Pace International Law Review

Volume 28
Issue 1 *Spring 2016*

Article 2

April 2016

Controversy Over Information Privacy Arising From the Taiwan National Health Insurance Database Examining the Taiwan Taipei High Administrative Court Judgement No. 102-SU-36 (Tsai v. NHIA)

Chen-Hung Chang
American University Washington College of Law

CONTROVERSY OVER INFORMATION PRIVACY ARISING FROM THE TAIWAN NATIONAL HEALTH INSURANCE DATABASE EXAMINING THE TAIWAN TAIPEI HIGH ADMINISTRATIVE COURT JUDGMENT NO. 102-SU-36 (*TSAI V. NHIA*)

Chen-Hung Chang*

ABSTRACT

This article examines the limitations of the application of traditional information privacy theory to disputes relating to modern technologies. If information privacy is understood as an individual's right to full control over his information, activities involving the collection, process and use of personal data cannot be conducted without the data subject's consent because his privacy rights would be affected as a result of such activities. Instead of the *privacy interest* approach, this article introduces a *privacy harm* approach to reconcile the defects of traditional privacy theory. The *privacy interest* approach helps identify situations in which an individual's information privacy conflicts with the free flow of information, and the *privacy harm* approach comes into play to precisely evaluate and determine the reasonable extent of protection of the respective interest. This article applies this privacy-harm-oriented approach to Taiwan Taipei High Administrative Court Judgment, *Tsai v. NHIA*, to examine that the modified

* S.J.D. candidate, American University Washington College of Law. Email: chihshein@gmail.com. The author would like to thank the production staff of Pace International Law Review for their assistance in preparing this paper for publication.

information privacy theory is helpful to resolve the information privacy dispute at issue.

This article elaborates the reasons why imposing a universal rule that the data controller must obtain the data subject's consent before using his health data is of no real help in protecting health privacy and is detrimental to medical research. This notion can be supported by the following concepts: 1. shifting the liability of privacy protection to the data subject will increase the risk of privacy invasion; 2. in the multi-faceted privacy interest concept, granting decision-making rights to an individual cannot guarantee privacy protection; 3. it will add unreasonable costs to medical research.

By applying the *privacy harm* approach, this article further analyzes the importance of considering the likelihood of privacy harm regarding health information. In this approach, because *identifiable* health information and *identified* health information are subject to different likelihoods of privacy harm, different degrees of privacy protection and privacy rules should apply to them in their respective contexts.

TABLE OF CONTENTS

I. Introduction.....32
II. Privacy Controversy over the Taiwan National Health Database — Examining the Taiwan Taipei High Administrative Court Judgment No. 102-Su-36.....40
A. Background.....40
B. Plaintiffs' Allegation.....43
C. The NHIA's Defenses.....44
D. Court Judgment.....45
1. Controversy over the Application of Old and New Privacy Laws.....46
2. The NHIA's Forwarding of the Health Insurance Data to the NHRI and CCHIA is Necessary for the NHIA to Exercise Its Statutory Duty.....47
3. The NHIA's Disclosure of Health Insurance Data Qualifies for the Exemptions in the Use of Personal Data for Specific Purposes Other than the Notified Purposes of Collection.....48
4. The Right to Consent Prior to Data Use and

the Right to Object after Data Use 50
III. The Legal Landscape of Privacy Laws with Respect to Personal Health Data 51
A. How Health Data is regulated in the Taiwan Personal Data Protection Act.....51
1. Definition of Personal Data in the PDPA 51
2. The Rights of Individuals in the PDPA 52
3. The PDPA Restrictions on Reusing Personal Data 53
B. Regulations of the U.S. HIPAA and HITEC for the Disclosure or Use of Personal Health Data for Research Purposes.....59
1. The HIPAA Privacy Rule Basics 61
2. HIPAA Research Provisions.....65
C. Applying the PDPA and HIPAA to *Tsai* 71
1. A Comparative Law Study of the PDPA and HIPAA Privacy Rule.....71
2. Shortages of HIPAA Privacy Rule and PDPA in Data Privacy Issues 74
IV. Suggestions of Modifications to the Information Privacy Theory 76
A. A Concept of Pluralistic Value of Privacy.....77
B. The Methodology of Constructing the Concept of Privacy 81
1. The Privacy Interest Approach 81
2. The Privacy Harm Approach.....88
C. Concept of Information Privacy Combining Privacy Harm and Privacy Interest.....92
V. Applying the Modified Information Privacy Concept to *Tsai*.....97
A. Unconditionally Requiring the Data Subject's Authorization will Become an Impediment to Medical Research Rather than a Pathway for Privacy Protection 97
1. Shifting the Burden of Privacy Protection to the Data Subject Would Cause an Adverse Impact on Privacy Protection.....98
2. Ensuring Individuals' Autonomy Right to Their Own Data Does Not Guarantee Privacy Protection 100
3. A Balance Check Between Public Interest of Medical Research and Threats to Privacy Protection 101
B. Applying a Privacy Harm Approach in

Categorizing Personal Data and Suitable Privacy Protection Standards....103
1. What Type of Personal Data are Protected in PDPA and HIPAA?....103
2. How PII Is Regulated in PDPA and HIPAA Privacy Rule....105
3. A Suggested Approach to Regulating Identifiable Health Information in the Use of Medical Research....109
C. Analysis of *Tsai*....113
VI. Conclusion....116

I. Introduction

Health information has always been regarded as highly sensitive personal data.[1] Any unwanted or unauthorized exposure of such data would cause significant harm to the subject of the data.[2] For instance, people do not want others to know that they carry certain physical or emotional diseases, such as sexually transmitted diseases, or that they have Acquired Immune Deficiency Syndrome ("AIDS"). If such personal health information is exposed, the individual will inevitably suffer emotional pain or unfavorable treatment in his social life or work. For example, an insurance company might establish a higher insurance premium based on the exposed health information even though this information is irrelevant to the scope of insurance coverage. Likewise, the likelihood of an individual obtaining a loan from a bank would be reduced if information that is socially regarded as unhealthy

[1] For purpose of this article, the terms "personal data" and "personal information" are used interchangeably, and do not refer to different definitions.

[2] *See* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 454 (1995).

is disclosed.[3]

Modern technology has significantly increased the risk of the unwanted exposure or dissemination of personal health information. Previously, when medical or health information was recorded on printed papers, a patient's health condition or medical treatment history was communicated privately between patients and doctors or medical facilities. A person could trust that health information was secure within this special relationship (confidentiality) between the physician and the patient. However, technological advances have changed the landscape in which medical records are recorded and stored. The flow of this sensitive information is no longer limited to patients and medical service providers.[4] With the widespread use of internet technology and mobile devices, medical records that are produced and maintained in digital formats can be easily transmitted without temporal or territorial constraints.[5] The more easily personal health information can be accessed and distributed, the larger the number of parties that can obtain this information to process, analyze and use it for their own purposes. Increasing numbers of resources have been dedicated to research to develop more advanced and evolved technology to improve the efficiency of the use of personal health information.[6] These phenomena have made health data more vulnerable to unwanted disclosure and have made patient/physician confidentiality less reliable with regard to health information privacy.

Modern technology has increased the difficulty of protecting privacy with respect of health data due to the rapid and broad information flow. However, it is also true that the collective use of individuals' health data may aid medical

---

[3] DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 399 (4th ed. 2011).

[4] *See* Gostin, *supra* note 2, at 512.

[5] *See generally* Patricia Sánchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: a Cyber-Patient's Bill of Rights*, 6 NW. J. TECH. & INTELL. PROP. 244 (2008).

[6] Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CAL. L. REV. 1765, 1782 (2010) ("The rise of cheap, mobile, and pervasive computing technologies that allow continuous, instant, and ubiquitous access to information is facilitating a new paradigm in which technology pushes healthcare delivery out of the clinical setting and into patients' everyday lives.").

research and improve medical science to benefit people.[7] The new big data technology facilitates medical research; however, sufficient data must be supplied to make the big data technology functional.[8] No medical research can be successful without a sizable database that accumulates sufficient data for a certain length of time.[9]

Tsai v. NHIA,[10] a recent and high profile lawsuit in Taiwan, illustrates the conflict between the benefits for medical research of using all citizens' medical data and the privacy threats to individuals when their medical records are exposed to others, and their most sensitive personal data are disclosed without their knowledge. This article will examine the relevant privacy issues in *Tsai* and will discuss whether the traditional privacy theory that was applied to try this case is still adequate to resolve privacy issues involving the use of modern technologies.

The debate in *Tsai* is whether health authorities may use personal health information that they have collected in the course of performing national healthcare services for other

---

[7] *See id.* at 1778.

[8] According to the report of "Beyond the HIPAA Privacy Rule," the advantages of information-based health research include that:

> It is often faster and less expensive than experimental studies; it can analyze very large sets of data and may detect unexpected phenomena or differences among subpopulations that might not be included in a controlled experimental study; it can often be undertaken when controlled trials are simply not possible for ethical, technical, or other reasons, and it can be used to study effectiveness of a specific test or intervention in clinical practice, rather than just the efficacy as determined by a controlled experimental study. It can also reexamine data accrued in other research studies, such as clinical trials, to answer new questions quickly and inexpensively.

COMM. ON HEALTH RESEARCH & THE PRIVACY OF HEALTH INFO.: THE HIPAA PRIVACY RULE, IOM, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 118 (Sharyl J. Nass et al. eds., 2009), http://www.ncbi.nlm.nih.gov/books/NBK9578/.

[9] *See generally* Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595 (2014); Nicolas Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385 (2012); Cate, *supra* note 6, at 1778-83.

[10] Tsai v. NHIA, FĂ YUÁN FĂLÜ WĂNG (法源法律網) [LAWBANK], No. 102-Su-36 (Taipei High Admin. Ct. May 14, 2014) [hereinafter Tsai, 102-Su-36].

purposes, such as allegedly promoting public welfare, without obtaining consent from the data subjects. What makes this case more complicated is that the plaintiffs whose health data were disclosed by the health agency were not unaware that the health agency had used their personal data. The data subjects strongly expressed their objections to the health agency's use of their personal data for purposes that were not communicated to them when they gave their consent. Before filing the lawsuit, the plaintiffs expressly requested that the health authority should refrain from using their health data.

Tsai involves a dilemma of two conflicting rights. The data subject plaintiffs alleged that they were exercising their privacy rights granted in the Taiwan Constitution and the privacy laws against intrusion of privacy. They added that this case did not involve just any data; their health data were at stake, and such highly sensitive information deserves greater privacy and protection. The defendant, the Taiwan National Health Insurance Administration, contested that it was reusing all citizens' health data that it previously collected with the goal of improving public healthcare services and devising healthcare policies that could benefit all citizens. Part II of this article will provide a background summary of the facts and court decisions on this dispute and will identify the relevant interests at stake.

In Part III, this article introduces the relevant privacy laws and regulations in Taiwan and the United States (U.S.) related to health information, and conducts a comparative law analysis that applies those respective States' laws and regulations to *Tsai*. In both jurisdictions, the relevant laws dictate that an individual's right to full control over his own data could be sacrificed when the competing interest trumps privacy rights, and there is no exception for sensitive health data. This policy decision might be acceptable, but it requires justifications as to why a fundamental human right that enjoys stricter protection in civil law countries can be compromised. The current privacy theory does not afford an adequate explanation in this respect, and does not support this policy decision. The current privacy theory was developed based on the notion of protecting fundamental human rights (e.g., privacy rights), and has always viewed fundamental human

rights as priority rights. To bridge the gap between the current privacy theory and privacy laws and regulations, it is time to reconsider whether the conventional privacy theory is still adequate to resolve new privacy disputes. For instance, in terms of health data, the laws in both jurisdictions exclude non-personally identifiable information (Non-PII) and limit privacy protection to personally identifiable information (PII) only. There is nothing wrong with excluding Non-PII from privacy protection, but this article notes that it could be problematic to apply a universal standard to all PII without taking into account different circumstances of data use. Conventional privacy theory does not support an approach that views PII in different contexts to address the issue regarding the occasions on which a data controller may use personal health data for medical research. A new approach is required to facilitate medical research and to ensure at the data subjects' rights are not infringed to the most reasonable extent possible.

Given the above problem, in Part IV, this article examines the limitations of the application of traditional privacy theory to disputes relating to modern technologies and proposes modifications to the traditional privacy theory. The first step is to correctly identify the effects to information privacy caused by new technologies and to correctly identify the rationale to offer protection. Based on this foundation, this article proposes a methodology to construe a modified concept of information privacy and applies this concept in *Tsai* to examine whether the proposed methodology is helpful to resolve the information privacy dispute at issue. This article recognizes that the concept of privacy is dynamic and multi-faceted. Instead of pursuing a definition that is universally applicable, a practical approach would involve categorizing privacy in different contexts.

