Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan's Open Data Policy and Practices

Ching-Yi Liu
Wei-Ping Li
Yun-Pu Tu

Follow this and additional works at: https://digitalcommons.law.uw.edu/wilj

Recommended Citation
Ching-Yi Liu, Wei-Ping Li & Yun-Pu Tu, Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan's Open Data Policy and Practices, 30 Wash. L. Rev. (2021). Available at: https://digitalcommons.law.uw.edu/wilj/vol30/iss3/8

This Article is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington International Law Journal by an authorized editor of UW Law Digital Commons. For more information, please contact jafrank@uw.edu.
Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan's Open Data Policy and Practices

Cover Page Footnote
Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan's Open Data Policy and Practices

Ching-Yi Liu†, Wei-Ping Li††, & Yun-Pu Tu†††

Abstract: Governments and private sector players have hopped on the open data train in the past few years. Both the governments and civil society in Taiwan are exploring the opportunities provided by the data stored in public and private sectors. While they have been enjoying the benefits of the sharing and flowing of data among various databases, the government and some players in the private sectors have also posed tremendous privacy challenges by inappropriately gathering and processing personal data. The amended Personal Data Protection Act was originally enacted as a regulatory mechanism to protect personal data and create economic benefits via enhancing the uses of public and private sector data. In reality, the Act has instead resulted in harm to Taiwan’s data privacy situation in this big data era. This article begins with an overview of the Taiwan’s open data policy history and its current practices. Next, the article analyzes cases in which the data sharing practices between different sectors have given rise to privacy controversies, with a particular focus on 2020, when Taiwan used data surveillance in response to the COVID-19 pandemic. Finally, this article flags problems related to an open data system, including the protection of sensitive data, de-identification, the right to consent and opt-out, and the ambiguity of “public interest,” and concludes by proposing a feasible architecture for the implementation of a more sensible open data system with privacy-enhancing characteristics.


INTRODUCTION

Issues surrounding big data, artificial intelligence, and data privacy, are among the most popular topics in today’s privacy law scholarship.1 For example, the Special Rapporteur on the right

† Professor of Law, National Taiwan University & Research Professor with Joint Appointment, Institutum Iurisprudentiae, Academia Sinica, Taiwan; J.S.D., The University of Chicago Law School, U.S.A. LL.M., Harvard Law School, U.S.A.
†† Ph.D. Student, Philip Merrill College of Journalism, the University of Maryland, College Park, U.S.A.; LL.M., University of Pennsylvania Law School, U.S.A.
††† Ph.D. Student, University of Washington, U.S.A.; Research Assistant, Academia Sinica, Taiwan; Intellectual Property Law & Policy L.L.M, University of Washington, U.S.A.

1 See, e.g., JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (2012); Michael Froomkin & Zak Colangelo, Privacy as Safety, 95 WASH. L. REV. 141 (2020); Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477 (2006); Harry Surden, Structural Rights in Privacy, 60 SMU L. REV. 1605 (2007). For discussion of various data privacy issues, see, e.g., Ifeoma Ajunwa et al., Limitless Worker Surveillance, 106 S. CAL. L. REV. 735 (2017); Lothar Determann, Healthy Data Protection,
to privacy by the Office of the United Nations High Commissioner for Human Rights (OHCHR) has discussed many of these issues in detail. Privacy, a primary fundamental human right recognized by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), is the right to control one’s personal information by deciding how their information is collected and used. For individuals, a breach of personal information poses a potential threat to identity theft. For organizations, the unauthorized collection and inadequate processing of personal data may create a tremendous risk of lawsuits or penalties. For example, the California Consumer Privacy Act (CCPA) in the U.S. grants data subjects a private right of action if a company that keeps subjects’ unencrypted and unredacted information fails to implement reasonable procedures to protect the subjects’ personal information, and a breach results from the company’s failure.

There are multiple regulatory restrictions and legal frameworks in place for safeguarding the right to data privacy. The European Union’s General Data Protection Regulation (GDPR) and the United States’ Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLB) are perhaps the regulations that have attracted most of the

5 Id.
attention over the past few years. 9 More recently, novel but thorny
issues arising out of the need to manage the COVID-19 pandemic
have challenged data governance and regulation around the
world. 10 The pandemic created a growing urgency for
governments to track and surveil their citizens in the name of
public health, which in turn impacted individual autonomy and the
right to data privacy. 11

The past decade preceding the pandemic also witnessed a
wave of open data initiatives.12 More governments and
corporations embraced the idea of “open data,” which has been
described as “accessible public data that people, companies, and
organizations can use to launch new ventures, analyze patterns
and trends, make data-driven decisions, and solve complex
problems.” 13 By adopting open data initiatives, governments and
corporations have released raw data sets that are collected, stored,
and buried deep in databases to the public. 14 Open data initiatives
have rendered government records more accessible to the public,
curried technological innovation, increased economic

9 See Jonathan Keane, From California to Brazil: Europe’s Privacy Laws Have
Created a Recipe for the World, CNBC (Apr. 8, 2021 1:32 AM),

10 See generally Chuan-Feng Wu, COVID-19 and Democratic Governance in
Taiwan: Challenges and Opportunities, U.S.–ASIA LAW INSTITUTE (Jan. 28, 2021),

11 Joseph A. Cannataci (The Special Rapporteur on the Right to Privacy),

12 See e.g., White House Open Data Initiatives, OBAMA WHITE HOUSE
https://obamawhitehouse.archives.gov/open (last visited Nov.18, 2020); State of New York
Open Data, STATE OF NEW YORK (2020), https://data.ny.gov/ (last visited Nov. 18, 2020);
visited Nov. 18, 2020); see also Amy Harmon, As Public Records Go Online, Some Say
region/as-public-records-go-online-some-say-they-re-too-public.html; Jan Whittington et
al., Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government,

13 JOEL GURIN, OPEN DATA NOW: THE SECRET TO HOT STARTUPS, SMART
INVESTING, SAVVY MARKETING, AND FAST INNOVATION 9 (2014).

14 See, e.g., Markus Perkmann & Henri Schildt, Open Data Partnerships Between
Firms and Universities: The Role of Boundary Organizations, 44 RSCH. POL’Y 1133,
development, and motivated civic engagement. However, the open data initiatives have also received criticism. Some critics question whether this data use is appropriate and whether a single reckless act could cost data subjects’ privacy interests, for instance, cases have shown that individuals still can be identified by combining de-identified health records and voter registration records. Privacy interests must be considered when making open data policies. A comprehensive data protection program is the key to fulfilling promises that open data advocates have envisioned.

Although “the right to privacy” is not enumerated in Taiwan’s Constitution, the Constitutional Court of Taiwan has long recognized the right to privacy as an indispensable fundamental right and thus protected under Article 22 of the Constitution for purposes of preserving human dignity. Recent data privacy controversies in Taiwan exemplify the need for a more thoughtful and comprehensive privacy protection mechanism. The Taiwanese government and civil society have explored the opportunities provided by data stored in both the public and the private sectors since 2009. While the sharing and flowing of data among various benefits has created numerous benefits, there are some downsides. Some government and

15 See generally Ben Green, THE SMART ENOUGH CITY (2019) (ebook); BEYOND TRANSPARENCY (Brett Goldstein et al. eds., 2013); BETH SIMONE NOVECK, SMART CITIZENS, SMARTER STATES (2015); SMART CITIES CYBERSECURITY AND PRIVACY (Danda B. Rawat & Kayhan Zrar Ghafoor eds., 2018); HOW SMART IS YOUR CITY? TECHNOLOGICAL INNOVATION, ETHICS AND INCLUSIVENESS (Maria Isabel Aldinhas Ferreira ed., 2020).


17 See Judicial Yuan Interpretation No. 603 (Sept. 28, 2005) (Taiwan).


19 For example, during a disastrous dust explosion happened in Taipei in 2015, the Taipei municipal government released the data of casualties and aid shortage to the public. With the shared data, the tech community and the government collaborated to establish systems to allocate and coordinate aid resources. Id. at 56.
private sector actors intend to capitalize on this data usage and pose tremendous privacy risks to Taiwanese people by inappropriately gathering and processing personal data. The Personal Data Protection Act (PDPA) was originally enacted to serve as the ultimate regulatory foundation for protecting personal data in 1995, when it passed as the Computer-Processed Personal Data Protection Act. However, the PDPA has not only failed to sufficiently protect personal data, but it has in fact worsened the data privacy landscape in Taiwan. Further, the PDPA’s articles are outdated, having not been substantially amended since 2015. The law is also lacking several important privacy protection concepts, such as the right to opt-out, the right to be forgotten, and data portability, all of which are concerns internationally.

This article focuses on open data policy’s development in Taiwan and provides a critical analysis of the potential downsides to its privacy scheme. Part I begins with an overview of Taiwan’s open data initiatives and current practices. Part II analyzes specific case studies where the data sharing practices in different sectors have resulted in privacy erosions. Part III concludes with feasible solutions for implementing a more sensible open data system with privacy-enhancing characteristics.

II. OPEN DATA AND PRIVACY PROTECTIONS IN TAIWAN

A. The History of Open Data and the PDPA

In 2005, the Legislative Yuan, Taiwan’s legislative body, passed the Freedom of Government Information Law (FOGIL),

---

which serves as the legal basis for citizens who want to request information from the government. However, the open data initiative did not take root until 2009, when several groups in civil society promoted open data policies. For example, the Association of Digital Culture brought society’s attention to the power of data during a deadly typhoon disaster in August 2009. The Association collected information released by the government to coordinate rescue missions, which helped to rapidly allocate resources to people in need.

The demand for open data in Taiwan continued to grow and attracted more people to explore the potential of data. For example, the Fukushima Daiichi nuclear disaster spurred Taiwanese concerns about the safety of Taiwan’s nuclear power plants and electricity supply. Consequently, a group of hackers and experts who possessed electricity generation data began investigating Taiwan’s electricity issues and released data to the public that had long been kept in the Taiwan Power Company’s private database.

Meanwhile, some Taiwanese government ministers attempted to map out strategies and formulate policies of open government and open data after witnessing the efforts of civil groups and open government initiatives in other countries, particularly the United States. In November 2012, the Executive Yuan, the executive branch of Taiwan’s central government,

---

24 Li Bo-Yu (李柏昱), FangZai 2.0 Jhuanti (Wu): TsShun JhuKon GuanMinHeZhuoLi [防災 2.0 專題(五): 資訊志工官民合作力] [Disaster Prevention 2.0: Information Volunteers; The Government and the People Work Together], PANSII (2013), https://pansci.asia/archives/44612.
25 Id.
29 LEE & TSENG, supra note 18, at 7.
passed a resolution to promote open data nationwide. The resolution was subsequently followed by further regulations and guidelines, including the “Open Government Data Operating Principle for Agencies of the Executive Yuan,” and the “Regulations for the Use of the Government Open Data Platform.” The official open data portal website, which deposits all available data from Taiwanese central and local governments, has been online since April 2013. On this website, central and local governments as well as individuals and private sector groups are able to share data sets. As of November 20, 2020, there are 47,747 datasets available on this website. In addition, the central government has encouraged companies to utilize government data and engage in projects that promote the public interest. The “Google Taiwan Natural Disaster Management Plan” is a noticeable public interest promoting project. As suggested by the name of the plan, it is a Google product that uses data from different departments of the central government to map out any natural disasters on the island in a real-time manner.

