did not purport to be legislation and was legitimate as "an administrative tool in regulating the internal conduct of law enforcement agencies", it was not capable of constituting a set of "legal procedures" for the purposes of article 30.[12] Finally, the court granted a temporary validity order to suspend the effect of these declarations for a period of six months for the reason that there would be a "real threat to the rule of law" if LEAs were unable to conduct covert surveillance until corrective legislation could be put in place.[13] The Court of Final Appeal later set aside the temporary validity order and ordered a suspension of the declarations of unconstitutionality for the same time period instead, since, according to the court, the present case was only able to satisfy the lower level of necessity which was required by a suspension,[14] although Chan has argued that there is no practical difference between the two.[15]

The Interception of Communications and Surveillance Ordinance was finally enacted on 9 August 2016 as a result. Under the ICSO, both interception and covert surveillance are prohibited unless authorised as prescribed under the statute.[16] "Interception" means the carrying out of any "intercepting act" in respect of any communication, which is the inspection of the contents of the communication in the course of its transmission by a postal service or telecommunications by a person other than its sender or intended recipient. Covert surveillance means "any surveillance

[11] *Leung Kwok Hung* (n 1 above), paras 133-134.
[12] *Leung Kwok Hung* (n 1 above), para 151.
[13] *Leung Kwok Hung* (n 1 above), para 185.
[14] *Koo Sze Yiu and Another v Chief Executive of the HKSAR* (2006) 9 HKCFAR 441.
[15] Johannes Chan, "Some Reflections on Remedies in Administrative Law" (2009) 39 HKLJ 321.
[16] Interception of Communications and Surveillance Ordinance, ss 4-5.

carried out with the use of any surveillance device for the purposes of a specific investigation or operation" where the subject is entitled to a reasonable expectation of privacy and the surveillance is carried out in a manner to ensure the subject is unaware of it and is likely to result in the obtaining of any private information about the subject. Covert surveillance is further classified into "Type 1" and "Type 2", where Type 2 surveillance means covert surveillance which is carried out with the use of a listening, optical surveillance, or tracking device, and which does not involve entry into any premises without permission, the interference with the interior of any conveyance or object, or electronic interference with the device. Type 1 surveillance is any other form of covert surveillance.[17] For Type 1 surveillance or interception, judicial authorisation is required and provided for under sections 8 to 13. For Type 2 surveillance, executive authorisation is required and provided for under sections 14 to 19. The requirements for issuing, renewing, or continuing these prescribed authorisations are set out under section 3, that the interception or the covert surveillance must be necessary for and proportionate to the purpose of preventing or detecting serious crime or protecting public security.

Additionally, a new role of Commissioner on Interception of Communications and Surveillance ("the Commissioner") is established under section 39, who is responsible for overseeing the compliance of LEAs with the ICSO and who can carry out reviews of cases and examinations of applications by individuals. A Code of Practice has also been issued under section 63, with which law enforcement agents are required to comply.

[17] Interception of Communications and Surveillance Ordinance, s 2(1).

The ICSO was further amended in 2015, incorporating many recommendations made by the first Commissioner Woo Kwok-Hing, including giving more express powers to the Commissioner to inspect protected products of covert operations.[18]

3. The ICSO as a piece of corrective legislation

As can be seen from the previous section, the ICSO was enacted as a piece of corrective legislation directly in response to the *Leung Kwok Hung*/*Koo Sze Yiu* judgment. Its objective, then, is to provide a legal basis for LEAs' interception and covert surveillance operations in order to satisfy firstly, the requirement under article 30 of the Basic Law that authorities may not infringe upon the freedom and privacy of communication of residents except in accordance with legal procedures and to meet the needs of public security or for investigation into criminal offences and secondly, the requirement under article 39 that the "rights and freedoms enjoyed by Hong Kong residents shall not be restricted unless as prescribed by law". In this section, I will discuss the implications of the ICSO on two fundamental rights that are most likely to be engaged, namely the right to privacy and the right to fair trial, and ask whether the ICSO has fulfilled its purpose as a piece of corrective legislation and whether the law should go further to afford better protection to these rights.

The ICSO: providing a legal basis for interception and covert surveillance

[18] Security Bureau, *Legislative Council Brief: Interception of Communications and Surveillance (Amendment) Bill 2015* (4 February 2015).

