



Crisis of Personal Data Protection During the Construction of E-government

- Reaction and limits of Hong Kong privacy laws

Yongxi CHEN
PhD candidate
Faculty of Law



香 港 大 學

THE UNIVERSITY OF HONG KONG

Outline

1. Repeated incidents of personal data leakage in Hong Kong
2. Legal requirements about Privacy
3. Case I – Data security in the outsourcing process
4. Case II – Use of data apart from original purpose in e-Service
5. Suggestions for improvement



Background: E-government in HK

- “Digital 21 Information Technology Strategy” in 1998, 2001, 2004.

- Achievements in E-government infrastructure, accessible and user-friendly interface and joining bureaux and departments to deliver one-stop services
 - 90% of the services that are amenable to the electronic means of delivery are provided with an e-option.
 - Over 80% of government procurement tenders are conducted through electronic means.
 - HK is regarded as a "mature city" in terms of E-government leadership
 - Ranked first in Asia/Pacific in terms of the percentage of urban Internet users accessing E-government services or information.

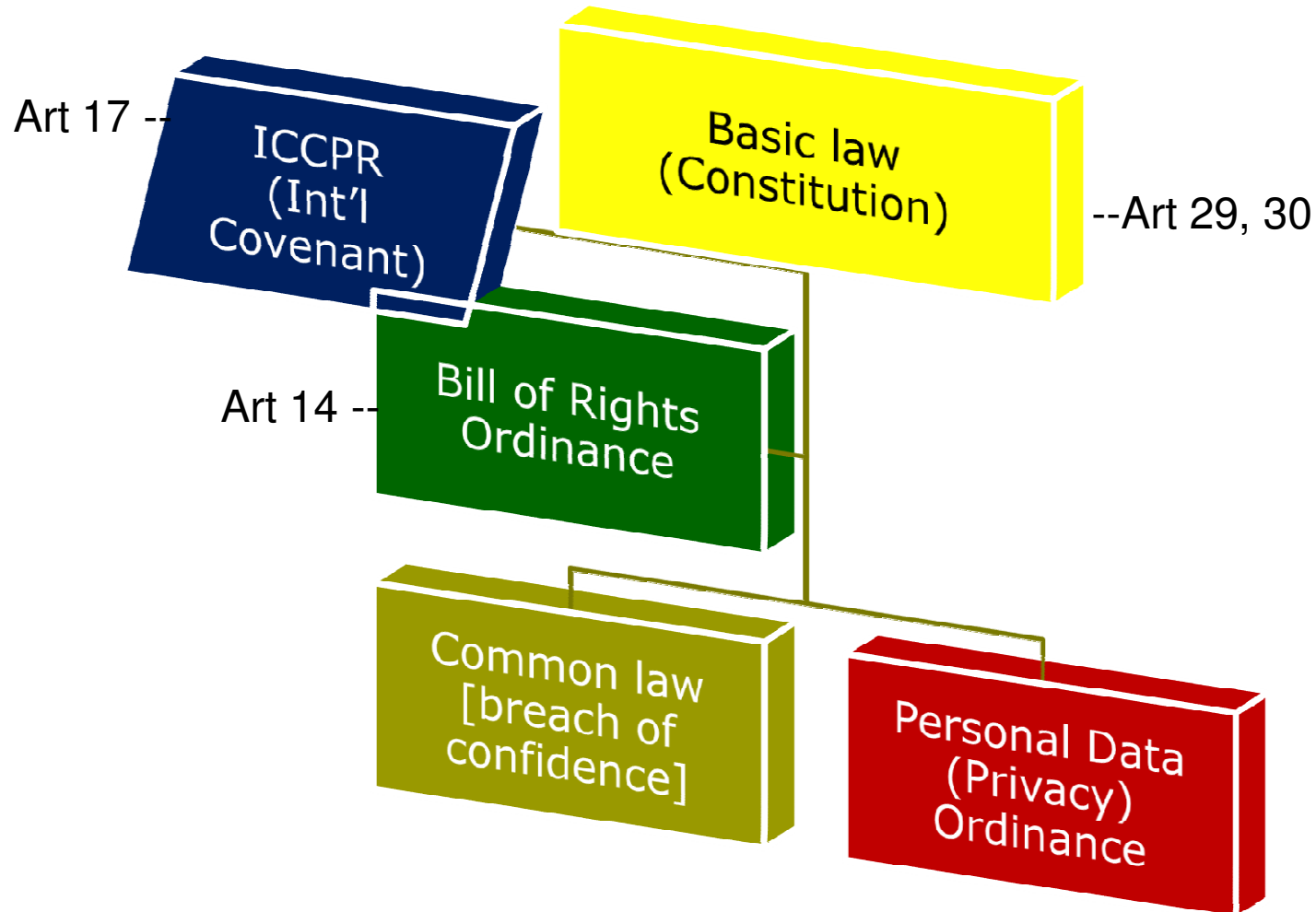
Sources: <http://www.info.gov.hk/digital21/e-gov/eng/index.htm>