Some Taiwanese local governments that witnessed this open data trend responded by creating their own open data
initiatives. Taipei City Government was the first among local government to make its data accessible on a local data platform, “Data.Taipei.” On “Data.Taipei,” the Taipei City Government outlines the goals of the website, including to provide citizens easier access to government data, to enhance the transparency and efficiency of the city government, and to promote the data’s value-added application. Other local governments, including New Taipei City, Taichung, Tainan, Kaohsiung, and Taoyuan, have also begun building their own open data websites. In 2018, the governments from these six special municipalities became the first Asian cities to sign the Open Data Charter (ODC). Local associations have taken actions to facilitate open data initiatives too. In 2013, the Taipei Computer Association established the Open Data Alliance, an example of nongovernmental advocacy for open data.

The Executive Yuan named 2015 as the first year to actively promote open data and big data usage. That same year, Taiwan also received recognition as the top open data country on the Global Open Data Index, which greatly emphasized Taiwan’s progress in the field of open data at the central and local level.


Shian, supra note 33.


See Taiwan City’s Open Data Grabs First Place in Asia, NATIONAL DEVELOPMENT COUNCIL (July 31, 2017), https://www.ndc.gov.tw/News_Content.aspx?n=114AAE178CD95D4C&sms=DF717169EA26F1A3&s=BEFA5CB8BDC7E2A6%E3%80%82

See Su Wen-Bin (蘇文彬), GuoNei ChengLi Open Data LianMeng TueiDong KaiFang ZihLiao YingYong FaJhan (國內成立 Open Data 聯盟推動開放資料應用發展) [The Open Data Alliance Was Established in Taiwan to Promote the Development of Open Data Applications], iTHOME (Sept. 14, 2013), https://www.ithome.com.tw/node/82633.

Zhonghua Minguo Xingzeng Yuan [Executive Yuan of R.O.C.], MaoKwei: CiDong Open Data ShenHua YingYong YuanNian JiaSu ShihChu JengFu ZihLiao (毛揆：啟動 Open Data 深化應用元年 加速釋出政府資料) [Premier Mao: Launching the First Year of Deepening the Application of Open Data to Accelerate the Release of Government Data], EXECUTIVE YUAN (Feb. 5, 2015), https://www.ey.gov.tw/Page/9277f759e41ccd91/bb1d1b5-f098-4ed0-8e88-8ab2e9764a03.

See generally LEE & TSENG, supra note 18, at 29.
government levels. To accelerate the release of data, the Executive Yuan required every department to establish a consulting committee dedicated to open data matters.\textsuperscript{46} By mid-2015, more than 30 committees were implemented throughout most of the departments under the Executive Yuan.\textsuperscript{47} The committees are composed of members from both the government and private sectors, and they are responsible for reviewing the data releasing process in each department.\textsuperscript{48}

However, discussions about open data policies among government and private sector participants still failed to include a comprehensive privacy protection framework.\textsuperscript{49} Nor were any sufficiently detailed instructions or regulatory efforts put forth to protect personal data during the process of data disclosure.\textsuperscript{50} Although there have been governmental efforts to incorporate personal privacy guidelines,\textsuperscript{51} the existing Open Government Data Principle and pertinent administrative regulations only provide government agencies with general guidelines when government employees use and process data. Whenever controversies about personal data protection arise, government agencies mostly rely on the PDPA to justify their data gathering, processing, and reuse practices.\textsuperscript{52} Unfortunately, the PDPA remains a regulatory regime with multiple flaws.


\textsuperscript{48} DATA.TAIPEI, supra note 40.

\textsuperscript{49} See e.g., LEE & TSENG, supra note 18, at 7–8.


\textsuperscript{51} The “Open Government Data Operating Principle for Agencies of the Executive Yuan” (the primary guidelines for government agency, amended in 2019) provides an example. There are only two items in the Principle related to privacy and personal data: Point 5 & Point 15. It also suggests that the PDPA and the Cyber Security Management Act are the only laws necessary to comply with when processing personal data.

\textsuperscript{52} See generally GeZiFa Wen yu Da (個資法問與答) [Personal Information Questions and Answers], NATIONAL DEVELOPMENT COUNCIL, https://pipa.ndc.gov.tw/Ne ws.aspx?n=7D3602579D2BF23F&sms=2F28806F8A42AE16 (last visited Apr. 11, 2021).
The PDPA was originally enacted as the Computer-Processed Personal Data Protection Law (CPPDPL), in 1995.\(^5^3\) To help garner support from the General Agreement on Tariffs and Trade, the Legislative Yuan enacted the CPPDPL to guarantee to the World Trade Organization that Taiwan would provide appropriate privacy protection for personal data.\(^5^4\) As its name suggests, the CPPDPL only applied to data processed by computers.\(^5^5\) Therefore, this law did not require data collectors or processors to specify why they were collecting, processing, or using data, nor did it ask data collectors or processors to de-identify the data.\(^5^6\) The CPPDPL was eventually replaced by the PDPA in 2010, where the legislators vowed to grant greater rights to individuals to control their own personal data and require data collectors and processors to provide more protections.\(^5^7\)

Nevertheless, the insufficient data privacy protection guidelines issued by the Executive Yuan and the PDPA have resulted in several controversies that have further increased legal uncertainties.\(^5^8\) These uncertainties cause concerns for both citizens who may be uncomfortable about their personal data being disclosed and for civil servants responsible for handling personal data daily.\(^5^9\) A 2017 survey showed that more than 80%


\(^{57}\) Chang, supra note 55, at 152.

\(^{58}\) See generally Shian, supra note 33.

of civil servants believe the current law is insufficient for handling open data duties, while private citizens agree that it is reasonable for the government to restrict the usage of open data to protect privacy.\footnote{The survey question is: “on a scale from 1[strongly disagree] to 5[strongly agree], indicate how you agree or disagree with the following statement: To protect privacy, it is reasonable that the government imposes restrictions on data accessibility.” The average score of the surveyed participants was 3.95. \textit{Id.} at 198.}

For years, Taiwan’s civil society and government have endeavored to excavate data stored within the government and private companies and tried to capitalize on the potential of such data. \footnote{See LEE \& TSENG, supra note 18, at 31–52 (noting Taiwan’s open data cases).} Nevertheless, a comprehensive privacy protection framework remains absent from the process of opening data. \footnote{See, e.g., Shian, supra note 33; see also Open Culture Foundation, supra note 18.} PDPA flaws discussed below demonstrate how it may fail to protect citizens’ privacy when data subjects’ information is being shared.

\section*{B. Key Controversies Raised by the PDPA}

\subsection*{1. The protection of sensitive data.} — The PDPA provides more data protections than any previous Taiwanese legislation. For example, the PDPA extends privacy protection to all data, whether it is stored in computers, in print, or processed in both government agencies and private sectors. \footnote{GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act], ch. I, art. 2.} Moreover, the PDPA mandates that under most circumstances, data collectors should inform data subjects of collection purposes and obtain consent from the subjects. \footnote{\textit{Id.} arts. 6–7.} The law also distinguishes between “general personal data” versus “sensitive personal data,” which includes medical records, healthcare data, genetics information, sex life data, physical examination reports, and criminal records. \footnote{\textit{Id.} art. 6.} Nevertheless, because Article 6 of the PDPA required stronger protection of “sensitive personal data” and other strict regulations, it faced fierce opposition from the private sector because “it would cause tremendous hardships for corporations to abide by the law”
should it be implemented. As a consequence, this contentious Article and the other articles related to its enforcement were suspended, leading to the amendments in 2015.67

Taiwan’s Ministry of Justice claimed that the purpose of the 2015 amendment was to “keep [the law] up with the current social circumstances.”68 For instance, under the amended PDPA, “written consent” is no longer required for the collection of personal data, unless it is sensitive data.69 This means that even implicit words of consent, verbal or written, can meet the PDPA consent requirement.70 The Ministry of Justice reasoned that relaxing the consent requirements could ease the potential administrative burdens on government agencies and save costs for private sector actors.71 Civil society groups such as Taiwan Association of Human Rights disagreed and criticized this clause and other aspects of the amendment, arguing that the Ministry of Justice was trading individuals’ rights to privacy for convenience and benefits for data collectors and processors.72 The amended PDPA not only fell short of many individuals’ expectations of closing the loopholes in data protection laws, but it also increased risks of privacy violations. The following scenarios exemplify

---

66 See Chang Jin-Hao (張景皓), GeZihSiouFa DaZhueiZong SanJenYi TiaoWen RenDai LiFaYuan ShenYi (個資修法大追蹤 3 爭議條文仍待立法院審議) [Tracking the Amendment of the Personal Data Protection Act: Three Controversial Articles Are Waiting to Be Deliberated by the Legislative Yuan], iHOME (Sept. 30, 2013), https://www.ithome.com.tw/node/82912.


68 Huang, supra note 67.

69 GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act], ch. I, art. 7.

70 Id.

71 FaWuBu dui GenRen ZiLiao BaoHuFa BuFen TiaoWen XiuZheng ShuoMing (法務部對個人資料保護法部分條文修正說明) [Ministry of Justice Explanation to The Amendments of The Personal Information Protection Act], art. 7 (2015).

how the amendments may put data subjects at privacy risks in open data cases.

2. De-identification. — Although the purpose of the PDPA is to protect personal data, the law only addresses the issue of de-identification in a general way. De-identification refers to the process used to prevent someone's personal identity from being revealed. The 2015 amendment merely requires that when government agencies or academic institutions reuse data for any purpose other than that for which it was originally collected, they must de-identify the data so that the information will not lead to the identification of a specific data subject. The PDPA’s Enforcement Rules promulgated under the Ministry of Justice further elaborated on the de-identification process, stating that the “data may not lead to the identification of a specific data subject.” The Enforcement Rules then provide that deidentification “shall mean the personal data [be] replaced with codes” and a data subject’s name shall be “deleted … partially concealed, or processed via other means to the extent that the data subject may not be directly identified.”

However, these enforcement rules do not provide any guidance regarding the extent to which the data should be deidentified or how much personal information should be removed. This lack of guidance gives rise to thorny questions. For instance, is the de-identification considered strong enough if the data subject cannot be identified at the first glance of the information? Should the de-identification be irreversible so that the data subjects cannot be identified if their data is combined with other data sets?

Another issue raised by the PDPA concerning de-identification is the lack of guidance denoting who bears the responsibility of ensuring the process is done successfully. The relevant provisions discussing de-identification state that the

75 GenRen ZiLiao BaoHuFa ShiXing XiZe (個人資料保護法施行細則) [Enforcement Rules of the Personal Data Protection Act] art. 17.
76 Id.
information “may not lead to the identification of a specific data subject” after its processing by the provider or from the disclosure by the collector, but no direction is given on who must complete this step. This ambiguity could result in further privacy disputes as both providers and collectors could theoretically shed the burden of de-identification under the statutory language. Without a clear understanding about whose responsibility it is to de-identify the data, the actual de-identifying process could be delayed and result in further risks of privacy violations.

3. The right to consent and opt-out. — Informed consent is an important mechanism for individuals to control the flow of their information. The 2010 PDPA amendment required data collectors to obtain written consent from data subjects under general circumstances. However, to ease the burden on data collectors, particularly in situations where there are large volumes of data, the 2015 amendment lifted this requirement for written consent, except when collecting sensitive personal data. Now, when dealing with non-sensitive personal data, data collectors or providers do not need to obtain “written consents.” In other words, verbal consent, not written consent, is sufficient under these circumstances.

