International Journal of Communication 13(2019), 1684–1698 1932–8036/20190005

Who Decides What Is Personal Data? Testing the Access Principle with Telecommunication Companies and Internet Providers in Hong Kong

LOKMAN TSUI
STUART HARGREAVES[1]
The Chinese University of Hong Kong, Hong Kong

Do personal data protection laws allow citizens to access their personal data? We answer this question by testing the data access principle of the Personal Data Privacy Ordinance (PDPO) with telecommunication companies and Internet providers in Hong Kong. In our study, we submitted data access requests to telecommunication companies and Internet providers for a range of information, including subscriber information, call logs, IP addresses, geolocation data, and whether they had shared any of this data with third parties. We argue that the telecommunication companies failed to (1) let users see their personal information in a comprehensive manner, including IP addresses or geolocations; (2) tell users whether they indeed process such information; (3) offer the possibility of correction or deletion; and (4) tell users whether they have shared this data with third parties, including law enforcement.

Keywords: access principle, personal data protection, surveillance

The data access principle grants anyone the right to request access to his or her data from a data controller, in theory. But how well does the data access principle work in practice? We answer this question by testing the effectiveness of the data access principle of the PDPO with telecommunication companies (telcos) and Internet providers in Hong Kong. We submitted data access requests to telcos and Internet providers for a range of information, including subscriber information, IP addresses, geolocation data, and whether they had shared any of this data with third parties.

Lokman Tsui: lokman.tsui@gmail.com
Stuart Hargreaves: stuart.hargreaves@cuhk.edu.hk
Date submitted: 2017–10–03

[1] This research project received a C-Grant from the Centre for Chinese Media and Comparative Communication Research and was made possible with the help of the Citizen Lab at the University of Toronto, Inmedia Hong Kong, and Keyboard Frontline. The authors especially want to thank Mr. Craig Choy, Miss Glacier Kwong, Miss Yee Ting Yu, and Miss Michelle Lam for their invaluable help. The authors also thank Miss Rachel Cheung, Miss Karen Hung, and Miss Kinko Wong for their research assistance.

Personal data collected and gathered by the telcos and Internet providers hold great commercial value and represent a massive and growing market globally. According to *AdAge*, the global market for telco user data was worth $24 billion in 2015 and is estimated to be worth $79 billion by 2020 (Kaye, 2015). However, given the presence of various data protection laws, companies seeking to profit from this global market for telco user data face potential challenges. SAP, for instance, has stated that it is primarily focused on selling its services in North America and the Asia-Pacific region, "because it cannot get the data it needs from telcos representing consumers in the E.U., where data protections are stricter than in the U.S. and elsewhere" (Kaye, 2015, para. 8). In North America, following significant industry lobbying, the United States Congress voted in 2017 to introduce rules to expand the ability of Internet providers, including the cable and telephone industry, to harvest and sell personal information they gathered from monitoring the actions of their users. But what about the state of personal data protection in the Asia-Pacific region, including in Hong Kong?

Adopted in 1996 by the Hong Kong government, the PDPO was the first personal data protection framework in the Asia-Pacific region. A key provision of the PDPO—and central to our project—is the "data access" principle, which allows residents to ask data controllers for information held about them and to correct it if it is inaccurate. A key reason for granting citizens the right to access their own personal data is that this right is essential to safeguarding personal data protection. The privacy commissioner cannot monitor every institution; thus, by allowing citizens the ability to monitor the institutions that hold their data, the idea is that this will keep the institutions accountable and facilitate the necessary trust. The PDPO's access principle is modeled on a similar provision in the E.U.'s Data Protection Directive. Newman (2008) has argued that privacy rules from the European Union have gained more traction and wider adoption than the rules of the United States, suggesting that the Hong Kong case will be, to some extent, representative of the experience of other jurisdictions that similarly have adopted the European Union data privacy regime—or, at the very least, serve as a useful baseline for these future studies. Hong Kong also has one of the highest penetration rates of smartphones in the world with a mobile subscriber penetration rate of 237% as of June 2017, making it a very attractive market for telcos to harvest personal data (Office of the Communications Authority, 2017). There has also been growing concern about state surveillance in Hong Kong among activists and civil society groups associated with democratic reform and the Umbrella Movement (Hargreaves, 2017; Tsui, 2015). An effective data access principle might make individuals aware of the kind of information about them that is relatively easily obtainable by the state. Together, these factors suggest Hong Kong represents an interesting strategic case study for determining the effectiveness of data access principles in data protection regimes generally.