1. Repeated incidents of personal data leakage

March 2006	Data leak on a commercial website which contains the names, addresses and even criminal records of around 20,000 people who had lodged complaints about the Police
May 2006	Personal data of around 3000 individuals participating in a slogan competition held by the Leisure and Culture Services Department were released onto Internet
October 2006	Education Bureau uploaded to its official website, without prescribed consent, personal information of more than 200 primary school teachers who had attended the training programme arranged by the bureau during year 2002-2003
December 2006	In a public online chat site were disclosed the data of some 900 police officers, including identifying details such as the rank and mobile phone numbers which should have only been accessible in restricted internal website
April 2007	Confidential business details of hundreds of companies that have opposed trademark applications were found easily accessible in the online trademark search system set up by the Intellectual Property Department for trademark inspection service

2. Regime of Privacy Protection in HK



ICEGOV 2007, Macao, China



2.2 Personal Data (Privacy) Ordinance

- An “European style” law (1995)
 - Follows the Data Privacy Principles issued by OECD and based itself on the EU Data Protection Directive
- Protects “Data/Informational privacy”
- Protective Body: Privacy Commissioner
 - Promoting the overall compliance
 - Own motion investigation and public reporting of contravention of the Ordinance
 - Inspection of the compatibility of information system
 - Issuance of codes of practice and guidelines



2.3 Data Protection Principles

- ❑ Confers Six aspects of data rights to data subjects against data users
- ❑ DPP 1 – Purpose and manner of **collection** of personal data
- ❑ DPP 2 – **Accuracy** and duration of retention of personal data
- ❑ DPP 3 – **Use** of personal data
- ❑ DPP 4 – **Security** of personal data
- ❑ DPP 5 – Availability of information about privacy **policy**
- ❑ DPP 6 – **Access** to personal data by data subject



3. Case selecting

Two typical aspects of data protection loopholes

Independent Police Complaints Council (IPCC) Case	Intellectual Property Department (IPD) Case
arising during internal outsourcing process [Gov2Gov]	occurring in external online service/regulation [Gov2Cityzen]
Data processing that should be kept confidential as required by security obligation.	Data handling that should allow public access as to fulfil the regulator's statutory obligation.



3. IPCC case:

Breach of data security requirement in engaging outsourcing contractor

3.1 Facts:

Complaints Against Police Office (CAPO)



Independent Police Complaints Council (IPCC) Ms. X



Contractor



Sub-contractor: Mr. Y



newsgroup.talk.railway - Mozilla Firefox

http://72.14.203.104/search?q=cache:JPMvHpb0-BI:ah4.org/pnews230/indexing.php?server=news.newsgroup.com.hk

Google is neither affiliated with the authors of this page nor responsible for its content.

阿四俱樂部 News Service

newsgroup.talk.railway		Login	Group List
Num	Subject	Author	Time
427	黑暗未來	新人王	2006/03/16 19:37
426	試一試	Suki	2006/03/16 15:19
425	Re: 黎總辭左職,咁之前話左共同進退的其他總監.....	<author>	2006/03/16 14:13
424	馬鐵千燈罩隨時脫落	Eurostar 歐洲之?..	2006/03/16 13:28
423	Re: 東鐵sm有人士改動	不平人	2006/03/16 13:22
422	Re: 東鐵SM中...	猩猩	2006/03/16 13:11
421	黎總辭左職,咁之前話左共同進退的其他總監.....	123	2006/03/16 12:42
420	六壯士玩完,但橫班仲有好多死士隨時侯命,上啦我支持你	死士委員會主席牛 ..	2006/03/16 01:13
419	Re: 條友又做返主席.....唉.....	田大少	2006/03/16 01:07
418	Re: 東鐵SM中...	電車女	2006/03/16 00:59
417	尖東站NEO	電車女	2006/03/16 00:54
416	Re: 東鐵sm有人士改動	新人	2006/03/16 00:42
415	Re: 條友又做返主席.....唉.....	南瓜	2006/03/16 00:14
414	黎小[田]事件成因	南瓜	2006/03/16 00:12
413	Re: 條友又做返主席.....唉.....	GUN	2006/03/16 00:10
412	Re: 東鐵sm有人士改動	GUN	2006/03/16 00:08
411	Re: 有冇LMC work train D料	無名	2006/03/15 22:35
410	Re: 東鐵sm有人士改動	無名	2006/03/15 22:12
409	東鐵SM中...	電車男	2006/03/15 20:59
408	[BT]警監會(IPCC)機密資料公開下載	李少光	2006/03/15 20:37

First Prev Next Last Page 1 of totaling 20 page(s) Post Refresh

PHP News Reader v2.6.3 SOURCE CODE ncl Language: English

Done

Data remain reproduced by bitTorrent and Caches in search engine

ICEGOV 2007, Macao, China



IPCC case

3.2 Breach of DPP4

□ DPP4: Data Security

- “all **practicable steps** shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are **protected against unauthorized or accidental access, processing, erasure or other use**”.

