Public Policy Research Funding Scheme

公共政策研究資助計劃

Project Number :
項目編號： 2019.A3.018.19B

Project Title :
項目名稱： Privacy Challenges and Big Data in Smart City
智慧城市中的私隱問題

Principal Investigator :
首席研究員： Dr IP Iam Chong
葉蔭聰博士

Institution/Think Tank :
院校 ／智庫： Lingnan University
嶺南大學

Project Duration (Month):
推行期 (月) ： 15

Funding (HK$) :
總金額 (HK$)： 268,870.00

智慧城市中的私隱問題

研究報告

Privacy Challenges and Big Data in Smart City

葉蔭聰博士，嶺南大學文化研究系
Dr. IP, Iam-chong, Department of Cultural Studies, Lingnan University
傅景華博士，香港大學新聞及傳媒研究中心
Dr. FU, King-Wa, Journalism and Media Studies Centre, The University of Hong Kong
梁旭明博士，嶺南大學文化研究系
Dr. LEUNG, Yuk-ming, Department of Cultural Studies, Lingnan University
梁啟智博士，中文大學新聞與傳播學院
Dr. LEUNG, Kai-chi, School of Journalism and Communication, The Chinese University of Hong Kong

2020年，11月

Project code：2019.A3.018.19B

行政摘要

i) 研究摘要

香港為了跟隨全球趨勢，加強全球競爭力，不斷廣泛使用資訊科技，並於2017年提出智慧城市藍圖，其中一項挑戰，就是保障個人私隱及修訂相關法律，以適應數碼年代裡，廣泛收集及處個人資料的活動。但是，香港政府仍然過份重視科技推動未來的光明面及商機，但並未有效應對社會對私隱的關注。

1990年代中，隨著《個人資料（私隱）條例》於1995年通過，個人資訊私隱專員公署成立，監督條例的執行；多年來，它致力與歐洲的規管框架同步，例如之前的《數據保護指令》（1995）及《通用數據保障條例》（2018）。然而，我們發現，條例及公署所涵蓋的範圍多針對私人企業，例如向它們推廣保護及尊重個人資料的文化。然而，條例與公署皆無法處理各種新型個人資料及私隱，以及它們變動中的性質，尤其是公眾關心的「監控國家」（surveillance state）問題；根據條例，只要個人資料收集涉及防止及偵查犯罪，便幾乎立即得到豁免。此外，公署向私人企業推廣私隱影響評估（Privacy Impact Assessments），但是，它無法要求政府部門就著新使用的資料收集技術去進行評估。

近年，在香港政治爭議之中，資訊及監控科技引起對私隱的關注，甚至造成社會恐慌，在政治衝突中，對人面識別科技的懷疑愈來愈大，去年（2019）環繞「多功能智慧燈柱」試驗計劃及沙田第一城建議的新門禁系統，成為兩個標誌性個案。

我們的個案研究發現，私隱的關注遠遠沒有得到重視。首先，現有規管架構與公眾期望之間的存在重大落差。公署無法舒緩公眾的擔憂，無法監管政府部門如何應用新的資訊搜集技術，尤其是執法部門。但是，隨著公眾對政府愈來愈不信心，許多人卻擔心警察有大型監控計劃。第二，新

型個人資料及私隱深深嵌入在社會及政治關係之中，公共與私人的界線不能單以技術及法律來界定清楚，它經常轉變，亦因應著政治氣候變化，它的含糊性更會導向社會恐慌及激烈抗爭。

ii) 研究項目對政策影響和政策建議的摘要

基於我們的個案研究及分析，我們作出以下建議：

1. 政府的首要任務是重建公眾的信心。就著私隱相關的政策，政府該向公眾作出承諾，不使用某些政治敏感的科技，例如自動化及無差別的人面識別監控技術；

2. 同樣，政府應考慮參考英國的《自由保護法》（2012），立法限制政府部門（包括執法部門）處理個人資料的方法及程序；

3. 修改條例，嚴格規定政府部門及大型企業機構，在應用新資訊科技收集及處理個人資料前，要進行私隱影響評估（PIA）；

4. 政府部門及大型企業機構應向公眾提供更詳盡的流程圖，標示清楚個人資料的流向、資料庫地點及不同機構及司法管轄區間（例如香港與中國大陸）的資料轉移限制等等；

5. 因應港區國家安全法，我們建議政府成立一個獨立法定機構，類似英國的情報專員辦公室，監管以國家安全之名進行的個人資料收集及處理。

Executive Summary

i) Abstract of the research

Hong Kong's public and private sectors, following the global trend to strengthen its global competitiveness, have made wide use of information technologies. The government decided to follow the lead and drew a smart city blueprint in 2017. One of the major challenges concerns the protection of individual privacy and updating privacy law in view of the digital age which features the pervasiveness of personal data collection and processing. However, the government often over-emphasizes the bright side of our technologically-driven future and the new business opportunities, but yet does not effectively address the escalating privacy concerns.

In the mid-1990s, after the enactment of the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (the Ordinance) in 1995, the Office of the Privacy Commissioner for Personal Data (PCPD) was set up to oversee the implementation of and compliance with the Ordinance. Over the years, it has strived to keep abreast of the regulation in EU law, such as Directive 95/46/EC (Data Protection Directive) and General Data Protection Regulation (GDPR, 2018). Our study, however, found the scope of the Ordinance and PCPD too limited to the private sector, i.e. promoting the culture of protecting and respecting personal data. Yet they fail to address the changing nature of the new forms of personal data and privacy, especially the public concern about "surveillance state". For example, personal data involved in prevention and detection of crime is exempt from any provision of this Ordinance. While PCPD promotes the practice of Privacy Impact Assessments (PIA) to the private sector, it is not capable of requiring

the government departments to conduct assessment of their adoption of new information technologies for collecting and processing personal data.

In recent years, in the midst of political feuds, information and monitoring technologies raise privacy concerns and even social panic in Hong Kong. Skepticisms of the use of facial recognition technologies have loomed over in recent political conflicts. The controversies over the “Multi-functional Smart Lampposts” Pilot Scheme and the City One Shatin’s proposed new access system serve as two landmark cases.

Our case study revealed that the privacy concerns have not been sufficiently addressed. First, there is a huge gap between the current governance mechanisms and the public expectation. While PCPD promotes the culture of protecting information privacy, it fails to ease public concerns. It is barely capable of monitoring the government departments’ adoption of new technologies of data collection, especially the law enforcement authorities. However, along with the increasing public's distrust of the government, many people are worried about the possible massive program of police surveillance. Second, the new forms of personal data and privacy are deeply embedded in socio-political relations. This boundary between the public and the private domains could not be defined simply in technical and legal terms. Instead it constantly shifts and is heavily dependent on political climate. The ambivalence of the new form of privacy sometimes lends itself to social panics and agitations.

ii) Layman summary on policy implications and recommendations

Based on our case study and analysis, we make the following recommendations:

1. The first task for the government is to regain the public's confidence. Regarding the policies related to privacy, it should make a public statement to promise not to implement some politically sensitive technologies, such as automated or random facial recognition;
2. Likewise, the government should consider enacting an ordinance similar to the Protection of Freedoms Act (2012) in the UK which imposes requirements on the government departments (including law enforcement authorities) in relation to certain processing of personal data;
3. Amendment of the Ordinance is needed for requiring the government departments and sizable private companies to conduct Privacy Impact Assessment (PIA) before adoption of new information technologies for collecting and processing personal data;
4. The government departments and sizable private companies should provide the public with more detailed charts for specifying clearly the flow of personal data, the location of databases, and the restrictions on the transfer of data across different institutions and jurisdictions (e.g. Hong Kong and mainland China).
5. In view of the enactment of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region, we recommend the government to set up an independent and statutory body similar to that of Intelligence Services Commissioner in the UK to monitor the personal data collection and processing for national security.

目錄

第一章：引言

自1990年代以來，發展與應用資訊及傳播科技已成為大部份先進城市的重要策略，香港特區政府分別在1998年、2001年、 2004年 及2008年發表《數碼21資訊科技策略》（簡稱《數碼21》）。過去二十多年，香港已成為世界上其中一個領先的網絡化城市，2013年時，《福布斯》雜誌更稱香港為繼矽谷及紐約之後的頂級科技城市。

2013年，特區政府開始檢討《數碼21》，以「智慧香港」、「智慧生活」作口號。翌年，建議成立創新及科技局，並構想「智慧城市藍圖」。除了網絡連繫，資料數據是整個藍圖的核心，當中包括公共及個人領域的數據收集、儲存、處理、傳送，以建造創新的管理及服務系統。

不過，這種向前看的光輝願景，容易遮蔽原有及衍生的問題。2017年的，顧問報告指出，保障個人資料私隱、制訂適用於智慧城市功能的私隱原則、更新現有法律架構、推行更多保障措施是極大挑戰（PWC 2017: 144）。儘管如此，無論是政府或公眾，皆嚴重低估這方面的問題。

關鍵之處不單在於如何參考外國的相關的法例、規管框架及技術，而在於市民及整體社會面對個人資料數碼化時的反應，因為政府體制及私人公司性質的不同，市民與政府的關係亦有重大差異，例如代議民主、人權體制及監察制度的健全程度有很大差別，簡單移植歐盟的一切未必解決最主要的問題。

一方面，我們的生活環境充斥著所謂「大數據」（big data），使我們對個人私隱的理解，逸出了過去既有的簡單個人資料，使我們對更多不同類型的個人資料產生差異極大的認知、想像及情感反應（例如對攝錄影像及人臉識別的抗拒）。另一方面，數據收集及處理涉及更多不同平台，當中涉及不同的政府部門及私人機構，令個人及社會的警覺及關注變得更複雜。例如，僅憑日常觀