As Hartmann J summarised in *Leung Kwok Hung*, the Basic Law requires the fundamental right to freely and privately communicate with others to be protected by law in two ways: firstly, "directly" through article 30, which refers specifically to the "freedom and privacy of communication", and secondly, "indirectly" through article 39, which incorporates provisions of the International Covenant on Civil and Political Rights (ICCPR) as applied to Hong Kong. Article 39 of the Basic Law gives constitutional recognition to article 14 of the Hong Kong Bill of Rights, equivalently article 17 of the ICCPR, which refers more broadly to the right against arbitrary or unlawful interference with one's privacy, family, home, or correspondence. The Human Rights Committee has further elaborated on the meaning of "unlawful" and "arbitrary". The prohibition of unlawful interference means that "no interference can take place except in cases envisaged by the law" and the prohibition of arbitrary interference is to "guarantee that even interferences provided for by the law should be in accordance with the provisions, aims and objectives of the Covenant" and should be "reasonable in the particular circumstances".[19] Moreover, the relevant legislation must "specify in detail the precise circumstances in which such interferences may be permitted", and decisions to make use of such authorised interferences must be made on a case-by-case basis by the designated authorities.[20] The Law Reform Commission (LRC) in its 2006 report on covert surveillance, to which the Government referred when drafting the ICSO, also expressed that, in order to satisfy the requirement of legality, the law regulating surveillance activities must be "readily accessible and precise so that individuals will be aware of the circumstances and the

[19] UN Human Rights Committee, "General comment No.16: Article 17 (Right to privacy)" (1988) UN Doc, paras 3-4.
[20] *ibid*, para 8.

conditions under which public authorities may resort to the use of such intrusive powers".[21]

The ICSO has been generally accepted as being able to provide the legal basis required for LEAs' infringement of individuals' right to privacy by way of interception and covert surveillance. In the case of *Ho Man Kong*, for example, Ribeiro PJ stated that courts' role in relation to article 30 of the Basic Law is to "balance the right to privacy of communications against the public interest in protecting public security and in investigating crime", and the ICSO in turn "provides the machinery and framework for striking that balance".[22] Indeed, by providing a detailed legislative framework for LEAs to conduct interception and covert surveillance activities, subject to case-by-case authorisations by designated judges and authorising officers in accordance with the section 3 criteria that the act is necessary for and proportionate to the purpose of preventing or detecting serious crime or protecting public security, the ICSO appears to fully comply with the "in accordance with legal procedures" requirement under article 30 of the Basic Law and the guarantee of protection against arbitrary and unlawful interference under article 17 of the ICCPR.

Having established that the ICSO fulfils its purpose of filling in the "legislative lacuna" that rendered LEAs' covert surveillance and interception practices illegal, I will now turn to analyse some other aspects of the current legal framework which are worth noting in the discussion of human rights in this area of law. Although the ICSO is able

[21] The Law Reform Commission of Hong Kong, *Privacy: The Regulation of Covert Surveillance* (March 2006), para 7.
[22] *Ho Man Kong v Superintendent of Lai Chi Kok Reception Centre and the Commonwealth of Australia* [2014] HKEC 424, para 7.

to provide the legal basis for legitimate interferences of the right to privacy, there are some remaining loose ends that the current law has yet to make provisions for.

Loose ends: a case for more effective protection of fundamental rights?

The right to be protected against arbitrary or unlawful interference with privacy by both public and private bodies

The first notable feature of the ICSO is that, despite the requirements of the relevant constitutional provisions and the LRC's recommendations, it applies only to LEAs including the Customs and Excise Department, the police, the ICAC, and the Immigration Department and does not prohibit or regulate the conduct of private individuals in the area of interception of communications and surveillance.[23] Article 30 of the Basic Law, however, prohibits infringements upon the freedom and privacy of communication by *both* Government departments and individuals. The Human Rights Committee has also stated clearly in the General Comment on article 17 that the article 17 right is required to be "guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons", giving rise to obligations on the part of the state to adopt legislative and other measures to give effect to such protection.[24]

The LRC has made recommendations in relation to both interception of communications and covert surveillance. In its 1996 report, the LRC recommended the creation of a new criminal offence of "intentionally intercepting or interfering with communications", as the main existing legislation regulating interception, section 27

[23] Interception of Communications and Surveillance Ordinance, sch 1.
[24] UN Human Rights Committee (n 19 above), para 1.

of the Telecommunications Ordinance, was seen as too narrow, prohibiting only the interference with telecommunication *equipment* but not *telecommunications* in general.[25] In its 2006 report on covert surveillance, the LRC recommended the creation of two offences of "trespass into private premises with intent to observe, overhear or obtain personal information" and "placing, using, servicing, or removing a sense-enhancing, transmitting or recording device (whether inside or outside private premises) with the intention of obtaining personal information relating to individuals inside the private premises in circumstances where those individuals would be considered to have a reasonable expectation of privacy".[26] Neither of these recommendations was adopted in the Interception of Communications and Surveillance Bill ("the Bill").