Data collectors or providers do not need to obtain any form of consent in other conditions, such as collecting data for a public interest purpose, academic research, or assisting government agencies. From a data collectors’ perspective, the 2015 amendment has removed the hurdle of obtaining consent when a large number of data subjects are involved, which is true in most open data initiatives. Data subjects, on the other hand, have gained

---

78 See Huang Yen-Fen (黃彥棻), GeZihFa XiZe ChLu, GaoZhi yu ShuMian TonYi 2 DaxianZhi FangKuan (個資法細則出爐，告知與書面同意 2 大限制放寬) [The Released Rules of PDPA, Relax the 2 Limitation to Inform and the Written Consent], iTHOME (Nov. 4, 2011), https://www.ithome.com.tw/node/70655.
79 Id.
80 Id.
little while simultaneously losing the right to refuse their data from being used without clear consent.

Still worse, according to the PDPA, data subjects can only request their information be deleted or discontinued from processing or use when the specific purpose of data collection no longer exists or the dataset period expires. Except for the above situations, data subjects cannot choose to “opt-out” of the databases or programs. 83

4. The ambiguity of “public interest.” — The term “public interest” appears repeatedly throughout the PDPA and serves as an exception for data collectors or providers to avoid certain legal obligations. For example, the PDPA mandates that a government agency shall only use personal data for the specific purpose of collection and within the necessary scope of its duty. 84 However, Article 16 allows government agencies to use data for purposes other than the original purpose behind collecting the data if the use is for “public interest.” 85 Other provisions in the PDPA also allow “public interest” exemptions, such as data uses for news reporting purposes. 86 However, no explicit definition of “public interest” is given.

Without a workable definition of “public interest,” there is no limit to the number of exemptions that could be invoked. Throughout Taiwan’s history, the government has often used “maintaining social order” and “promoting administrative efficiency” as justifications for policing its people. 87 Therefore, the risk of data collectors or data processors excessively utilizing this “public interest” exemption may perhaps be even higher.

When the Legislative Yuan passed the PDPA in 2010, legislators were aware of the possible controversies that might arise from the undefined term “public interest.” 88 However, the legislators explicitly chose to keep the term undefined and instead made an “additional resolution” to deal with this issue when

83 Id. ch. I, art. 11.
84 Id. ch. II, art. 16.
85 Id.
86 Id. ch. I, arts. 6, 8–9; ch. III, arts. 19–20.
87 See Kuo & Chen, supra note 56, at 259–60 (highlighting the cases in which the government used “social order” as a basis to sacrifice Taiwanese citizens’ privacy rights).
88 See Huang, supra note 78.
passing the law. In the additional resolution, the legislature asked the Ministry of Justice to define “public interest” in the Enforcement Rules of the PDPA after consulting experts and members from civil society. But since then, the Ministry of Justice has not responded to the request. Consequently, the government and the courts usually determine that this public interest requirement has been satisfied if a program is carried out for public purposes in the public sector, as open data initiatives are. But the data users (in most cases, the government) and the courts have never carefully analyzed an open data regime to determine what the public interest at issue is, nor have they weighed the importance of a claimed public interest against an individual’s right to privacy. Under this current legal framework, those who employ public interest justifications usually prevail and individuals’ privacy interests are diminished even further.

While the Taiwanese is working to support the rapidly growing data initiatives in the country, the PDPA remains the only available mechanism to ensure privacy protections. A privacy protection mechanism with numerous undefined terms and loopholes as the only avenue for protecting individuals’ data privacy therefore continues to contribute to the privacy perils of Taiwan’s open data initiatives.

III. CASE STUDIES

The Electronic Toll Collect System, the Taiwan National Health Insurance Research Databases, and the COVID-19 surveillance measures recently implemented in Taiwan provide three examples of the flaws in Taiwan’s open data initiatives. These case studies highlight the need to adequately address data

89 See Liu Ching-Yi (劉靜怡), BuSuan JinBu de LiFa: “GenRen ZiLiao BaoHuFa” ChuBu PingXi (不算進步的立法: 『個人資料保護法』初步評析) [A Legislation that is Not Really Progressive: A Preliminary Comment on Personal Information Protection Law], 153 TAIWAN L. REV. 147, 156–64 (2010).
90 Id.
92 See Liu, supra note 89, at 162.
93 Id.
privacy concerns when examining open data policies. They also showcase the urgent need to address the current flaws in the PDPA – the lack of protection for sensitive data, the lack of a private right to consent and opt-out, and the ambiguity of the term “public interest.”

A. Open Data and the Electronic Toll Collect System

The Electronic Toll Collect system illustrates how a database established by a public-private partnership can be exploited by a private company, and moreover, how the government misused data in the name of the ambiguous “public interests” embedded within the PDPA.94

In 2004, Taiwan’s Ministry of Transportation and Communication commissioned the Far Eastern Electronic Toll Collection (Far Eastern), a private corporation, to build the Electronic Toll Collect system (ETC) on the country’s highways to replace traditional toll-collecting by workers in toll booths.95 Under the build-operate-transfer contract (BOTC), a type of public-private-partnership contract, Far Eastern was granted the right to operate the ETC and the associated data system for twenty years before returning the right of operation back to the government.96

Taiwan’s traditional toll booths were all successfully replaced by the ETC by 2013.97 The ETC collects and records information about vehicles driving on the highways, including time of day, location, distance traveled, and amount paid.98 For the ETC to gather tolls, many vehicles are equipped with e-Tags,

---

94 Ho Ming-Syuan (何明諠), ShuWei ShiDai de YinSi BianJie: yi JianBao ZiLiaoKu yu ETC JiaoTong ZiLiaoKu WeiLi (數位時代的隱私邊界: 以健保資料庫與ETC交通資料庫為例) [The Rights to Privacy in the Digital Age: The Case of the Health Insurance Research Database and the ETC Traffic Database], 3 TAIWAN HUM. RTS. J. 1 39, 147–49 (2016).
96 Id.
98 Chang, supra note 55, at 147.
gadgets that help the ETC identify cars and record data. As of January 2020, 87.94% of all registered vehicles in Taiwan were equipped with e-Tags. The ETC can also scan the license plates of vehicles that are not equipped with e-Tags, which enables the ETC to record information about all vehicles using the highways, whether they have e- Tags or not.

This system has created a comprehensive database of traffic data and has proved to be incredibly helpful for Taiwanese government agencies and the private sector. However, potential privacy violations may ensue alongside the beneficial uses of the data. For example, in 2013, Far Eastern unilaterally instituted a policy that charged third parties for the e-Tag data they obtained and used for their own purposes. The policy was severely criticized by civil society, with many claiming that Far Eastern was profiting off of selling e- Tags users’ personal data. The policy was subsequently disapproved by the supervising government agency, the Freeway Bureau of the Ministry of

---


100 In January 2020, Far Eastern claimed that 7,140,000 cars in Taiwan were equipped with e-Tags. The government record shows that the total number of automobiles in Taiwan was 8,119,056 in the same month. Thus, the percentage of the cars equipped with e- Tags was roughly 87.94%. See Jian-Jih Guo (郭建志) GuoDao JiCheng ShouFei LiaoJhouNian e-tag ShengJi uTagGO (國道計程收費六周年 e-tag 升級 uTagGO) [After Six Years of Toll Charges, E-tag Was Ugraded to uTagGO], COM. TIMES (Jan. 15, 2020), https://ctee.com.tw/livenews/ctee/aj/a08616002020011511282804; The List of Numbers of Registered Automobiles, MINISTRY OF TRANSP. AND COMM., https://stat.motc.gov.tw/mocdb/stmain.jsp?sys=100&fundid=a3300 (last visited Nov. 21, 2020).

101 See Lu, supra note 67.

102 Ho, supra note 94, at 147.

103 For example, the National Taxation Bureau of Kaohsiung uses the data on the number of tolls paid by tour buses to audit the bus companies and determine if they have honestly filed their taxes. See You Lan Che Ye Shen Ba Xiao Shou E Bing Wei Yin Lu Ke Guan Guang Xiang Dui Cheng Zhang Guo Shuei Yu Jiang Jia Chiang Duei You Lan Che Yeh Jhe Cha He (遊覽車業申報銷售額並未因陸客觀光相對成長 國稅局將加強對遊覽車業者查核) [The Declared Sales of the Tour Bus Industry Did Not Grow Relatively with the Sightseeing of China Visitors: the Taxation Bureau Will Increase Tax Auditing], LAW BANK (Sept. 14, 2013), https://www.lawbank.com.tw/news/NewsContent.aspx?NID=113954.


105 Id.
Transportation and Communication (Freeway Bureau) and eventually retracted by Far Eastern.\footnote{106}

One year later, the Criminal Investigation Bureau demanded that the Freeway Bureau and Far Eastern hand over all vehicle travel information, including license plate numbers, travel time logs, locations, video images, and vehicle data of individuals who were not criminal suspects.\footnote{107} Far Eastern initially refused to turn over the data, turning to the Ministry of Justice for legal opinions.\footnote{108} However, Far Eastern later reached an agreement with the Criminal Investigation Bureau stating that the transportation data cannot be reviewed until the Criminal Investigation Bureau’s requests were approved by prosecutors.\footnote{109} Far Eastern later released its “Policy to PDPA Protection” that addresses its relationships and interactions with the government as “comply[ing] with the PDPA” without clearly indicating whether any of the data has been or will be handed over to the Criminal Investigation Bureau.

The government’s utilization of the data stored in the ETC e-Tag system did not stop at the agreement with Far Eastern. In 2015, as the number of open data initiatives in Taiwan continued to grow, the Freeway Bureau decided to make all ETC data open to the public and available online.\footnote{111} Under this system, anyone can simply visit the Freeway Bureau’s website and download both

\footnotesize

\footnote{106}{Id. Yогуан Меити Баодоу Гудао Динжи Шофеи (ETC) Дучау eTag Shuhao Konshie Gezi Zi Shuomin (有关媒体报道国道电子收费(ETC) 阅读 eTag 序号恐逸个资之说明) [A Clarification on the News Reporting on the Possible Leak of Personal Data as A Result from ETC’s Reading of eTag], FREEWAY BUREAU (May 7, 2013) https://www.freeway.gov.tw/Publish.aspx?cnid=193&p=4429.}

\footnote{107}{Liu Si-Yi (劉世怡), Diaoyue Singchejilu Reyi Singshihjyu Shuoming (調閱行車紀錄惹議 刑事局說明) [Access to Driving History is Controversial, National Police Agency Explain], CENT. NEWS AGENCY (Jan. 11, 2014), https://www.cna.com.tw/news/firstnews/201401110016.aspx; See also Lu, supra note 67.}

\footnote{108}{Lu, supra note 67.}

\footnote{109}{Id.}

\footnote{110}{Geren Ziliao Baohu Fangshi ji Zhengce Shengming (個人資料保護方式及政策聲明) [The Policy and Approach to Protect Personal Data], FETC (Mar. 2, 2021) https://www.fetc.net.tw/UX/UX0901SharePoint/UX090101HtmlContent?processId=UX04030103.}

real-time and historical de-identified data on traffic, vehicles’ speed, travel routes, and other related information.112