U.S. legal practice supports this article's proposition that privacy cannot be categorized into one simple concept that is applicable to all cases. In adjudicating privacy disputes, the U.S. Supreme Court recognizes that privacy is a multifaceted concept that can be divided into three categories: decisional

privacy, spatial (or physical) privacy and information privacy.[11] Echoing the U.S. Supreme Court's position, the Taiwan Constitutional Court declared that the privacy right under Article 22 of the Taiwan Constitution refers to the right to protect one's "spatial (or physical) privacy right" and one's "information privacy right."[12]

The next question is how to appropriately categorize privacy in different contexts. The approach currently adopted by both the U.S. Supreme Court and the Taiwan Constitutional Court falls short in dealing with information privacy issues, and requires updates and modifications. Currently, the determining factors for categorizing privacy issues hinge on the nature of the relevant privacy interest or interests. There are flaws in the characterization of privacy based on related interests. This methodology is subject to a great risk of overestimating the need to protect privacy, and is likely to underestimate the need for protection of others' rights and public welfare. For example, if information privacy is understood as an individual's right to full control over his information, then activities involving the collection, process and use of personal data cannot be conducted without the data subject's consent because his privacy rights would be affected as a result of such activities.

Instead of the *privacy interest* approach, this article introduces a *privacy harm* approach to reconcile the defects of traditional privacy theory. The *privacy interest* approach is based on the presumed right that every person should retain full control over his personal information. The traditional information privacy right is understood in this concept as meaning that each person has a presumed interest in having full control over his personal information, and this interest should be protected in all circumstances. However, even if one cannot fully control one's personal data, it should not be concluded that the subject of that data's release has suffered privacy harm. This article proposes another approach to construing the concept of privacy that emphasizes the context of privacy harm. Privacy harm has been an important factor in

---

[11] *See infra* Section IV.A.

[12] *See infra* Section IV.A.

U.S. torts law for adjudicating privacy in invasion claims.[13]

This article introduces the *privacy harm* approach to supplement and modify privacy theory but does not attempt to abolish the *privacy interest* approach. Privacy interest and privacy harm represent two crucial faces of privacy protection. Privacy interest represents the positive face of privacy regarding the benefits of privacy protection. To devise a privacy policy, it is essential that the interests of privacy protection should be demonstrated at the outset to achieve support for such a policy. In contrast, privacy harm is an important factor in balancing possible conflicts between an individual's subjective expectation of privacy protection and the objective standard of whether privacy harm actually exists from society's perspective. Only when both elements are satisfied can one invoke the individual's right to privacy protection.

A two-layer analysis that adopts both the *privacy interest* and *privacy harm* tests is of particular importance to construct the theory of information privacy. The core of information privacy protection lies in one's right to control one's personal data. Nonetheless, recognizing the interests of information privacy does not mean that all types of personal data deserve full and equal protection. Different types of personal data and different levels of secrecy associated with a subject's data naturally affect the likelihood for data use to cause privacy harm and the scale of damage incurred. In other words, the *privacy interest* approach helps to identify situations in which an individual's information privacy conflicts with the free flow of information, and the *privacy harm* approach comes into play to precisely evaluate and determine the reasonable extent of protection of the respective interest. This article applies this

[13] *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (proposing four types of privacy harm in the U.S. tort law: 1. Intrusion: "Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs"; 2. "Public disclosure of private facts: Public disclosure of embarrassing private facts about the plaintiff"; 3. False light: "Publicity which places the plaintiff in a false light in the public eye"; 4. Appropriation: "Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.") The above four types of privacy harm were later recognized in the Restatement (Second) of Torts, edited by Prosser, which are now generally accepted tort law concepts. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

privacy-harm-oriented approach to real cases to examine whether this approach is helpful in resolving information privacy disputes.

In Part V, this article elaborates the reasons why imposing a universal rule that the data controller must obtain the data subject's consent before using his health data will impede medical research rather than providing a pathway to protecting health privacy. This approach is of no real help in protecting health privacy and is detrimental to medical research. This notion can be supported by the following concepts: 1. shifting the liability of privacy protection to the data subject will increase the risk of privacy invasion; 2. in the multi-faceted privacy interest concept, granting decision-making rights to an individual cannot guarantee privacy protection; 3. it will add unreasonable costs to medical research.[14]

By applying the *privacy harm* approach, this article further analyzes the importance of considering the *likelihood* of privacy harm regarding health information. In this approach, because *identifiable* health information and *identified* health information are subject to different likelihoods of privacy harm, different degrees of privacy protection and privacy rules should apply to them in their respective contexts.[15] Since identifiable information cannot be directly linked to a certain person, the risk of privacy harm associated with identifiable information is naturally less than the risk with identified information. To protect the interest of the free flow of personal information, there is no reasonable basis to apply the rigid privacy rules that were designed for identified information to identifiable information. A general rule for the design of specific rules for privacy protection should be that the greater the likelihood that the information can be linked to a certain person and the greater the risk of an individual's personal identity being exposed, the greater the amount of protection should be granted to ensure an individual's right to control his personal information.

Lastly, this article provides an evaluation of the core issue of *Tsai:* whether it is a prerequisite for the data controller to

---

[14] *See infra* Section V.A.

[15] *See infra* Section V.B.

obtain the data subject's consent in disclosing or using personal health information when conducting medical research. This article proposes that the personal information at issue should be regarded as "key-coded information" that should be categorized as identifiable information, and the disclosure or use of such data is unlikely to result in the same degree of privacy harm as what would be caused by identified information.[16] As such, it is not necessary to apply the informed consent principle. *Tsai* provides an opportunity to examine whether the court has correctly applied and interpreted Item 5 of Article 16 of the Taiwan Personal Data Protection Act ("PDPA"), wherein the data controller may freely reuse personal data for research purposes if such data "cannot identify a certain person."[17] A reasonable interpretation of this clause, as proposed in this article, should be interpreted as the inability to "directly identify a certain person." Based on this interpretation, as long as the health agency has processed the personal data in such a way that the data cannot directly identify the plaintiff, the health agency may use or disclose the plaintiff's health data for research purposes without obtaining prior consent from the plaintiff.

II. Privacy Controversy over the Taiwan National Health Database — Examining the Taiwan Taipei High Administrative Court Judgment No. 102-Su-36

A. Background

Taiwan launched a national health insurance ("NHI") program in 1995 to provide health insurance coverage and medical care benefits to Taiwanese nationals and foreigners working in Taiwan.[18] As of 2015, following two decades of its

---

[16] *See infra* Section V.C.

[17] Gèrén zīliào bǎohù fǎ（個人資料保護法）[Personal Information Protection Act] FǍ YUÁN FǍLÜ WǍNG (法源法律網) [LAWBANK], Dec. 30, 2015 (Taiwan), http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL010627 [hereinafter PDPA] (The PDPA is originally in Taiwanese. The PDPA is also called Personal Information Protection Act in some Taiwan law databases when said law is translated in English. There is no official English version or translation of PDPA in Taiwan.).

[18] National Health Insurance Administration Ministry of Health and

implementation, 99.9% of Taiwan's population is enrolled in the program.[19] The NHI program is administered by the Taiwan National Health Insurance Administration (NHIA), the Ministry of Health and Welfare (MHW) of the Executive Yuan (formerly the Department of Health, "DOH"). The NHIA, as the government agency in charge of the national insurance program, has collected, processed and retained all insurance and medical information on the insured persons and service providers (hereinafter, "Health Insurance Data") in the course of handling the health insurance affairs.[20]

The Health Insurance Data were not only utilized by the NHIA in providing healthcare services but were also applied by third parties entrusted by the NHIA to conduct academic research. Since 1998, the NHIA has annually sent the Health Insurance Data to the National Health Research Institutes ("NHRI"), a state-sponsored private research institution.[21] As part of the NHRI's research work, a centralized health data center, the National Health Insurance Research Database ("NHIRD"),[22] was created. The information stored in the

---

Welfare, National Health Insurance Program overview, http://www.nhi.gov.tw/English/webdata/webdata.aspx?menu=11&menu_id=590&webdata_id=3189&WD_ID=590 (last visited May 5, 2016).

[19] National Health Insurance Administration, Ministry of Health and Welfare, Executive Yuan, *2015-2016 National Health Insurance Annual Report*, San-Kuei Huang, at 4 (2015), http://www.nhi.gov.tw/epaper/ItemDetail.aspx?DataID=4030&IsWebData=0&ItemTypeID=3&PapersID=359&PicID=.

pdf (last visited May 5, 2016) (As of 2015, it has been two decades since the NHI program was launched in 1995; the enrollment rate has reached 99.9969%, and 93% of hospitals and services providers have join the NHI program.).

[20] NATIONAL HEALTH INSURANCE ADMINISTRATION MINISTRY OF HEALTH AND WELFARE, NHIA overview, http://www.nhi.gov.tw/english/index.aspx?menu=8& menu_id=30 (last visited Mar. 10, 2016).

[21] NATIONAL HEALTH RESEARCH INSTITUTES, Overview, http://english.nhri.org.tw/NHRI_WEB/nhriw001Action.do (last visited May 5, 2016) ("The National Health Research Institutes (NHRI) is a non-profit foundation established by the government with its organization charter created by an Act of Congress (Legislative Yuan) and signed in 1995 by President Teng-hui Lee. Being an autonomous research organization under the supervision of the Department of Health, Executive Yuan, the NHRI is dedicated to the enhancement of medical research and the improvement of health care in this country.").

[22] Cáituán fǎrén guójiā wèishēng yán jiù yuàn shèzhì tiáolì (財團法人國家衛生研究院設置條例) [National Health Research Institutes Establishment

NHIRD has been opened since 2000 to allow access on a per-application basis by researchers and scientists who need to conduct medical-related research.[23]

In a continued effort to improve healthcare services and to aid the reform of public health policies, the Executive Yuan initiated a National Health Informatics Project ("NHIP")[24] and established within the MHW the Collaboration Center of Health Information Application ("CCHIA") on May 3, 2009.[25] Since its operation on February 1, 2011, the CCHIA has served as a national database wherein other government agencies may access the Health Insurance Data through the CCHIA. The CCHIA data may be combined with other personal data, such as household registration and tax returns, to enable the government's collaborative use of personal data, as the MHW expected when creating the CCHIA.[26]

It was the goal of the CCHIA that the open and free flow of Health Insurance Data accessible to the government agencies and academic researchers would provide analysis and research results based on these personal data, and that would be helpful for the government to provide improved health care services to citizens. In sending the Health Insurance Data to the CCHIA database, the NHIA has vowed to protect individuals' data privacy.[27] Among the data privacy and security measures that the NHIA has undertaken, the NHIA has declared that all Health Insurance Data are scrambled and de-identified before being released to the CCHIA to ensure that individual

---

Act], art. 1, FĂ YUÁN FĂLÜ WĂNG (法源法律網) [LAWBANK], Feb. 3, 1999 (Taiwan), http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL013285.

[23] Tsai v. NHIA, 2014 FĂ YUÁN FĂLÜ WĂNG (法源法律網) [LAWBANK], No. 102-Su-36, at reasoning ¶ v. (Taipei High Admin. Ct. May 14, 2014) (Taiwan).

[24] Press Release, National Development Council, CEPD Press Release Historical data area (2001- 2014/1/21); Health Informatics Project overview, http://www.ndc.gov.tw/News_Content.aspx?n=C90548F2DB23E8B9&sms=AB593F5AE64A02BE&s=CBC61A22871DB59F (Apr. 23, 2007).

[25] MINISTRY OF HEALTH AND WELFARE, Collaboration Center of Health Information Application CCHIA Application overview, http://www.mohw.gov.tw/cht/DOS/DM1.aspx?f_list_no=812 (last visited Mar. 10, 2016).

[26] *Id.*

[27] *Id.*

identification is not traceable.[28]

Eight individuals filed separate petitions to the NHIA in May and June of 2012 claiming that the NHIA should not transfer their personal data to any third parties for purposes not related to health insurance affairs.[29] The petitioners were denied by the NHIA and initiated a joint administrative lawsuit with the Taiwan High Administrative Court against the NHIA, requesting that a restraining order be issued to prohibit the NHIA from disclosing their personal health data without their consent.[30]

B. Plaintiffs' Allegation

The subjects of the data alleged that the NHIA's unauthorized transfer or disclosure of their personal data to third parties exceeded the scope of consent they originally gave when agreeing that the NHIA could collect their personal data. The plaintiffs alleged that the NHIA failed to obtain their consent when reusing the data for other purposes not indicated or agreed upon by the data subjects. According to the then-effective privacy protection law in Taiwan (i.e., the Computer-Processed Personal Data Protection Act, "CPDPA"), if the data controller wishes to use personal data in a manner inconsistent with the purposes stated when the data were collected, this manner of secondary use is not permissible unless it is necessary for the government agency to perform its duties or the situation qualifies for any statutory exemptions.[31] The provision of personal data by NHIA to others, as the plaintiffs alleged, does not fall under the statutory functions of the NHIA, which are limited to policy making, administration and supervision of public health affairs.[32] In other words, the data were not properly used within the necessary scope of the specific purposes of data collection.