察我們便知道，香港不少市民對政府，特別是執法部門（例如警察）特別敏感，而遇上中國大陸的政府及公司被懷疑涉及其中時，對個人私隱的關注更會大增。

然而，香港的《個人資料（私隱）條例》（以下簡稱「條例」） 早在1995年通過，並於1996年年底生效，同時，亦成立獨立法定機構「個人資料私隱專員公署」，這些法律、規管框架及機構，都是資訊科技大量被使用、「大數據」暴增之前已訂下來的。在過去二十五年，公署不斷提醒業界關注歐盟的相關指引，但本港條例除了在2012年有少許修訂及增補，但都沒有針對新的資訊環境及個人私隱關注作重大修訂。

在過去幾年，尤其是2019年反修例運動中，新型的個人資料及私隱議題更捲進了嚴重的政治衝突。因此，我們急需對此進行研究及檢討，並在政策及法例層面對提出改革方案。

第二章：研究目的

因此，我們有需要研究資訊及科技環境轉變，公眾反應以及規管架構之間的互動，並結合本地的文化及政治動態，才能制定出符合新形勢及香港需要的保障個人私隱的新措施。本研究大致包括以下幾方面：

1. 回顧有關資訊資本主義、大數據及智慧城市的相關理論討論，把香港的智慧城市發展計劃放在較宏觀及全球的脈絡；
2. 審視香港以外其他智慧城市及地區（例如韓國的松島新城或歐盟地區）在處理個人私隱方面的新嘗試，包括在法律、教育及公共政策上應對智慧城市的私隱挑戰，並提出有關香港智慧城市的建議；
3. 進行使用者及深入訪談，了解他們如何管理個人私隱，並提出增強公眾意識的策略；
4. 探討政府、企業及公民社會在其他智慧城市及地區之間的互動，並探尋智慧城市的數據管理模式。

我們除了審視相關法例及政策文件外，也以質性研究方法，進行了焦點訪談及個人深入訪談。由於個人私隱問題涵蓋範圍極大，為了令研究比較集中，所以本研究聚焦在兩個近年發生的熱門個案及爭議，它們都是2019年8月期間發生的，分別是反修例運動期間的「智慧燈柱」事件，以及「第一城人臉識別」的爭議。

本報告會根據這兩個個案，並結合我們對香港個人資料、私隱的保護政策及法例的分析，聚焦在個人使用者在日常生活中處理個人相關資料的模式、政府政策及企業管治之間的差距，從而提出政策建議。

第三章：研究方法

3.1. 研究焦點

在最初設計本研究時，我們曾打算搜集及分析大約二十家公司的私隱政策聲明。我們的確曾搜集及分析，但我們後來決定並不以此為研究重點。因為，這些政策聲明皆大同小異，一般公司也參考及遵照私隱專員的建議。同時，這些公司涵蓋十分廣泛的行業，這樣會令研究失去焦點。缺乏焦點及議題，不容易看到現有法例及框架有甚麼問題，難以探討政府、企業及公民社會的互動。同時，爭議性議題亦有助訪問使用者，更能發掘他們重點關注所在，從而看到與現有規管架構之間的落差。所以，我們最後決定不籠統地針對原計劃書中所列的健康及交通兩大範野，而選擇兩起事件，它們分別關於公共空間及私人空間裡個人資料搜集的爭議，這更能提出較針對性的政策建議，以達成研究目標。

3.2. 分析文獻與法律

我們除了回顧跟智慧城市、大數據及私隱等一般性學術文獻外，我們聚焦在香港與西方國家相關的法律與規管框架緣起，以及當中相關的問題及爭議。我們也會討論近年的新趨勢及新的規管嘗試，並對比出香港的制度特點，並中看到它的限制與問題。

3.3. 焦點訪談及個人訪談

我們選擇了2019年兩宗與大數據、智慧城市及私隱有關的爭議，分別是政府的多功能智慧燈柱，以及沙田第一城的人面識別保安系統爭議。前者的個人資料使用者為政府，收集範圍在公共空間；後者的個人資料使用者為私人保安公司，收集範圍在私人空間。分析這兩個個案，我們可以看到市民面對大數據環境中私隱問題的反應，包括他們如何感知與認知，以及當中的共性與差異。

我們運用滾雪球方式，找了12位曾參與去年反修例運動的參與者，年齡在22-60歲，共完成了兩個焦點訪談。焦點訪談內容環繞著他們使用資訊科技，尤其是手機、應用程式及社交媒體的經驗

，以及他們對私隱的理解。後來由於新冠肺炎爆發，以及限聚令的實施，所以我們難以再組織焦點訪談，於是改以個人訪談。我們另外找了14位受訪者，年齡在28-40歲，當中只有一位有參與去年的運動，希望找到政治立場不同的人進行對比。

除此之外，我們針對個案二，找了15位沙田第一城的居民訪問，其中8位是業委會成員只願意填寫我們提供的問卷。此外，我們也訪談了屋邨的保安公司經理。關於受訪者名單及訪問問題，詳情可見附錄。

3.3. 個案簡介

個案一：多功能智慧燈柱（Multi-functional Smart Lampposts）

「 多功能智慧燈柱」（下簡稱「智慧燈柱」）本是《2017年施政報告》 提出的試驗計劃，是推動智慧城市發展的三項基礎建設之一，其目的包括：

1. 提供便捷訊息服務；
2. 收集各類實時城市數據；
3. 加強城市及交通管理；
4. 配合第五代（5G）流動通訊服務。

在報告中，並沒有提及智慧燈柱有任何監控功能，但是，與智慧燈柱同時推出的另外兩項基建分別是：

1. 「數碼個人身分」：市民能以此進行身份認證，網上交易及獲取政府的服務；
2. 革新電子政府系統，以及設立「大數據分析平台」，令政府各部門能運用雲端服務等科技，提升運作效率和網絡安全。

據政府說，智慧燈柱的用途如下：

1. 收集實時氣象數據、空氣質素數據及交通流量;
2. 收集所得的數據會成為開放數據(open data)，通過「資料一線通」網站(data.gov.hk)向公眾發放。
3. 流動網絡營辦商可使用燈柱作為街道設施，安裝無線電基站，鋪設5G網絡；
4. 免費公共 Wi-Fi 服務。

在2019年6月之前，智慧燈柱得到媒體關注極少，在互聯網上也少看到有人談論該項目。我們搜尋過Wisers Information Portal中的關鍵詞「智慧燈柱」，由2017年1月至2019年6月有315筆資料，談論到私隱問題的只有36筆，其餘大部份報導及文章都是介紹計劃內容、進展，以及敦促政府加快推動智慧城市相關項目。簡言之，媒體輿論並沒有很關注智慧燈柱裡涉及私隱問題。事實上，2018年9月，一份問卷調查發現，受訪的年青人（15-34歲）中只有7.7% 受訪者表示了解「多功能智慧燈柱」，相較「數碼個人身份」（18.5%）還要低（《香港仔》，2018.9.27）。在差不多同一時間，政府亦諮詢了區議會，並於2019年1月開始安裝，直至6月底安裝了50支。

但是，智慧燈柱這個冷門話題，隨著2019年6月開始的「反逃犯條例修訂」運動，在7月突然開始變得熾熱。

2月13日香港政府提交修訂《逃犯條例》及《刑事事宜相互法律協助條例》的草案後，不少公眾、政黨及公民團體指責政府破壞中港兩地的「司法防火牆」，香港人面臨被遣返中國大陸的風險，但政府拒絕再進行諮詢，卻一意要交由立法會表決通過。爭議開始時，主要是議會內反對派與建制派的對抗，及後演變成6月10日的百萬人遊行抗議，以及6月12日二讀時金鐘的大規模警民衝突，之後是長達半年幾乎無日無之的警察與抗爭者的街頭對抗，雙方的武力回應亦急劇升級。因此，在示威者及輿論中漸漸形成對警察權力及暴力的反感，害怕執法者監控。事實上，根據我們在示威現場觀察，這次抗議其中一個特點是，自6月12日開始已有大量示威者（不單）帶上口罩，防止警察辨認，而警察在反修例示威前或後，皆曾使用監控鏡頭找出參與示威的人作出檢控。

進入7月後，智慧燈柱與私隱的爭議熱起來。在反修例運動期間，LIHKG（即「連登」）是其中一個重要的討論區，甚至有人在此發起行動。我們發現，在2019年7月前，只有4篇帖文關於智慧燈柱，分別是2019年4月及2018年1月。但在7月，突然出現了24篇，8月時更有61篇，而且跟帖的人眾多。類似情況也發生在傳統媒體之中，7月開始，智慧燈柱與私隱疑慮便迅速發酵。

公眾關注聚焦在智慧燈柱會否成為類近中國大陸式的監控系統，對街頭所有人進行人面識別，成為警察及政府用來打壓示威者的工具。甚至有人懷疑，智慧燈柱收集的數據會與中國大陸政府分享。7月16日，政府公開宣佈，因為公眾對私隱的關注，不會啟動燈柱某些功能，包括監察非法棄置廢物、收集車牌號碼的攝錄機，以及探測行車時間與車速的藍牙探測器。資訊科技辦公室於8月初，宣布成立「「多功能智慧燈柱」技術諮詢專責委員會」（簡稱「燈柱委員會」），第一次會議為8月12日，研究智慧燈柱的私隱保障技術及措施，並承諾公開會議內容。但是，隨著反修例運動的展開，不信任政府的情緒蔓延，政府的暫緩決定，以及相關措施，遠未能緩解民情。

8月24日，有示威者拆毀九龍灣常悅道20支智慧燈柱，燈柱內的設備全面曝光。8月25日，負責供應及安裝燈柱的公司TickTack Technology宣佈，鑒於公司董事之家人及僱員人身安全受威脅，退出相關項目。於是，整個試驗計劃可以說是要被迫暫停。2019年10月4日，有示威者在觀塘市中心附近破壞10支智慧燈柱。