The Freeway Bureau’s choice to publicize the ETC’s data unsurprisingly elicited worries and criticisms from civil society.113 First, critics expressed concerns that the disclosure of the data, though de-identified, would violate the PDPA if the government did not obtain consent from data subjects.114 According to the PDPA, if a government agency uses individuals’ personal data, the use shall be in accordance with the specific purpose of the data’s collection.115 The ETC was originally intended to collect highway tolls. However, data about the all vehicles, including travel time logs, locations, and images are also collected and stored in the ETC database.116 One could argue that the data can therefore only be used for toll-collecting, as this was the original specific purpose of the data collection, and other uses irrelevant to collecting tolls on the highway fall outside the scope of the original purpose.117

To counter this argument, the Freeway Bureau contended that publicizing the ETC data aligns with public interests.118 Under the exception outlined in Article 16 of the PDPA, an agency may use data beyond the specific purpose of collection if necessary to further public interest.119 The Freeway Bureau

114 Id.
115 GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act] ch. I, art. 5.
116 See Lu, supra note 67.
117 See Lu Yi-Ron (呂苡榕), WoMen You BuBe Etag KueiKan De QuanLi Ma? (我們有不被 Etag 窺看的權利嗎?) [Do We Have the Right to be Free From Surveillance Under Etag?], INITIUM MEDIA (June 14, 2016), https://theinitium.com/article/20160614-taiwan-eTag2/.
118 Ho, supra note 94, at 148.
119 GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act] ch. II, art. 16 (“[A] government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases: . . . 2. where it is necessary for ensuring national security or furthering public interest; . . . 5. where it is
claimed that making the data publicly available online satisfies this public interest requirement. For example, by reading and downloading the data online, the public can develop a better understanding of traffic patterns and make more sophisticated public transportation plans.

Nevertheless, the Freeway Bureau’s proffered “public interest” purpose still leaves several issues open. For example, it will be difficult for the government and the data subjects to ensure that the data, which can be downloaded for free by anonymous users all over the world, is used for public good. Furthermore, if a company uses the data to develop a traffic monitoring application and sells the app for a profit, it seems unlikely that the company’s use of the data in this for-profit manner should be construed as a public interest matter.

Another legal conflict relating to the use of ETC data arose in 2017 and explicitly showcases the ambiguity of the term “public interest.” The Motor Vehicles Office of the Directorate General of Highways in HsinChu acquired vehicle images from the ETC database, identified them, and then issued traffic citations to vehicles driving on the shoulder of the road. One of the issues in this case was whether the Motor Vehicles Office could use the data without obtaining consent from the data subjects. The Taiwan HsinChu District Court ruled that the ETC image data could not be used as evidence of illegal driving because the Office’s use of data was unrelated to the original purpose of toll-collecting. The Court further pointed out that without the data subjects’ consent, necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject.”.


121 Id.

122 Ho, supra note 94, at 148.

123 Id.


125 Id.

126 Id.
the Office’s use of data would increase the subjects’ privacy risk. As a result, the public interest exception in this case did not prevail.

Another concern from critics is the effectiveness of de-identifying e-Tag data. Article 16 of the PDPA allows certain exceptions when government agencies use data for other purposes than what it was originally collected for but requires the agencies to de-identify the data when making them available for secondary use. However, the PDPA fails to clearly indicate whether the agencies must obtain informed consent from data subjects if the uses of data will exceed the original purpose of the data collection. In the traffic database that the Freeway Bureau opened to the public, the only data removed was license plate numbers. The Freeway Bureau claimed that removing the license plate numbers effectively de-identified the data, and thus, there was no need to obtain consent. However, even without license plate numbers, user identification is still possible given the amount of data released. Information about vehicles’ departure locations, destinations, and travel times is released. When traffic is light, one could theoretically identify the vehicles that use highways by compiling all of this accessible information. Furthermore, a person could use the images of a vehicle, the time, and the location of the vehicle traveling on the highway to surveil the travel route of the driver. Unfortunately, as discussed, there are no requirements regarding the security level or necessary thresholds for data de-identification in the PDPA. Therefore, under this loose regulatory regime, the simple step of removing vehicles’ license plate numbers might be enough to satisfy the

127 Id.
128 Id.
129 GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act] ch. II, art. 16 (“[A] government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection.”).
131 Id.
132 Id.
133 See The List of Numbers of Registered Automobiles, supra note 100.
135 Id.
136 Lu, supra note 67.
PDPA’s de-identification requirement for using the data without obtaining consent from data subjects. However, this potential conclusion could have severe negative ramifications in terms of privacy protection. Since there is no clear prohibition on data compiling under these circumstances, critics worry that the data could be combined with other information and used for surveillance.\(^\text{137}\)

The above examples highlight not only the imprudent and insufficient privacy practices of Far Eastern and the Freeway Bureau, but also underscore a greater issue in the PDPA overall – the PDPA’s ambiguities have left data subjects, specifically the drivers travelling on Taiwan’s highways, in privacy peril.

\textbf{B. Taiwan’s National Health Insurance Research Databases}

Since 1995, the Taiwanese government has mandated that all citizens with official residency and all foreign nationals living in Taiwan with an Alien Resident Certificate be covered under the National Health Insurance (NHI) program to receive affordable medical services.\(^\text{138}\) As of June 2019, a total of 23,894,289 people were participating in NHI, equating to 99.9\% of the population.\(^\text{139}\)

The government agency in charge of the program is the National Health Insurance Administration (NHIA), a department within the Ministry of Health and Welfare (MHW).\(^\text{140}\) To successfully administer national health insurances affairs, the NHIA must collect, process, and maintain both insured patients’


and service providers’ information.\textsuperscript{141} The information collected by the NHIA includes the personal data of patients, costs of the medical treatment received, and appointment schedules.\textsuperscript{142}

Since the NHI program is mandatory and almost all Taiwanese citizens are covered, a vast amount of potentially valuable personal data has been collected. In 1998, the NHIA transferred the data from the insurance program to the National Health Research Institute (NHRI), a non-profit foundation for medical research funded primarily by the government.\textsuperscript{143} The NHRI proceeded to establish the National Health Insurance Research Database (the Database) to maintain all “registration files and original claims for reimbursement” that were transferred from the NHI program.\textsuperscript{144} The Database also made these files and claims available to academics who wished to use the data for research.\textsuperscript{145}

Nevertheless, the NHIA was questioned for failing to properly de-identifying their medical data.\textsuperscript{146} The NHRI defended itself and claimed that the personal identification numbers were encrypted and patient birth dates were deleted (although the birth year and month were retained) before the NHIA transferred the data into the Database.\textsuperscript{147} The NHRI also de-identified the data again before making it available for research purposes.\textsuperscript{148} Further, the NHRI argued that to use the data from the Database for

\textsuperscript{141} See JianKang yu YiLiao ZhiLiao de JiaJhih YingYong (Er): Cyuanmin Jiankang Baosian ZhiLiaoakou Jianjie (健康與醫療資料的加值應用 (二): 全民健康保險資料庫簡介) [Health and Medical Data Value-Added Application 2: Introduction to the National Health Insurance Database], PANS\textsuperscript{142} Ci (July 8, 2012), https://pansci.asia/archives/18437.

\textsuperscript{142} Id.

\textsuperscript{143} Overview, NATIONAL HEALTH RESEARCH INSTITUTE (NHRI), https://www.nhri.edu.tw/eng/About/more?id=757957da67f54478bb0030e32d0bc70d (last visited Mar. 10, 2020).


\textsuperscript{145} Id.

\textsuperscript{146} See, e.g., Tsai et al. v. National Health Insurance Administration, 102 NianDu Su Zi No. 36 (102 年度訴字第 36 號判決) (Taipei GaoDeng XingZheng FaYuan (臺北高等行政法院) [Taipei Administrative High Court], 2014) (Taiwan); Tsai et al. v. National Health Insurance Administration, 106 NianDu Pan Zi No. 54 (106 年度判字第 54 號判決) (ZuiGao XingZheng FaYuan (最高行政法院) [Supreme Administrative Court], 2017) (Taiwan).

\textsuperscript{147} Tsai (Taipei Admin. High Ct. 2014) at 8–11.

\textsuperscript{148} Id.
research purposes, an individual must fill out an application form and submit their plan to an institutional review board (IRB) for approval.\textsuperscript{149} The NHRI then consults experts to decide whether to grant permission to applicants.\textsuperscript{150}

In 2011, in addition to the Database, the MHW established what became the Health and Welfare Data Science Center (Data Center) to consolidate all valuable health information from the NHI Program and make it available to both academic researchers and government agencies.\textsuperscript{151} The goal of this data consolidation was to facilitate governmental policy-making, promote medical research, and encourage innovation.\textsuperscript{152} Since 2016, the Data Center has taken over the Database and became the sole resource for NHI Program information.\textsuperscript{153} Currently, the Data Center Database is operated and maintained by the MHW.\textsuperscript{154} To de-identify the data, the MHW staff will encrypt the data in their own site before turning it over to the Data Center.\textsuperscript{155} The Data Center also requires that researchers who want to access the data for research purposes personally visit the Data Center and conduct all data analysis while physically in the center.\textsuperscript{156} The Data Center uses this process to reduce the risks of a data leak or any abuse of the data.\textsuperscript{157} The process of accessing data in the Data Center Database is the same as the process of applying for data within the

\begin{flushleft}
\textsuperscript{149} Id.

\textsuperscript{150} Id.\textit{ Application Process, NATIONAL HEALTH INSURANCE RESEARCH DATABASE, https://nhird.nhri.org.tw/apply_01.html (last visited Mar. 11, 2020).}


\textsuperscript{152} Id.

\textsuperscript{153} See Ho, supra note 94, at 143; see also \textit{Latest News, NATIONAL HEALTH INSURANCE RESEARCH DATABASE, http://nhird.nhri.org.tw/news (last visited Mar. 11, 2020). The announcement on the webpage states that the database service has been terminated as of June 2015. All original data in the database was returned to the NHIA.}


\end{flushleft}
Database: a researcher must submit forms and plans, and these must be approved by an IRB and reviewed by experts.\textsuperscript{158}

The NHIA does not request consent from its data subjects either before, during, or after the processing this vast array of personal health information.\textsuperscript{159} This is significant because, in this situation, the data subjects are the individuals insured under the program – 99.9\% of the Taiwanese population.\textsuperscript{160} These data subjects also have no opportunity to request for data controllers or processors to stop using or processing their information.\textsuperscript{161} This means that 99.9\% of the population in Taiwan has no right to any form of opt-out mechanism regarding their potentially personal medical data.