Literature Review

The access principle has been called "perhaps the most important privacy protection safeguard" (OECD, 1980, para. 58; see also Bygrave, 2001) and is included as the right of access under the General Data Protection Regulation. The access principle has been part of the PDPO since it came into force in 1996 and thus has been around for more than two decades in Hong Kong. The access principle consists of four components:

> to know that an organization is indeed processing information about one; to see that information; to correct or delete it if it is inaccurate, obsolete, or incomplete; and to have some means of redress if the organization is not sufficiently forthcoming or compliant. (Bennett & Raab, 2006, p. 121)

On a structural level, the access principle empowers the data subject to exercise a limited form of surveillance on the institution collecting his or her data. Brin (1999) has long argued that there is little we can do to prevent institutions from gathering data on us, but instead, we should focus our attention on countersurveillance, where we watch the institutions that are watching us. The access principle in this sense is an implementation of Brin's suggestion of countersurveillance, allowing the individual to monitor the institutions that hold their personal data, ensuring a level of transparency, accountability, and responsibility.

Despite the importance of the access principle for ensuring privacy protection and that it has been around for decades, relatively few scholars have done research on it. Perhaps the most comprehensive work was done by Norris, de Hert, L'Hoiry, and Galetta (2017, p. 2), who called the right of access the "natural precondition" of the ability to exercise all the other rights related to privacy. They submitted access requests in ten different European jurisdictions, across a range of institutions and companies, and found significant differences in what they refer to as the "law in books" and the "law in action," suggesting that although the law might look strong on paper, the actual state of protection in practice is a lot weaker. They argued that citizens face significant barriers even getting to the point of how and to whom to submit a request to, and even if they manage to submit a data access request successfully, it is unlikely they will get a meaningful response (Norris et al., 2017). Similar findings were made by Ausloos and Dewitte (2018), who submitted access requests to sixty institutions across the European Union. Like Norris et al. (2017), they argued that the access principle was not working in practice and found that access rights are largely not adequately accommodated. Issues that were common across all the controllers included a lack of awareness, having no idea or scope of the access principle; lack of organization, including no architecture in place to handle requests; and lack of motivation—such as delays, bad faith, and a long time to get a reaction. In another research, access requests were submitted to 32 private and public organizations in the Netherlands by Asghari, Mahieu, Mittal, and Greenstadt (2017), who found that the process was disorganized, with some relying on evasion tactics. Last but not least, an important pioneering study was done by Hilts and Parsons (2014) in the Canadian context. Examining how telcos and Internet providers collect, process, or share our personal data, and how effective personal data protection laws are in protecting our privacy, Hilts and Parsons (2014) concluded that Canadian privacy law does not work well and is in urgent need of reform. They also argued that from their findings, the definition of personal data is, at best, unclear. Together, the research so far has primarily focused on testing the access principle in Western countries across a large and wide range of institutions. To build on this body of knowledge, it would make sense to test the access principle in countries and regions outside of the European Union and to continue to test the access principle by zooming in on a particular industry, allowing for a more detailed or in-depth study, such as the one done by Hilts and Parsons (2014).

Taking a step back, the fundamental building block of personal data protection laws is the concept of "personal data." But what is "personal data," and why does its definition matter? According to the PDPO, personal data is "any information that directly or indirectly allows you to infer the identity of a living individual" (PDPO, 2013, para. 2). "Personal data" as a legal categorical concept divides the world into data that is personal and data that is not personal. Baked into this category is the assumption that anything that is "personal data" is vulnerable to privacy harm, but other (nonpersonal) data is not. In other words, any exercise in defining data as personal (or not) therefore also becomes a question of whether the data in question is worthy of legal protection. In the context of telcos and Internet providers, this raises questions about whether data such as IP addresses and geolocations can be defined as personal data. IP addresses can reveal what websites an individual has visited, whereas geolocation data can reveal where an individual was at what time. Legal scholars have argued that IP addresses should be considered personal data. For example, Schwartz and Solove (2011, p. 1840) suggested that "IP addresses can lead to identification of a person even without account information from an ISP," arguing that IP addresses should be considered personal data, but especially so in the case of the ISP. However, researchers have also argued that the "law in books" might not always match the "law in action" (Norris et al., 2017, p. 1), and that especially the definition of personal data can be problematic (Schwartz & Solove, 2011; see also Purtova, 2017). One way to answer these questions is to test the access principle with telcos and Internet providers.