In the Legislative Council (LegCo) Brief for the Bill, the Security Bureau explained that the Bill only sought to "provide for the authorization of interception of communications and covert surveillance operations by LEAs" and that it did not apply to non-Government parties or the state.[27] The Security Bureau further justified the decision to not create generally applicable criminal offences, stating that although the Government accepted that there should be protection against the infringement of the right to privacy of communication by both Government and non-Government parties, regulation of the latter should be deferred to a later exercise so that corrective legislation to regulate LEAs' conduct in the area could be enacted as soon as possible.

[25] The Law Reform Commission of Hong Kong, *Privacy: Regulating the Interception of Communications* (December 1996), ch 4.
[26] The Law Reform Commission of Hong Kong (n 21 above), ch 1.
[27] Security Bureau, *Legislative Council Brief: Interception of Communications and Surveillance Bill* (March 2006), para 17.

The decision to enact the ICSO as we know it today, as a piece of legislation mainly to provide LEAs with a legal basis for their interception and surveillance activities, is perhaps understandable given the urgent need for the Government at the time to make new legislation in response to the *Leung Kwok Hung*/*Koo Sze Yiu* judgment within a period of six months. However, almost 12 years after the enactment of the ICSO and after an amendment exercise in 2015, no new legislation has been enacted which attempts to criminalise the interception of communications in general or covert surveillance by private individuals or bodies. When prompted on the question in the LegCo in 2013, the then Secretary for Constitutional and Mainland Affairs Raymond Tam's reply seemed to have backtracked even more from the Government's position in 2006, stating that the Government needed to consider whether the conduct of "non-public officers" should be regulated at all in the area.[28]

Some may argue that there are already a number of existing laws which currently regulate the interception of communications by both public and non-public parties, such as section 27 of the Telecommunications Ordinance, section 29 of the Post Office Ordinance, section 161 of the Crime Ordinance, and the Personal Data (Privacy) Ordinance (PDPO), all of which were suggested by Tam in the same reply.[29] However, these pieces of legislation do not, separately or together, constitute an adequate framework for regulating or criminalising private interception or surveillance. As has been mentioned above, section 27 of the Telecommunications Ordinance suffers from not prohibiting the interception of communications in general but requiring

[28] – "LCQ5: Protection of freedom and privacy of communication of Hong Kong residents", *news.gov.hk*, 3 July 2013. Available at http://www.info.gov.hk/gia/general/201307/03/P201307030382.htm (visited 28 November 2018).
[29] *ibid*.

"damage" or "removal" of or "interference" with a "telecommunications installation". While the Post Office Ordinance does deal with the interception of mail in transmission, it can hardly be said to be relevant to the cases of interception that the ICSO is or any future legislation will be attempting to address, which generally involve the interception of telecommunications. As for section 161 of the Crime Ordinance, the "hacking" offence, which prohibits the access to a computer with various criminal or dishonest purposes, it is clearly distinct from the regulation of interception of communications which is a very specific act of unauthorised inspection of the contents of a communication in the course of its transmission.[30] Finally, while the PDPO obliges data users to follow the prescribed data protection principles in relation to personal data, i.e. data which relates directly or indirectly to a living individual and from which the individual may be identifiable,[31] not all instances of interception and surveillance engage such personal data. For example, the interception of a class of messages may lead to the collection of personal data of some but not all participants of those communications, and those whose personal data are not engaged will fall outside the scope of the PDPO's protection. More importantly, data protection laws and interception/surveillance laws protect two different aspects of the right to privacy. While the PDPO protects personal data that may become the subject of interception or covert surveillance by ensuring that data users collect, use, and retain the data lawfully in accordance with the data principles, the protection of one's private communications against arbitrary and unlawful interference protects against the very act of interception or surveillance, which, regardless of whether personal data is