In 2012, eight individuals from several civil rights organizations, including the Taiwan Association of Human Rights, filed a lawsuit against the NHIA and claimed that the NHIA’s transfer of the data within the Data Center Database out to third parties did not align with public interests.\textsuperscript{162} They also argued that the data was not properly de-identified.\textsuperscript{163}

According to the PDPA, medical records are categorized as sensitive information and thus should not be collected, processed, or used by the government or non-government entities.\textsuperscript{164} However, sensitive information may be used by these parties when it is necessary to do statistical or academic research for the purpose of public interests, such as for “healthcare, public

\begin{itemize}
\item[\textsuperscript{158}] See The Review Instructions for the Application of the Health and Welfare Data, supra note 155.
\item[\textsuperscript{159}] See Tsai et al. v. National Health Insurance Administration, 102 NianDu Su Zi No. 36 (102 年度訴字第 36 號判決) at 3, 6 (Taipei GaoDeng XingZheng FaYuan (臺北高等行政法院) [Taipei Administrative High Court], 2014) (Taiwan).
\item[\textsuperscript{161}] See Tsai (Taipei Admin. High Ct. 2014) at 3, 6.
\item[\textsuperscript{162}] Id.
\item[\textsuperscript{163}] See Chang Chen-Hung, Controversy over Information Privacy Arising from Taiwan’s National Health Insurance Database, 40 CHUNG YUAN CHRISTIAN UNIV. L. REV. 185, 187 (2018).
\item[\textsuperscript{164}] GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act] ch. I, art. 6.
\end{itemize}
health, or crime prevention.”165 However, a government agency that intends to use this information for the public interest and in a way beyond the scope of the original collection purpose shall also have the data de-identified.166

In Tsai et al. v. NHIA, the plaintiffs first argued that, because the NHIA did not obtain consent from the data subjects, their process and use of the data should be limited to the scope of the agency’s statutory duties under Article 6 of the PDPA.167 Furthermore, they argued that because there was no public interest involved in the agency’s publication of the data to the public, the disclosure of the data to third parties violated the data subjects’ privacy. In response, the NHIA argued that there was a relevant public interest because the data had been helpful to research and resulted in academic periodical publications. The plaintiffs subsequently responded to this counterargument by claiming that the NHIA could not prove a direct link between the public interest and the research or academic publications.170

The plaintiffs also argued that the NHIA gave the third parties improperly encrypted data.171 Without proper encryption, individuals could be re-identified by combining the data stored in the Databases with data stored elsewhere. The plaintiffs argued that this was a direct violation of the PDPA.173 In response, the NHIA maintained that the data had been through multiple layers of encryption, which should be effective enough to ensure the data’s security and prevent the re-identification of data subjects.174

---

165 Id. ch. I, art. 6. Additionally, Article 15 of the PDPA mandates that a government agency that is going to collect or process personal data must provide a specific purpose for the collection or processing and comply with one of the following conditions: “1. where it is within the necessary scope to perform its statutory duties; 2. where consent has been given by the data subject; or 3. where the rights and interests of the data subject will not be infringed upon.”

166 Id. ch. II, art. 16.

167 See Tsai (Taipei Admin. High Ct. 2014) at 3, 6.

168 Id.

169 Id.

170 Id.

171 Id. at 5, 37.

172 Id.

173 GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act] ch. I, art. 16.

174 See id. ch. I, art. 16; see also Tsai et al. v. National Health Insurance Administration, 106 NianDu Pan Zi No. 54 (106 年度判字第 54 號判決) at 6 (ZuiGao XingZheng FaYuan (最高行政法院) [Supreme Administrative Court], 2017) (Taiwan).
The plaintiffs also raised the issue of the right to opt-out from subsequent data uses, citing precedent from the Constitutional Court of Taiwan.175 In the precedent, Interpretation 603, the Court elaborated that people should be equipped with the right to control their own personal data because they must be able to decide whether or not to disclose it, and, if so, “to what extent, at what time, in what manner and to whom” such information will be disclosed.176 Further, individuals also have the right “to correct any inaccurate entries contained in their information.”177 In a separate opinion, the Court also stated that the freedom from unwanted intrusion into one’s private life and individual’s autonomy over one’s own personal data are recognized as constitutional rights.178 However, the Court pointed out that the right to control personal data is not absolute and could be burdened with certain restrictions by the State.179

Citing the Constitutional Court of Taiwan, the Tsai et al. plaintiffs argued that the “right to control personal data” includes not only the right to consent to how one’s personal data will be processed and used, but also the right to an opt-out mechanism – the right to request their personal data not be used or processed.180 The PDPA even explicitly stipulates that individuals cannot waive their right to “demand the cessation of the collection, processing or use of his/her personal data.”181 This implies that there is a right to opt-out. The plaintiffs contended that if they were not given the opportunity to consent, then they are at least entitled to the right to request that the use of their data cease.182

The plaintiffs lost their case in the Taipei High Administrative Court (High Court), and subsequently appealed to

175 See Tsai (Taipei Admin. High Ct. 2014).
176 Interpretation No. 603, 2005 47 JUDICIAL YUAN GAZETTE 1, 1 (Sifayuan Dafaguan Huiyi Sept. 28 2005).
177 Id.
179 Id.
180 See generally Tsai (Taipei Admin. High Ct. 2014).
181 GenRen ZiLiao BaoHuFa (個人資料保護法) [Personal Data Protection Act] ch. I, art. 3.
182 Tsai (Taipei Admin. High Ct. 2014) at 4.
the Supreme Administrative Court (Supreme Court).\textsuperscript{183} In 2016, the Supreme Court also ruled against the plaintiffs, finding in favor of the NHIA.\textsuperscript{184}

In response to the plaintiffs’ first argument that the NHIA was unable to prove that there was a direct public interest related to the use and disclosure of their personal data, both the High Court and the Supreme Court found that both Databases were established to add value to the plaintiffs’ raw data by assisting with public health matters and academic research.\textsuperscript{185} They also held that the results from the Databases could further enhance the overall welfare for all citizens, thus finding a public interest justification in the use and disclosure of the personal data by the NHIA.\textsuperscript{186}

In making their determinations, both courts employed balancing tests. The High Court emphasized that the PDPA’s purpose is to “protect” rather than maintain “the secrecy” of personal data.\textsuperscript{187} In other words, there are many ways to “protect” the data, and this may include maintaining its secrecy, but they are not one in the same. Therefore, when an individual’s privacy right conflicts with the public interest, an individual’s right to control their own data should “stand back” for the public interest.\textsuperscript{188} The High Court also found that the databases contributed to medical studies that were beneficial to all citizens, and this was more important than the protection of individual privacy.\textsuperscript{189} In addition, the High Court determined that the NHIA had properly de-identified the data and thus had used the data the manner least

\begin{itemize}
\item \textsuperscript{183} See generally Tsai et al. v. National Health Insurance Administration, 106 NianDu Pan Zi No. 54 (106 年度判字第 54 號判決) (ZuiGao XingZheng FaYuan (最高行政法院) [Supreme Administrative Court], 2017) (Taiwan).
\item \textsuperscript{184} Id.
\item \textsuperscript{185} Id. Tsai (Taipei Admin. High Ct. 2014).
\item \textsuperscript{186} See Tsai (Taipei Admin. High Ct. 2014) at 14 (“The goal of establishing HWDC is adding value to individual health raw data and thus generating collective data that is worth putting into application. This data can also enhance the quality of decisions on public health, on academic research, and on innovations in health as well as medical industry, and bring about benefits to all the Taiwanese people… It is obvious that the data is used for academic purposes and is characterized by public interest.”); see also Tsai (Sup. Admin. Ct. 2017), at 38 (“The macro data on all the citizens’ body, health, and medical treatment plays a significant role in the progress of national health and welfare, which also holds great public interests.”) (Translated).
\item \textsuperscript{187} Tsai (Taipei Admin. High Ct. 2014), at 17.
\item \textsuperscript{188} Id.
\item \textsuperscript{189} Id.
\end{itemize}
harmful to an individual’s privacy. The High Court ultimately held that the NHIA’s disclosure of the data was indeed necessary and proper.

The Supreme Court also balanced the public’s interests against an individual’s privacy right. The Supreme Court recognized that data is a valuable social resource, and a comprehensive database is an important and useful public good. The Supreme Court pointed out that the government’s data collection resembles “sampling” in conducting a study. The Supreme Court elaborated, emphasizing that “in the process of sampling, one needs to be sure the samples could precisely be representative of the original population...if we allow there are [sic] any options for the samples, the quality of the samples would be severely impacted.” Thus, the Supreme Court found that it would be unreasonable to allow the plaintiffs to opt out of the databases simply to protect the individuals’ right to privacy. In its decision, the Supreme Court expressed concern that other individuals may follow the plaintiffs’ lead if individuals are granted the right to opt-out, and this result could squander the efforts and the expenses that the NHIA had spent on gathering the data and building the databases.

The Tsai et al. v. NHIA case has revealed several alarming perils of open data in Taiwan. First, it is apparent that a detailed and thoughtful privacy protection program is absent from Taiwan’s implementation of its open data initiatives. In Tsai et al.,

190 Id.
191 Id.
192 Id.
193 Id. at 36 (“Information is a social resource of great worth. The cost of collecting information is also expensive (The more the information, the more expensive for collecting the information.). (“How if being used properly, the information could generate more benefits. Therefore, a comprehensive database would be an important public good.”) (Translated).
194 Id. at 37.
195 Id. (“As for thoroughly excluding specific subjects’ data for the reason of respecting individuals’ information privacy, it would exceed reasonableness and even become an obstacle to the realization of public interests... If allowing the selection of the samples that are gathered, the quality of sampling result would be gravely impacted.”) (Translated).
196 Id. at 42. (“[I]f a few people were allowed to opt out of the [sampling], then a majority of individuals could also ask for the same treatment on the basis of the requirement of enforcement equality, which would further bring about the “broken window effect,” and result in the unnecessary waste of the cost of data gathering.”) (Translated).
the NHIA lacked a sophisticated de-identification and monitoring process while simultaneously being responsible for collecting and handling almost every Taiwanese resident’s health information. By relying solely on a questionable de-identification process, the NHIA ignored all other viable options for protecting their data subjects’ privacy.

The next question raised by Tsai et al. concerns the extent of de-identification and how much must be done to achieve the protection of personal data. Although the PDPA requires that data subjects must not be able to be identified after information is processed or disclosed, the law itself remains ambiguous about what exactly “de-identification” means and to what extent de-identification is necessary. The PDPA leaves it open, relying instead upon the discretion of government agencies and decisions made by courts. As a result, the strength of privacy protections for Taiwanese citizens is uncertain and hinges on the internal procedures of government agencies and judges’ understanding and recognition of privacy.

In Tsai et al. v. NHIA, the Supreme Court chose to blame data predators for possible privacy violations. However, the peril that results from the combination of dispersed databases is exactly where privacy advocates should focus their concern. In contrast to this opinion from the Supreme Court, the international community and international organizations, such as the


199 Id.

200 Tsai et al. v. National Health Insurance Administration, 106 NianDu Pan Zi No. 54 (106年度判字第 54號判決) at 36 (ZuiGao XingZheng FaYuan (最高行政法院) [Supreme Administrative Court], 2017) (Taiwan).

Organization for Economic Co-operation and Development, have recognized that governments must be responsible for enhancing database safeguards and protections. Governments worldwide have opted for intensified privacy protection to provide a safer and more trustworthy data environment that can further encourage the development of data usage. Nonetheless, in Tsai et al., the Supreme Court strayed from this international regulatory trend and therefore missed the opportunity to urge Taiwan’s government toward a stronger privacy protection regime, particularly for the protection of sensitive medical data.

The Taiwanese government has wrongly equated “public purpose” with “public interest.” Even worse, the decisions analyzed above further depicts that courts, without any adequate deliberation on the constitutional meaning of data privacy, rushed to endorse the government’s mistaken view of the definition of “public interest” in the PDPA. However, in reality, the PDPA does not address the standards that should be used to determine “public interest.” Neither the High Court nor the Supreme Court provided sophisticated reasoning in answering these questions about whether and how reasonable and feasible criteria should be established in PDPA. Rather, the courts mistakenly equated public purpose with “public interest” – if the defendant claimed the measures were adopted for a public purpose, whether for medical research or innovation, the courts assumed that there was a potential public interest. This same “public interest” rationale also led the Supreme Court to deny the opt-out right and require that the plaintiffs’ health data remain indefinitely in the Database regardless of the plaintiffs’ opposing desires.