The plaintiffs added that even if the NHIA's duty is

---

[28] *Tsai*, No. 102-Su-36, at reasoning ¶ v.

[29] *Id*. at reasoning ¶¶ i, ii.

[30] *Id*.

[31] Computer-Processed Personal Data Protection Law Act [CPDPA], art. 8 (1995) (Taiwan) http://twse-regulation.twse.com.tw/EN/law/DAT06.aspx?FLCODE=FL010627&FLDATE=19950811&LSER=001.

[32] *Tsai,* No. 102-Su-36, at reasoning ¶ iii. (May 14, 2014).

broadly defined to justify the provision of personal health data to others for research purposes, the personal data submitted by the NHIA to NHIRD and CCHIA were not properly encrypted, leading to a possible breach of privacy by disclosing the subjects' personal identities.[33] The data the NHIA submitted were allegedly loosely protected and may have been traceable to individuals' personal identity, and the disclosure of their personal information created significant concerns about privacy invasion.[34] It was further argued by the plaintiffs that even if the NHIA had the authority to transfer the Health Insurance Data to the NHIRD and CCHIA without the individuals' consent, the subjects of the data should be entitled to demand that the NHIA stop using their personal data, which is part of their privacy rights as granted in the Taiwan Personal Data Protection Act.[35]

C. The NHIA's Defenses

The NHIA argued that its use of the plaintiffs' personal data was within its statutory duty and was in compliance with the specific purposes. The NHIA argued that it has met one of the exemption to reuse personal data for purposes outside the scope of the purposes of data collection as stipulated in the CPDPA, which permits data reuse when "it is necessary for the purpose of academic research and would not cause significant harm to data subjects."[36]

In response to the plaintiffs' claim that individuals own the right to full control over their personal information both "before" and "after" the data misuse, and therefore are entitled to stop the NHIA from reusing the data, the NHIA argued that the privacy laws do not support the plaintiffs' positions. The NHIA explained that since the law has permitted the NHIA to reuse personal data for specified purposes outside the scope of the purpose of data collection, this means that the law has restricted the data subjects' right to control their personal data

[33] *Id.*
[34] *Id.*
[35] *Id.* at reasoning ¶ iii.
[36] CPDPA, *supra* note 31, at art. 8, ¶ 7.

both before and after the NHIA's reuse of their personal data.[37] The plaintiffs' allegation that they have the right to raise objections to stop the NHIA from using their personal information runs afoul to the purpose of allowing the NHIA to use personal data in the public interest. The NHIA alleged that if the law permits the NHIA's use of personal data without obtaining consent from the data subjects, then it is equal to permission for the NHIA to use such data without intervention from the data subjects, meaning that that the data controller's right to use personal data prevails over the interest of the individuals in refusing such use of data.[38]

Additionally, the NHRI, which assisted the NHIA in the lawsuit, claimed that all the data provided by the NHIA was encrypted, so that the NHRI could not identify specific individuals; therefore, the data transfer by the NHIA to the NHRI is not subject to the PDPA.[39]

D. Court Judgment

The Taipei High Administrative Court ("High Court") dismissed the plaintiffs' lawsuit on May 14, 2014.[40] The plaintiffs filed an appeal, and the Supreme Administrative Court ("Supreme Court") remanded the case to the High Court for re-trial on November 13, 2014.[41] The Supreme Administrative Court vacated the High Court's judgment on the grounds that the pertinent case should be governed by the "PDPA"[42] rather than its precedent, the CPDPA (which was renamed and amended the Taiwan PDPA on May 26, 2000).[43] The Supreme Court ruled that the High Court should re-examine the issues by applying the correct law.[44] Because the Supreme Court vacated the High Court's judgment on the

[37] *Tsai,* No. 102-Su-36, at reasoning ¶ iv. (May 14, 2014).

[38] *Tsai,* No. 102-Su-36, *at* reasoning ¶ iv.

[39] *Id.* at reasoning ¶ v.

[40] *Id*. at holding.

[41] Tsai v. NHIA, 2014 FĂ YUÁN FĂLÙ WĂNG (法源法律網) [LAWBANK], No. 103-Pan-600 at holding (Sup. Admin. Ct. Nov. 13, 2014) [hereinafter *Tsai*, No. 103-Pan-600].

[42] PDPA, *supra* note 17.

[43] *Tsai*, No. 103-Pan-600, at reasoning ¶ viii.

[44] *Id.*

grounds of incorrect application of the law without addressing the merits of the dispute over privacy invasion, this article will focus on the reasoning of the High Court's judgment in examining the relevant privacy issues.

The High Court's judgment can be summarized as follows.

1. Controversy over the Application of Old and New Privacy Laws

This dispute occurred at a time when the Taiwan privacy law was undergoing a major amendment. The primary issue of the dispute lies in the determination of which data protection law should apply in relation to the NHIA's transfer of Health Insurance Data to the NHRI and CCHIA. Taiwan adopted its first personal data protection law, the CPDPA, in 1995 ("Old Privacy Law"), the same year the European Union ("EU") adopted the Data Protection Directive.[45] After more than ten years, the Old Privacy Law underwent an overhaul to provide comprehensive data protection to respond to new privacy threats in the wake of a rapidly evolving technology changes. It was amended and renamed the PDPA on May 26, 2010 ("New Privacy Law"). The New Privacy Law became effective on October 1, 2012.

Under the New Privacy Law, sensitive personal data (i.e., personal data relating to medical treatments, genetic information, sex life, health checks and criminal records) are subject to stricter requirements in terms of how such data can be processed and transferred.[46] The Health Insurance Data that the plaintiffs are addressing falls under the scope of the defined sensitive personal data under the New Privacy Law. However, the provisions relating to sensitive personal data are not yet effective due to controversy over the difficulty of implementing such provisions. The High Court's interpretation of the application of the old and new privacy laws is that the NHIA is not subject to the New Privacy Law in

[45] Parliament and Council Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [hereinafter EU Data Protection Directive].

[46] PDPA, *supra* note 17, at art. 6.

terms of its handling of the Health Insurance Data, because the privacy provisions relating to sensitive data was not yet effective as of the date of the trial and the Health Insurance Data was not specifically regulated under the New Privacy Law. Although the New Privacy Law has set certain requirements for the NHIA's compliance in the process of collecting and using personal data,[47] such requirements are only applicable when non-sensitive personal data is involved. The High Court therefore concluded, despite the fact that the pertinent dispute occurred after the implementation of the New Privacy Law, that whether the Health Insurance Data can be legally used by the NHIA shall be subject to the Old Privacy Law, which does not distinguish general personal data from sensitive personal data. As a result, the High Court ruled that the NHIA's collection and use of the Health Insurance Data should be subject to Articles 7 and 8 of the Old Privacy Law, whereas the legislative reasons of Articles 15 and 16 of the New Privacy Law may be taken into consideration as a reference.[48]

The Supreme Court disagreed with the High Administration Court's interpretation of the law and ruled that although the provisions relating to sensitive personal data were pending implementation, issues involving sensitive personal data should be regulated as non-sensitive data and should still be subject to the New Privacy Law. In other words, although there is no special law or regulation applicable to sensitive personal data, the New Privacy Law applies to sensitive personal data and non-sensitive data in the same manner.[49]

2. The NHIA's forwarding of the Health Insurance Data to the NHRI and CCHIA is Necessary for the NHIA to Exercise Its Statutory Duty

When reviewing the issues regarding whether the NHIA may resort to its statutory duty to justify its provision of the Health Insurance Data to third parties for research purposes,

---

[47] *Id*. at art. 15, 16.

[48] *Tsai,* No. 102-Su-36, at reasoning ¶ vii.

[49] *Tsai*, No. 103-Pan-600, at reasoning ¶ viii.

the High Court gave a positive answer. In the court's findings, the Organization Act of the National Health Insurance Administration, Ministry of Health and Welfare (Organization Act of NHIA) stipulated in Article 1,[50] and in Paragraphs 5 and 8 of Article 2,[51] that the NHIA is in charge of the planning and implementation of policies relating to the national health insurance program and the enhancement of the quality of the nation's healthcare services and all related matters. The High Court ruled that because the NHIA is responsible for all matters relating to the national health insurance program, which should reasonably include regular review and evaluation of the implementation results through academic research to facilitate improvement of the healthcare services offered in the national health insurance program, it should be within the scope of the NHIA's duty to provide the Health Insurance Data to the NHRI and CCHIA for research purposes.[52]

3. The NHIA's Disclosure of Health Insurance Data Qualifies for the Exemptions in the Use of Personal Data for Specific Purposes Other than the Notified Purposes of Collection

The High Court ruled that the pertinent dispute should be determined pursuant to the Old Privacy Law because the New Privacy Law is silent with regard to the collection and processing of sensitive personal data. However, it also considered the relevant provisions in the New Privacy Law in rendering the judgment because the latter has offered stronger privacy protection to individuals. The Court explained that

---

[50] Wèishēng fúlì bù zhōngyāng jiànkāng bǎoxiǎn shǔ zǔzhī fǎ (衛生福利部中央健康保險署組織法) [Organization Act of the National Health Insurance Administration, Ministry of Health and Welfare] art. 1, FǍ YUÁN FǍLÜ WǍNG (法源法律網) [LAWBANK], Dec. 28, 1994 (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL013281 (Article 1 of Organization Act of NHIA "For the purpose of administering the National Health Insurance affairs, the Ministry of Health and Welfare has established the National Health Insurance Administration.").

[51] *Id*. at art. 2, ¶ 5, 8 ("NHIA shall be in charge of the following matters: . . . 5. The formulation, planning and implementation of the review of medical services provided by the National Health Insurance and enhancement of medical quality. . . 8. Any other matter in relation to the National Health Insurance.").

[52] *Tsai* v., No. 102-Su-36, at reasoning ¶ vii.

Article 8 of the Old Privacy Law provides that government agencies may only use personal data for purposes within their exercise of duties and should comply with the purposes of data collection except for the numerated exemptions.[53] One of the exemptions is that data controllers may use collected data for other purposes if it is necessary for the purpose of academic research and that the use of personal data will not cause significant harm to the data subject.[54] A similar but more stringent requirement for data use is set forth in the New Privacy Law. Item 5 of Article 16 of the New Privacy Law provides that government agencies shall not use personal data collected for other purposes unless "it is necessary for government agency or research institution to use data for public interest on statistics or the purpose of academic research, and such use of data will not lead to the identification of a certain person after the treatment of the provider or by the disclosure of the collector."[55] When comparing the relevant data processing requirements in the Old Privacy Law and New Privacy Law, the Court first concluded that the latter has offered stronger protection and should apply to this dispute to fulfill the data protection requirement as declared by the Constitutional Court in its Decision No. 603, wherein the right to information privacy is officially recognized.[56]

In reviewing whether the NHIA's disclosure of Health Insurance Data to the NHRI and CCHIA to establish the national health data center satisfied the data use requirements in both the Old and New Privacy Laws, the Court determined that this data transfer was permissible because it was conducted for academic research in the public interest.[57] Moreover, the data involved was properly de-identified and should not harm the interests of the data subjects.[58] Although it is true that the Health Insurance Data were not used by the NHIA for purposes directly related to the provision of national health care services, the Court took into account the academic

---

[53] CPDPA, *supra* note 31, at art. 8.
[54] *Id*. at art. 8(7).
[55] PDPA, *supra* note 17, at 16(5).
[56] *Tsai*, No. 102-Su-36, at ¶ vii v.
[57] *Id*.
[58] *Id*.

research purpose behind the data use with the aim of improving medical services. The Court also noted that the data transferred to the NHRI and CCHIA were de-identified to avoid identification of specific individuals to protect the privacy of the data subjects. Therefore, the Court concluded that the NHIA should have satisfied the requirement of Item 7 of Article 8 of the Old Privacy Law that it is necessary for the purpose of academic research and that the use of personal data will not cause significant harm to the data subject and does not run afoul of Item 5 of Article 6 of the New Privacy Law.[59]

4. The Right to Consent Prior to Data Use and the Right to Object after Data Use

With regard to the plaintiffs' claim that the right to information privacy encompasses the right to consent prior to use and the right to object after use, the High Court ruled that the two alleged rights bear the same nature and should be interpreted using the same rationale. The High Court found that since both the Old and New Privacy Laws permitted data use by controllers for specified purposes other than those for which the data subjects expressed consent when allowing controllers to collect their data, it is tantamount to a statutory restriction upon the rights of the data subjects in preventing their personal data from unauthorized use. The same rule also applies when the data subject wishes to exercise his right to ask the data controller to delete or remove any unwanted disclosure of personal data. If the NHIA has a legal ground in sending Health Insurance Data to the NHRI and CCHIA for research purposes, there is no reason to allow the data subjects to exercise their right to demand that the NHIA stop using their personal data. Otherwise, the statutory exemptions to allow government agencies to use personal data to serve the public interest would be in vain and would lead to the incorrect interpretation that the right to information privacy is an absolute right, which is not the intended goal of privacy laws.[60] Given this context, if the NHIA is permitted to use the data for purposes not identified at the time of collection when the public

[59] *Tsai*, No. 102-Su-36, at ¶ vii.
[60] *Id.*

interest is involved, the plaintiffs shall have no legal standing to stop the NHIA from using the data.[61]

III. The Legal Landscape of Privacy Laws with Respect to Personal Health Data

A. How Health Data is regulated in the Taiwan Personal Data Protection Act

There are two types of laws in Taiwan that regulate the collection, processing and use of health information. The first type of law specially addresses human body research and personal biological information, including the Human Subjects Research Act,[62] the Human Biobank Management Act[63] and the Medical Care Act.[64] The other type of privacy law provides general rules for health data protection, mainly the PDPA.[65] *Tsai* does not involve biological information and does not relate to human body research, so the following discussion will only cover the PDPA.