[30] Interception of Communications and Surveillance Ordinance, s 2(1).
[31] Personal Data (Privacy) Ordinance, s 2(1).

ultimately collected, infringes the individual's right to privacy once it goes beyond their reasonable expectation of privacy. In other words, data protection laws protect the "informational" aspect of the right to privacy, whereas interception/surveillance laws protect the "personal" aspect of privacy.[32]

As the ICSO now stands, there is no regulation of interception and surveillance by private individuals. Moreover, no criminal liability is attached to any violation of the prohibition of interception of communications and surveillance by law enforcement agents under sections 4 and 5. Although any victim of unauthorised activities may receive payment of compensation as decided by the Commissioner if their case has been found in their favour, and any failure to comply with provisions of the ICSO and its Code of Practice under section 63 will presumably lead to disciplinary actions within the LEAs, these measures are ultimately not as powerful as criminal sanctions, especially since the Commissioner may not give notice to the individual if they consider that such notice would be prejudicial to the prevention or detection of crime or the protection of public security.[33] Even where the Commissioner decides to issue an notice to an individual, they are prohibited from giving reasons for their determination, leaving individuals with little information and no avenue to appeal.[34] Since the ICSO was enacted, the Commissioner has received multiple reports of irregularities or non-compliance from LEAs relating to their interception and covert surveillance activities every year, with as many as 18 such cases in 2017 which include incidents of incomplete removal of access right to interception products, non-reporting of

[32] Michael Jackson, "Right to Privacy, Unlawful Search and Surveillance" in Johannes Chan and C. L. Lim (eds), *Law of the Hong Kong Constitution* (Hong Kong: Sweet & Maxwell, 2nd edn, 2015), ch 22.
[33] Interception of Communications and Surveillance Ordinance, ss 44(6) and 48(3).
[34] Interception of Communications and Surveillance Ordinance, ss 46(4) and 48(4).

heightened legal professional privilege cases, and reporting by a wrong prescribed form, among others.[35] The Commissioner found no violation of the ICSO in any of these cases, often agreeing with LEAs' judgment that these irregularities or incidents were 'genuine mistake[s]' involving no 'foul play or ulterior motive' and deeming LEAs' proposed remedial measures, which include non-disciplinary and disciplinary actions and enhancements to administrative procedures, appropriate.[36] These ongoing 'incidents' identified by the Commissioner, which are often characterised as minor operational errors made by individual law enforcement agents, in fact raise fundamental concerns about the effectiveness of the ICSO in regulating LEAs' behaviour and the necessity of criminalisation,

As the LRC has argued, interception of communications is a serious intrusion upon individual privacy which warrants the use of criminal sanctions. Moreover, the application of criminal law in this area would ensure that police assistance would be given to the victim.[37] While the consideration of press and other freedoms may require exemptions or defences to the offence and careful drafting of the law, it is not an argument for not considering legislating in this area at all, given that criminal sanctions are already used to protect communications (albeit unsatisfactorily) in Hong Kong, as seen in the Telecommunications Ordinance and the Post Office Ordinance. Many common law jurisdictions have also already criminalised the interception of communications, as seen in section 3 of the UK Investigatory Powers Act 2016, section 184(2) of the Canadian Criminal Code, and the US Wiretap Act. In all of these

[35] The Commissioner on Interception of Communications and Surveillance, *Annual Report 2017 to the Chief Executive* (June 2018), ch 6.
[36] *ibid.*
[37] The Law Reform Commission (n 25 above), ch 4.

examples, the act of "intercepting a communication" constitutes an offence without requiring any tampering with an equipment.

The admissibility of intercepted or covertly recorded materials and the right to fair trial

As with the two cases that sparked the controversy regarding the legality of the ICAC's operations, *Li Man Tak* and *Shum Chiu*, case law involving the ICSO almost exclusively concerns the admissibility of evidence obtained by means of interception of communications and covert surveillance.