Nevertheless, testing the access principle with telcos and Internet providers remains largely understudied. Ohm (2008) argued that the lack of studies on Internet providers represented an important oversight, because Internet providers potentially know just as much if not more about their users than Google or Facebook. According to Ohm (2008), "Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP). ISPs carry their users' conversations, secrets, relationships, acts, and omissions" (p. 1417). He continued to argue that "until the very recent past, they had left most of these alone because they had lacked the tools to spy invasively, but with recent advances in eavesdropping technology, they can now spy on people in unprecedented ways" (Ohm, 2008, p. 1417). Published in 2008, his point about technological advances creating new economic incentives for ISP surveillance becomes even more salient now, given the development and importance of big data. It is against this backdrop that we need to understand the 2017 decision by the U.S. Congress to allow Internet providers to sell their users' information, or why *AdAge* predicts a $79 billion global industry of personal data by 2020, what Zuboff (2015) has dubbed "surveillance capitalism." More recently, Viljoen (2018) has argued that "Facebook's surveillance is nothing compared with Comcast, AT&T and Verizon" (article title).

There is little to no research done on the access principle of the PDPO in Hong Kong. However, some scholars have researched the PDPO more broadly (Greenleaf & McLeish, 2012). Others have looked at the PDPO's ability to protect privacy about e-government initiatives (Yu, 2005), cookies (Mo, 2015), and more traditional avenues, such as records held by employers or medical records (Cheung, 2012). Cheung (2012) argued that there is a rising awareness of the importance of personal data protection given the increasing number of complaints, especially in direct marketing. The Privacy Commissioner's Office (PCPD) has also reported that the number of complaints has been on a steady rise in the last few years (PCPD, 2016a). The 2010 Octopus case represents a key moment in the development of public awareness of privacy issues in Hong Kong and may help explain this rise. Octopus facilitates a smart card

service allowing its users to pay conveniently for a range of services, including transport, convenience stores, etc. However, news broke in 2010 that Octopus was selling user data—including payment histories and addresses—to third parties, including insurance companies, for direct marketing purposes. This led to widespread public outrage, and ultimately to a strengthening of the PDPO, with an amendment enacted in 2012 that strictly limited the ability of companies to conduct direct marketing based on the personal data of Hong Kong residents. In recent years, there also has been increasing concern about surveillance in Hong Kong, alongside the influence of China on the rule of law in the SAR (Hargreaves, 2017; Tsui, 2015). However, despite increased public awareness of the importance of personal privacy, almost all the research here are legal analyses of the PDPO and related court cases; there are no studies examining whether the access principle is effective in protecting people's personal data in Hong Kong in practice.

Methodology

The goal of the project is to test how telcos and Internet providers in Hong Kong respond to the access principle. The project consisted of two phases: the first phase was primarily preparation work for the submission of access requests, whereas the second phase consisted of the actual submissions and the analysis of the results.

Preparation for Submission

We recruited volunteers by sending an email to university students, asking them to participate in the research project. The students were a mix of graduate and undergraduate students and mostly from a communication or journalism background. They received no compensation for participation in this study.

For the study, we selected the seven major telcos and Internet providers in Hong Kong: SmarTone, Three, Hong Kong Telecom, Hong Kong Broadband, i-Cable, China Unicom, and China Mobile. We recruited a total of ten volunteers, making sure that we had at least two volunteers for each telco (some volunteers had accounts with multiple telcos). We looked up the contact information of the company's privacy officer, to whom the access request would be sent; some accepted email, while others would only accept requests by postal mail. Finally, we notified and explained our study to the PCPD. We also reached out to the telcos, but they showed no interest in meeting with us to talk about the study.