1. Definition of Personal Data in the PDPA

The PDPA should encompass activities involving the processing of personal data as broadly as possible. Personal data in the PDPA is defined broadly to encompass any type of information that can be used to directly or indirectly identify or make possible the identification of a natural person. Therefore, Item 1, Article 2 of the PDPA defines personal information as

> [T]he name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic

---

[61] *Id*.

[62] Réntǐ yán jiù fǎ（人體研究法）[Human Subjects Research Act], FǍ YUÁN FǍLÙ WǍNG（法源法律網）[LAWBANK], Dec. 28, 2011 (Taiwan), http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL063770.

[63] Réntǐ shēngwù zīliào kù guǎnlǐ tiáolì（人體生物資料庫管理條例）Human Biobank Management Act, 2012, FǍ YUÁN FǍLÙ WǍNG (法源法律網) [LAWBANK], http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL052186.

[64] Medical Care Act, 2014, FǍ YUÁN FǍLÙ WǍNG (法源法律網) [LAWBANK], http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL013534.

[65] PDPA, *supra* note 17.

> information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and/or other information which may directly or indirectly be used to identify a living natural person.[66]

The PDPA regulations entitled the "Enforcement Rules of the Personal Information Protection Act" stipulated in Article 3 determine what it means to identify a person indirectly: "'Other information which may be used to identify a natural person indirectly' . . . shall mean that the government agency or the non-government agency possessing the information can not directly identify the specific person without comparing to, combining with or connecting to other information."[67]

In summary, the PDPA only protects personal information that may be used to identify a natural person directly or indirectly and does not cover other information that cannot identify a natural person.

2. The Rights of Individuals in the PDPA

a. Informed Consent

The PDPA requires written consent from data subjects whose personal data are collected, processed or used, with a few exceptions.[68] Before providing written consent, the data subject must be provided with adequate notice before the entity first collects personal data.[69] The PDPA further stipulates informed consent as follows.

Article 8 of the PDPA provides that, unless the law has otherwise exempted, the data collector shall inform the data subject of the following when collecting personal information:

> 1. The name of the government agency or the non-government agency; 2. Purpose of collection; 3. Classification of the personal information; 4. Time period, area, target and way of the use of personal information; 5. Rights of the Party and ways to exercise

---

[66] *Id*. at art. 2.

[67] Gèrén zīliào bǎohù fǎ shīxíng xìzé (個人資料保護法施行細則) [Enforcement Rules of the Personal Information Protection Act], art. 3, FǍ YUÁN FǍLÙ WǍNG (法源法律網) [LAWBANK], Sep. 26, 2012 (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010628.

[68] PDPA, *supra* note 17, at art. 15-16, 19-20.

[69] *Id.* at art. 8.

> them as prescribed in Article 3; 6. The influence on his rights and interests while the Party chooses not to provide his personal information;[70]

Article 9 of the PDPA provides that data collectors who do not obtain personal information directly from the data subject shall inform the data subjects of the source of their personal data and the information contained in Item 1 to Item 5 of Paragraph of the preceding Article, before it processes or uses such data.[71]

b. Right to Access Personally Identifiable Information (PII)

Article 10 of the PDPA provides that upon the request of the Party, the government agency or non-government agency should reply to the inquiry, offer a review or provide duplication of the personal information collected, with the exception of the following: (1) when national security, diplomatic and military secrets, macro-economic interests or other major national interests may be harmed; (2) when the performance of official duties may be interfered with; and (3) when the major interests of the collecting agency or a third person may be affected.[72]

c. Right to Amend

The data subject has the right to request that the data controller keep personal data accurate and delete or stop using the personal data when the originally intended purpose no longer exists, unless the laws state otherwise or the data subject has given written consent.[73]

3. The PDPA Restrictions on Reusing Personal Data

As stipulated in Paragraph 1, Article 6 of the PDPA, it is prohibited to collect, process or use personal data that is related to medical, genetic, sexual life, physical check results and criminal records, unless any of the following conditions are met:

---

[70] PDPA, *supra* note 17, at art. 8, ¶ 1.
[71] *Id.* at art. 9.
[72] *Id.* at art. 10.
[73] PDPA, *supra* note 17, at art. 11.

> (1) When in accordance with law; (2) when it is necessary for the government agency to perform its duties or for the non-government agency to fulfill the legal obligation, and when there are proper security measures; (3) when the party has disclosed such information by himself, or when the information concerned has been publicized legally; or (4) when the personal information is collected, processed or used under certain methods by a government agency or an academic research institution based on the purpose of medical treatment, personal hygiene or crime prevention, statistics and/or study.[74]

The most relevant clause applicable to *Tsai* is the last item, wherein the data controller may collect, process or use personal health data for purposes of medical, hygiene, statistics or academic research without obtaining consent from the data subjects. This article authorized the relevant competent authorities to consult with the Ministry of Justice to write the implementing rules with respect to the scope process and relevant compliance procedures. As of this date, the implementation rules have not yet been drafted.

When the PDPA was promulgated on May 26, 2010 and became effective since October 1, 2012, the legislator stated that the provision related to health information (i.e., the above-mentioned Article 6 of the PDPA) would be implemented on a date to be decided by the Executive Yuan. As of this date, this article is not yet effective. Due to this fact, when the Taipei High Administrative Court was asked to try *Tsai*, the court could not apply Article 6 of the PDPA. Instead, the Court decided to apply the predecessor of the PDPA, the abolished CPDPA.[75]

The Court seems to have misunderstood the legislative intent of enacting Article 6 of the PDPA. As expressly stated in the legislative explanation, this article was drafted because certain types of personal data are of a sensitive nature and are subject to a higher risk of privacy harm to an individual if these data are improperly collected, processed or used. The legislator took into account the EU Directive 95/46/EC[76] and wrote Article 6 of the PDPA to provide a higher degree of

---

[74] *Id.* at art. 6, ¶ 1.

[75] CPDPA, *supra* note 31; *Tsai,* No. 102-Su-36, at ¶ vii..

[76] EU Data Protection Directive, *supra* note 44.

protection and stricter standards for data collection, processing and use for five types of personal data: medical, genetic, sexual life, physical check results and criminal records.[77] The PDPA intentionally affords two distinct levels of protection and rules for general personal data (or non-sensitive personal data) and sensitive personal data. The general rule is applicable to general personal data and the enhanced protection is only applicable to sensitive data. Article 6 of the PDPA is such an enhanced protection rule. Accordingly, even though Article 6 of the PDPA is not yet effective and no enhanced protection is available for sensitive data at this time, there is no reason why sensitive data are not protected by the other clauses of the PDPA that offer general privacy protection. Fortunately, the appeal court rectified the incorrect interpretation of the PDPA that the court adopted and recognized that sensitive data should be subject to the PDPA, not the CPDPA.[78]

The privacy rule applicable to non-sensitive data in the case in which public agencies wish to collect and process personal data is provided in Article 15 of the PDPA:

> Except the information stated in Paragraph 1 of Article 6, the government agency should not collect or process personal information unless there is a specific purpose and should comply with one of the following conditions: 1. it is within the scope of job functions provided by laws and regulations; 2. a written consent has been made by the Party; and 3. the rights and interests of the Party may not be harmed.[79]

For public agencies to use health information, Article 16 of the PDPA provides the following:

> Except the information stated in Paragraph 1 of Article 6, the government agency should use the personal information in accordance with the scope of its job functions provided by laws and regulations, and in compliance with the specific purpose of collection. [80] However, the information may be used outside the scope upon the occurrence of one of the following conditions: 1. Where in accordance with law; 2. Where it is for national security or to promote public interests; 3. Where it is to prevent harm on

---

[77] PDPA, *supra* note 17, at art. 6 ("legislative intent").

[78] *See Tsai*, No. 102-Su-36, at reasoning ¶ viii.

[79] PDPA, *supra* note 17, at art. 15.

[80] *Id.*

> the life, body, freedom or property of the Party; 4. Where it is to prevent harm on the rights and interests of other people; 5. Where it is necessary for public interests on statistical analysis, or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector; 6. Where such use may benefit the Party; and 7. A written consent of the Party has been obtained.[81]

For a non-government agency to collect or process health information, Paragraph I, Article 19 of the PDPA provides that:

> Except the information stated in Paragraph 1 of Article 6, the non-government agency should not collect or process personal information unless there is a specific purpose and should comply with one of the following conditions: 1. Where in accordance with law; 2. Where there is a contract or quasi-contract between the Party and the agency; 3. Where the Party has disclosed such information by himself or when the information has been publicized legally; 4. Where it is necessary for public interests on statistical analysis, or the purpose of academic research conducted by a research institution. The information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector; 5. Where a written consent has been made by the Party; 6. Where the public interest is involved; and 7. Where the personal information is obtained from publicly available resources.[82] However, it is exempted if the information is limited by the Party on the processing or use and the interests of the Party should be protected.[83]

For a non-government agency to use medical information, Paragraph 1 of Article 20 of the PDPA provides that

> Personal data may be used only for the purposes for which it has been collected subject to the following exceptions where: 1. it is in accordance with law; 2. it is to promote the public interest; 3. it is to prevent harm to the data subject's life, body, freedom or property; 4. it is to prevent harm to other persons' vital rights and interests; 5. it is necessary for a government agency or a research institution to conduct statistical data analysis or

[81] *Id.*
[82] *Id.* at art. 19.
[83] *Id.* at art. 19.

> academic research, provided that the data, after been processed by data provider or disclosed by data collector, can no longer connect with a person's identity; and 6. written consent has been given by the data subject.[84]

In *Tsai*, the disputed issue is whether the defendant NHIA, as a government agency, may collect, process and use the plaintiffs' health data that record their visits to the hospital for certain diseases and the diagnoses and treatments provided by hospitals. These data were collected by the NHIA in the course of providing national health insurance services. Based on these facts, the applicable laws would be Articles 15 and 16 of the PDPA. The plaintiffs did not contest that the NHIA was authorized to collect their health data; therefore, there was no dispute regarding the application of Article 15. What the plaintiffs alleged was that the NHIA did not obtain their consent to transfer their health data to the NHRI and CCHIA and that such data reuse violated the PDPA, particularly Article 16 of the PDPA.