The question of admissibility of evidence concerns a defendant's right to fair trial, which is protected under article 10 of the Bill of Rights through article 39 of the Basic Law, that "everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law". Being a well-established common law principle, the right to fair trial is also protected under article 87 of the Basic Law and arguably implied in article 35, which highlights a number of related rights including the right to confidential legal advice, access to the courts, choice of lawyers, and to institute judicial review.[38]

The test for the admissibility of improperly obtained evidence pre-ICSO was set out thoroughly in *Chan Kau Tai*, a case which involved, inter alias, whether evidence obtained by the ICAC using covert surveillance at the defendant's office was admissible at trial against him: firstly, courts must take account of any breaches of constitutional rights, but any such breach would not automatically result in the exclusion of the resulting evidence; the court then has the discretion to admit or

[38] Johannes Chan, "Right to Fair Hearing in Non-Criminal Process" in Johannes Chan and C. L. Lim (eds), *Law of the Hong Kong Constitution* (Hong Kong: Sweet & Maxwell, 2nd edn, 2015), ch 20.

exclude the evidence using a "balancing exercise" between "the interest in protecting and enforcing constitutionally guaranteed rights" and "the interest in the detection of crime and bringing criminals to justice". In this exercise, the breach of constitutional rights is an important factor whose weight depends mainly on the nature of the right involved and the extent of the breach.[39] Ma CJHC further emphasised that the test guaranteed the defendant's right to fair trial, taking a broad view of the overall circumstances which include not only the fairness of the actual trial itself, but also the overall behaviour of the investigating authority. Where the admission of the evidence in light of the circumstances "would be such an affront to the public conscience" or "the integrity of the criminal system is so compromised that the court must step in to put a stop to it", it should be excluded.[40]

The enactment of the ICSO did not changed the common law rule that improperly obtained evidence may be admitted in trial, though in the post-ICSO case of *Muhammad Riaz Khan*, a case involving a secret recording of an incriminating conversation between the defendants and an undercover agent, the court reformulated the test: evidence obtained in breach of a defendant's constitutional rights can be received if, "upon a careful examination of the circumstances, its reception (i) is conducive to a fair trial, (ii) is reconcilable with the respect due to the right or rights concerned (iii) appears unlikely to encourage any future breaches of that, those or other rights".[41] Ultimately, this test is still one balancing "the interests of individual defendants and those of society as a whole".[42]

[39] *HKSAR v Chan Kau Tai* [2006] 1 HKLRD 400, para 116.
[40] *ibid*.
[41] *HKSAR v Muhammad Riaz Khan* [2012] HKEC 725, para 20.
[42] *ibid*.

Hong Kong courts' approach can therefore be characterised as an "integrity" approach, which is that "a court should not act upon evidence obtained by state officials by methods that were so fundamentally wrong that for the court to take the resulting evidence into account would compromise the integrity of the criminal process".[43] The integrity approach has long been entrenched in common law systems such as the UK,[44] New Zealand[45], Australia,[46] and Canada.[47] Within the framework of this integrity approach, however, I suggest that a more balanced and holistic view of what the "integrity of the criminal process" entails is needed.

First of all, it is clear that, although there have not been any cases since the enactment of the ICSO where evidence is sought to be admitted which has been obtained by means of unauthorised or otherwise unlawful interception of communications or covert surveillance, in theory, such evidence may be admitted under the current balancing test. This is as the LRC has recommended in its 2006 report, that materials should not be excluded simply on the ground of their having been obtained unlawfully but may be admissible if, "having regard to all the circumstances, including whether the materials had been obtained lawfully, it appears to the court that the admission of such evidence would not have an adverse effect on the fairness of the proceedings".[48] Of course, practically speaking, any such unauthorised activity would allow the defendant to challenge the admissibility of the material at trial and it may well be the case that the court will find, under the balancing test, that the integrity

[43] Andrew Ashworth, "Exploring the integrity principle in evidence and procedure" in Peter Mirfield and Roger Smith (eds), *Essays for Colin Tapper* (Oxford: Oxford University Press 2003).
[44] Police and Criminal Evidence Act 1984, s 78.
[45] *R v Shaheed* [2002] 2 NZLR 377 and Evidence Act 2006, s 30.
[46] Evidence Act 1995 (Cth), s 138.
[47] Canadian Charter of Rights and Freedoms, s 24(2).
[48] The Law Reform Commission (n 21 above), ch 5.69.