The Submission Process

The data collection ran from January to August 2016, over half a year. In an email, we explained to the volunteers our research as well as their rights under the PDPO, including explaining the access principle, and that the telco or Internet provider was legally required to give them a reply in writing within forty working days.

To ensure methodological consistency, we provided the volunteers with the same template letter. We asked them to fill out the template with their personal information, to include a copy of their identity cards, and to send them to the privacy officer of their telco(s). We further explained that, for our research,

we had no need to know the specific data they got back, but that we were instead interested in the data types, or, in the case of denial, the specific language used for denying access to the data. Finally, we asked the volunteer to notify us if they got a response. If there was no follow-up, we would contact the volunteer after forty working days, the period in which the telco is legally required to respond.

The template letter specifically mentions the access principle under the PDPO, requesting access to the following data:

- Subscriber information that you store about me, my devices, and/or my account;
- Call logs (e.g., numbers dialed, times and dates of calls, call durations, routing information, and any geolocational or cellular tower information associated with the calls);
- Text and multimedia messages (sent and received, including date, time, and recipient information);
- Mobile app data—information collected about me or persons/devices associated with my account while using one of your company's mobile device applications;
- Geolocation data collected about me, my devices, and/or associated with my account (e.g., GPS information, cell tower information);
- IP address logs associated with me, my devices, and/or my account (e.g., IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit, and the times, dates, and port numbers);
- Disclosures to third parties: any information about disclosures of my personal information or information about my account or devices provided to other parties, including law enforcement and other state agencies; and
- Other: any additional kinds of information that you have collected, retained, or derived from the telecommunications services or devices that I, or someone associated with my account, have transmitted or received using your company's services.

We specified the date range as follows: "from the creation of my account or from the earliest date since your company has retained my data (whichever is earlier) until the date of this request" with the goal to find out the data retention period (i.e., how long telcos keep this data).

Findings

We sent two requests to seven telcos for a total of fourteen requests. Of these fourteen requests, the telcos all gave a response within the forty-day period. The telcos all answered that they could provide the basic account information and call logs. None of the telcos would give access to any of the other data we requested, including IP addresses and geolocation data associated with the user's account. Throughout the process, we encountered many challenges including evasion tactics and a lack of awareness of the access principle on the side of the telcos. What follows is a more detailed description of these challenges, organized in the following manner: data collection, data retention, data disclosure, and comments on the overall process of a data access request.

Data Collection: What Personal Data Do Telcos Collect?

Though a response to a data access request is legally mandated under the PDPO to be sent in writing, the telcos' initial response was often not to send a written response back to the volunteers. Instead, representatives—often from the customer relations department—made phone calls to the volunteers to respond to the data access requests. Some asked if the volunteer understood what he or she had requested; others gave the volunteers the impression that they were trying to discourage them from making the request, similar to the evasion tactics mentioned by Ausloos and Dewitte (2018). Almost all representatives said over the phone that they could not comply with the request because most of what the letter requested was not personal data, except for the subscriber information and the call records, which volunteers could find on their website, and that they considered this request completed as per the phone call. As mentioned, the law requires a written response, so in such cases, we asked the volunteers to contact the telco again and ask for a response in writing. This met with initial resistance from the telco until the volunteer pointed out that a written response is legally required under the PDPO.

Telco responses to the data access requests can be broadly categorized in two types: The first type of response is the legal response. Here, telcos argue that the requested data is not "personal data" as they interpret it; therefore the request was not bound by the PDPO, and they had no obligation to provide access to this data. Examples include the following response from China Unicom (emphasis ours):

> Kindly take note that we are unable to provide the following information which is not collected, held or retained by us **or is not considered as personal data**:
>
> a. All logs of IP addresses associated with you, your devices, and/or your account.
> b. The geo-locational information about you, your devices, and/or associated with your account.
>
> Here's another example from Hong Kong Broadband:
>
> According to the Personal Data (Privacy) Ordinance, personal data means any data:
>
> a. relating directly or indirectly to a living individual;
> b. from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
> c. in a form in which access to or processing of the data is practicable.
>
> As per our tele conversations on XXXX 2016, we may provide the listing of subscriber information (i.e., item (b) of your letter) as **other items either do not comply with the above definition, or the requested data are not related to our business**. . . .
> Also, in accordance to Part 8 of Personal Data (Privacy) Ordinance, it provides exemptions from access and use limitation requirements for data which are likely to prejudice security, defense and international relations, crime prevention or detection; assessment or

> collection of any tax or duty, news activities; health; legal proceeding; due diligence exercise; archiving; handling life-threatening emergency situations etc.