□ With particular regard to

- “(a) the kind of data and the harm that could result if any of those things should occur;
- (b) the physical location where the data are stored;
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
- **(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and**
- **(e) any measures taken for ensuring the secure transmission of the data. ”**



IPCC case

3.2 Breach of DPP4

- ❑ IPCC claimed they operated in accordance with Security Regulations, data were classified

But,

- ❑ IPCC did not formulate its own **privacy policy or any specific procedure** regarding the handling of personal data, especially
 - reliable physical location of personal data
 - secure transmission of data by electronic means
 - measures adoptable when releasing data to a third party, including contractor
- ❑ Failed to direct Ms. X to provide clean data for testing purpose, an **alternative less intrusive** to privacy.
- ❑ Lack of **proactive measures** assuring data security in the outsourcing process and contract
 - no general confidentiality clause imposing contractors to take all possible steps to safeguard the confidential information when they receive, use and manage it
 - no clause prohibiting EDPS from sub-contracting its services under the contracts, hence no proper measures to ensuring the integrity, prudence and competence of persons having access to the data.



IPCC case

3.3 Limited remedy

- The Commissioner :
 - Held IPCC did not present due caution nor take reasonably practicable safeguards ...completely contravened DPP4
 - Served an enforcement notice
 - But if IPCC adopted the steps set forth in the notice within the period required, it won't assume further responsibility - after the serious contravention!
 - 'Everyone is allowed one mistake' - Privacy Commissioner
 - Unable to suggest apology or compensation from IPCC to the affected data subjects



IPCC case

3.3 limited remedy

- Civil procedure under PD(P)O:
 - Burdon of proof is on the data subjects unassisted by the Commissioner
 - Risk of disclosure his identity for a second time

- Common law tort “Breach of Confidence”
 - Sophisticated and uncertain

- Judicial review under BORO and Basic Law
 - civil compensation not available



4. IPD case

Wrongful disclosure of personal data in Online Inspection Service

4.1 Facts

- Interested parties supply info to IPD when filing
 - opposition to an application for registration of a trade mark
 - a counter-statement (i.e. the original applicant's response to the opponent)
- Public are legally entitled to view these documents

- IPD established Online Trademark Register to facilitate public inspection

- By accepting the "Privacy Statement" issued by IPD, trademark applicants voluntarily provided sensitive commercial info as proofs to justify their claims, which were also automatically uploaded to the Registry and accessible by general public.



IPD Case

4.2 Disputed Issues

1. Is IPD a data user in relation to the unsolicited information?

□ Definition of personal data in PD(P)O

- “(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.”

□ IPD received the unsolicited personal information together with the necessary information, among which the names of the parties concern are indispensable. Associated with the concrete names, the data subject of the unsolicited information is practicably identifiable to IPD.



IPD Case

4.2 Disputed Issues

2. Does the general acceptance of “privacy statement” constitute “consent” for subsequent disclosure of voluntarily provided commercial information?

□ DPP 3:

Personal data shall not, without **prescribed consent** of the data subject, be used for the purposes **other than the purpose for which they were originally collected or a directly related purpose.**

□ Privacy statement in Online registry:

“Personal data provided in this form will be used by the Intellectual Property Department and can be disclosed for purposes relating to the administration of the Trade Marks Ordinance and its subsidiary legislation”



IPD Case

4.2 Disputed Issues

- ❑ Prescribed consent: “the express consent of the person given voluntarily” in PD(P)O.
 - overbroad
 - does not follow EU Data Protection Directive, who emphasises that the consent should be expressed in a specific and informed manner

- ❑ It is obviously beyond the data subject’s **reasonable expectation** that these personal and commercial information, provided as evidence, would be automatically open to the online inspection by anyone, including business competitors.

- ❑ General acceptance without being **informed of the concrete handling process and imparting agreement on this specific point** doesn’t amount to “prescribed consent” to freely disclosure thereafter.

- ❑ The Commissioner confirmed:
“the fact that a particular type of personal data is passively collected through a website does not mean that the personal data should automatically be published on the internet.”