of the criminal justice system would be so compromised if the evidence was admitted that it ought to be excluded. However, from a disciplinary point of view, there is no reason why the ICSO should not expressly prohibit the use of evidence obtained as a result of *unauthorised* interception or covert surveillance activities, or at least build in a strong presumption against the use of such evidence which can be rebutted only by the LEAs' evidence that the breach is inadvertent and that all reasonable steps have been taken to prevent such a breach. If the very purpose of the ICSO is to regulate LEAs' activities in detecting and investigating crimes, then it makes no sense for the ICSO to continue to allow evidence obtained through unauthorised activities to be used in court. Given now that the ICSO has provided a clear framework for authorisations (including emergency ones) for the two types of surveillance and interception of communications, there is no excuse for LEAs to be conducting any unauthorised interception and surveillance activities, unlike the situation before the ICSO, where unlawful interception or covert surveillance was possibly the only means by which LEAs could obtain evidence for certain crimes, as seen in *Li Man Tak*.[49]

Although it may seem that the proportionality test conducted by the court at the admissibility stage, that the admission of the evidence is "reconcilable with the respect due to the rights concerned", may be reformulated the same way as the test under section 3 of the ICSO, that the infringement of the individual's right to privacy must be proportionate to the purpose of the detection or prevention of serious crimes, they are not the same: as the incriminating evidence has already been collected at the admissibility stage, it is much more likely that the court will find the balance falling in

[49] *Li Man Tak* (n 5 above).

favour of admitting the evidence for the purpose of preventing the now evident and possibly serious crime. This point is made even more cogent by the fact that, short of the extreme circumstances in *Shum Chiu* where there is a deliberate violation of not only an individual's right to privacy but also legal professional privilege, there seems to be a tendency for courts to consider the reliability of the improperly obtained evidence the only relevant factor in the assessment of whether the trial would be rendered unfair by the admission of the evidence.[50] As evidence obtained by interception or covert surveillance, unlike other improperly obtained evidence such as confessions obtained from defendants who are denied confidential legal advice, are often inherently reliable, courts more often than not decide in favour of admitting the evidence. This is not to say that courts have necessarily made the wrong decision in those cases, but that more attention is perhaps due to other aspects of what constitutes a "fair trial" that would uphold the integrity of the criminal process. In *HKSAR v Wong Kwok Hung*, for example, in deciding that tape recordings of conversations the defendant and a prosecution witness obtained in breach of the defendant's right to privacy were admissible, McMahon J focused much on the reliability of the evidence and stated that excluding the evidence would have been an "extremely undesirable course of events as it would have required the best evidence of the content of those conversations to be ignored".[51] Moreover, he expressed the view that "public interest outweighs the breach of the applicant's right [to privacy] by a considerable margin" in the case.[52] However, it must be remembered that the public

[50] Arnold Liang Hung Pun, "The Admissibility of Evidence Obtained in Breach of Constitutional Rights in Hong Kong" (2013) 14 *Asia-Pacific Journal on Human Rights and the Law* 67.
[51] *HKSAR v Wong Kwok Hung* [2007] 2 HKLRD 621, para 68.
[52] *ibid*.

interest lies not only in preventing crimes and convicting criminals, but also in courts' protecting fundamental rights against illegitimate intrusions by LEAs.

Therefore, in considering the "integrity of the criminal process", there should be extra caution against admitting materials resulting from unauthorised interception or surveillance activities falling under the ICSO, and courts should pay more attention to the effect of the breach of fundamental rights in the balancing exercise and avoid focusing solely on the reliability of the evidence, otherwise they risk conveying the message that LEAs can simply ignore the requirements of the ICSO as long as strong, reliable evidence is obtained in the end. The integrity of the criminal process does not only require that reliable evidence by admitted in order to prevent serious crimes, but also that the rights of defendants be upheld and improper acts by the law enforcement discouraged, if not condemned. As Ashworth argues:

> "A legal system must reach a decision on an acceptable demarcation between permissible and impermissible methods…Once agreement has been reached the rights which flow from it should be respected and protected. An essential part of taking such an agreement seriously is to protect suspects and accused persons from any disadvantage resulting from an infringement of the rights declared or implied."[53]

Although Ashworth has made this argument in relation to the "protective" or "remedial" approach to the admission of improperly obtained evidence, it is equally applicable to the integrity approach, as the latter, in determining whether to admit particular piece

[53] Andrew Ashworth, "Excluding Evidence as Protecting Rights" (1977) 3 *Criminal Law Review* 723, 733.

of evidence, is really about striking a balance between the disciplinary element and the protective element, along with the relevance and strength of the evidence.