Article 16 of the PDPA is a reflection of the use limitation principle: government agencies can only use personal data for the same purposes for which they collected that data. Considering the occasions on which personal data may be reasonably used for other purposes, the same article enumerates seven exceptions in which government agencies may use personal data for other purposes. In *Tsai*, the NHIA provided health data that were processed in a manner that would de-identify the persons to the NHRI and CCHIA to establish a national health data center for academic research and for government agencies to access. The transfer of personal health data by the NHIA went beyond the original purposes when such health data were provided by the data subjects to the NHIA. The NHIA must prove that it has qualified for any of the numerated statutory exemptions to make the data transfer legitimate. The most relevant exception to which the NHIA may appeal would be Item 5, Article 16 of the PDPA, which stipulates that "where it is necessary for government agencies or academic research institutions to pursue public interest, for statistical analysis, or

---

[84] *Id*. at art. 20. (the quoted language is a translation from Taiwanese to English by the author).

for academic research, and such data have been processed in a manner that the data cannot identify a certain person, or the manner of disclosure cannot identify a certain person."[85]

To qualify for this exception to reuse personal data, the government agency has to substantiate that the contemplated data reuse is necessary for it to perform its statutory authorization, and it must qualify in three aspects: (1) the entity that reuses the personal data must be either a government agency or an academic research institution; (2) the purpose for the reuse of personal data is necessary to pursue the public interest, statistical analysis or academic research; and (3) the data have been processed to the extent that the data cannot identify a specific person.[86]

In *Tsai*, the entities that used the plaintiffs' health data included the NHIA, NHRI and CCHIA, which are government agencies and branches within the MHW. The NHRI was entrusted by the NHIA to construct and operate the national health data center; the NHRI is regarded as an extension of the NHIA. Furthermore, the NHIRD was established for medical research purposes to improve medicine and hygiene services. The plaintiffs seem unable to contest the fact that the NHIA met the first two requirements for the exceptional reuse of heath data. Most of the debates in *Tsai* involved whether the heath data at issue were processed to the extent that the data could not identify a specific person. The Court ruled in favor of the NHIA that the data were duly encrypted and could not be linked to a specific individual.[87]

The NHIA added that it has made additional efforts to ensure the personal data are safely stored in the NHIRD and any access to the database is strictly regulated. The NHIA, with the authority granted by the PDPA, amended in 1998 the Rules for Applications to Access the National Health Insurance Research Database, [88] which was renamed the Rules for

---

[85] *Id*. at art. 16, cl. 5.

[86] *Id*.

[87] *Tsai*, No. 102-Su-36, at reasoning ¶ vii.

[88] Quánmín jiànkāng bǎoxiǎn yánjiū zīliào kù – jiā zhí fúwù shēnqǐng yuánzé (全民健康保險研究資料庫 – 加值服務申請原則) [National Health Insurance Research Database – Rules for Applications to Access] (2003), http://nhird.nhri.org.tw/rule_02.html. (last visited Mar. 21, 2016).

Applications to Access the National Health Insurance Research Database Value-Added Service,[89] which the NHRI needed to comply with in reviewing the application to access the health information database. Pursuant to Section 3 of the Application Rule, applications to obtain "value-added health insurance data" are equivalent to human body research, and applicants should submit their proposals to the Research Ethic Boards and obtain the boards' approval before conducing the research pursuant to the Human Subjects Research Act.[90]

B. Regulations of the U.S. HIPAA and HITEC for the Disclosure or Use of Personal Health Data for Research Purposes

In 1996, the U.S. Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [91] to "improve [the] portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."[92] The U.S. Department of Health and Human Services (HHS), with the authority granted by HIPAA, [93] published the Standards for Privacy of Individually Identifiable Health Information in December 2000 (often referred to as the "HIPAA Privacy Rules")[94] and modified some of the rules in August

---

[89] *Id.*

[90] *Id.*

[91] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 U.S.C., 42 U.S.C. and 18 U.S.C.).

[92] *Id.* at preamble.

[93] SOLOVE & SCHWARTZ, *supra* note 3, at 431-32 ("Congress did not legislate privacy rules within HIPAA itself. Rather, congress established a deadline of August 21, 1999, for it to return to this topic and enact comprehensive legislation to provide for privacy of medical information. The Act also provided that if Congress failed to act by that date, then the Department of Health and Human Services was to promulgate regulations with regard to health privacy.").

[94] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82, 462 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160, 164).

2002.[95] The HIPAA Privacy Rules are considered the first comprehensive federal regulations to provide a minimum level of protection for all states on health information privacy.[96]

In 2009, the U.S. Congress passed the American Recovery and Reinvestment Act of 2009, which includes the Health Information Technology for Economic and Clinical Health (HITECH) Act.[97] The HITECH Act was designed to "create a national standard of safeguards to protect the confidentiality, integrity, and availability of electronic [protected health information]."[98] In January 2013, the HHS issued the "Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules"[99] (often referred to as the "HIPAA Omnibus Rule") to strengthen data privacy and data security protection for individuals' health information. The HIPAA Omnibus Rule implemented changes to HITECH and the Genetic Information Nondiscrimination Act of 2008 ("GINA").[100] The most significant amendments strengthened the protection of information privacy in the Breach Notification Rule[101] and expanded the scope of parties that are subject to the HIPAA Privacy Rules. In the amended HIPAA Omnibus Rule, business associates[102] as well as their

---

[95] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14, 776 (proposed Mar. 27, 2002) (codified at 45 C.F.R. §§ 160, 164).

[96] *See* SOLOVE & SCHWARTZ, *supra* note 3, at 432.

[97] Pub. L. No. 111-5, 123 Stat. 115, 226-79 (2009).

[98] Kevin Twidwell & Brianne McClafferty, *New HIPAA Rules Go into Effect: Lawyers Need to up Their Game in Protecting Private Health Care Information,* 39 MONT. LAW. 14, 14 (2014).

[99] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. §§ 160, 164).

[100] *See* Darci Bentson, *HIPAA, HITECH and the 2013 Omnibus Changes*, 39 Mont. Law. 5, at 5, n. 1 (2014).

[101] *See* Twidwell & McClafferty, *supra* note 98, at 16.

[102] Bentson, *supra* note 100, at 6 ("Prior to the 2013 Omnibus Rule, Business Associates were held responsible for maintaining the privacy of protected health information via contractual arrangements that were required of Covered Entities prior to disclosing or providing access to PHI to

subcontractors[103] were covered by the rule.

1. The HIPAA Privacy Rule Basics

To apply the HIPAA Privacy Rule, we should first ascertain who is subject to the rule, what information is protected by the rule and what rights the data subjects have with regard to the data controllers.

a. The Covered Entities

The HIPAA Privacy Rule does not apply to all persons who use or disclose personal health data; it only applies to "covered entities."[104] "Covered entities" include the following:[105]

(1) A health plan, which refers to "an individual or group plan that provides, or pays the cost of, medical care."[106]

(2) A health care clearinghouse:

> Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.[107]

(3) A health care provider refers to "a provider of services, a provider of medical or health services, and any other person

---

that Business Associate. Now, with the Omnibus changes, Business Associates are directly governed by HIPAA and are subject to many of the same rules and sanctions as the Covered Entities.").

[103] 45 C.F.R. § 160.103 (2014) (definitions of "Business Associate" and "subcontractor").

[104] 45 C.F.R. § 160.102 (2013).

[105] *Id.*; 45 C.F.R. § 160.103 (2014) (definition of covered entity).

[106] 42 U.S.C. § 1320d (2010); 42 U.S.C. § 300gg-91 (2015); *Id.* (definition of "health plan").

[107] 42 U.S.C. § 1302 (2015); 45 C.F.R. § 160.103 (definition of "health care provider").

or organization who furnishes, bills, or is paid for health care in the normal course of business."[108]

In addition to the above covered entities, given that on many occasions covered entities are not able to complete all assignments and outsource part of their work, which may involve personal health information, to other entities, the business associates that are engaged by the covered entities to handle personal health data are also subject to HIPAA. A "business associate" is defined in HIPAA as follows:

> Business associate includes: (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.[109]

b. Protected Health Information (PHI)—Individually Identifiable Health Information

The HIPAA defines "health information" as follows:

> any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[110]

HIPAA is only applicable to PHI. PHI is individually identifiable health information that includes information (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or

---

[108] *Id.*

[109] 45 C.F.R. § 160.103 (definition of "business associate").

[110] *Id.* (definition of "health information").

medium.[111] HIPAA excludes some individually identifiable health information that is already regulated in other laws or regulations: "(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232 g; (ii) In records described at 20 U.S.C. 1232 g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years."[112]

HIPAA further defines individually identifiable health information as follows:

> Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[113]

c. Data Subjects' Rights

When the scope of covered entities and health information is ascertained, the next issue is the rights that are afforded to the data subjects. In HIPAA, the subjects of PHI have the following rights:

(1) Right to consent to the use or disclosure of PHI: Except for reasons of treatment, payment, or health care operations, covered entities should obtain authorization from the data subjects before they can use or disclose PHI.[114] However, in the following circumstances, the covered entities may use or disclose PHI without authorization from the data subjects:

> (a) Uses and disclosures required by law; (b)Uses and disclosures for public health activities; (c)Disclosures about victims of abuse,

---

[111] *Id.* (definition of "protected health information").

[112] *Id.*

[113] 45 C.F.R. § 160.103 (definition of "individually identifiable health information").

[114] 45 C.F.R. § 164.502 (2015).

> neglect or domestic violence; (d) Uses and disclosures for health oversight activities; (e) Disclosures for judicial and administrative proceedings; (f) Disclosures for law enforcement purposes; (g) Uses and disclosures about decedents; (h) Uses and disclosures for cadaveric organ, eye or tissue donation purposes; (i) Uses and disclosures for research purposes; (j) Uses and disclosures to avert a serious threat to health or safety; (k) Uses and disclosures for specialized government functions; (l) Disclosures for workers' compensation.[115]

In the above exceptions where no consent is required from the data subjects, the most relevant part upon which this article focuses is the above (i) use and disclosure for research purposes.

(2) Rights to request privacy protection for PHI: Such rights include the right of an individual to request restriction of use and disclosure[116] and the right to require confidential communication of PHI.[117]

(3) Right of access to PHI:

> An individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for: (i) Psychotherapy notes; (ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and (iii) Protected health information maintained by a covered entity that is: (A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or (B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).[118]

(4) Right to amend: An individual has the right to request that "a covered entity amend protected health information or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set."[119]

(5) Right to an accounting of disclosures of PHI: HIPAA

---

[115] 45 C.F.R. § 164.512 (2015).
[116] 45 C.F.R. § 164.522(a) (2015).
[117] 45 C.F.R. § 164.522(b) (2015).
[118] 45 C.F.R. § 164.524 (2015).
[119] 45 C.F.R. § 164.526 (2015).

grants subjects the right to "receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested."[120]

2. HIPAA Research Provisions

a. The Definition of Research

HIPAA provides exceptions wherein the data controller may use personal data without the data subject's consent if such data will be used and disclosed for research purposes. The HIPAA Privacy Rule defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[121] Using this definition, research is distinguishable from "healthcare operations." HIPAA also provides that the data subject's consent can be exempted if the data is used for reasons of healthcare operations. Healthcare operations refer to activities involving quality assessment and improvement activities.[122] Examples include outcome evaluation and the development of clinical guidelines; population-based activities related to improving health or reducing healthcare costs; protocol development; case management and care coordination or contacting of healthcare providers and patients with information about treatment alternatives; reviewing the competence or qualifications of healthcare professionals or evaluating practitioner and provider performance; health plan performance; conducting or arranging for medical review, legal services, and auditing functions; business planning and development; and business management and general administrative activities of the entity.[123]

---

[120] 45 C.F.R. § 164.528 (2015).

[121] 45 C.F.R. § 164.501 (2015) (definition of "research").

[122] *Id.* (definition of "health care operations").

[123] *Id.*; Steinberg v. CVS Caremark Corp., 899 F. Supp. 2d 331, 338 (E.D. Pa. 2012) ("[F]ederal regulations permit the disclosure of Protected Health Information under certain circumstances, including for 'treatment, payment, or health care operations.' The term 'health care operations' is defined to include 'contacting of health care providers and patients with information

The reason for distinguishing "research" from "healthcare operations" is that when PHI is used or disclosed for research activities, the data subject's authorization is generally required but may be exempted in certain circumstances. However, the covered entity may use or disclose PHI for purposes of healthcare operations without the data subject's consent.[124]

b. Permitted Uses and Disclosures for Research Purposes

Let us apply the HIPAA Privacy Rule in the case in which covered entities wish to use personal information for research purposes. The first step is to ascertain whether the information should be recognized as individually identifiable health information (i.e., PHI). Because the Privacy Rule is applicable only to PHI, using non-individually identifiable health information for medical research is not subject to the Privacy Rule. It is important to decide whether the personal data are PHI to apply the Privacy Rule. The Privacy Rule contains two methods for a covered entity to determine whether the health information is individually identifiable.

The first de-identification approach is the "safe harbor method," under which the covered entity has removed all of the following eighteen enumerated identifiers from the personal information that it has collected:

> (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the

about treatment alternatives.' The CAC's allegations suggest two types of disclosures of customer data in this case. First, the defendants, at the request of pharmaceutical companies, include information in letters to consumers' physicians—including patient names and prescriptions—in order to suggest the provision of alternate medications. CAC ¶¶ 19-22. The plaintiffs do not allege that this type of information is disclosed to any parties other than patients' existing health care providers or used for any purpose other than for informing patients of treatment alternatives. This is a permissible disclosure of PHI under HIPAA; it falls within the 'health care operations' exception of Section 164.501 because it is a communication made to a health care provider with information about treatment alternatives.").

[124] Stacey A. Tovino, *The Use and Disclosure of Protected Health Information for Research Under the HIPAA Privacy Rule: Unrealized Patient Autonomy and Burdensome Government Regulation*, 49 S.D. L. REV. 447, 454 (2004).

> Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000 ; (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section.[125]

To apply this safe harbor method, it is required that the "covered entity does not have actual knowledge that the [remaining] information could be used alone or in combination with other information to identify an individual who is a subject of the information."[126]

In the second approach (also known as "statistical standard"), [127] a covered entity may determine that health information is not individually identifiable if "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable."[128]

After confirming whether the personal information is individually identifiable, the principle is that the covered entities shall obtain prior authorization before they may use or disclose the individually identifiable health information.

---

[125] 45 C.F.R. § 164.514 (b)(2)(i) (2015).

[126] *Id.* at (b)(2)(ii).

[127] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1737 (2010).

[128] 45 C.F.R. § 164.514(b)(1) (2015).

However, because the regulator of HIPAA recognizes that the use and disclosure of personal health information may be necessary and beneficial to medical research, the Privacy Rule has set forth certain exemptions for which the covered entities may use or disclose personally identifiable information without the authorization of data subjects, as elaborated below.

(1) "Limited Data Set" of Information: The safe harbor method requires the removal of nearly all identifiers of personal information that may not be helpful to achieve the original goal of improving medial research development, especially when the research requires the analysis of residence locations in a contagious disease research or requires age information to research inheritance disease.[129] A modified rule, the "limited data set" of information, is therefore adopted to decrease the hardship that the safe harbor method has caused to medical research.

A limited data set of information is personal information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

> (i) Names; (ii) Postal address information, other than town or city, state, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.[130]

In the safe harbor approach, personal information is regarded as non-personally identifiable only when all eighteen elements to identify a person are removed. In contrast, the limited data set approach is more flexible. For example, for an address of a person, the town or city, state, and zip code can be retained. It is also not mandatory to delete the date or month, such as one's birthdate and month, although such information

---

[129] *See* Tovino, *supra* note 124, at 457.

[130] 45 C.F.R. § 164.514(e)(2) (2015).

is usually relevant for personal identity. It is also not required to delete any other unique identifying numbers, characteristics, or codes. To qualify for the limited data set, users may enter into an agreement for the use of personal data[131] wherein the users represent and guarantee that they are bound by the applicable obligations to protect personal data, such as to re-identify the subject of the personal data.[132] As such, the users may use the limited data set information without obtaining authorization from the data subject.[133]

(2) Reviews preparatory to research: The second type of use of PHI without obtaining authorization from the data subject involves a situation in which the researchers simply review the information for preparatory purposes for research. In such cases, the covered entity shall obtain from the researcher representations that

> (A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and (C) The protected health information for which use or access is sought is necessary for the research purposes.[134]

In fact, this is not equivalent to the application of PHI for research purposes because the research work has not yet begun.

(3) Research on decedent's information: The third

---

[131] *Id.* at (e)(4)(i) ("A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.").

[132] *Id.* at (e)(4)(ii)(C) ("Provide that the limited data set recipient will: (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (5) Not identify the information or contact the individuals.").

[133] *See* Tovino, *supra* note 124, at 458.

[134] 45 C.F.R. § 164.512 (i)(1)(ii) (2015).

exception is that the covered entity may use or disclose the decedent's PHI if the covered entity obtains from the researcher

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents; (B) Documentation, at the request of the covered entity, of the death of such individuals; and (C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.[135]

(4) Board approval of a waiver of authorization: The fourth exception for which no authorization is necessary from the data subject for the covered entity to use or disclose PHI is when the covered entity has obtained from the institutional review board **("**IRB")[136] or the privacy board[137] an approval of a waiver of authorization. To qualify for this exception, the covered entity should obtain written documentation regarding the following:[138]

> a. The waiver of authorization has been approved by either an IRB or a privacy board meeting specified standards; b. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved; c. The IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization, satisfies three criteria; d. A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board; e. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and f. The

---

[135] *Id.* at (i)(1)(iii).

[136] *Id.* at (i)(1)(iii)(A) ("An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107.").

[137] *Id.* at (i)(1)(iii)(B) ("A privacy board that: (1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests; (2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and (3) Does not have any member , participating in a review of any project in which the member has a conflict of interest.").

[138] *Id.* at (i)(2)(i).

> documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.[139]

In the above requirement (c), the IRB or privacy board must review whether the following three elements are satisfied:

> (A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements. . . (B) The research could not practicably be conducted without the waiver or alteration; and (C) The research could not practicably be conducted without access to and use of the protected health information.[140]

C. Applying the PDPA and HIPAA to *Tsai*

Pursuant to Article 6, Paragraph 2 of Taiwan's PDPA, the scope, procedure and applicable rules for government agencies or academic research institutions to collect, use or disclose personal medical or health information for medical, sanitation, statistical or academic research purposes shall be designed by the relevant central authorities after consultation with the Ministry of Justice.[141] MHW is in the process of drafting the regulations that will serve a similar function as the HIPAA Privacy Rule.[142] Therefore, the Privacy Rule is an important source of foreign law that would aid the MHW in forming the regulations to implement Taiwan's PDPA in terms of personal health information.

1. A Comparative Law Study of the PDPA and HIPAA Privacy Rule

One of the key issues in the *Tsai* case is whether the Plaintiff has a legal standing to stop the defendant from using

---

[139] Tovino, *supra* note 124, at 459-60 (citation omitted).

[140] 45 C.F.R. § 164.512(i)(2)(ii).

[141] PDPA, *supra* note 17, at art. 6, ¶ 2.

[142] *See* 江睿智 [Jiang Rui Zhi], *健保巨量資料 將開放研究* [],經濟日報 [ECONOMIC DAILY NEWS] (Aug. 12, 2014), http://health.udn.com/health/story/5999/370275-%E5%81%A5%E4%BF%9D%E5%B7%A8%E9%87%8F%E8%B3%87%E696%99-%E5%B0%87%E9%96%8B%E6%94%BE%E7%A0%94%E7%A9%B6.

or disclosing personal data to protect his information privacy.[143] The Taiwan PDPA and the U.S. HIPAA Privacy Rule both abide by the first rule that personal autonomy should be respected and that an individual should freely decide how his personal data may be used.[144] Under this concept, the basic rule is that the covered entity should obtain written consent from the data subject before using or disclosing personal health information.[145] Nonetheless, both the Taiwan PDPA and the U.S. HIPAA Privacy Rule recognize that the use and disclosure of personal health information may aid medical research.[146] As such, a number of exceptions are imposed in both laws for the data subject's authorization to be exempted for research purposes. There are a number of differences between the two laws, which are summarized as follows.

a. Difference of Covered Entities

The HIPAA Privacy Rule limits its application to the covered entities and business associates because these parties regularly address a substantial volume of personal health data. The PDPA, in contrast, has broader coverage and is applicable to all public agencies and academic research institutions. Both public agencies and academic research institutions usually possess a substantial volume of personal health data. However, in addition to medical research institutions, entities such as insurance companies or medical service providers may regularly address large volumes of personal health data. Although Article 6 of the PDPA stipulates that sensitive personal data, including medical and health data, are subject to a higher level of privacy protection and requests that the MHW should implement a regulation to set forth the rules for protecting health data, it is important for the MHW to consider which entities address substantial health data and are most likely to use or disclose health data for research purposes and therefore should be subject to the PDPA and the privacy regulations. The approach the MHW should adopt is to

---

143 *Tsai*, No. 102-Su-36, at reasoning ¶ iii.
144 *See supra* Parts III.A and III.B,.
145 *See id.*
146 *See supra* Parts III.A.3 and III.B.2,.

consider which entities possess a large volume of personal health data rather than to decide which entities qualify for the definition of academic research institutions.

b. The Covenants to Use or Disclose Health Data for Research Purposes

In the absence of authorization by the data subject, the PDPA provides an exemption for the data controller to collect or use personal data when it is necessary for public interest on statistics or for academic research conducted by a research institution. The data may not lead to the identification of a certain person; neither the manner nor disclosure can identify an individual; or the data must have been de-identified. In contrast, the HIPAA Privacy Rule provides three exemptions: reviews preparatory to research, research on decedent's information, and IRB's or privacy board's approval of a waiver of authorization. For the research on decedent's information, although the PDPA does not expressly provides an exemption for the disclosure or use of decedent's information, the application of the PDPA would result in the same conclusion because the deceased's information is excluded from the PDPA. It is expressly stipulated in Article 2 of the PDPA regulations, *i.e.*, in the Enforcement Rules of the Personal Information Protection Act, that "A person referred to in the PDPA means a living nature person."[147] The other two exemptions where the data controller is permitted to collect and process personal data without obtaining consents from the data subject is worthy of consideration for the MHW to include in the drafting of privacy rules, in particular the board approval of a waiver of authorization, to be elaborated below.

c. The Definition of PHI

In the HIPAA Privacy Rule, a clear definition of health information is given because it is an important premise as to whether a certain piece of information should be categorized as personally identifiable health information. Instead of defining

[147] Enforcement Rules of the Personal Information Protection Act, *supra* note 66, at art. 2.

personally identifiable health information in the PDPA, the PDPA legislator has authorized the MHW to define it in the regulations that the MHW is drafting. The Privacy Rule may serve as important reference material in the MHW draft regulations. Before the regulations are written and implemented, because the relevant provisions in the PDPA related to sensitive personal data are not yet effective, the pertinent case involving personal health data is subject to the general provisions that also apply to other types of non-sensitive data. In considering whether the data controller may use personal health data for other purposes without obtaining the data subject's authorization or consent under the exception in which "the manner of disclosure or the processed data is unlikely to identify a certain person," the interpretation of the above rule may take into account the Privacy Rule.

2. Shortages of HIPAA Privacy Rule and PDPA in Data Privacy Issues

a. The Adequacy of Depriving the Data Subject's Decision-Making Right for His Own Health Data

The traditional information privacy mechanism was designed based on the premise of a control-driven approach and developed pursuant to the fair information practice principles (FIPPs).[148] A fair observation is that this traditional approach focuses on the procedural phase to ensure that the data subject has the right to decide whether and how his personal data are collected and used. There are a number of commonly known

[148] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS XX-XXI (1973), http://www.justice.gov/opcl/docs/rec-com-rights.pdf. (The Fair Information Practice rests on five basic principles: "[1.] There must be no personal data record-keeping systems whose very existence is secret . . . [2.] There must be a way for an individual to find out what information about him is in a record and how it is used. . . . [3.] There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. . . . [4.] There must be a way for an individual to correct or amend a record of identifiable information about him. . . [5.] Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.").

principles surrounding the FIPPs, including notice-and-choice (informed consent) and transparency rules. All of these rules have the same goal of ensuring the data subject's full control over his personal data.

The crux of *Tsai* rests on the issue that the data subject cannot exercise his right to prevent his personal data from being applied for the nation's medical research projects. Both the PDPA and the Privacy Rule make it possible for a person's right to control his personal information to not be fully protected even if highly sensitive health data are involved. The legislators of the PDPA and the Privacy Rule seem to have decided that the public interest that may be generated by medical research trumps the right of health privacy when making policy decisions. However, if we acknowledge that the core concept of information privacy is to ensure one's right to control over his personal information, we should not ignore the possibility that the controller's collection and use of such data would endanger the fundamental value of information privacy. This type of invasion of human rights is especially intolerable in civil law countries where the core of constitutional fundamental human rights is guaranteed.[149] As such, it is important to present a modified information privacy theory to justify the policy decisions of the PDPA or the Privacy Rule.

b. The PII/Non-PII Dichotomy Approach Falls Short of Dealing with Data Use for Medical Research

The PDPA adopted a dichotomous approach to distinguish personal information into identifiable and non-identifiable information. Only identifiable information is protected in the PDPA. The HIPAA Privacy Rule adopts a similar rule in terms of health data, and only personally identifiable health information is subject to the Privacy Rule. There is a special category of personal health information created in the Privacy Rule, a limited data set of information, to accommodate the need for academic research. The limited data set allows research to disclose or use personal data, including the subject's address, birth date/month/year and any other unique

[149] 李惠宗 [LI HUI ZONG], 憲法要義 [THE ESSENCE OF THE CONSTITUTION] 85 (4th ed. 2008).

identifying number, characteristic, or code without obtaining the authorization of the data subject as long as the controller has signed an agreement in a form acceptable in the Privacy Rule.

This article proposes that a more delicate approach may be developed to modify the above dichotomous method. One of the methodologies could be categorization, that is, setting forth different types of personal information and granting all such information different degrees of privacy protection. Another possible approach is to leave the decision to the IRB or the privacy board to conduct a case-by-case review.