燈柱委員會由2019年8月至本報告撰寫時（2020年10月），共開了七次會議。總體方向上，要求政府披露更詳細的技術資料、應用目的與範圍，並以私隱友善技術取替在私隱問題較受爭議的技術，包括以光學雷達(LiDAR)取代攝錄機。

<u>個案二：沙田第一城「人工智能面部識別」爭議</u>

2018年12月20日，沙田第一城委員會（下稱「業委會」）第212次委員會會議，會上討論及通過了於沙田第一城第34座至36座「提升大廈保安安智能門禁系統」。這套系統包括三個部份：

1. 門禁系統（Access System）
2. 人工智能面部識別（AI Face Recognition）
3. 訪客QR Code系統（Visitor QR Code System）

此新系統將取代此三座的保安員，只有1-2名保安員在第七期控制室當值，遙控此三座的保安工作。住戶使用新的智能卡，系統會自動識別面孔，包括尾隨進入大堂的人士。若遇上陌生人，會將大門鎖上並使用對講座查詢。預約的訪客，由業戶向管業處申請，獲取QR Code，訪客在指定日期及日時使用QR Code入內。

根據會議紀錄，以及我們的訪談，此新系統的目的，是要解決保安業從業員人手不足的問題，同時，提升保安系統的服務質素。計劃試驗後再探討全面推廣的可行性，若全面實施，可減省26名保安員（約為現在人數的25%）。

據業委會成員表示，相關會議紀錄曾放在屋苑的公眾地方，但一直沒有收到居民的反對意見。

2019年8月開始，可能也因為反修例運動產生對監控的強烈關注，有住戶在網上表示擔心個人資料會被人另作他用，包括讓執法部門監視居民的活動，侵犯個人隱私；而業委會主席的新民黨身份，亦令人猜疑他推動計劃的政治動機。同時，亦有人質疑系統造價過高（80萬）。8月14日晚上，有居民包圍第一城業委會主席，要求交代，事件擾攘至深夜。主席後來表示，由於爭議太大，決定「撤回」計劃。

2019年11月區議會選舉，原區議員競逐連任，此議題亦成為議題之一。最後，他敗選，屬反對黨的候選人當選。2020年7月17日業委會改選，52座中有36名新人當選各座主席，原有業委會中多人敗選，包括原業委會大會主席。

第四章：研究成果/發現

4.1.「智慧城市」：一種大數據治理與監控

在「智慧城市」這類大口號背後，是大數據的全球趨勢。學者Rob Kitchin指出，「智慧城市」主要指整個城市（包括人、動物、物、環境等等）被無時無刻及無處不在地建構及監控，而且是透過電腦及網絡運算進行；而運用這些功能進行創新及管治的人則被視為「智慧人」（”smart people”）（Kitchin 2014），它也指向一種透過科技而促進的市民與政府的關係，以及所帶來的治理問題（World Bank 2015）。換言之，大量個人數據透過互聯網、資訊科技產品收集，經過電腦化處理分析，呈現個人及群體行為與互動的型態、趨勢及連繫。

而更有趣的是，大數據並不止於此，它指的是一個不斷衍生的過程：政府、公共機構、私人公司等把這些處理過的數據，又反饋回到個人與群體，影響我們的行為及互動，並再回到大數據的搜集、處理及分發的循環。例如智能手錶紀錄維生指數、身體狀況、地理位置等個人資料，並選擇性地回饋到使用者，甚至與更大的數據庫作比較，成為一種可以銷售推廣的資訊服務，促進我們進一步運用及使用，從中又再生產更多的搜集及處理數據的機會。

在這種新形勢下，私隱所涉及的不再限於個人的既有資料，例如姓名、身份證號碼、手機號碼、地址等等，而是不停被資訊系統生產的東西，甚至是連我們個人也不知道、不理解及不能掌握的。例如，很少人可以完全取得自己的數碼足跡，但足跡卻無時無刻被記錄，經處理及組合過的資訊，形成數據分佈與形態，更超出我們可以接觸及理解範圍。

這些不斷衍生的資料，我們可以統稱為新型個人資料，它的性質與過去的個人資料非常不同。學者Luciano Floridi指出（2005），網絡及數碼資訊科技是一種新的資訊科技，與過去的資訊科技如電報、電話等，在私隱方面有根本的差別：

舊有的個人資料是有限的個人既定的資料，相對容易劃下界線。例如，身份證號碼只限於提供給政府及有限的私人公司（如電力公司、電訊公司等），盡量不作公開透露；家居生活的種種，發生在物理區隔的空間內，界線相對容易為個人及他人所辨識。因此，這些個人資料構成的私隱界線也相對穩定。但是，新型的個人資料在互聯網及資訊科技工具中幾乎是無限的，而且，公私界線不是只有一條，多重公私界線會交疊起來，甚至在不同時間及地點中重新再劃的。

此外，資訊科技的發展不單會減少資訊流通的阻力，減低了私隱的保護，增加了個人取用得別人的資訊能力，但與此同時，又會反過來增加阻力。例如，手機短訊消除了被身旁的人偷聽的可能，甚至有加密通訊技術，防止截取；同時，也是更重要的是，它改變了私隱所存在的資訊環境，因此，個人資料及私隱性質變得不一樣，我們對它的理解、評價及管理也會不一樣（Floridi 2005: 6）。

在所謂「智慧城市」中，由於大數據無處不在，也是我們的生活的一部份，因此，我們既因為它帶來方便，所以難以完全切割，而且，每一類新型的個人資料都引起我們不同的考量。例如，我們會日益擔心手機、應用程式、網站以至政府的執法及情報部門會記錄我們的行蹤；但是，當我們查看網絡地圖時，網絡定位為我們提供方便，有人甚至自己主動標示位置（香港俗稱「打咭」），在社交媒體上分享。除了特定時刻，我們未必很在意，此即為學者所指的「私隱悖論」（privacy paradox）（Barnes, 2006）。

一些學者認為，這是因為公眾缺乏認識所致（Acquitis and Gross 2005; Litt and Hargittai, 2014），但亦有人指是理性的計算結果，即衡量過獲得的好處比風險要多（Taddicken, 2014）。因此，保障私隱成為一項持續不斷及改變的自我管理，也被視作為個人責任（卻又無法完全履行），但

同時，私隱本身在網絡服務日益發達的情況下，變成了一種商品，為了服務及便利而不同程度地出賣給別人（Hull, 2015），甚至形成一種冷感與犬儒主義，不太用力及認真地保障 (Hargittai and Marwick 2016)。有學者（Lutz, Hoffmann and Ranzini 2020）把這種犬儒主義分四類，分別是：不信任、不確定、無力及放棄。這些具有新自由主義理性特徵的態度，遮蓋了個人私隱其實是在網絡環境中不斷被催生、捕捉、保護及入侵，是資訊化的資本主義的重要面向之一。在這個環境裡，個人的力量很有限，政府與大企業卻在主導。

4.2. 重新概念化私隱

因此，我們有必要重新概念化私隱：

1. 首先，私隱不再是一個固定的領域，可以一勞永逸地劃分清楚，相反，它是一個在特定時空裡的商議及劃定的關係，同時也是當下暫時宣稱結果。有研究指出，不少使用者視個人資料為一種交換物品，只要人們覺得「出賣」了自己的個人資料能換來服務、好處及方便，便會有限度地公開，有時又會激烈地指控及保護。因此，「私隱」的界線並不由個人界定，而要視乎服務交換的對手；

2. 私隱比過去更加關係到個人與政府、通訊平台、大企業或組織化的團體的關係，因為，資訊科技發展（也加上社會及城市空間的個人化發展）令我們有能力防止身邊的特定普通人侵犯私隱，但是，卻把我們暴露在眾多資訊平台裡，平台背後的公營或私營機構更有能力接觸到我們的個人資料，對私隱被侵犯的擔心更多來自這些未能界劃清楚的地方（Floridi 2005: 9）。因此，私隱並不再像固定的領域，而是眾多複雜及動態的關係。當中尤其涉及個人與擁有各種權力機構之間的關係，因為，這些機構在未能界劃清楚的地方擁有各種權力，例如政府的執法部門有能力可以在大氣電波、互聯網上截取通訊，社交媒體平台也無時無刻在搜集個人資訊，而政府及社交媒體只限定在特定的司法管轄地區（例如香港不少網民擔心中國政府及與之有關的中國互聯網公司）；

3. 這些關係並不能只用技術條件來理解，甚至有時是逸出了法律規管框架，當中包括彼此間的觀感、信任、情感、權力關係、形象等等，也涉及特定時刻。例如，在2019年的社會抗爭時刻，人們對政府或跟政府相關的機構，完全不信任，產生難以判定真偽的情況。這種狀況在日常裡以麻木及犬儒態度表現，但在特定政治時刻有可能會變成社會反抗及恐慌。例如本報告稍後部份討論的智慧燈柱、人面識別系統，令人產生激烈抗拒，無論對方提出多少保證及解說也於事無補。

4.3. 香港個人資料（私隱）保護制度的問題

《個人資料(私隱)條例》（下簡稱《私隱條例》）自1996年起已生效，它的源起是法律改革委員會在1994年發表的《有關保障個人資料的法律改革》報告書，當中建議政府就個人資料及私隱立法，並成立香港個人資料私隱專員公署。成立之時，雖然資訊科技的應用及發展，仍然尚在初階段（例如互聯網及智能手機仍未普及），但按照報告書所說，立法的重要背景就是預視資訊科技爆發式發展，並聚焦在資訊私隱（information privacy）之上（香港法律改革委員會，1994）。