This response starts with citing the legal definition of personal data according to the PDPO. They then state that the requested data do not comply with this definition, again in their interpretation. They also felt compelled to include Part 8, which states there are certain exemptions that give them the right to prevent access to the requested data. In addition to arguing that the requested data is not personal data, they are also trying to argue that if the data were to be personal data, there are other reasons (e.g., the exemptions) why they might not be able to provide access.

The other type of response is what we call the Ostrich response (i.e., "we pretend you never requested this data"). A typical response is to respond to the request for the data types they can or wish to comply with but to ignore the rest of the request. Here is an example from Hutchison Telecommunications Hong Kong:

> We refer to your data access request dated XXXX. Please be informed that the handling fee of this request is HK$200, based on our understanding of Personal Data we keep of you. Besides, please note that bill statement and detailed call records for the last six months, if applicable, are available on our website XXXXX. Should you require a paper copy of any specific bill statement/detailed call records, or a copy of your contract, our charge is XXX per month for bill statement/detailed call records, and $80 per contract, respectively. Please let us know whether you wish us to send you a paper copy of any particular bill statement/detailed call record and/or your contract.

This response only mentions the availability of bill statements, call records, and a copy of the contract. It pretends that the volunteer never asked for access to other types of data, including IP addresses and geolocation data.

A slightly more revealing example is one by SmarTone, where they simply say the request for certain data types is "N/A" without stating any reason.

> We refer to your letter relating to the enquiry on the captioned, please find below our responses to your questions:
>
> * You can login to "My Account" via our corporate website to check your past 12 months call details record.
> * N/A
> * N/A
> * N/A
> * Please refer to Privacy Policy Clause 6
> * You can login to "My Account" via our corporate website to check your past 12 months Text & multimedia messages record.

* You can login to "My Account" via our corporate website to check the Sales and Service Agreement record.
* N/A

In the case of SmarTone, a look at their privacy policy reveals that in section 3(b), they have the following language where they say that they collect personal data such as your location data or your searching and browsing history.

> In support of the telecommunications and other services provided by SmarTone, information may be automatically collected by SmarTone on how you use SmarTone's products and services, including but not limited to:
>
> (i) the telephone numbers and/or email addresses of calls, texts, MMS, emails and other communications made and received by you and the date, duration, time and cost of such communications;
> (ii) your searching, browsing history (including websites you visit) and location data;
> (iii) Internet PC location for broadband, address location for billing, delivery and installation.

In other words, they can neither deny that they collect this type of personal information (after all, they say they do in their privacy policy), nor do they have a reason for not giving the user access to it. SmarTone was the only telco that specifically listed in their privacy policy the possibility of collecting a user's searching, browsing history, and location data.

Data Retention: How Long Do Telcos Keep Our Data?

How long do telcos keep or store the data? The longer they keep it, the more data they have and the richer and more accurate the profiles are that they can build and sell. It is important to note that there are legal limitations on how long data can be kept. Section 26 of the PDPO stipulates that personal data must be deleted when the data is no longer required for the purpose for which it was used, unless any such deletion is prohibited under any law or it is in the public interest not to have the data erased (PDPO, 2013). It is also worth emphasizing that in Hong Kong, telcos are not legally mandated to keep data for law enforcement purposes. In our letters, we specifically requested data "from the creation of my account or from the earliest date since your company has retained my data (whichever is earlier) until the date of this request" with the goal to find out the data retention period. Unfortunately, we did not make much headway with this inquiry, given that telcos consistently argued that the data we requested was not personal data, with two exceptions: call records and subscriber information.