IV. Suggestions of Modifications to the Information Privacy Theory

The *Tsai* case highlights the data protection issue when the government intends to use personal data for purposes that were not expressly intended by individuals when providing their data. The crux of the dispute lies in the controversy of whether the NHIA has the authority to disclose the Health Insurance Data that it has collected in the course of performing its statutory authority in operating national healthcare affairs for purposes other than those for which individuals were notified when consenting to the collection of the Health Insurance Data. The purpose of the use of this health information is mostly related to the public interest, and the difficult issue is whether data reuse for public interest overrides the privacy interest of data subjects when the data subjects have expressly raised objections to such data reuse. The data involved here are health data, which are generally classified as sensitive data and require a higher level of privacy protection compared to non-sensitive personal data. The interest in protecting the privacy of the subjects of health information competes with the benefits, as the NHIA has alleged, of applying the Health Insurance Data collaboratively with other data in conducting academic research with the goal of improving the provision of healthcare services and helping to reform national health policies, which is presumably valuable to society as a whole. The need to place a higher level of privacy protection on health information compared to situations in which only non-sensitive data are involved creates

more difficulty in weighing the two competing interests in this dispute.

The reasoning of the *Tsai* court judgment signals that one cannot assert one's right of autonomy as an absolute right in a conflict of medical research interests. This position obviously poses a great challenge to the traditionally recognized privacy protection principle, FIPPs, which is primarily grounded on the premise that the data subject retains and controls his personal data. The *Tsai* court judgment's position, which denied the absolute right of individual to have control over his personal data, will render the long-adopted FIPPs impossible to sustain. This article provides an analysis of the effect on FIPPs as a result of this court judgment on health information.

The only sensible means of addressing this problem is to return to the basic question of why we need to protect information privacy. Only when the rationale for the protection of information privacy is properly perceived can we resolve this dispute. This chapter will examine and restructure the concepts of privacy.

A. A Concept of Pluralistic Value of Privacy

The right to privacy can be observed in multiple legal concepts. The United State Supreme Court, in adjudicating privacy disputes, does not attempt to characterize privacy as a single concept and has recognized that privacy can be divided into three categories.[150] The first well-known concept is "decisional privacy," which the Court has characterized as a fundamental right of personal decision making regarding "marriage, procreation, contraception, consensual sexual relations, family relationships, child rearing, and education."[151] Additionally, based on the Fourth Amendment,[152] the Court

[150] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-05 (1998); Yvonne F. Lindgren, *Personal Autonomy: Towards a New Taxonomy for Privacy Law*, 31 WOMEN'S RTS. REP. 447, 451-68 (2009); Fred H. Cate & Beth E. Cate, *The Supreme Court and information privacy,* 2(4) INT'L DATA PRIVACY L. 255, 256 (2012), http://idpl.oxfordjournals.org/content/2/4/255.full.pdf+html.

[151] Cate & Cate, *supra* note 144, at 257.

[152] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

interprets "spatial (or physical) privacy" as the right to be free from unreasonable search and seizure.[153] The third privacy concept is "information privacy (data privacy)," which refers to the constitutional right of an individual to protect himself/herself from the invasion of government-compelled disclosure of personal information and the right to control information about oneself.[154]

The right to freedom of residence and the right to confidential communications, as granted by Articles 10 and 12 in the Taiwanese Constitution,[155] generally mirror the right to spatial (or physical) privacy and information privacy as declared by the U.S. Supreme Court. The Taiwanese Constitutional Court also declared in its decision No. 603 that the right to privacy granted in Article 22 of the Taiwanese Constitution [156] encompasses the right to refrain from the invasion of private spatial and physical areas as well as the right to control information about oneself.[157]

---

probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[153] *See* Katz v. United States, 389 U.S. 347, 348 (1967) (holding that the Government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment and because the Fourth Amendment protects people rather than places, presence or absence of a physical intrusion in any given enclosure is not determinative.); *see also* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006).

[154] Whalen v. Roe, 429 U.S. 589, 600 (1977) ("The mere existence in readily available form of the information about patients' use of Schedule II drugs creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations. This concern makes some patients reluctant to use, and some doctors reluctant to prescribe, such drugs even when their use is medically indicated. It follows, they argue, that the making of decisions about matters vital to the care of their health is inevitably affected by the statute. Thus, the statute threatens to impair both their interest in the nondisclosure of private information and also their interest in making important decisions independently.").

[155] MINGUO XIANFA art. 10 (1947) http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL000001 ("The people shall have freedom of residence and of change of residence."); *Id.* at art. 12 ("The people shall have freedom of privacy of correspondence.").

[156] *Id.* at art. 22 ("All other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution.").

[157] *See* Interp. No. 603, Sīfǎ yuàn fǎxué zīliào jiǎnsuǒ xìtǒng (司法院法學

The three privacy concepts declared by the U.S. Supreme Court and the two privacy categories confirmed by the Taiwanese Constitutional Court both indicate that the constitutional right to privacy has more than just a single meaning.

In U.S. tort law, privacy is protected based on multiple types of interests. In 1960, in his essay titled "Privacy," Professor William L. Prosser identified four types of privacy invasion in U.S. tort law.[158] The first type is the right to refrain from intrusion upon one's seclusion or solitude or into his private affairs.[159] The second is the right to refuse public disclosure of private facts.[160] The third type of privacy tort is recognized when one is placed in a false light in the public eye.[161] The last privacy tort refers to appropriation conducted for the wrongdoer's advantage of the plaintiff's name or likeness.[162] The above four types of privacy harm were later recognized in the Restatement (Second) of Torts edited by Prosser and have since become generally accepted tort law concepts.[163]

Unlike the above U.S. common law privacy torts, tort law in Taiwan adopts a continental (civil) law regime wherein torts are expressly stipulated in the respective statutory provisions. The Civil Code of Taiwan in Article 18[164] presents the general

---

資料檢索系統) [Judicial Yuan Of The Republic of China Law and Regulations Retrieving System], (Sept. 28, 2005) (Taiwan), http://jirs.judicial.gov.tw/eng/CETransfer.asp?goto=c&datatype=c02&code=603 (translation available at http://jirs.judicial.gov.tw/eng/FINT/FINTQRY03.asp?Y1=2004&M1=&D1=&Y2=&M2=&D2=&cno=&kw=&btnSubmit=Search&sdate=20040000&edate=99991231&keyword=&page=12&total=148&seq=125).

158 *See* Prosser, *supra* note 13, at 389.

159 *Id*. at 389-92.

160 *Id*. at 392-98.

161 *Id*. at 398-401.

162 *Id*. at 401-07.

163 *See* RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW INST. 1977).

164 MÍNFǍ (民法) [CIVIL CODE OF TAIWAN] art. 18 (2014) (Taiwan), http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL001351 [hereinafter CIVIL CODE OF TAIWAN] ("When one's personality is infringed, one may apply to the court for removing. When one's personality is in danger of being infringed, one may apply for prevention. In the preceding paragraph, an action for damages for emotional distress may be brought only if it is otherwise provided by the act.").

elements of invasion of personal rights and stipulates in respective articles the various types of personal rights, including health, reputation, credibility and privacy rights.[165] When invasion of privacy is alleged, the most relevant provisions the court applies to adjudicate are Articles 184[166] and Paragraph I of Article 195, which provide that when one party illegally invades another party's privacy right, either intentionally or negligently, the first party shall be responsible for compensating the aggrieved party's damage suffered as a result of such wrongdoing.[167] When the violation is significant and has caused non-economic losses to the aggrieved party, the compensation shall include such non-economic losses.[168] If the above-mentioned four types of U.S. privacy torts are litigated in Taiwan, the first two privacy torts—invasion of private life and disclosure of personal matters—will be adjudicated under Articles 184[169] and Paragraph I of Article 195.[170] With regard to the privacy of "false light," which is recognized as privacy tort under U.S. tort law, the Taiwan court does not adjudicate this issue under the privacy tort law. Rather, allegations of false light are generally regarded as a general type of personality tort.[171] With regard to the last type of U.S. privacy tort, appropriation, the court normally regards this as the right of likeness instead of applying the privacy torts.[172]

---

[165] *Id.* at art. 195.

[166] *Id.* at art. 184 ("A person who, intentionally or negligently, has wrongfully damaged the rights of another is bound to compensate him for any injury arising therefrom. The same rule shall be applied when the injury is done intentionally in a manner against the rules of morals. A person, who violates a statutory provision enacted for the protection of others and therefore prejudice to others, is bound to compensate for the injury, except no negligence in his act can be proved.").

[167] *Id.* at art. 195, ¶ 1 ("If a person has wrongfully damaged to the body, health, reputation, liberty, credit, privacy or chastity of another, or to another's personality in a severe way, the injured person may claim a reasonable compensation in money even if such injury is not a purely pecuniary loss. If it was reputation that has been damaged, the injured person may also claim the taking of proper measures for the rehabilitation of his reputation.").

[168] *See* J.Y. Interp. No. 603, *supra* note 157, at holding ¶ 1.

[169] CIVIL CODE OF TAIWAN art. 184.

[170] *Id.* at art. 195, ¶ 1.

[171] 王澤鑑 [WANG ZE JIAN], 人格權法 [RÉNGÉ QUÁN FǍ] [PERSONALITY LAW] 268 (2012).

[172] Taiwan Supreme Court No. 93-Tai-Shang-706 (Apr. 8, 2004)

From the above, we may conclude that in both U.S. common tort law and Taiwan civil tort law, the right to privacy is a multi-faceted legal concept that is inherently difficult to comprehend with a single definition.

B. The Methodology of Constructing the Concept of Privacy

1. The Privacy Interest Approach

To establish the infrastructure of legal concepts of privacy, the most straightforward manner is to identify the privacy interests that require protection. Two major approaches are commonly adopted, as elaborated in the paragraphs below.

a. A Unified Definition of Privacy Concept

The first approach is to look for a unified definition of the content of core values of privacy. Some have proposed that the core value of privacy is to make things private,[173] which is a simplified definition. Other propositions attempt to give privacy a more comprehensive definition by defining privacy as the right to ensure self-development, self-respect, friendship, love and trust.[174] Some definitions are based on control theory by defining privacy as "control over access to oneself and to information about oneself."[175] Similar propositions state that privacy is the right to "control over when and by whom the (physical) parts of us (as identifiable persons) can be seen or heard (in person or by use of photographs, recordings, TV, etc.), touched, smelled, or tasted by others."[176] Some propose that

(Taiwan).

[173] *See* Daniel J. Solove, *Understanding Privacy*, HARV. U. PRESS, May 2008, at 14.

[174] Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1967) ("Privacy is closely implicated in the notions of respect and self-respect, and of love, friendship and trust. Quite apart from any philosophical analysis this is intuitively obvious. In this section I shall try to make the connection explicit. In general it is my thesis that in developed social contexts love, friendship and trust are only possible if persons enjoy and accord to each other a certain measure of privacy.").

[175] Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV. 809, 812 (2007).

[176] Richard B. Parker, *A Definition of Privacy,* 27 RUTGERS L. REV. 275, 283-84 (1974).

privacy should be understood as the right to determine the conditions for realizing personal identity, in which privacy is defined as a matter of establishing the boundaries between the self and others.[177] Some understand privacy as individual "autonomy" and propose that privacy "generally involve[s] an interest in independence in making certain fundamental or personal decisions, and thus they do concern autonomy to determine for oneself what to do."[178] Privacy is also defined as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[179]

However, none of the above definitions alone can properly address privacy disputes. If the definition of privacy is too abstract, it is impractical to apply it to real cases to resolve privacy controversies, and the definition does not aid in the clarification of the concept of privacy. For example, viewing privacy as the right to ensure individual autonomy or to ensure self-respect does not help in providing a universal definition of privacy. Nearly every human right is related to the right to make one's own decisions because everyone should have the right to determine his personal living style, which involves the fundamental human right of all living beings to protect their dignity. Because all human rights stem from the right to make one's own decisions and control one's life, this basic definition (i.e., self-control) is not unique to the right to privacy and is therefore not appropriate to serve as the definition of privacy. If privacy is nothing more than the right to ensure autonomy and independence of one's decisions, there is no need to give privacy special protection. In other words, if we propose that privacy is a stand-alone human right, there must be certain interests that must be protected by enforcing the right to privacy. If privacy is defined as the right to ensure self-determination, this definition fails to distinguish the right to privacy from other human rights because other rights also share this common nature, and it would be questionable

---

[177] Thomas P. Crocker, *Ubiquitous Privacy*, 66 OKLA. L. REV. 791, 792 (2014).

[178] JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 44 (1997).

[179] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

whether privacy deserves the status of a stand-alone human right.