IPD Case

4.3 Redress facing the future

- ❑ Com’r issued written warning to IPD
- ❑ Com’r articulated Policy requirements:
 1. Fulfilment of statutory duty should not be and is not an excuse for government agency to allow uncontrolled access to personal data online
 2. Proportionality test:

“in situations where personal data are to be made publicly available online, a data user shall exercise due care to ensure that **only personal data that are required for fulfilling the purpose of use** are to be disclosed, particularly when sensitive personal data are involved”
 3. Implied Positive obligation on Gov.:

block exterior access to all personal data under its control which is not explicitly allowed by the data subject



IPD case

- IPD adopted proactive actions, besides those proposed by the Commissioners
 - screened all in-coming information, whether solicited or not and blocked out any identity card or passport numbers found;
 - Amended privacy statements in the forms as to make those submitting information fully informed that the information will be made available on the Internet for inspection and that the information for evidence purpose can be supplied at a later stage and will not be uploaded to the Internet



5. Suggestions for improvements

- ❑ Clearer awareness of risks imposed by digitalization
- ❑ Formulation of comprehensive policy for particular purpose of personal data protection
- ❑ Modification of privacy laws
- ❑ Effective cooperation of supervisory forces



5.1 Awareness- extra risks

- E-Gov. turns personal information more vulnerable to unauthorized access and makes the damage thereby caused harder, if not impossible, to recovery, especially given
 - Voluminous sensitive personal information will be collected and stored in a centralised manner
 - The end of “practical obscurity”: What used to be stored in dim archives of the administration and impracticably accessible by general public now can be easily searched out by anyone in the aid of powerful search engines and other sophisticated ICTs
 - It’s impossible for any government to control the global data flow online and retrieve the privacy information leaked out.
 - Incompatibility between diverse E-Gov systems entails outsourcing public-private participation, yet interoperability also entails risk of data security

- Consent and trust is the basis of the construction of digital government, which will be severely undermined by government’s inaction to secure these data due to its negligence of the relevant risk



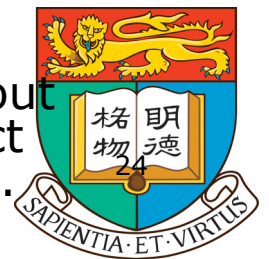
5.1 Awareness- more responsibility

- While enjoying the bonus of the digital environment, such as efficiency and transparency, government should be fully aware of the extra threats thereby brought to privacy.
- It therefore bear **more positive obligation** than before to prevent potential contravention of privacy rights and should adopt **more responsive policies** to the public concern.



5.2 Privacy policy - comprehensiveness

- Data security policy ≠ < privacy protection policy
 - Data security measures serve mainly for maintenance of official secrecy. It is uncertain whether they have satisfied, if not contradicted, the minimum requirements of data protection laws (DPP4).
 - Some data security rules may contradict with DPP6 allowing data subjects to access his data.
- A complete data protection policy also demands fair and proportionate collection, use and detention of personal data:
 - besides releasing no more personal data than necessary or consent by data subjects (DPP3),
 - the government should minimize as much as possible the collection and retention of these data, and use these data exclusively for the purpose for which they were collected(DPP1).
 - It is also the government's obligation to provide citizens with broad opportunities to know what personal data about them the government holds, whether the data are correct and how they are handled, as implied by DPP2 and DPP5.



5.2 Privacy policy - proportionality

- E-Government should always consider the availability of alternative approaches that are less intrusive to privacy rights



5.3 Responsive legislation

- Try to be responsive to, if not catch up with, the pace of ICTs and their impact on privacy.
 - Enlarge the scope of protected data/informational privacy
 - Equip the Commissioner with remedial tools so as to reduce the cost of data subjects in seeking redress.
 - Mechanism of periodical revise of laws in alignment with loopholes tore up by ICT developments



5.4 Institutional cooperation

- ❑ Closer cooperation between Commissioner, who confronts incompatibility of law and advancement of ICTs and special panels in legislative body, who is capable to motivate necessary amendment
- ❑ Better Coordination among Commissioner, The Government Chief Information Officer (GCIO) and Authority of Security to harmonize governmental policies regarding data processing
- ❑ Mobilizing the IT professional associations to adopt effective measures and highlight members' responsibilities as data users
- ❑ Expediting communication between legislator, Media and the public, and engaging stakeholders' participation into privacy policy making.



Open for comments and critiques. Thank you!

“The privacy bomb had been dropped a long time ago, at the beginning of the digital era. It had merely taken time for the public to feel the bomb's reverberations.”

(Alana, 2006)

And it's high time for participants of E-Governance to tackle this hot potato, before E-initiatives are flooded in the public's outcry and mistrust.