《私隱條例》的訂立與公署的設立，主要目的是處理與個人資料及侵犯私隱相關的投訴與調查，包括搜集、處理、儲存及漏露等等，調查的主要目的是去糾正相關的做法。此外，公署也負責與各界別商討實務守則、教育與宣傳，特別跟從最新的國際規範與準則。《個人資料(私隱)條例》雖然訂明適用於公共（包括政府）及私營機構，與《香港人權法案條例》一樣，也強調把國際公約、規範與準則納入本地法律，但是，《私隱條例》在制衡政府方面的用意及作用比後者少很多。我們從以下特徵可以看到：

1. 《私隱條例》中指明，政府在執法及管理時根據法例，公署便可以說是無能為力；事實上，「防止或偵測罪行的目的」便可立即引用第58(2)條的豁免，因此，《私隱條例》對刑事執法部門的制約作用極小；

2. 《私隱條例》中亦沒有特別訂明政府違反後的後果，相關罰則（例如執行通知及拒絕執行等）主要應用在私人機構及個人；

3. 政府的全面無差別的監控活動，基本上不受公署及《私隱條例》監管，因為，公署不只一次引用2000年的一個案例（Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data [2000] 2 HKLRD 83），指若資料使用者只是在公共領域中收集及整合資料，而不是針對某一可辨別的個人，則《私隱條例》不適用。公署在2019年8月21日及2020年6月22日回應傳媒查詢時皆指出，除非相關裝置是為了「匯集關於某一已被／將被識辨身份的人士的資訊」，否則不算作「收集」（香港個人資料私隱專員公署，2019a及2020）；至於搜集及儲存之後再識別某人身份，則未能清楚確定是否為《私隱條例》所監管範圍；

4. 同時，《私隱條例》也沒有要求資料使用者（包括政府）就任何資訊及通訊技術或設備的使用諮詢私隱專員。

從過去二十多年《私隱條例》實施來看，公署專員在政府的各項工作中只是擔當諮詢及顧問角色，例如，專員是多功能智慧燈柱技術諮詢專責委員會的成員之一，政府也沒有責任在使用某項監控手段之前徵詢公署。而公署的工作，則偏向集中在監管企業、資訊網絡平台收集及使用個人資訊的操作，是否有違《私隱條例》，並跟他們商討及提供新近的國際守則，用他們的說法，是「以期在業界加強尊重個人資料私隱的文化」。在條例的修訂建議上，公署也並沒有針對最受爭議的政府監控活動，而是朝著加強監察私人機構，包括設立強制性資料外泄通報機制、資料保留時限、提高罰則等等（立法會秘書處，2020）。

還有一點與此相關，由於公署的監管工作針對網絡資訊平台、社交媒體，所以，對個別市民牽涉其中的泄露個人資料及侵犯私隱的工作特別著重。例如，2019年反修例運動及衝突期間，所謂

「起底」事件突然暴增，無論是官員、警察及其家屬，又或者是不同政見人士，都有被人在互聯網上泄露個人資料事件。根據《香港個人資料私隱專員公署 2019 年工作報告》，公署接獲4,208宗「起底」事件，並聯合警察進行行動，拘捕違反《私隱條例》的個人，去信涉事的 16 個網上平台，要求移除共 2,500多 條違法的連結。

此外，雖然《私隱條例》訂立時已意識資訊科技的發展，但是，《私隱條例》仍然傾向以一般性原則規管不同機構及科技，即所謂「原則性」及「科技中立性」。在《私隱條例》當中，只有特別針對「直接促銷」（direct marketing）的條款，至於與新型個人資料，以及隨之以來的搜集、儲存、處理等問題，並沒有特別條款處理。然而，在2020年公署提出的修例方向，建議修訂「個人資料」的定義，以涵蓋「與可識辨身份的自然人有關的資料」，算是一個進步，根據這個新定義，IP地址、定位等資料亦會包含在內。

廣義來說，保障個人資料與私隱在香港，並不只有公署及《私隱條例》。

《香港人權法案條例》第II部第14條規定，「任何人之私生活、家庭、住宅或通信，不得無理或非法侵擾，其名譽及信用，亦不得非法破壞」，原則上市民可以以此訴諸法院。《基本法》第30條訂明，香港居民的通訊自由和通訊秘密受法律的保護，除因公共安全和追查刑事犯罪的需要，香港居民的通訊自由和通訊秘密受到保護。因此，2006年訂立的《截取通訊及監察條例》，及後來在2016年作出修訂，一直受公眾關注。條例規定，只有針對「嚴重罪行」及「保障公共安全」，特定執法部門才向相關小組法官申請進行監聽，同時，亦受到截取通訊及監察事務專員監管。然而，執法部門及法官對「公共安全」的界定十分寬鬆，而且，該修訂條例裡的「通訊」只針對電話通訊，沒有涵蓋以網絡數據傳送的即時通訊、電郵等，執法部門要監控這些通訊，只需向裁判官申請即可。有議員、市民及民間團體要求擴大「通訊」定義（鄺頌晴，2016；獨立媒體（香港），2015），但不獲政府接納。

此外，包括稅務局、入境處等政府部門，各自有相關條例防止泄露市民的個人資料。同時，銀行業及保險業亦有類似條例作規管；但這些條例大都只能針對既有及傳統的個人資料。香港作為普通法地區，認為自己私隱受侵犯，可以以「違反保密責任」（breach of confidence）為理據入稟法院，追討賠償，以及申請禁制令。

總體來說，公署及《私隱條例》的設置（這裡並非指專員及相關職員個人有偏見），多只能針對民間、私人企業、互聯網，而對政府的監管制衡，以及政府與市民之間有關個人資料及私隱的爭議，可以說是幾乎無能為力。而其他的法例規管，對限制政府及與政府關係密切的大企業、機構及個人（例如受僱的黑客），尤其是在資訊科技通訊環境中對新型個人資料及私隱的威脅，幫助極為有限，成本及門檻也非常高，例如事後的民事訴訟、司法覆核及禁制令等，都要面對政府及大機構龐大的司法資源。

4.4. 外國的新實踐：歐盟的《通用數據保障條例》

香港規管資訊私隱始於1990年代，一直參考西方國家。由於美國一直只在各州就著個人資料外泄立法，在聯邦政府層面只有各部門的立法（例如健康資訊、金融資訊）等等（Houser and Voss 2018: 16），情況有點像過去香港的情形；同時，美國政府又對利用個人資料發展的互聯網經濟採取相對放任的態度，有意鼓勵以美國為基地的互聯網及新經濟大企業（如當年的Google及Yahoo，以及後來的Facebook），只打算平衡消費者的權益，因此，規管部門是聯邦貿易委員會（Federal Trade Commission），僅針對欺詐及不公平交易。

香港在全球互聯網經濟中，並不屬於領導者，而是使用者及消費者，她在私隱規管上不採取美國模式是有一定道理的。因此，在1990年代，香港政府草擬《私隱條例》時，除參考經濟合作及發展組織1980年的私隱指引外，便是1995年的《資料保障指令(歐盟指令)》（Data Protection Directive 95/46/EC）。2018年5月，歐盟的新的訂立的《通用數據保障條例》（General Data Protection Regulation）生效，公署也是亦步亦趨，除了協助業界遵守歐盟的新及高的標準（香港

個人資料（私隱）專員公署，2020），也參考當中的原則及概念，提出修訂本港條例的建議。事實上，由1990年代開始，歐盟訂立比美國的私隱規管嚴格得多的標準，是有一定的全球政治經濟議程的，就是為了回應影響力擴及歐洲以至全世界的美國新經濟而設的，並提出對資訊資本主義不同的價值觀、框架及發展策略（Hasselbalch and Tranberg 2016: Chapter 10），而斯諾登（Edward Snowden）揭露美國政府的內部機密文件及稜鏡計劃，更可能是2018年生效的《通用數據保障條例》的背景。

歐盟的《通用數據保障條例》提出的標準，主要包括：

1. 不論機構及企業是否在歐盟，只要針對所有向歐盟人士提供服務或監察的，都要受到規管。此點提出了跨越司法管轄區的規管標準；
2. 資料處理的定義採取廣義，包括任何是否自動化的收集、記錄、組織、構建、儲存、改編、經輸等等；
3. 個人資料的定義也包含所有識別代號，不限於傳統個人資料或網上代號，還包括生物特徵、經濟、文化及社交身份，包括人面識別；
4. 要求機構及企業設立保障資料主任及資料保障影響評估；
5. 在「特別類別」的個人資料（或稱作「敏感資料」）中，加入性取向、基因資料或生物辨識資料，當中包括人面識別，這類別資料需要比一般個人資料更多的理據（包括是否必需的目的）才能收集，處理上也需要更高規格。
6. 對「同意」處理個人資料上作出更嚴格規定，包括隨時取消「同意」；此外提升了「被遺忘權」；
7. 在不同司法管轄區之間資料轉移作出更嚴格限制，要受歐盟委員會評估是否有足夠保護，現在只有13個國家或地區獲發足夠度評估決定，不獲發決定或不獲准的地區，不得進行資料轉移。有一點值得注意，獲發的地區並不包括中國大陸及澳門。

正如之前所言，歐盟訂立的規管框架，帶有特定議程，是應對新型個人資料及私隱的一個取徑。它有一定效用，但只能涵蓋一部份問題，特別針對美國領導的互聯網及新經濟，以及大西洋兩岸