---

203 Id.
204 See Tsai et al. v. National Health Insurance Administration, 102 NianDu Su Zi No. 36 (102 年度訴字第 36 號判決) at 18 (Taipei GaoDeng XingZheng FaYuan (臺北高等行政法院) [Taipei Administrative High Court], 2014) (Taiwan) (The High Court pointed out that the NHIA’s giving data to third parties was “…for academic research. The transfer of the data was for academic purposes, which was obviously in the public interest.”); Tsai (Sup. Admin. Ct. 2017) at 36. (The Supreme Court did not specify what “public interest” is. Instead, the Supreme Court proceeded to state that “the establishment of a large database was very important for quantitative research.”).
205 See Tsai (Sup. Admin. Ct. 2017), at 36, 37; Tsai (Taipei Admin. High Ct. 2014), at 16.
C. Data Sharing and Surveillance Practices in Response to COVID-19

During the early stages of the COVID-19 pandemic, the fear of the virus prompted sentiment of unity within the Taiwanese community. Spurred by people’s need for public safety, the Taiwanese government adopted stringent surveillance measures. The data sharing and surveillance practices implemented to combat COVID-19 have demonstrated how the democratic government’s actions, while supported by citizens’ wishes for effective control over the pandemic, might impact civil rights and liberties. Taiwan’s story may even imply the possibility that citizens are willing to sacrifice privacy in exchange for public safety in emergency situations. However, it triggers another critical concern: would this anomalous violation of privacy intended to be temporary become “normalized” as a long-standing practice?

In early 2020, COVID-19 plunged the world into a global pandemic, Governments around the world declared states of emergency and adopted technological measures to deal with the outbreak. These measures included data surveillance on

---


individuals’ travel history via data sharing within multiple databases maintained by government agencies, via requesting communications data from private sector actors such as internet and telecommunications companies, and via contact tracing, personal location, and health condition tracking through mobile software applications (apps). Taiwan’s government was no different, as it also employed data sharing and surveillance measures in response to COVID-19. Each response implicates Taiwanese fundamental rights to privacy and other constitutional liberties. In this section, we first discuss the approaches to data sharing and surveillance that the Taiwanese government employed in its response to COVID-19. Next, we present a constitutional and legal analysis of the regulatory measures adopted by Taiwan and how these measures might compromise the protection of citizens’ fundamental rights in the name of saving lives from COVID-19.

In response to the outbreak of COVID-19 in Wuhan, China, at the end of 2019, the Taiwan NHIA linked their medical Database with the “immigration database” maintained by the National Immigration Agency to track whether an individual had traveled into Taiwan from Wuhan. This combined database was
eventually linked to include the travel history of citizens coming into Taiwan from Japan, Korea, and other nearby countries if the nation reported growing COVID-19 outbreaks. The primary purpose of linking these databases was to allow physicians to automatically check for a patient’s travel history and determine if there was any risk of COVID-19 exposure. However, this vast access to information led to some extreme and absurd results when individuals with recent travel histories sought medical services. For instance, a woman with a toothache was rejected by 10 dentists because of a recent visit to Hokkaido, Japan.

Although from the outbreak in late 2019 to April 2021, Taiwan has fortunately managed to keep the COVID-19 outbreak largely under control within the country, the following case ironically illustrates the inadequacies of the travel history surveillance system. The first wave of confirmed cases in Taiwan came after a Taiwanese navy ship with dozens of sailors returned from a visit to Palau in early April. Legislator Chen Jiau-hua (陳椒華) revealed that some of the sailors with confirmed cases of COVID-19 visited health clinics after disembarking in

---

217 See Chang Ming-Xuan (張茗喧), 147 Wan ZengDao Rih Han MinJhong JiCi Cha JianBaoKa MiaoCha LyuYouShih (147萬曾到日韓民眾即起插健保卡秒查旅遊史) [1.47 Million Individuals Who Had Traveled to Japan and/or South Korea Who Have Visited Japan and South Korea, Can Be Checked With Their Health Insurance Card], CENTRAL NEWS AGENCY (Feb. 21, 2020), https://www.cna.com.tw/news/firstnews/202002215012.aspx.


220 Since the outbreak of COVID-19 until April 2021, the total number of cases in Taiwan was 1,057, with 11 deaths and 1022 recovered (data on April 12, 2021). However, ever since May 2021, Taiwan was caught short by the outbreak of the UK variant, the COVID-19 cases increased in a sudden. According to the Taiwan Centers for Disease Control, the total number of cases in Taiwan is 7,806, with 99 deaths and 1,133 recovered (this is current as of May 29, 2021). See COVID-19 Cases Report, TAIWAN CENTERS FOR DISEASE CONTROL, https://sites.google.com/cdc.gov.tw/2019-ncov/taiwan (last visited May 29, 2021).

Taiwan, but the clinics were not alerted to their travel history when they checked their health insurance records. Furthermore, since May 2021, Taiwan was caught short by the outbreak of the B.1.1.7 variant, and the COVID-19 cases increased in a sudden. Professor Chunhuei Chi, the director of Oregon State University’s center for global health, described Taiwan as “a victim of its own success”. He further explained that although Taiwan had locally eliminated the virus in early 2020, it neither prioritized the procurement of vaccines nor stayed up to date with the new COVID-19 variant’s increased transmissibility and high asymptomatic rate.

To deal with the sudden rapid growth of the COVID-19 cases, the Central Epidemic Command Center (CECC) has adopted data sharing and surveillance approaches like collaborating with the telecommunication service providers to single out certain citizens as “high-risk group” in the health insurance card. Yet, this policy confused local hospitals and raised questions like “should we refuse the patients from the high-risk group?” or “where can those patients in the high-risk group to be transferred?” were emerged. In other words, the data sharing and data surveillance practices adopted by the Taiwanese government without clear legal authority may not be as effective as claimed. The positive aspects of mitigating and containing the COVID-19 pandemic by linking a patient’s travel history to their


223 Id.


225 Id.

226 Id.

227 See Xie Xing-En (謝幸恩) & Hong Ling-ling (洪玲玲), *NeiBu WenJian PuGuang! ZhiHui ZhongXin Jing MiLing JianCe WanHua 60 WanRen ZuJi TiaoChu GaoFengXian XuQun ZhuJi JianBaoKa (內部文件曝光!指揮中心竟密令監測萬華 60 萬人足跡 挑出“高風險族群”註記健保卡)* [Internal Document Exposed! CECC Secretly Commanded Monitor the Footprints of 600,000 People in WanHua Single Out the “High-Risk Groups” and Mark Up in the Health Insurance Card], YI MEDIA (毅傳媒) (May 26, 2021), https://yimedia.com.tw/covid19/117647/?fbclid=IwAR0Lu02D0kcZzA4Dg-g-6o7WRF5AVGhucScjMLwfjfabp5YUWa4BzhRueDs.

228 Id.
health insurance card, are greatly diminished if some patients’ need for medical services are rejected without justification and individuals’ privacy rights are traded in exchange for inconsistent travel history alerts. Here, we present several approaches to data sharing and surveillance that the Taiwanese government employed in its response to COVID-19: the “M-Police,” the “Intellectual Surveillance Electronic Fence System,” and the “Taiwan Social Distancing App.”

1. The “M-Police.” — In 2007, the National Police Agency (NPA) of the Ministry of Interior began to build a police cloud computing device called the “Police Mobile” (known as the “M-Police” infrastructure) to promote and increase law enforcement effectiveness. From 2012 to 2016, the basic platform of the Police Cloud Computing and the Police Mobile Computer System was established. Information in 31 databases from six government agencies concerning people, vehicles, criminal cases, objects, time, places, photos, and videos was integrated into the platform to enhance the efficiency of criminal investigations. The “M-Police” also use commercial smartphones to easily customize to police equipment that decrease the heavy weight. Essentially, the “M-Police” is the deployment of big data policing platforms that aggregates and analyzes massive amounts of personal information. However, although helpful, this expansive amount of combined data can lead to discrimination and privacy invasions, which occurred in Taiwan during the COVID-19 pandemic.

In late February 2020, a young Indonesian woman who worked in several northern Taiwanese hospitals was Taiwan's

---


230 Id.

231 Id. According to one of the contractors who helped the NPA establish the infrastructure, the Cloud Computing System provides 17 police applications, which include M-Police Integrated Query System, Real Time Audio and Video Transmission System, Instant Photo Comparison System, Instant License Plate Recognition System, Citizen Interview System, Police Instant Message System, Police Regulations Query, Police Common Operational Procedures Inquiry, etc. In addition to these powerful tracking applications, the Cloud Computing System also integrates the Cloud Police Mission Dispatch System, the Suspicious Vehicle Track Inquiry System, and the Police Service App. The system has significantly improved the efficiency of police in tracking individuals.

232 Id.
32nd confirmed COVID-19 case.\(^{233}\) The woman was an undocumented migrant.\(^{234}\) She was hired to work as a caregiver for an elderly man who was hospitalized and diagnosed as Taiwan's 27th COVID-19 case from February 11 to February 16.\(^{235}\) The NPA helped the Center for Disease Control (CDC) track down this undocumented caregiver through the M-Police, and the CDC subsequently placed the woman in a negative-pressure isolated ward for quarantine and testing.\(^{236}\) When explaining the details of this confirmed case to the press, government authorities publicized the woman’s past locations and movements.\(^{237}\) The authorities also revealed many closed-circuit images retrieved from the Police Cloud Computing System to show that she had visited numerous sites in greater Taipei by traveling on buses, the Taipei Rapid Transit Corporation Metro Service, the Taipei Mass Rapid Transit, and Taiwan Railways Administration trains.\(^{238}\) Every detail that the M-Police had accumulated and retrieved about this woman was then widely reported in the newspaper, on TV news stations, and throughout the internet.\(^{239}\) It is apparent that even without any emergency use or exception clauses that may have relaxed data privacy regulations, many private details about the life of this young Indonesian woman were unnecessarily collected and revealed without adequate considerations or her consent.

2. The “intellectual surveillance electronic fence

---

\(^{233}\) Taiwan Centers for Disease Control Press Release, Taiwan Confirms Foreign Caregiver of Case #27 as 32nd Case of COVID-19, CDC (Feb. 26, 2020), https://www.cdc.gov.tw/En/Bulletin/Detail/QMZlqDJORsFvH6k9GJHB2Q?typeid=158.


\(^{235}\) See Taiwan Centers for Disease Control Press Release, supra note 233.


\(^{237}\) Id.