4. Surveillance in the "digital age"?

After Edward Snowden's revelations in 2013 about the extent of online surveillance undertaken by Government intelligence agencies, and with the widespread use of social media such as Facebook and Twitter and online messaging tools such as WhatsApp today, recent concerns surrounding covert surveillance have been directed towards the possibility of online snooping by LEAs. The advent of Web 2.0 and the almost ubiquitous use of the Internet for communication, entertainment, research, and other purposes have created a massive amount of user-generated information and an even larger amount of metadata, which are created whenever users conduct any activity online and all logged and stored on servers. Another implication of the bulk of communications moving online is that such information has become increasingly important to law enforcement for purposes of crime detection and prevention.

Currently, data such as Internet connection records or telecommunications records kept by information communication technology (ICT) companies do not fall under the ICSO, since it only covers the interception of communications "in the course of transmission" and physical surveillance that makes use of a "surveillance device". The PDPO will apply where personal data is involved, but it is unclear how much of such data is actually "personal data" where they relate to an identifiable individual. The Government's official position is that, when investigating crime, LEAs may request

necessary information related to crime detection from persons or organisations concerned, including subscribers' information such as account names and IP addresses, for locating witnesses, evidence, or suspects.[54] This is done "as part of LEAs' routine law enforcement efforts"[55] and "in accordance with duty-related laws, established procedures or guidelines", which ensure that "the relevant requests are only made when it is necessary for performing duties".[56] When asked if the Government plans to regulate and increase the transparency of LEAs' practices in this area by drawing up guidelines and releasing reports regularly, the Government's response was that they did not have plans to make any change as the current mechanism has been "functioning effectively and efficiently".[57]

According to data provided by the Government at the request of LegCo member Charles Mok, not only LEAs covered by the ICSO such as the Customs and Excise Department and the police but also a variety of other Government departments, including the Agriculture, Fisheries and Conservation Department, the Companies Registry, the Inland Revenue Department, and the Office of the Communications Authority made requests for information disclosure to ICT companies from 2015 to 2016. These requests were made to both local and foreign service providers and social media platforms and the data requested were primarily metadata including user account details and IP addresses. The justification for these requests was mainly crime detection and prevention or statutory enforcement.[58] The dataset provided was

[54] – "LCQ15: Interception of Communications and Surveillance Ordinance", *news.gov.hk*, 29 April 2015. Available at http://www.info.gov.hk/gia/general/201504/29/P201504290534.htm (visited 28 November 2018).
[55] *ibid*.
[56] – "LCQ10: Government's requests for information disclosure and removal made to information and communication technology companies", *news.gov.hk*, 1 March 2017. Available at http://www.info.gov.hk/gia/general/201703/01/P2017030100385.htm (visited 28 November 2018).
[57] *ibid*.
[58] *ibid*.

however incomplete, with the relevant departments unable to provide a significant portion of the information.

There is certainly a case to be made for including requests for information disclosure made by Government departments to ICT companies in the ICSO or otherwise making legislation to regulate such requests. The prevalence of the Internet in all spheres of life has made online snooping a potentially much more serious intrusion into one's private life. Interestingly, the Government when responding to inquiries about the extent of data requests often tries to downplay the severity of the potential interference with rights and justify the current unregulated state of affairs by emphasising that these requests "do not involve requests for records of the content of any non-open communications".[59] However, that metadata necessarily reveal less about an individual than the content of their communications is a misconception. Compared to traditional telecommunications records, Internet connection records reveal so much more than just the timing of a message or the locations of its sender and recipient. As Bernal argues:

> "Monitoring the websites we visit isn't like having an itemised telephone bill…it's like following a person around as they visit the shops (both window shopping and the real thing), go to the pub, go to the cinema, turn on their radio, go to the park, visit the travel agent, look at books in the library and so forth."[60]

[59] LCQ15 (n 54 above).
[60] Paul Bernal, "A few words on Internet Connection Records", *Paul Bernal's Blog*, 5 November 2015. Available at https://paulbernal.wordpress.com/2015/11/05/a-few-words-on-internet-connection-records/ (visited 28 November 2018).

In other words, these requests for online metadata made by the Government are in fact far less akin to the interception of communications than to physical surveillance where an individual is being followed around and having their every move recorded while going about one's day. Although it could be argued that one does not have a "reasonable expectation of privacy" and thus no right to privacy to be interfered with where one is generating public content online by, for example, posting or commenting on social media, where one is simply browsing or using services such as banking or shopping services on their private network connection, one might arguably have an even higher expectation of privacy than when one is doing the equivalent acts in public physically as one is not physically "seen" and has no reason to suspect anyone is monitoring their online activity. Moreover, as we have found out from eerie online advertisements that are often able to show us exactly what we want, seemingly innocuous information such as what websites one has visited and how long one has stayed on a page can reveal an unexpectedly large amount of private information about a person.