之間的關係。但由於它的規管框架的主導性，會令人過份專注在它所涵蓋的範疇，而忽略了其他部份，以及其他取徑。例如，把昔日歐盟的《資料保障指令(歐盟指令)》，或最近的《通用數據保障條例》，完全搬進香港的私隱專員公署及《私隱條例》，令人誤以為私隱問題就是它所涵蓋的，以為只要完善公署的監管原則與範圍，以及修訂條例便可解決問題。事實上，近年廣受關注的私隱問題，例如智慧燈柱、監控攝錄機、人面識別、網上搜證等等，暴露出專員公署的作用極為有限，尤其是碰上執法部門（例如警察），更未能符合公眾對它過高的期望。

4.5. 外國的新實踐：提防監控國家

近年歐美的一些發展，尤其是英國的例子，特別值得我們留意。

英國國會及人權團體很早便注意到政府大量監控的問題。2009年，英國上議院出版了相關報告，當中已要求英國政府修訂《數據保護法》，例如，規定政府在使用任何新的監控手段、數據收集及處理、分享數據安排等，都要進行數據保護影響評估（Privacy Impact Assessment, PIA），向公眾公佈外，並經專員公署審視及批准（House of Lords Constitution Committee 2009: point. 460）。這部份後來納入在歐盟新修訂的《通用數據保障條例》，英國雖然公投決定脫歐，但仍然會把歐盟相關標準納入英國本土法例。

英國有一個與香港的私隱專員公署相類似的資訊專員辦公室（Information Commissioner's Office），它不只是負責適用歐盟的《通用數據保障條例》，它還執行另外三個英國條例，包括《數據保護法》（2018）、《資訊自由法》（2000）及《環境資訊法規》（2004）。值得注意有幾點：

1. 資訊專員由英女王直接任命，同時，跟其他公職人員一樣，任命受「公職人員委任專員」（Commissioner for Public Appointments）監管；
2. 《數據保護法》（2018）在其第3、4部份，分別有規管執法部門及情報機關的條款，因此，資訊專員能監管執法部門，而香港的《私隱條例》則幾乎豁免；

3. 2012年所立的《自由保護法》進一步把《資訊自由法》擴充至政府部門的資料庫，由資訊專員監管部門處理個人資料的日常工作。

換言之，在西方國家，有關個人資料及私隱事務的專員，通常是獨立於政府的法定機構監管政府，特別是執法部門。而香港的相類似的法定機構及專員則沒有這種制衡權力，這權力主要用在監管政府以外的企業及機構，香港的私隱專員與政府的關係則比較像合作者。

此外，近年外國有一個新趨勢，針對個別技術，不同國家也有不同的反制措施。總體而言，並不是對所有資訊監控技術，採取擁抱態度。例如，美國三藩市、奧克蘭、柏克萊及薩默維爾已禁止市政府（包括警察部門）使用人面識別技術（Conger, Fausset and Kovaleski 2019），波特蘭市政府打算不只禁止政府使用，就連私人企業也禁止（Captain 2019）。甚至在香港，經歷2019的爭議後，部份資料收集及處理科技也被棄用。

4.5. 科技決定論與期望落差

首先，無論是政府、私隱專員、沙田第一城的業委會成員及保安公司，都嚴重低估了市民對資訊監控科技的反應，尤其是究竟市民如何理解與感知新型私隱，並沒有清晰及深入的了解。

低估的原因之一，是政府及相關監控者普遍持著一種發展主義觀點，過份強調智慧城市為全體社會帶來的好處，把智慧城市帶來的問題設定為如何盡快趕上的問題，而對它帶來的私隱挑戰重視不足。例如，2017年的《香港智慧城市藍圖顧問研究報告》中，它的口號是「智慧香港 – 擁抱創新及科技，構建強大經濟，提升生活質素，使香港成為著名的智慧城市」，在政府有關智慧城市的文件中，只提及檢討及更新私隱指引，並沒有把新資訊技術及其應用視之為潛在的挑戰與威脅。正如私隱專員所指出，現時並沒有規定要求公私營機構對新資料收集技術進行私隱影響評估，包括該科技是否會過度搜集個人資料，該技術有多大程度上是必要手段。而私隱專員公署推廣評估時只集中向企業，並沒有向政府游說或施加壓力。

原來安裝在智慧燈柱內的藍芽接受器便是一個很好的例子。我們沒有證據證明政府部門想偷偷利用藍芽設備來監控市民，但是，運輸署很明顯覺得用藍芽來測量車速是趕上先進科技，所以便馬上應用上了，因為現在車輛的收音機及音響皆有藍芽ID及訊號發出；這是一個很典型的科技決定及發展主義案例。運輸署對私隱的潛在威脅卻沒有考量，會否過度搜集能辨認市民身份的藍芽ID（一種新型個人資料），而且，更沒有考量它是否一種必要手段。香港無線科技商會執委杜振康指出，要測量車速，既可用雷達，又可用監測環境的低清攝錄機，藍芽裝置不是必需的（杜振康，2019），相反，現在有太多個人裝置都有藍芽裝置，造成私隱的疑慮。後來，燈柱委員會亦建議不安裝藍芽，運輸署也接受，這說明公眾及政府部門經研討後，也認為該設備對測量車速並不是必要的。

至於沙田第一城業委會及保安公司，對人臉識別的理解，完全以一種技術角度去看。他們都視之人臉識別為簡單的技術性資料（只是「面部的數據化特徵」），而不會去看大數據潛在的處理、流通及應用可能。他們認為，新系統可以減省人手，提升服務品質，但之前從來沒有衡量計算利弊，例如，究竟減省人手的好處，是否抵得上破壞居民對業委會及保安公司的信任？

總的來說，政府以至私隱專員公署的文件中，一直並沒有提出防止「監控國家」（surveillance state）的議程；在西方國家十多年前，這已成為公眾議題（例如英國國會在2009年的報告），甚至有相應的法律措施應對。在2013年斯諾登揭露美國政府的稜鏡計劃後，監控更成為西方國家熱門話題之一；同一時間，國際社會與學界，也關注中國的龐大監控工作，這方面在本地部份媒體更一直是持續熱點。

這些問題意識，本應在近年日益惡劣的中港關係及政治衝突之中，成為政府的議程。但是，政府似乎有意地壓下這類議程，視而不見，卻把私隱保護問題只限定在與西方國家接軌之上，例如，引入歐盟《通用數據保障條例》，對本地政治處境及市民關懷敏感度不足，沒有做出特定的應對策略，尤其缺乏聚焦在政府相關的監控問題上，於是監管與公眾的期望便有明顯落差。

雖然《通用數據保障條例》加強了對資訊企業的監管，私隱專員亦花了大量工作在這方面。但是，面對私人企業營運的資訊平台及工具，我們的受訪者傾向以個人方式規避、選擇性使用、調較來保護個人私隱，從而取得起碼的安全感；又或因為能獲得服務與便利，因此能有條件地接受。然而，我們受訪者最在意又覺得自己無能對抗的，是執法及政府部門，但這卻因為《私隱條例》的豁免（偵查及防止犯罪）而無法規管。在智慧燈柱的事例中我們看到，該計劃提出了兩年，也沒有一個專責委員會處理當中可能涉及私隱問題，在2019年8月輿論沸騰之前，私隱專員並沒有多少介入。爭議發生後，政府才匆匆成立了委員會檢討智慧燈柱，但在這個時候，私隱議題早已成為極度政治的爭議，甚至捲入社會恐慌之中了。

事實上，在私隱專員公署的日常工作中，也看到它對政府監控的忽視。例如，2018年的個人資料使用者抽查中，只涵蓋了44家不同行業的公司，卻沒有針對公營機構。另一個例子是，在眾多公署製作的小冊子、單張及宣傳中，卻鮮有教導市民如何就私隱問題向政府部門問責，特別是執法部門在何種情況下取用個人資料時為合理，卻極少提及。但是，私隱專員公署也認為，《私隱條例》當中的豁免，並非讓執法機構可以任意或不公平地收集個人資料，它甚至引用高等法院原訟法庭於Cinepoly Records Co Ltd v Hong Kong Broadband Network Ltd一案中裁定，「向資料使用者要求提供有關資料時，不能單靠空口講白話（bare allegation），而是必須提出有力的證據（cogent evidence）及有關披露的必要性（necessary）」（2019b）。但是，公署暫時並沒有在這方面向公眾（以及其他有可能被執法人員要求提供個人資料的機構）提供教育性物品及指引。

總的來說，政府傾向視私隱為可以管理的風險，對風險的理解，限於資訊科技及經濟活動帶來的資料泄露風險，而沒有（或很遲才）看到，甚至在某些個人資料被收集、生產、處理之前，資訊科技本身在特定的政治及社會條件下，會引起強烈的私隱關注。處理不當會迅速發酵成公眾恐慌，加深市民對政府公權力的不信任，捲入政治衝突與政府的正當性危機。本報告所分析反修例運動中的兩個個案便已充份說明問題。

4.6. 新型個人資料的特徵

我們可以看到新型個人資料的特徵，也是造成私隱保護的新挑戰，我們大致可以由以下幾方面去看：

特徵一：無力感與私隱

由於我們現在身處於一個大量資訊科技運作的環境，在日常生活中，我們未必對當中的私隱問題很在意，因為，個人資料的收集、生產與流通，個人又無能為力去改變，相反，又可能帶給我們服務與便利。加上政府及企業鼓吹「智慧城市」這一類科技發展主義願景，減弱公眾對各類潛藏私隱問題的意識，只會感到持續、廣泛但程度不大的擔心。因此，政府及監管部門要了解公眾關心甚麼也不容易，在問卷式民意調查中有時也未必看得很清楚。

一般受訪者認為，進入智能手機年代後會意覺得這方面的問題，他們的反應有點矛盾及含糊，可以概括為抗拒、擔心、「投降」及無奈接受：

「我呢d其實係超抗拒，當有手機，即係進入呢個智能手機時代我就超抗拒嘅，抗拒到我諗2011年啦，我就投降啦。點解會話投降呢，因為我自己工作方面都會有小小掂到即係嗰邊……」（受者者B，2020年1月11日）