\(^{239}\) See Chen Wei-ting & Matthew Mazzetta, Migrant Caregiver Confirmed as Taiwan’s 32nd COVID-19 Case, FOCUS TAIWAN (Feb. 26, 2020), https://focusatwai\indent
— As part of the governmental effort to contain the spread of COVID-19, the National Communication Commission (NCC), the most important regulator of telecommunication companies in Taiwan, demanded that five major telecommunication service providers in Taiwan deploy an “Intelligent Surveillance Electronic Fence System” (Surveillance System) to individuals’ cell phones to trace their movements in quarantine. The NCC supervises the Surveillance System and monitors whether individuals stay in their quarantine location by reviewing locations detected on their phones. The Surveillance System, deployed on individuals’ cell phones, is connected to the M-Police. Whenever any individual has left

---


her or his quarantine site, the Surveillan
tce System sends a short
message service (SMS) alert to the individuals, related
administrators, and the local police on duty.\footnote{Id. Moreover, the post on March 24, 2020, on the Facebook page of the Ministry of the Interior, R.O.C. addressed clearly by stating that: “ZhiYao NiBenRen LiKai DianZi WeiLi, WoMen JiHui MaShang MaShang FaJianXun GaiNi, DaDianHua GaiNi” (只要你本人離開電子圍籬，我們就會馬上發簡訊給你、打電話給你!) [Once you left the quarantine site, we will send a SMS to you and call you right away!], see https://www.facebook.com/moi.gov.tw/photos/a.160470208674715/3265323943495986/?type=3 (last visited May 29, 2021).} The police and the
civil affairs officers then arrive at the quarantine site to investigate
its condition and attempt to locate the individual who left.\footnote{Id.} If it
the quarantine order is properly obeyed, no penalty or other
control measures will be imposed on the individual.\footnote{Id.} However,
if the officers determines that quarantine is violated, a serious
penalty will follow.\footnote{Id.} This practice presents several complex
questions regarding the extent of the government’s reach into an
individuals’ private affairs. For example, is it appropriate for the
government to electronically “fence” a person in this fashion? Is
this practice, which essentially fences and freezes civil rights and
liberties, equivalent to an embrace of authoritarianism? This
normalization of an arguably draconian regulation in the name of
public health remains an unanswered question in the realm of
personal privacy protection. Will this “fencing” and tracking of
citizens be as destructive to democracy as many privacy violation
measures advocated for and adopted by governments in the years
following the September 11, 2001 terrorist attacks in the United
States?\footnote{See Taiwan Centers for Disease Control Press Release, JhueiZong Geli JianYiJhe WuBi ShouFa WeiJheJjia JhongCcaiFa (居家隔離, 檢疫者務必守法, 違者加

3. The “Taiwan social distancing app.” — Taiwan social
distancing app was developed in mid-March 2020, under
instruction from Taiwan’s Vice Cabinet Premier Chen Chi-Mai.
This app uses Bluetooth technology to measure the distance

between individuals.\textsuperscript{251} Chen Chi-Mai asserted that the app is completely voluntary to use, and the data collected by the app would be encrypted and not be used to investigate individuals’ locations.\textsuperscript{252} Still, critics from Taiwan’s civil society have raised questions as to whether collecting and processing the data will create privacy issues.\textsuperscript{253}

During May 2021, when Taiwan experienced a huge COVID-19 outbreak, the CECC announced that the Taiwan social distancing app had been launched for public use.\textsuperscript{254} The health authority has begun upload data to servers maintained by the CDC after obtaining consent from confirmed cases. The app will then automatically notify app users who have contacted with the confirmed case in the past 14 days and ask them to monitor their health status.\textsuperscript{255} The government and this app’s developer claimed that users’ privacy will be rigorously protected since users do not need to register their personal information; moreover, the app uses Bluetooth device signal to estimate the physical social interactions,\textsuperscript{256} and transforms data to anonymous hashed identification stored on each individual’s device for up to 28


\textsuperscript{252} Pan, supra note 251.

\textsuperscript{253} See, e.g., Taiwan RenQuan CuJinHui (台灣人權促進會) [Taiwan Association for Human Rights], GongWei WeiJi zhong RuHe BaoZhang GongMinQuan (公衛危機中, 如何保障公民權) [Protecting Civil Liberties During a Public Health Crisis], MEDIUM (Mar. 18, 2020), https://medium.com/@tahr1984/protecting-civil-liberties-during-a-public-health-crisis-1de3c6d8e724.


\textsuperscript{255} Id. See also Taiwan SheJiao JuLi App Chang Jian WenDaJi (「臺灣社交距離 App」常見問答集) [FAQ for "Taiwan Social Distancing App"], CDC (May 25, 2021), https://www.cdc.gov.tw/File/Get/Meq89j-Rb_TFbIM5dEfmAA.

days. However, the app’s effectiveness is so far limited. According to the CDC, although the app already had more than 800,000 downloads, only 29 new community infections of COVID-19 were reported via this app.

The M-Police system, the Electronic Fence, and the Taiwan social distancing app, are the primary surveillance measures that the Taiwan public authorities have employed to fight the COVID-19 pandemic. However, these measures raise questions about the extent to which society should accept trade-offs between a public interest in health and safety and individual privacy. In light of the legal implications of these pandemic-response measures, we argue that public health interests can be achieved without sacrificing digital privacy and accepting widespread surveillance. The M-Police system, the Electronic Fence, and the Taiwan social distancing app indeed provide some pandemic prevention and control. However, these measures may also result in the erosion of individuals’ rights to privacy and liberty. In Taiwan, three laws must be examined to properly analyze the legal implications of these pandemic response measures: the Communicable Disease Control Act (CDC Act), the Special Act for Prevention, Relief and Revitalization Measures for Severe Pneumonia with Novel Pathogens (COVID-19 Special Act), and the PDPA.

According to several prominent Taiwanese legal scholars who specialize in public health law, “these measures were not carefully scrutinized according to the rule of law and constitutional principles.” They correctly noted that:

The Personal Data Protection Act sets out rules for collecting, processing, and using personal

---

257 Id.
259 From the outbreak in 2019 to April 2021, the total number of cases in Taiwan is 1,057, with 11 deaths and 1,022 recovered. See COVID-19 Cases Report, TAIWAN CENTERS FOR DISEASE CONTROL, https://sites.google.com/cdc.gov.tw/2019-ncov/taiwan (last visited Apr. 12, 2021).
data, such as lawfulness, purpose limitation, data minimization, and data security, but it has long been plagued by inflexible legal transplant and legal formalism without taking into account local contexts and failed to provide a healthy regulatory environment.\(^{261}\)

These experts question whether, despite the CDC Act and the COVID-19 Special Act authorizing the government to impose “other necessary measures,” connecting multiple databases and collecting and analyzing surveillance data should actually be qualified as one of these “other necessary measures.”\(^{262}\) Consequently, they believe the measures cannot survive legal scrutiny.\(^{263}\) Similar views have been expressed by other scholars. For example, some have expressed concerns that the enforcement of regulatory measures regarding data sharing and contact tracing has gone beyond the legal limit authorized by the PDPA and the CDC Act.\(^{264}\) These scholars therefore recommend that the scope of “public interest” as used in the PDPA be further clarified, particularly in the context of fighting the battle against COVID-19.\(^{265}\) Scholars have also argued that neither the CDC Act nor the PDPA have defined how the surveillance data may be used, transferred, and shared.\(^{266}\)

While most of the technological measures and data sharing platforms implemented in response to the pandemic offer public health benefits, they also pose grave threats to personal autonomy and significant risks to information privacy. China's COVID-19 health code application system is an example of

\(^{261}\) Id.

\(^{262}\) Id.

\(^{263}\) Id.

See Lee Chung-Hsi (李崇僖), Zai WunYi ManYan jhong JianShih GeZih BaoHu FaJhih (在瘟疫蔓延中檢視個資保護法制) [Examines the Legal System of Personal Data Protection in the Spread of The Plague], 387 TAIWAN. L.J. 39, 40 (2020).

\(^{265}\) Id. at 41.

raising concerns over privacy. For technology-assisted efforts like tracing travel history and monitoring and enforcing self-isolation restrictions to be effective, they must be deployed by trusted legal advisers. Contact tracing must also be planned with extensive safeguards to protect data privacy at the outset. Without safeguards, “individuals may be unwilling to participate.”

Furthermore, collecting data in a “privacy-respecting way” requires “legal, organizational, and computational safeguards” to successfully manage the remaining risks the population faces.

As Professor Ryan Calo highlighted in his testimony to the Senate Committee on Commerce, Science, and Transportation in April 2020:

There are myriad potential applications of technology to the fight against the novel coronavirus—too many to detail here. Each carries with it a measure of promise and of peril . . . does this intervention do enough in the fight against the novel coronavirus to offset its impact on privacy, civil liberties, or other important values? I submit that not all proposed interventions will meet this simple test.

See e.g., Helen Davidson, China’s Coronavirus Health Code Apps Raise Concerns Over Privacy, THE GUARDIAN (Apr. 1, 2020), https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy. According to this post, The China Health Code application system, which follow people to move around after lockdown, have become an integral part of Chinese authorities’ management of citizens. Raise concerns over privacy by lacking transparency over how the app works and what data it is storing.


Professor Ryan Calo is the Lane Powell and D. Wayne Gittinger Professor at the University of Washington School of Law. His research fields are Privacy Law and Law and Technology. For the past few years, he has been a pioneer in Artificial Intelligence and Law. See Ryan Calo, UNIV. WASH. SCHOOL OF LAW, https://www.law.uw.edu/directory/faculty/calo-ryan (last visited Nov. 23, 2020).

The debate over the appropriate amount of governmental access to personal data should be permitted during the COVID-19 pandemic will continue. Public health, economic recovery, and personal privacy are incommensurable. However, there is no need for these goals to suffer at the expense of each other.272

As Professor Lawrence Gostin 273 suggested, “it is important to carefully balance public health with rights to privacy and liberty.”274 He further explained that “exercising public health powers unmoored from constitutional rights is unwarranted.”275

As the Constitutional Court of Taiwan has made clear, the right to privacy is protected by the Taiwan’s Constitution.276 Therefore, Taiwanese legislators and policymakers must consider and encapsulate these constitutional privacy rights in the rules they make and enforce, regardless of a pressing global emergency. They must ensure that partnerships with technology or telecommunications companies respect privacy when they conduct data analysis.277 They must also ensure that justice and democracy are not unduly sacrificed or burdened in exchange for health and security.278

In Taiwan, the current laws and regulations underpinning data sharing and surveillance measures in reaction to the COVID-19 crisis include the CDC Act, the COVID-19 Special Act, and PDPA.279 The PDPA specifically is supposed to play a key role in

---

273 Lawrence O. Gostin is a Professor at Georgetown University. Professor Gostin directs the O’Neill Institute for National and Global Health Law and is the Founding O’Neill Chair in Global Health Law. See Lawrence O. Gostin, GEORGETOWN LAW, https://www.law.georgetown.edu/faculty/lawrence-o-gostin/ (last visited Nov. 23, 2020).
275 Id.
276 See Interpretation No. 689, surpa note 178.
277 Milano, supra note 268.
the protection of data privacy in this challenging time. However, it is apparent the current PDPA is limited, and the need to surveil, test, and track citizens has not been balanced with legitimate privacy concerns as Taiwan public authorities attempt to contain the spread of the highly infectious disease.

III. RECOMMENDATIONS FOR PROTECTING INFORMATION PRIVACY IN TAIWAN’S BIG DATA FUTURE

A. Change the Mindset and Establish a Framework

The above scenarios describe controversial instances where data has been released to the public and exemplify that Taiwan is facing a crucial turning point in its open data policies. Each case displays the lack of a comprehensive privacy protection program, the current flawed privacy protection law, and the governmental and judicial failure to recognize the importance of individual privacy protection. Each of these factors contributes to a heightened risk of ongoing privacy violations in Taiwan.