Telcos keep track of who we call, for how long, at what time, and so on. They also agree that this call log data is personal data. From the responses we received, we can infer the maximum period of call logs the volunteer is able to retrieve. Some telcos deem it necessary to keep call records for as little as three months, some for as long as a year. Regarding the data retention periods for types of data other than call records, including IP addresses and geolocation data, we were not able to make much headway with

this line of inquiry. However, there was at least one response we received that was inconsistent with the other responses. The letter read as follows:

> We refer to your data access request of 3 July 2016 and further request of 12 August 2016, and our replies to you of 8 July 2016 and 10 August 2016.
>
> Please be informed that the data of August 2014, which you have requested has exceeded our retention period and has been discarded accordingly, including:
>
> 1. Mobile device software information;
> 2. Geolocational data; and
> 3. IP address logs.

This telco response suggests that their data retention period does not exceed two years. However, their answer also seems to imply that they agree that the listed data types should be considered personal data, in contrast to the other responses we received. Further research is necessary to see to what extent this is an exception (or an error) or not.

From our findings, not only is it unclear how long the telcos will retain the data while we are customers; it is even unclear how long the telcos will keep the data once we have canceled our accounts with them. For example, Three Hong Kong felt the need to point out to the media that if the contract ends, after "a certain period of time," the personal data will be deleted (Yingbao, 2016). The other telcos were silent in this regard.

Data Disclosure: Have Telcos Shared Our Data With Third Parties?

The data access requests also asked for information about whether the individual's personal data has been shared with third parties. The exact language in the letter is as follows:

> Disclosures to third parties; Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies.

None of the responses answer the question we asked, which is whether they have shared personal data, not whether they might. Hong Kong is lagging compared with other jurisdictions, including South Korea and the Philippines, who grant citizens the right to know which third parties their data is shared with. Nevertheless, the nonresponses can be categorized into two types.

The first type of response is, again, the "Ostrich" response, where telcos simply ignored the relevant part of the request. The second type of response is the "we never share your data with any third parties" response. Representatives of China Mobile gave this response to our volunteers over the phone. Hong Kong Telecom and SmarTone provided a similar "we never share your data with third parties" answer in response to a media inquiry following our press conference (Yingbao, 2016). Critical here are what counts as "third

parties": for example, does this include subsidiaries of the same mother company? Some telcos can be part of massive global conglomerates with many subsidiaries. The other critical words are "your data." For example, if the data is anonymized and aggregated, is it still "your data"? There is evidence to suggest that telcos might not sell your individual data linked to your name or other personal information, but they do sell this data in an anonymized and aggregated form. Whether this counts as "personal data" is still an open question in part because it is technically possible to reverse engineer the data and use it to identify individuals (Ohm, 2009; Schwartz & Solove, 2011).

Finally, we end with an atypical response. All telcos responded to our data access requests in writing, but only one telco said that although they received the request, they could not process it any further until the volunteer filled out another form. This telco was Hong Kong Telecom.

Permit A38 and Form OPS003: Bureaucratic Barriers to Data Access Rights

The famous French comic book hero Asterix must, in one story, fulfill Twelve Tasks, modeled after the twelve tasks Hercules had to fulfill. One of the tasks Asterix must fulfill is to get permit A38; he ends up stuck in an endless bureaucracy staffed by unhelpful administrators who direct Asterix to other similarly unhelpful colleagues elsewhere in the building to get another permit first. This cartoon came to mind when we received the letter that Hong Kong Telecom sent us in response to our data access request, in which we were asked to first obtain and then fill out Form OPS003 before the company could proceed with our data access request. The language was as follows:

> We note that you have made a Data Access Request, by which you requested us to provide 8 categories of information. Pursuant to s. 20(3)(e) and s. 67(4) of the Personal Data (Privacy) Ordinance ("PDPO"), a data subject who intends to make a Data Access Request is required to complete a Data Access Request Form [OPS003 (revised 09/2012)] prescribed by the Privacy Commissioner for Personal Data.

Note that the language says the form is required and that it is prescribed by the PCPD. Neither claims are accurate. According to the PCPD: "The data user may refuse to comply with your data access request ('your request') if it is not made in this Form (see section 20(3)(e) of the PDPO)."

So, the telco has the right to refuse your request if not made with the form. But the PCPD also states in a Guidance Note (PCPD, 2016b, p. 3):

> Sometimes, a requestor may not use the DAR Form to make the DAR but will simply say in his request that he wishes to obtain his personal data, or he is making a DAR or his request is made under the Ordinance. Although compliance with such request may be refused as it is not made on the specified form, data users are strongly advised to respond to the request if it substantially sets out the scope and details of the requested personal data because reliance on such ground of refusal is merely technical and the requestor may simply lodge another DAR using the DAR Form.