「因為我唔係讀IT，我係電腦白癡嚟嘅，幾乎係，咁當然我識普通嘅操作啦，但係可能係咁，我一開始對呢樣嘢唔敏感... 呢個係人都知道，佢偷聽你講嘢。咁其實我想講嘅係，由你開始信任呢樣嘢，大數據呢樣嘢，即係ok，應該係安全，到你宜家其實每分每秒，都冇話威脅你，但係話俾你知，其實我聽緊你講嘢，就會擔心呢樣嘢。」(受訪者K，2020年1月11日)

「問：大家都覺得Facebook係一定有收集大家嘅資料？

焦點訪談小組成員（同時）：一定有啦。

問：但係大家都係繼續用嘅。

K：無可厚非。」（2020年1月11日）

「就算沒有這種燈，也會有CCTV，你走到哪裡都給人知道。所以這不是我的concern」（受訪者MC，2020年6月3日）

我們在受訪者中，普遍感受到面對資訊科技的爆炸性發展，令個人有一種無力感。

特徵二：政治立場決定私隱關注

由於我們的焦點訪談只找到立場偏向反對派的受訪者，所以我們另外找到一些人進行個人訪問作對照，當中部份人比較親建制。我們發現，政治立場很大程度決定了他們對資訊科技對私隱威脅的觀感。反對派的受訪者大部份也很抗拒智慧燈柱及人面識別的技術，認為是侵犯私隱，但在親建制的受訪者中，大部份人也不覺得有大問題。例如，我們透過問卷訪問了八位與業委會成員，他們不單接受人面識別的技術，而且，並不覺得智慧燈柱有任何問題，他們覺得這只是有人在「炒作」。我另外訪問了多位政府立場親建制的受訪者，他們有同樣的反應。

「（CCTV）係好事黎，人係要監管的。如果係謹守自己嘅原則，我地行街，你影我囉！犯法先驚CCTV啫，你有乜私隱啫？而且，係由法團、管理公司、一班專業人員負責……宜家科技愈來愈先進，係會有人可以hack 入去，但你問我，我始終覺得係利多於弊。」（業委會成員KW，2020年6月3日）

「這（智慧燈柱）完全看政府出發的目的是甚麼，如果政府單純想，怎樣實踐……滿足一個社會需求的話，這是一個很好的做法。［那你覺得香港政府怎樣？］這我不太擔心。……你現在走在街上也會有CCTV，也有人收集你的資料」（受訪者JY，2020年6月3日）

「其實都冇乜私隱，你黎咗同你影張相，就係咁簡單，人面識別只係一堆數據，你耳仔幾高，眼與眉有幾高，耳仔距離，同埋嘴唇、人中嘅距離，一大堆數字，就知道呢個人就係佢。宜家連帶口罩都做到，佢就係做呢個數據分析，佢嘅意思係，佢進入屋邨，就知道佢係我地其中一個成員，開門俾你，你係stranger，就唔俾你……就係咁簡單。」（保安公司經理，2020年6月3日）

「智慧燈柱係搜集交通及天氣資料，根本不涉及私隱問題，政府應及早介紹及解釋相關用途，免被炒作。」（業委會成員H，2020年7月30日）

親建制立場的人談話時，比較能分享監管者的角度，也信任政府等監控者，認為自己只要守法便沒有私隱問題，智能化的監管系統只是一個技術手段（「人面識別只係一堆數據」），也避無可避。

事實上，我們訪問的沙田第一城居民，相當部份是反對派的支持者，他們則持相反觀點。值得注意的是，他們也較年輕（40歲以下），覺得自己是被監視者，深深感受與想像到私隱被威脅。由於區議員兼任業委會主席二十年左右，他又是新民黨黨員，他一直又與屋邨的保安公司合作無間，同時，與他關係密切的業主代表，也多是年齡比較大的（八位回覆問卷的，有7位60歲以上）。他們覺得安裝人面識別、收集大量數據，是為了屋邨安全。這個現象也可以理解為私隱深陷在不同政治立場及年齡群體之間的關係。

以下幾個特徵，主要來自政治立場上屬反對派的受訪者。

<u>特徵三：社會及政治關係中的私隱</u>

新型私隱並不像是一個固定的領域（domain），而是隨著新資訊科技、社會科技與政治變動而衍生的想像關係（relationship）。大部份受訪者都沒有很實質地被侵犯私隱，造成嚴重傷害，但他們在想像中感受到可能的威脅。然而，這並不代表這是無中生有的，它存在於不同處境、與不同對象（政府、企業、資訊平台）的日常關係，因為這種想像，人們會持續規避、爭持及商議的箇中的關係。

首先，許多受訪者說得很清楚，他們與政府之間的關係決定了他們對私隱問題的擔憂，而他們不相信政府，也感受不到香港有有效的監管（當然，他們覺得中國大陸的問題更嚴重）：

「K：我覺得呢d資料俾政府或者大財團把握住，唔可以講冇問題，但係如果有一個好嘅制度去制衡去監察其實係冇問題嘅。但係問題係喺香港嚟講絕對係冇呢樣嘢囉，冇一個監察系統啦，冇一個好嘅制度啦，更加唔好講一個民主制度去令政府聽我哋講。所以我嘅意思係呢樣嘢其實係會concern嘅，我哋一舉一動俾人監視住，但係更加concern嘅係我哋冇一個好嘅制度去令我哋係會放心，所以會更加驚。

Z：其實我覺得係，類似囉，其實點解會擔憂呢，最主要係我哋對呢個政權失去咗信任。當然啦以前電腦計算冇咁犀利，就分析唔到影片啊，宜家電腦計算越嚟越犀利，睇片就自動AI認片，咁呢個係一個原因啦。第二個原因係揸住d數據嘅人拿嚟做乜，因為我哋對政權失去咗信任，所以先至更加驚。

A：政權其一，但係其實大財團都係□，真係唔知呢一班人想點。如果你拿住大數據，嗰把係刀嚟□其實。即係對一d普通人嚟講，你唔可以控制到但係佢可以控制到你，所以佢點用把刀，冇適當監管係唔得嘅，但係香港，sorry，監管係咩嚟□，食得□？

K: … 所以簡單d嚟講，我哋係concern嘅，除咗純粹係私隱上嘅問題，係因為我哋對政權不信任，更加concern。」（2020年1月11日）

對政府的信任關係破產，導致對私隱的焦慮及不安全感大增。根據香港大學民意調查計劃於2019年1月至6月間的調查顯示，不信任香港特區政府的受訪者，由37.1%暴升至60.2%，信任者由43.8%大跌至 27.9%。我們可以想像，私隱危機感亦會隨之而增。

面對私隱威脅，每位市民都或多或少也有一些手段去管理自己的私隱，管理的方式也呈現兩個特點，都涉及個人與外界及特定機構的關係：

a. 自我控制

由於對政府的不信任，以及感到監管機構的無力，所以，多採取自我控制，切斷某些關係，例如盡量不把個人資料，包括不用手機上網上銀行，不使用公共的Wifi（包括公司提供的），以及謹慎選擇服務供應商、手機及應用程式。除此以外，部份受訪者甚至會控制自己在社交媒體上的活動及分享的內容。

受訪者A指：「應該話你要有個概念，Facebook係條街嚟嘅...咁你喺條街都可以講得嘅嘢，你咪喺嗰度講囉。其實上網所有空間都係條街嚟□，你喺條街講得嘅嘢你就喺嗰度講囉。」

她這個比喻獲得幾乎所有受訪者認同，所以，他們也盡量不把私人事放在社交媒體，以及互聯網其他空間。其中兩位受訪者完全不加同事為朋友，不想讓同事知道自己的社交圈子內的事，另外亦有幾位受訪會同時擁有幾個社交媒體的帳戶，有些認為「私人」的事，只會限於某個帳戶。但他們也承認，有時也會免不了把屬私人的內容放了在社交媒體上。

然而，相對上，他們對於單對單通訊會比較放心，因為他們覺得只會跟信任的人通訊。而且，現在市面上的加密通訊工具，他們也會使用。

b. 中港區隔的「防火牆」

不少受訪者對中國大陸政府的監控十分敏感，既因為一直以來香港人對中國大陸有政治恐懼，也因為中國政府對互聯網實行相當嚴密的審查，因此大部份受訪者都會用各種方法建立起香港與中國大陸的區隔。

「其實我諗，即係好老實，任何app都會有嘢流出去，一定會嘅，但係個問題係，我哋去睇嘅話，係嗰d嘢會漏咗去邊度，即係相對嚟講，你漏去美國，佢走去screen你d嘢，即係佢嗰個extend唔會去到咁盡啦，唔會話真係走去審查你嗰個思想傾向個d，即係佢哋主要嚟講係去睇一個反恐，嗰方面嘅嘢會比較多。咁即係其實好老實嘅，就算冇呢d嘢，當年最古老嘅，我哋仲寄緊信嘅時候，其實佢哋都係有辦法開咗你d信，睇完之後send番俾你□，嗰陣時都有呢d嘢。只不過係當我哋去驚，去忌嘅時候呢，我哋係睇緊係一個咩樣嘅政權去拿呢d資料去做乜嘢咋嘛。……就唔會用大陸手機啦，一定唔會，因為我諗佢個backdoor會多啦，宜家都會開始揀番d app啦，睇下邊d app，譬如話大陸出嗰d，都會鏟走晒。」（受訪者L，1月12日）

正如以上所說，市民會採用一些自我管理的手段，去營造一個稍有信心的通訊環境，其中一個方法就是隔絕，或與不信任的源頭保持距離。此外，對於要到中國大陸工作的受訪者，通常會有兩部手機，一部在香港用，通常是蘋果手機，另一部在中國大陸用，通常是Android系統的手機。同時，盡量不把「私人嘢」放進在中國大陸使用的那一部。