To rectify the mistakes that have been made while implementing Taiwan’s open data programs, government agencies and private companies must reorient their mindset. Both public and private sectors must realize that when citizens disclose personal data, they often have no choice but to give out this data and retain no control over the flow of their information. This means that these individuals often have a reasonable expectation that their information will be processed and used. Consequently, it is therefore reasonable to insist that government agencies and companies should bear the responsibility of protecting the personal data that they have been entrusted with and show meticulous care toward managing this data. By building robust information privacy protection mechanisms, the government and private sector actors should not only safeguard data subjects’ privacy, but they should shield those responsible for open data programs from potential litigation risks arising from legal

---

280 See Ho, supra note 94, at 145; see also Chang, supra note 55, at 147.
281 See Briefing Paper on Data and Privacy, supra note 201.
uncertainties, as illustrated by the Tsai et al. case.\textsuperscript{283}

Instead of downplaying the importance of privacy protection and viewing privacy protection as a hurdle impeding open data initiatives, government agencies and private entities should consider privacy issues at the outset. These actors could formulate open data strategies at the start and incorporate privacy risk assessments into every step of their planning – from data collecting to data processing to data reuses. This would not only enhance privacy protection for individuals, but it could also prove beneficials for the government agencies and private entities, as it allows them to address and solve any future issues before they arise. Dedicated privacy offices or advisory committees could also be implemented and would prove greatly beneficial. They could provide professional opinions and develop guidelines when agencies or companies make open data policies. The offices or committees could also undertake risk assessments before releasing data and could monitor privacy protection measures throughout an open data initiative.\textsuperscript{284} For example, in situations where a government agency must weigh public interests against an individuals’ right to privacy or when an agency considers what level of data de-identification is required, a committee or office could offer more scrupulous balancing tests and more detailed advice.\textsuperscript{285}

\textbf{B. Revamp the Privacy Law and the Related Administration Rules}

A set of sophisticated data protection regulations is the bedrock of a robust information privacy protection framework and

\textsuperscript{283} See, e.g., Tsai et al. v. National Health Insurance Administration, 102 NianDu Su Zi No. 36 (102年度訴字第36號判決) [Taipei GaoDeng XingZheng FaYuan (臺北高等行政法院)] [Taipei Administrative High Court], 2014 (Taiwan); Tsai et al. v. National Health Insurance Administration, 106 NianDu Pan Zi No. 54 (106年度判字第54號判決) (ZuiGao XingZheng FaYuan (最高行政法院) [Supreme Administrative Court], 2017) (Taiwan).


\textsuperscript{285} When conducting the human rights impact assessment, the committee serves to contextualize the rights and values in terms of the specific and local situations that are under assessment, to consider conflicting interest, and to assess and mitigate risks. Id. at 12.
the key to a successful open data program. This paper has discussed four issues that must be addressed by the current data protection regulations in Taiwan: (1) the protection of sensitive data; (2) de-identification requirements; (3) the right to consent and opt-out; and (4) the ambiguity of “public interest.”

To guarantee data subjects’ right to information privacy, a PDPA amendment must clarify who bears the responsibility of de-identification between the data controllers and data processors, offer more sophisticated regulations of de-identification, and put forth consent requirements for different kinds of data sets. An amendment must also provide an “opt-out” device to provide adequate means to fulfill the important right to consent and opt-out. Finally, an amendment should introduce a more comprehensive framework and clear guidelines to be considered when evaluating whether data use is necessary to further the public interest. This could include a balancing test for when government agencies or private companies must weigh and evaluate this “public interest” against individuals’ right to privacy.

With the vast number of public and private interests involved in open data programs, it is unlikely that a single provision in the law could cover all circumstances and scenarios. It would be impossible to enumerate all situations that are feasibly related to public interests or all methods of de-identification. However, the law and any subsequent enforcement rules could still provide the necessary rationales and basic instructions for the protection of different kinds of personal data.

The global trend of data regulation has been to distinguish different kinds of data, and then impose various de-identification requirements accordingly. This trend can be seen in the General Data Protection Regulation (GDPR) that was passed in 2016 and

---

286 See European Data Portal, Analytical Report 3: Open Data and Privacy, at 3 (July 15, 2020), https://www.europeandataportal.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf. In this Report, it is asserted that Open Data is an important means of increasing the access of data to citizens, companies, and civil society, and can promote economic growth, scientific research, and political and corporate accountability. A successful and sustainable Open Data program should be based on three pillars: (1) morally, the data publisher should consider the privacy of data subjects; (2) legally, data protection law must be respected; and (3) pragmatically, public confidence has to be maintained.

officially implemented in European Union member countries in May 2018. The GDPR implicitly categorizes different kinds of data as identified and de-identified data and demands different levels of de-identification for each category. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) also creates rationales, related standards, and two different paths of de-identification for healthcare providers or those who deal with personal health information to follow. After complying with the regulations to reduce privacy risks, the data controllers or users can make the secondary use of the sensitive data. The Taiwanese government could follow suit and implement a similar scheme with justifiable rationales, reasonable standards, and a sophisticated de-identification mechanism for healthcare providers and data users to comply with.

It is never easy to determine whether public interests or individual privacy should prevail. Other countries and jurisdictions are faced with this same issue and have made efforts to create rationales and put more stringent privacy protection mechanisms into existing regulations as complementary measures. For instance, the GDPR, like the PDPA, allows data controllers and processors to use personal data for purposes that are beyond their original collection purpose without obtaining consents from the data subjects, if the purpose is for public interests such as “statistical purposes or scientific research.” However, the GDPR also asks member states to specifically define what the “public interest” is and imposes more detailed

---

288 The GDPR text itself does not explicitly label these categories of data, but they can still be implied from the clauses and be matched with proper level of de-identification. See Mike Hintze, Viewing the GDPR Through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency, 8 INT’L DATA PRIV. L. 86, 87 (2018).


292 Id.
requirements for data safeguards accordingly. By comparing with the GDPR’s stringent regulatory mechanism with the ETC’s de-identification process of merely removing license plate numbers, for example, it becomes abundantly clear that Taiwan must create a more sophisticated scheme for data de-identification. This is particularly necessary to create an additional layer of protection for data subjects in instances when public interests are found to trump the individual right to privacy.

Canada’s information protection regulations provide a relevant example. When balancing public interests against the protection of data subjects’ health information, some provinces demand that research ethics boards (REBs) assess whether public interests override should apply to disclosure for health research purpose. Some even include a list of non-exhaustive public interests that REBs should consider in their regulations. Both the GDPR and Canada’s regulations show that the balance between public interests and the right to individual privacy is an issue worthy of deliberation by legislators, and the tension can only be tackled by creating more comprehensive privacy protection mechanisms. Institutional arrangements to help balance individual and public interests, such as REBs, might be a plausible mechanism for the Taiwanese government to implement as they aim to create a regime that better protects data privacy.

Even though open data programs provide several benefits, these benefits remain hazardous if the programs are implemented without thorough plans for privacy protection. A comprehensive

---

293 General Data Protection Regulation, supra note 264, art. 89(1) (“Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pseudonymization provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.”).


296 Id.

297 Id.
privacy protection plan would require the recognition of the importance of privacy protection, a robust framework for privacy protection, and comprehensive legal mechanisms. It is undeniable that Taiwan’s government and the civil society are committed to open data, and their efforts have been recognized. However, to keep the momentum going in a positive, balanced way, strengthening data privacy protection is an urgent must.

CONCLUSION

In this article, we analyzed the open data and privacy protection regime in Taiwan through two steps: (1) examining the history of open data and the PDPA and (2) identifying the key controversies raised by the PDPA. Next, we discuss four primary issues presented by the PDPA: (1) the protection of sensitive data, (2) de-identification, (3) the right to consent and opt-out, and (4) the ambiguity of “public interest.” Case studies of the ETC, the Taiwan NHI research databases, and the recent data sharing and surveillance practices to prevent the spread of COVID-19 were presented to showcase both the urgent need to address the PDPA’s flaws and the Taiwan’s perspective on the privacy perils of open data and data sharing.

Open data is a way to facilitate innovation. To ameliorate privacy concerns arising from disease control, epidemic prevention, or numerous other scenarios, it is important to understand why revealing exceedingly detailed information is unwarranted. When the COVID-19 pandemic began in 2020 and put the global population at risk, public authorities in Taiwan collaborated with information technology professionals to utilize open data and keep citizens informed. However, the government must not employ a “public interest” rationale solely to disguise or justify inappropriate uses of personal data or illegitimate surveillance of citizens. Though it is difficult to balance privacy protections against the public interest, the Taiwanese government must remain focused on creating and

See, e.g., Taiwan Can Help, https://taiwancanhelp.us/ (last visited Apr. 16, 2020). (creating the online system of the face mask inventories at drugstores in real time is an example of community collaboration of the information technology professionals in Taiwan utilizing open data and keep citizens informed).
implementing regulatory efforts that focus on limiting the scope and detail of individual data to be collected, used, and disclosed.

In today’s world, combining databases both domestically in Taiwan and on an international scale can bring together extensive amounts of individuals’ data. Therefore, this article suggests that, instead of viewing privacy issues as a stumbling block, legislation should focus on building robust regulatory privacy protection mechanisms to foster innovation and enhance open data initiatives and their goals of data sharing. Even under the PDPA’s current regulatory regime, the Taiwanese population has witnessed public authorities and corporations misuse citizens’ data and risk their privacy while attempting to tackle a public health emergency.

There is no doubt that sacrificing individual privacy protections for health and safety purposes may result in greater, perhaps even more authoritarian, governmental control and greater control by technology and telecommunications companies with undue influence. To avoid this unfortunate and undesirable result, the Taiwanese legal landscape should be reformed to facilitate regulatory audits and ensure that misuse and abuse of personal data do not occur when global emergencies, like the COVID-19 pandemic, transpire.

Lastly, we offer recommendations for reform. We propose implementing guidelines for de-identification requirements, clarifying the definition of the public interest exemption in the PDPA, and adding an opt-out mechanism as crucial first steps for

---


301 For instance, rather than disclosing precise locations of an infected individual to the public, the regulatory efforts should focus on less granular data that could be disclosed, with the same effect on tracking and quarantine. Concerns the lack of transparency from the government could be raised, and such concerns could be addressed by devising a suitable privacy-preserving methodology that also ensures trustworthiness. See e.g., Sangchul Park et. al., Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies, 323 JAMA 2129, 2129–30 (2020), https://jawork.com/journals/jama/fullarticle/2765252?guestAccessKey=6f0c542e-5345-4855-9d59-e1d2ca578a6&utm_source=fbpage&utm_medium=social_jama&utm_term=3295763982&utm_campaign=article_alert&linkId=87179293.
reform. Further, in shaping their open data policies, Taiwan should undertake risk assessments before releasing any data and monitor privacy protection measures throughout the life of any open data initiative, including at the outset. Additionally, a privacy office or advisory committee may be beneficial to provide professional opinions and develop sensible guidelines. Only by creating a trustworthy privacy protection system will Taiwanese civil society begin to feel comfortable allowing the collection, processing, use, and reuse of their personal data without worrying about an invasion in their private lives. While Taiwan has certainly hopped on the open data train in recent years, the country still has several changes to implement before the track is smoothly followed.