The use of this form is an unnecessary barrier that Hong Kong Telecom is imposing on users seeking to exercise their data access rights. As per the Guidance Note, if the request "substantially sets out the scope and details" of the requested personal data, then refusal to respond on the ground of not using the form is merely technical. Indeed, we asked the privacy commissioner in a direct meeting whether the use of Form OPS003 was required before processing a request. The privacy commissioner answered that the form is not required; instead, he generally explained that the form was made available by its office with the aim to help, support, and make it easier for users to file a Data Access Request, and its purpose is not to make it more difficult or add additional burden. Further, none of the other telcos asked us to fill out another form before responding to our requests, suggesting Hong Kong Telecom's refusal to respond to the request was indeed improper.

Conclusion

The findings of this project suggest that the access principle is not functioning well when it comes to the telecommunication industry in Hong Kong. They further suggest that the telcos have a disturbing lack of awareness about the access principle, the nature of personal data, and the general rights of data subjects. Specifically, the telcos failed to (1) let users have access to their personal data in a comprehensive manner, including IP addresses or geolocations; (2) tell users whether they indeed process such information; (3) offer the possibility of correction or deletion; or (4) tell users whether they have shared this data with third parties, including law enforcement. In terms of next steps, options include asking the privacy commissioners to issue an industry guidance note or going to court to seek clarification on whether data types such as IP addresses and geolocations are personal data. The findings also suggest that it might not be practical to burden every citizen with the expectation that he or she will monitor the institutions that collect his or her data. Instead, perhaps what we need are agents acting on behalf of the public who will use the right to access personal data to "look back" at the institutions that collect, process, and share our data. These agents could be journalists, lawyers, or policy experts who work for civil society organizations concerned about privacy, surveillance, and personal data protection.

The PDPO seeks to protect not only the personal privacy of Hong Kong residents but also to create a framework in which trade and innovation is stimulated. However, the findings of this study raise serious concerns over whether the legal concept of "personal data" is well positioned to protect future or new categories of data that might be personal. For example, what about the data we contribute or generate in dating or health apps, fitness trackers, and so on? And what other data might be sensitive or personal and deserving of protection in a world where every device is supposed to be "smart," online, and will capture our preferences, our behavioral data, and so on? Will the court have to decide every single time whether these new types of data are personal before citizens can get access to it? These are important questions that not only have implications for privacy and digital rights but also innovation and economic growth.

Finally, personal data is the key concept that personal data protection regulation is built on. If this concept is not rock solid and clear, then all the protection built on top of this collapses. At worst, the existence of personal data protection laws gives the companies a facade to hide behind where they can do what they want with the data because they say it is not "personal" data. At best, the findings suggest that "personal data" is a contested concept, one where the courts ultimately should decide whether IP addresses in the

hands of telcos are personal data. In the meantime, and in the absence of such court decisions, the industry has the power—and the incentives—to decide that data types such as IP addresses and geolocations are not personal data.

There is much concern about the ability of institutions and corporations to collect, use, and share personal data from a massive number of users around the world, in novel and unprecedented ways. The rise of digital and networked technology has only further accentuated concerns related to surveillance, privacy, and personal data, with the Snowden revelations underscoring these concerns (Greenwald, 2014). An important challenge to scholars is to understand how technological advances allow or enable surveillance practices that previously were not possible. These developments are not simply technological developments but also should be understood as important shifts in the structures of power in society. These shifts often favor the institution at the expense of the individual. In other words, it is necessary to not only understand the underlying technology but also to what extent institutions gain power, and to what extent these power shifts imply risks and threats to privacy specifically and life chances more broadly.

References

Asghari, H., Mahieu, R. L. P., Mittal, P., & Greenstadt, R. (2017). The right of access as a tool for privacy governance: Findings from individual requests & proposal for a crowd-sourced dataset of privacy practices. In *Proceedings of 17th Privacy Enhancing Technologies Symposium* (pp. 1–2). Minneapolis, MN. Retrieved from https://petsymposium.org/2017/papers/hotpets/rights-of-access.pdf

Ausloos, J., & Dewitte, P. (2018). Shattering one-way mirrors: Data subject access rights in practice. *International Data Privacy Law*, *8*(1). Retrieved from https://ssrn.com/abstract=3106632

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. Cambridge, MA: MIT Press.