特徵四：模糊領域裡的私隱關注

由於私隱是一種想像關係，在那些模糊而難以界定的領域裡最容易讓想像發展。例如智慧燈柱內的設備多種多樣，涉及多個政府部門，不同資訊，而且又是一個可以不斷更新升級的裝置，它的威力及可使用的可能會被無限想像；同樣，人面識別的技術可以有不同用途，接合上不同機構，因此，雖然所有使用者都不是很清楚，但它比起很多傳統個人資料更讓人感到焦慮不安。

「C：... 極端d講啦，我哋宜家喺現實世界嘅一舉一動全部都被記錄住，因為宜家IT越嚟越發展，即係你一舉一動，可能你出過街，搭過lift，個閉路電視影到你，即係嗰個moment個信息可能已經被某個人記錄咗，之後有機會被搵番，呢個人喺呢個時間出過街，咁樣。呢個係真係好恐怖，即係極端d嚟講。

K：但係呢個唔係喺好耐之前已經有，閉路電視，CCTV啊。

C：其實極端d嚟講，其實宜家隨住互聯網發展得越嚟越犀利，融入咗我哋生活裡面，我哋做嘅所有嘢我覺得已經係被記錄住囉。

B：其實我覺得CCTV一d問題都冇，因為全部斷開嘅，但係宜家有大數據，可以將全部嘢連埋。

C：冇錯，將所有嘢融合埋一齊。

A：如果own呢d資料嘅parties係分散嘅佢搵唔到d資料，因為資料太碎片啦，但係當你係一個政府，或者一個好大嘅財團去gather一大堆咁樣嘅資料呢，其實就危險，因為佢實在係太容易search啦。」（受訪者C，2020年1月11日）

「智慧城市」或「智慧燈柱」中的「智慧」會令人更想像出無限可能，尤其因為所有資訊技術都有可能透過互聯網、內聯網連結起來，再處理與分發，而想像到的通常都是負面的：

「M：我驚係多過CCTV嘅用途，佢智慧嗰個意思即係比CCTV更加多出，不過唔知多出咗d咩。即係CCTV可能就係拿段片去辨識，但係智慧燈柱佢本身……

L：其實宜家d CCTV唔單止係人面辨識，佢裝d唔同嘅software可以睇埋你嘅動作，可以用呢樣嘢去分辨到你。即係CCTV唔連上網，咁其實乜問題都冇，即係你純粹錄影。但係個問題係你錄影之後你要做好多process先可以將d資料用到，但係如果當你，一係連上網，佢已經即時可以做到好多嘢。」

一位政治立場並非反對派，也不那麼抗拒智慧燈柱的受訪者，亦表示理解部份人對智慧燈柱的反感與恐懼。她說：「走在街上會給人（私人公司的CCTV）收集，但燈柱的收集是，政府拿我的

數據去幹嘛？我在一家店或路邊，會給人收集，但它不會拿我的數據去幹嘛，或去分析，但是，智慧燈柱就會拿我的資料去分析，而且我沒有同意。」（受訪者MC，2020年6月3日）

特徵五：突發政治化

私隱的關注會突然在極短暫時間爆發，它以突發社會事件表現，針對特定科技物品、措施、權威機構；由於公眾感到缺乏參與途徑，又感到無力，所以有可能以體制以來的方式表達，與體制無法形成相對穩定與平和的協商關係。

在智慧燈柱事件中，由發酵到爆發，在兩個月以內發生。在2019年7月前，社會輿論幾乎毫無動靜，由於事件涉及十分複雜的技術問題，在政治氣氛還可以之時，並無太多討論與爭議。可是，當政治氣氛改變時，會很快獲得強烈關注甚至恐慌，以至發展成激烈的行動。沙田第一城的門禁系統爭議，亦有相類似的情況。在8月前，幾乎只有業委會成員才知悉這個試驗計劃，受訪的一般居民表示，他們只在2019年8月時才從互聯網及社交媒體上得知，因為，管理公司及業委會沒有大肆宣傳及諮詢居民。但是，當居民知道該試驗計劃時，相關資訊已夾雜在大量質疑、反對以至政治聯想的之中，因此容易短時爆發成質疑業委會主席的抗議。

第五章：政策影響及建議

1. 重建市民與政府的信任關係

   在大量市民與政府信任關係破產之際，任何私隱保障的政策改動成效都極為有限，甚至可以說是徒勞無功。我們在訪談中，部份受訪者甚至認為，任何政策改動也沒有用。因此，重獲市民對政府的信心是最為關鍵，除了一些較大的制度改動外（例如政制改革，這不在本報告的關注範圍），政府應主動及全盤向公眾承諾，不進行某些特別敏感的監控手段，自覺自我限制政府自己的權力，例如，承諾不會進行自動化及無差別的監控手段，包括如中國大陸政府進行的全民人臉認別監控、通話監聽及社會信用系統等等；

2. 限制政府處理資料的權力

   同樣道理，政府應考慮參考英國2012年訂立的《自由保護法》當中有關限制政府搜集、儲存、處理及使用市民個人資料的活動，公民團體及政黨應合力以限制推動立法；

3. 私隱影響評估（Privacy Impact Assessment, PIA）

   現在專員公署只對政府及私人機構建議進行評估，但沒有法定地位，應修訂法例使之成為法定要求，一定規模的公私營機構及企業，尤其在使用新的數據處理技術前，應進行評估。對於部份被特定部門標示為有問題或甚至被棄用的資訊科技手段，相關評估應與其他政府部門及私人機構分享，除了特殊情況，否則不應被重新使用。同時，相關評估應有一個公眾諮詢及討論部份，並預先讓個人資料擁有者參與其中。無論政府、企業、業委會、管理公司，不應過份依賴既有的諮詢渠道（例如區議會、業委會成員）。

4. 資料流向及處理流程圖

由於市民對私隱最大的恐懼來自不清楚的個人資料流向及處理方法，所以，無論是政府或企業應以更簡潔的方法，呈現資料的流向及處理，尤其是要標示出這些資料與政府、執法部門資料庫之間有何區隔，在何種條件也才會交予，同時，也應標明與其他司法地區（特別是中國大陸）的防火牆區隔。

5. 情報事務專員

《中華人民共和國香港特別行政區維護國家安全法》在十分短促的時間內訂立，引起社會爭議甚至恐慌。政府、政黨及公民團體應仿傚英國，設立有獨立性的情報事務專員（Intelligence Services Commissioner），檢視有關國家安全的執法活動中的資料搜集活動，是否有違相關準則及指引。

第六章：結論

從以上案例可見，「智慧城市」中最值得我們關注的，是有關運用大數據、資訊收集及處理系統進行城市治理的問題，當中涉及十分敏感的私隱議題，但政府及業界的「智慧城市」說法，過份強調只有光明的科技化前景，不單未能解決以上問題，甚至會製造更多問題。

香港自1990年代中以來，雖然有一個表面上跟得上國際標準（歐盟）的治理架構，但是，卻更針對性地處理到公眾對「監控國家」的關注及恐懼。這些關注與恐懼又與大數據有關，因為，大數據的大量收集及處理，製造了廣大而又界定不清的想像空間，當中的私隱已超出了特定的個人資料，而是無法清楚理解的、模糊但又與個人相關的領域。因此，讓市民感到個人的一切被監控與侵犯，隨時會造成無法想像的傷害。而在香港這種缺乏西方國家的民主制衡體制下的社會裡，又遇上香港自2014年以來連串的政治危機，包括2019年的反修例運動，以及最近的港區國安法立法，市民對政府，尤其是執法部門產生信任危機之時，這些關注與恐懼會更為嚴重。這亦是本報告討論的兩個個案的重要背景。

在這些新個人資料及私隱領域中，個人往往感到自己無能為力，但是，當政治氣氛轉變後，尤其是個人與監管機構的信任大跌，政治立場變得兩極化，無力感又會突變成社會恐慌與集體激烈抗拒。

因此，首要是重獲及重建市民信任，這一切都在於是否能建立起民主監察及制衡制度，這是極度複雜及困難的，更根本是一個政治體制問題。然而，我們相信，從資訊科技及私隱角度，可以作出第一小步。這一小步，政府應該更主動，把全面監控社會的問題提上公共議程，參考普通法民主國家，修訂及增訂相關法例，主動約束政府的權力，建立起制衡公權力、大企業及資訊科技發展的機制。

舉行公眾發布會的詳情

本研究除了承蒙香港特別行政區政府政策創新與統籌辦事處的「公共政策研究資助計劃」資助外，也獲得「文化及媒體教育基金」（Culture & Media Education Foundation）的協助及合作，初步研究成果亦曾在基金會主辦的「2019網絡媒體高峰會」上發表。

現正計劃在基金會於2021年1月17日舉辦的「網絡媒體高峰會」上向公眾發表報告，到時亦會邀請相關業界代表等出席評論回應。詳情會於稍後公佈。

此外，我們正在籌備撰寫學術論文，並物色適合的研討會及學術期刊發表。

參考書目

Acquisiti, A and Gross, R (2005) “Information revelation and privacy in online social networks (the facebook case),” in Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES), November 2005.

Barnes, S. B. (2006) ‘A privacy paradox: Social networking in the United States’, First Monday. firstmonday.org. Available at: http://firstmonday.org/article/view/1394/.

Floridi, L. (2005) ‘The Ontological Interpretation of Informational Privacy’, Ethics and information technology. Springer, 7(4), pp. 185–200.

Hargittai, E and Marwick A (2016) “What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy. International Journal of Communication 10: 3737–3757.

Hull, G. (2015) ‘Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data’, Ethics and information technology. Springer, 17(2), pp. 89–101.