Given the risk of serious violation of individuals' right to privacy posed by Government requests for metadata from ICT companies, the current unregulated and non-transparent state of affairs is clearly unsatisfactory. As required under article 39 of the Basic Law, any restrictions imposed on the rights and freedoms enjoyed by Hong Kong residents must be prescribed by law. As we have seen from the litigation leading up to the final enactment of the ICSO, administrative guidelines issued by the executive itself do not achieve sufficient legal certainty to meet such a requirement.[61]

[61] *Leung Kwok Hung* (n 1 above), para 150.

It is moreover unsatisfactory that the Government only released statistics of data requests when pushed by LegCo members' queries in a haphazard manner instead of publishing such information regularly. The Hong Kong Transparency Report has reported that Hong Kong is lagging behind other common law jurisdictions including South Korea, Taiwan, Australia, the UK, and the US in terms of both legal requirements for Government requests for metadata and mechanisms for routine disclosure.[62] The UK Investigatory Powers Act 2016, for example, sets out restrictions in relation to the authorisation of obtaining Internet connection records, in addition to the conditions already imposed on the authorisations of other forms of data collection by public authorities, and establishes the role of the Investigatory Powers Commissioner who must make annual reports including on statistics on the use of investigatory powers under the Act.[63] As the ICSO already provides a transparency and accountability mechanism via the role of the Commissioner, if the ICSO is amended to cover Government requests for Internet connection records or metadata from ICT companies, the role of the Commissioner can be easily expanded to include overseeing Government practices in this area and including the relevant statistics in annual reports. Before such an amendment is made or new legislation enacted however, the Government may still disclose such statistics without a statutory requirement, as it already does regarding the Code on Access to Information.[64]

[62] Journalism and Media Studies Centre of the University of Hong Kong, *2018 Hong Kong Transparency Report*, February 2018. Available at http://transparency.jmsc.hku.hk/wp-content/uploads/2018/02/HongKongTransparencyReport2018_EN-1.pdf (visited 28 November 2018).
[63] Investigatory Powers Act 2016, s 62.
[64] Journalism and Media Studies Centre of the University of Hong Kong (n 62 above), p 21.

5. Conclusion

It has been 12 years since the ICSO was enacted but there is still a dearth of work that discusses its implications on the protection of the right to privacy and the right to fair trial and whether or not it is a satisfactory piece of corrective legislation aside from simply fulfilling the constitutional requirement of providing a legal basis for LEAs' interception and covert surveillance activities. In this paper, I have contributed to the literature by giving a comprehensive overview of the legislative history of the ICSO and the current state of the law and highlighting the various aspects of law that are worth noting. The recommendations I have made are summarised as follows:

1. The Government should reconsider making the interception of communications and covert surveillance a criminal offence, as has already been recommended by the LRC in their reports on privacy before the enactment of the ICSO. This would mean that both public and private bodies will be prohibited from conducting interception or covert surveillance, but certain LEAs or Government departments may be authorised under the law, as is the case now, to carry out such activities as long as they are necessary for and proportionate to the legitimate purposes of crime detection and prevention or the protection of public security.
2. There should be at least a strong presumption against admitting as evidence materials obtained by means of unauthorised activities falling under the ICSO as the current balancing test set out in the *Riaz Khan* case can technically allow such materials to be admitted as evidence in court, which would defeat the purpose of the ICSO. Courts should also pay more attention to the different

aspects constituting a “fair trial” that would uphold the “integrity of the criminal process” other than the reliability of the evidence, such as the severity of any violation of the defendant’s rights.

3. As Internet connection records are becoming increasingly important for law enforcement and the investigation of statutory offences, LEAs and Government departments’ requests for such data from ICT companies should be regulated by law and the Government should publish statistics regularly to increase the transparency and accountability of the process, taking reference from other jurisdictions’ laws and practices.

All in all, although the ICSO has certainly responded to the Government’s immediate needs at the time of its enactment in 2006 to provide a legal basis for LEAs’ activities, the legal framework as a whole has not been adequate to address other challenges that have arisen over the years, and more can certainly be done to afford better protection to the right to privacy and the right to fair trial.