Brin, D. (1999). *The transparent society: Will technology force us to choose between privacy and freedom*. New York, NY: Perseus Books.

Bygrave, L. A. (2001). *Core principles of data protection*. Retrieved from http://www.austlii.edu.au/au/journals/PLPR/2001/9.html

Cheung, A. S. Y. (2012). An evaluation of personal data protection in Hong Kong Special Administrative Region (1995–2012). *International Data Privacy Law*, *3*(1), 29–41.

Greenleaf, G., & McLeish, R. (2012). Hong Kong's privacy enforcement: Issues exposed, powers lacking. *Privacy Laws & Business International Report*, 116, 25–28.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. London, UK: Macmillan.

Hargreaves, S. (2017). Online monitoring of 'localists' in Hong Kong: A return to political policing? *Surveillance & Society*, *15*(3/4), 425–431.

Hilts, A., & Parsons, C. A. (2014). Right to information in Canada: Drawing analogue law into a digital present. Retrieved from https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2504109

Hong, B. [洪寶瑩]. (2016). 「誰 可得」網站程式 助向電訊商查. 經濟日報 [Access my info: Website helps with checking telecommunication companies]. Retrieved from https://topick.hket.com/article/1421742/

Kaye, K. (2015). *The $24 billion data business telcos don't want to talk about*. Retrieved from http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/

Mo, J. Y. C. (2015). Cookies and browser-generated information: The challenge in Hong Kong under the Personal Data (Privacy) Ordinance. *Statute Law Review*, *38*(1), 57–68.

Newman, A. (2008). *Protectors of privacy: Regulating personal data in the global economy*. Ithaca, NY: Cornell University Press.

Norris, C., de Hert, P., L'Hoiry, X., & Galetta, A. (Eds.). (2017). *The unaccountable state of surveillance: Exercising access rights in Europe*. Berlin, Germany: Springer.

OECD. (1980). *OECD guidelines on the protection of privacy and transborder flows of personal data*. Retrieved from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Office of the Communications Authority. (2017). *Key communications statistics*. Retrieved from http://www.ofca.gov.hk/en/media_focus/data_statistics/key_stat/

Ohm, P. (2008). The rise and fall of invasive ISP surveillance. *University of Illinois Law Review*, *2009*(5), 1417. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344

Ohm, P. (2009). *Broken promises of privacy: Responding to the surprising failure of anonymization*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

PCPD. (2016a). *Upward trend in privacy complaints sees need for personal data protection and respect amongst individuals and organisations*. Retrieved from https://www.pcpd.org.hk/english/news_events/media_statements/press_20160126a.html

PCPD. (2016b). *Guidance note on proper handling of data access requests and charging of data access request fee by data users*. Retrieved from https://www.pcpd.org.hk/english/publications/files/DAR_e.pdf

PDPO. (2013). *Personal Data (Privacy) Ordinance*. Retrieved from https://www.elegislation.gov.hk/hk/cap486

Purtova, N. (2017). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation, and Technology*, *10*(1). Retrieved from https://ssrn.com/abstract=3036355

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYU Law Review*, *86*, 1814–1894. Retrieved from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs

Tsui, L. (2015). The coming colonization of Hong Kong cyberspace: Government responses to the use of new technologies by the umbrella movement. *Chinese Journal of Communication*, *8*(4), 447–455. Retrieved from http://www.tandfonline.com/doi/full/10.1080/17544750.2015.1058834

Viljoen, S. (2018). Facebook's surveillance is nothing compared with Comcast, AT&T and Verizon. *The Guardian.* Retrieved from https://www.theguardian.com/commentisfree/2018/apr/06/delete-facebook-live-us-still-share-data

Yu, J. W. K. (2005). Electronic government and its implication for data privacy in Hong Kong: Can Personal Data (Privacy) Ordinance protect the privacy of personal information in Hong Kong. *International Review of Law*, *19*(2), 143–163.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.