Kitchin, R. (2014) ‘The real-time city? Big data and smart urbanism’, GeoJournal. Springer, 79(1), pp. 1–14.

Litt, E. and Hargittai, E. (2014) ‘Smile, snap, and share? A nuanced approach to privacy and online photo-sharing’, Poetics . Elsevier, 42, pp. 1–21.

Taddicken, M (2014) “The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure.” Journal of Computer-Mediated Communication 19 (2014) 248–273.

Lutz, C., Hoffmann, C. P. and Ranzini, G. (2020) ‘Data capitalism and the user: An exploration of privacy cynicism in Germany’, New Media & Society, 22(7), pp. 1168–1187.

House of Lords Constitution Committee. (2009) *2nd Report, Surveillance: Citizens and the State*.

Houser, K. A. and Voss, W. G. (2018) ‘GDPR: The end of Google and facebook or a new paradigm in data privacy’, Richmond Journal of Law & Technology 25(1): p. 1-109.

Hasselbalch, Gry and Tranberg, Pernille. (2016) Data Ethics: The New Competitive Advantage. København: Publishare ApS.

The World Bank. (2015) “Smart Cities.” 8 January, URL: https://www.worldbank.org/en/topic/digitaldevelopment/brief/smart-cities

Conger, K., Fausset, R. and Kovaleski, S. (2019) “San Francisco Bans Facial Recognition Technology.” New York Times, May 14. URL: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Captain, S. (2019) “Portland plans to propose the strictest facial recognition ban in the country.” Fast Company. December 2. URL: https://www.fastcompany.com/90436355/portlands-proposed-facial-recognition-ban-could-be-the-strictest-yet

香港法律改革委員會小組，1994，《有關保障個人資料的法律改革》，香港：香港法律改革委員會。

香港個人資料私隱專員公署，2019a，〈公署回應有關政府安裝智慧燈柱所引起的私隱關注〉。URL: https://www.pcpd.org.hk/tc_chi/news_events/media_enquiry/enquiry_20190821d.html

香港個人資料私隱專員公署，2019b，〈公署回應有關香港警察隊員佐級協會的聲明中提及的豁免事項的查詢〉URL: https://www.pcpd.org.hk/tc_chi/media/response/enquiry_20190627.html

香港個人資料私隱專員公署，2020，〈公署回應傳媒查詢有關燈柱外掛裝置涉及私隱的事宜〉。URL: https://www.pcpd.org.hk/tc_chi/media/response/enquiry_20200622.html

立法會秘書處，2020，〈政制事務委員會：立法會秘書處為 2020 年 1 月 20 日會議擬備的背景資料簡介《個人資料(私隱)條例》的檢討〉。URL: https://www.legco.gov.hk/yr19-20/chinese/panels/ca/papers/ca20200120cb2-512-4-c.pdf

鄺頌晴，2016，〈嚴防「網絡老大哥」〉，《蘋果日報》，3月17日，「論壇」。

獨立媒體（香港），2015，〈聲明： 要求廉署及警方交待接觸黑客公司 修訂《截取通訊及監察條例》保公眾私隱〉，《香港獨立媒體網》。URL: https://www.inmediahk.net/node/1035960

香港個人資料（私隱）專員公署，2020，《歐洲聯盟《通用數據保障條例》2016最新資料》，香港：香港個人資料（私隱）專員公署。

2018，〈智慧城市藍圖 7 成青年未聞 不知九龍東作試點團體倡製短片宣傳〉，《香港仔》，9月27日。

杜振康，2019，〈【2019網絡媒體高峰會】「燈柱有智慧，市民冇私隱？」Smart City的新危機與可能〉上的發言。URL: https://www.youtube.com/watch?v=TgD635kKlms

附錄一：受訪者名單

焦點訪談
受訪者B，男，60歲
受訪者Z，男，40歲
受訪者C，男，30歲
受訪者Y，女，25歲
受訪者K，男，25歲
受訪者A，女，40歲
受訪者T，男，35歲
受訪者M，女，22歲
受訪者R，男，30歲
受訪者L，男，55歲
受訪者T，男，30歲
受訪者P，女，40歲

其他個人訪談
受訪者KC，女，28歲
受訪者WY，女，34歲
受訪者XH，男，30歲
受訪者WC，女，32歲
受訪者KC，女，30歲
受訪者CN，男，30歲
受訪者WS，女，33歲
受訪者MA，女，40歲
受訪者CJ，男，39歲
受訪者SA，女，36歲
受訪者AL，女，35歲
受訪者EL，女，39歲
受訪者MC，女，24歲
受訪者KY，男，24歲

沙田第一城個人訪談
業委會成員KW，男，60歲
管理公司經理，男，60歲
受訪者WH，女，25歲
受訪者AD，男，23歲
受訪者BN，男，30歲
受訪者CS，男，30歲
受訪者DY，男，40歲

沙田第一城問卷（八名前任業主代表）
業委會成員A，女，51-60歲

業委會成員B，男，60歲以上
業委會成員C，男，60歲以上
業委會成員D，男，60歲以上
業委會成員E，男，60歲以上
業委會成員F，男，60歲以上
業委會成員G，男，60歲以上
業委會成員H，男，60歲以上

附錄二：訪問問題

1. 焦點訪談及個人訪談的問題

a.關於設備

i. 正在使用多少部手提電話？不同電話的角色分別是什麼？

ii. 從什麼時候開始有電話的分工？為什麼有這樣的分工？

iii. 有人認為使用不同的電話處理不同事務有助於私隱保護，你的看法？

iv. 使用IOS系統還是Android系統，選擇系統的標準是什麼？

v. 兩個系統在私隱安全性上有什麼區別？

vi. 是否遇到過手提電話造成的私隱洩露問題？請舉例說明。

vii. 如何看待手提電話帶來的私隱洩露問題？有什麼應對策略？

b. 關於Apps

i. Facebook上是否存在私隱洩露情況？若是，請舉例說明。

ii. 如何保護Facebook上的個人私隱？

iii. Google上是否存在私隱洩露情況？若是，請舉例說明。

iv. 如何保護Google上的個人私隱？

v. 有些第三方平台需要用Facebook account或Google account登入，你如何處理？是否擔心由此造成的私隱洩露，為什麼？

vi. 你認為Facebook、Google這類大企業對個人使用者的私隱保護程度如何？你是否信任這些大企業，為什麼？

vii. 是否使用telegram？為什麼使用telegram？

viii. telegram和一般通訊軟件的區別是什麼？什麼情況下使用telegram？什麼情況下使用一般通訊軟件？

ix. 如何管理社交軟件上的私隱問題？譬如有些人在ig上分享生活，在Facebook上分享政見，你的策略是什麼？為什麼？

x. 你平日使用什麼App？會否擔心這些App會洩露私隱？如何應對？

xi. 會否因為私隱問題拒絕使用某些App？具體是哪些App？

xii. 是否有意識地將常用網絡工具進行分隔？具體來說如何分隔？

c.變化

i. 從什麼時候開始意識到私隱洩露是一個問題？什麼契機令你有了這個意識？

ii. 對私隱的意識在過去十數年間是否有變化？若有，有了什麼樣的變化，變化的原因是什麼？

d. 關於智慧燈柱

i. 對智慧燈柱有幾大程度上的了解？

ii. 是否留意到8月示威者拆燈柱的新聞？什麼時候留意到？對此你的看法？是否有必要拆燈柱，為什麼？

iii. 你是否擔心燈柱上的攝像頭對私隱的侵犯？為什麼？

iv. 智慧燈柱收集到的數據你認為應該如何處理？（使用與儲存上）

v. 關於CCTV

vi. 你對CCTV的看法？是一種保護還是一種對私隱的監控？為什麼？

vii. 對政府CCTV和民間私人CCTV的看法會否不同？若然，具體來說是什麼不同？為什麼會不同？

viii. CCTV越來越多，你的看法？有什麼應對的策略？

e. 關於eID

i. 對eID有幾大程度上的了解？
ii. 對eID的看法是什麼？支持還是反對，為什麼？
iii. 是否認為eID對個人私隱是一種侵犯，為什麼？
iv. 政府已經在推行eID，你認為有哪些可行的措施可以有效保護市民私隱？為什麼？

2. 問卷問題（沙田第一城業委會成員）

-你住在本屋苑多少年？
-你是否業委會成員？擔任了多久？
-你對業委會的工作是否滿意？原因？
-你對保安公司的工作是否滿意？原因？
-你對現在保安系統中的監控攝錄機有何評價？
-你多大程度上認同現時保安系統中的監控攝錄機的評價？
-你對現在保安員的設置有何評價？
-你對於現在保安員的設置有何評價？
-你對匙卡作為保安措施有何評價？
-你對於匙卡作為保安措施有何評價？
-整體來說，你是否滿意第一城的保安系統？原因？
-你認為屋苑有沒有一些重大的保安風險？
-你認為屋苑的保安系統該如何改善？
-你是否同意安裝新的智能門禁系統？
-你何時知道提升大廈保安智能門禁系統的建議？
-你最初如何知道大廈保安智能門禁系統的建議？
-你贊成安裝人工智能面部識別系統嗎？
-你對原來擬安裝的人工智能面部識別系統有何意見？
-你對原來擬安裝的訪客QR code系統有何意見？
-請問以下有哪些項目你認為屬於私隱（privacy）？
-去年8月發生智慧燈柱是否侵犯私隱的爭議，你有沒有聽過？
-你認為安裝在公共空間（街道及行人道）的智慧燈柱是否侵犯私隱？
-你對智慧燈柱的評價是？
-你最關注的私隱問題是甚麼？
-受訪者基本背景
年齡
家中成員數目
家庭每月收入
受教育水平