In contrast, a narrow definition of privacy would fail to protect the right to privacy. If privacy is defined as the right to protect private matters, by this definition, the right to privacy would fail to protect personal matters that have been made public because such information is not "private." With regard to claiming privacy as one's right to "control" his personal information, this right may be too broad and may hinder other human rights and public interests. As an example, if the goal is to allow everyone to be in full control of his/her personal information, personal information would not be allowed to flow freely and could not achieve the benefits that can only be achieved through the free flow of information.[180]

b. Categorizing Different Types of Privacy Interests

The above paragraph has illustrated that the attempt to find a universal definition of privacy will face the problem of insufficiently protecting privacy or overly protecting privacy. Therefore, some propose another option, which is to recognize that privacy is multi-faceted and contains various interests and rights and should therefore be defined from different angles.[181] This methodology has been adopted by the U.S. Supreme Court affirming that privacy has three categories. Some scholars have proposed more detailed categories for privacy. Professor Fred H. Cate presents the following aspects of privacy:

> (1) individual autonomy (the right to make decisions about marriage or family without government interference); (2) solitude and intimacy (the desire to limit access to a place or to oneself); (3) confidentiality (trade secrets and information disclosed subject to a promise of confidentiality); (4) anonymity (the desire not to be identified); (5) security (for oneself or one's information); (6) freedom from intrusion—whether physical (a trespasser) or technological (a hidden camera or microphone); (7) control of

[180] Ohm, *supra* note 127, at 1736 ("The free flow of information fuels the mode economy, nourishes our hunger for knowledge, shines a light on the inner workings of powerful institutions and organizations, and represents an exercise of liberty.").

[181] *See* Solove, *supra* note 168, at 41.

information about oneself.[182]

Professor Daniel J. Solove provides the following definitions of privacy: (1) "the right to be let alone;"[183] (2) "limited access to the self;"[184] (3) "secrecy;"[185] (4) "control over personal information;"[186] (5) "personhood" (the protection of one's personality, individuality, and dignity);[187] and (6) "intimacy" (control over or limited access to one's intimate relationships or aspects of life).[188]

We can compare the above with the three types of privacy affirmed by the U.S. Supreme Court. Decisional privacy refers to the interest of making decisions about personal intimate matters. Therefore, the focus is whether the matter is "intimate," that should be decided by the relevant persons.[189] As to whether such private matters or relationships should be kept secret or confidential, this does not relate to the core of the definition of decisional privacy. In this respect, if one disseminates videos downloaded from public sources containing others' sexual images, it would still likely be regarded as an invasion of privacy if the persons involved in the video did not give their consent to make the videos public because in such a case, the right to make a decision about intimate matters has been injured.

Spatial (or physical) privacy is respect for others' right to be let alone and to protect one's solitude. Therefore, it is necessary to limit access to a space or to oneself. For example, while a person is dining in a restaurant (which is a public place), if he has expressly indicated his intention to not be bothered (such as reserving an individual room of the restaurant), others' intrusion into the room is likely to be regarded as an invasion of privacy.

Information privacy claims that privacy is the right of a

---

[182] FRED H. CATE, PRVACY IN PERSPECTIVE 3-4 (2001).

[183] *See* Solove, *supra* note 168, at 15-18.

[184] *See id*. at 18-21.

[185] *See id*. at 21-24.

[186] *See id*. at 24-29.

[187] *See id*. at 29-34.

[188] *See id*. at 34-37.

[189] *See generally* Heidi Reamer Anderson, *Plotting Privacy as Intimacy*, 46 IND. L. REV. 311 (2013).

person to be in control of information about himself. The reason is that if one's personal information falls into the hands of others and is used in any manner desirable by the holder of such information, the subject of the data is subject to a huge risk that his credit cards may be used and his identity may be stolen, leading to possible damage to the person's interests. Therefore, since the type of personal data at issue is more closely related to the right of one's identity, a higher degree of protection should be granted to the right of personal control.

Each of the above concepts of protecting privacy has a specific focus but overlap in some respects. Matters that one wishes to keep private are usually those about one's intimacy. The desire to limit access to oneself or to be let alone usually involves decision to maintain secrecy. The control of information about oneself usually involves the decision of whether to limit access to such information by others to limit access to intimate relationships and to maintain the secrecy of certain aspects of life.

Due to the overlapping concepts of these notions of privacy, there are sometimes confusions and difficulties in distinguishing these different concepts. For example, special privacy claims the desire to limit access to personal space from intrusion. It is, in fact, a decision about oneself to protect one's solitude. In this respect, "solitude" is intertwined with "individual autonomy." Moreover, the element of confidentiality is often considered when evaluating the interests of privacy protection. For example, it is a common proposition that publicly available and non-confidential information is not protected by the right to privacy. However, if the focus of information privacy is to protect one's right to control his personal information, whether such information is confidential should not affect the determination of privacy protection. To summarize, establishing a legal concept infrastructure of privacy by differentiating respective privacy interests and developing multiple privacy concepts may be a theoretically correct methodology. However, applying the various privacy concepts could lead to insufficient protection privacy due to the overlapping areas of different concepts of privacy.

In addition to the above-mentioned privacy notions

stemming from the individual value of privacy, some scholars have recently proposed concepts of privacy based on social value.[190] This social-value-oriented theory was inspired by the concept that privacy is a notion generated in the course of a social life; therefore, the value of privacy cannot be correctly perceived without considering the social context.[191] The society in which one lives influences how privacy is perceived. Therefore, privacy protection should include the subjective expectation of individuals as well as objective elements from society. [192] Professor Julie E. Cohen proposes that "[s]ubjectivity, and hence selfhood, exists in the space between the experience of autonomous selfhood and the reality of social shaping."[193] This notion recognizes the social value of privacy and ensures a harmonious link between personal selfhood and societal norms. In other words, privacy "enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making."[194]

Privacy has an important function in fostering democracy; therefore, the genuine value of privacy must include its social aspect. The political scientist Priscilla M. Regan analyzes privacy in a social context and contends that the benefits of privacy protection include resisting the abuse of government power and fostering democracy.[195] In the Arab Spring, which

---

[190] *See generally* Chen-Hung Chang, *New Technology, New Information Privacy: Social-Value-Oriented Information Privacy Theory*, 10 N.T.U. L. REV. 127, 147-50 (2015); Arthur J. Cockfield, *Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies*, 40 U.B.C. L. REV. 41, 49-59 (2007).

[191] Julie E. Cohen, Symposium, *What Privacy is For*, 126 HARV. L. REV. 1904, 1905 (2013) ("[L]iberal privacy theory's descriptive premises about both the self and the nature of privacy are wrong. The self has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts.").

[192] *Id*. at 1927 ("Privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing, and those purposes must be taken into account when making privacy policy.").

[193] *Id*. at 1909.

[194] *Id*. at 1911.

[195] PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225-27 (1995) ("Privacy has value not just to individuals as individuals or to all individuals in common but also to the

was also called the "Jasmine Revolution," which occurred in 2011 throughout the countries of the Arab world,[196] online social networks played an important role in the protests. The catalyst of protests was the self-immolation of a young man who was unable to find work and who was selling vegetables at a roadside stand until a municipal inspector confiscated his wares.[197] His unfortunate death and the image of him dousing himself with gasoline and setting himself on fire was broadcasted through social media, leading many people who were dissatisfied with the existing system to begin the revolution and overthrow the twenty-three-year-long dictatorship government of Tunisia.[198] The protests then spread to other Arab countries. In these protests, social media such as Facebook and Twitter provided a valuable platform for people to express and communicate pro-democracy messages and helped the revolution fight against poor treatments by the dictatorship government. In the Arab Spring, if the governments had known who was initiating the protests and disseminating anti-government comments, the governments would have detained those who initiated the actions before they were able to upload messages to social media, and the messages would not have been circulated. In this case, when an individual is protected by information privacy rights to freely express his thoughts without fear, it also benefits society and fosters democracy.

In summary, if a concept of privacy is fundamentally based on one's right to control things about oneself, this privacy is unlikely to prevail when it conflicts with the social benefits that represent public interests. If privacy is based on an individual's own value, the government would lack standing to intervene in affairs between private sectors. In view of these deficiencies of the individual value of privacy, this article

---

democratic political system.").

[196] *See* Delinda C. Hanley, *Tunisia's Jasmine Revolution*, WASH. REP. (Mar. 2011), http://www.wrmea.org/2011-march/three-views-tunisia-s-jasmine-revolution.html.

[197] *See Arab Uprising: Country by Country – Tunisia*, BBC NEWS (Dec. 16, 2013), http://www.bbc.com/news/world-12482315.

[198] *See* Delinda C. Hanley, *Tunisia's Jasmine Revolution*, WASH. REP. (Mar. 2011), http://www.wrmea.org/2011-march/three-views-tunisia-s-jasmine-revolution.html.

proposes that privacy should incorporate social value. Using a concept of privacy with a social context, the government would be able to use its power to intervene to protect privacy.

2. The Privacy Harm Approach

If privacy is understood as the right to protect certain interests, this methodology is likely to claim an over-broad territory of privacy and to infringe on other rights or public interests. For example, when privacy is defined as the right to control information about oneself, activities that relate to the collection, processing and use of personal information cannot be conducted without the consent of the subject of the data because such activities will affect the interests of information privacy. However, the interest of controlling one's personal information is an abstract concept that assumes that there are certain information privacy interests that require protection; therefore, people should be protected to have full control over information about themselves. However, when this right to control is affected to a certain degree, it is uncertain whether corresponding harm will occur. To address this effect, a methodology has been proposed to comprehend a legal concept of privacy and to categorize different types of potential privacy harm that are likely to be affected. This approach has been adopted in U.S. privacy tort law. The Third Circuit court in *United States v. Westinghouse Elec. Corp.*,[199] several factors were considered to evaluate the potential harm in determining if information privacy was injured. The Court reasoned that "the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated."[200]

---

[199] United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980).

[200] *Id*. at 578 (3d Cir. 1980) ("The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.").

Out of the many methodological approaches, this privacy-harm based methodology was chosen by the U.S. White House in its Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015.[201] In Section 4, Definitions, "'Privacy risk' means the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional or other harm to an individual."[202] The "privacy risk" approach in the Consumer Privacy Bill of Rights Act of 2015 is based on the similar concept that a definition of privacy should consider the potential harm associated with the claimed privacy right.

Defining privacy rights from the angle of potential harm can better address the relationship between individual privacy and the related social context than other perspectives. This means that when one is recognized to have an abstract privacy interest, the existence of this privacy interest does not lead to the conclusion that objective privacy harm would be caused if the privacy interest were injured in any manner. The risk to privacy harm in the disclosure of personal information should be determined based on the social context of the circumstances. For example, it is a general understanding that one should have full control over all information about his cell phone usage and should have the right to information privacy over such information. A cell phone service provider developed a communication app that aims to make it possible for all users to know which service providers their phone book contacts are using so that the app users may decide whether to make phone calls to control their phone bills. It is true that the phone company that one uses is personal information, and the app's disclosure of such information might have affected people's right to control information about themselves. However, it is worth noting that such behavior does not necessarily cause harm to the phone user. In other words, the disclosure of information about the phone company of a phone user does not necessarily raise a privacy harm risk to individuals. The

---

[201] WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[202] *Id*. at 4.

potential privacy risk should depend on the social context in which the alleged privacy infringement is situated.

To summarize, privacy cannot be fully comprehended without knowing the associated social "contextual integrity."[203] Information privacy, then, is "a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones."[204]

Observing privacy from potential harm does not mean that privacy cannot be defined in a legal concept. On the contrary, giving privacy a specific conceptual notion is helpful to better comprehend and explore the value of privacy. The point is that the methodology should be one that uses a "bottom-up culture analysis" in de-constructing privacy issues and develops a map to address various privacy controversies.[205] The counterpart is to give privacy a universal concept and to apply such a unified concept top-down to all privacy issues,[206] which this article does not support. The rationale is that the value of privacy should be understood in its interaction with the world in which one lives.[207] Based on the "bottom-up culture analysis" approach, Professor Solove categorized four types of activities that are likely to cause privacy harm.

The first type is potential privacy harm caused by information collection.[208]For example, one may suspect that he has been watched and may conduct a self-inspection and change his work and life patterns.[209] This type involves harm that significantly affects one's decisions about oneself and that would force an individual to live in a highly emotionally stressed situation, resulting in a negative impact on one's

---

[203] *See generally* Chang, *supra* note 191, at 156-59.

[204] *See* HELEN NISSENBAUM, PRIVACY IN CONTEST: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 231 (2010).

[205] *See* SOLOVE, *supra* note 168, at 172-73.

[206] *See id*.

[207] *See id*. at 173-74.

[208] The "Information collection" category contains subcategories of conduct relating to surveillance and interrogation. For a detailed explanation, *see id*. at 106-17.

[209] *See id*. at 108.

mental and physical health.[210]

The second type relates to information processing, which is also likely to cause privacy harm.[211] Information aggregation is an example. Fragmented information may not reveal too many aspects of one's personal life. However, the aggregation and accumulation of personal information for a long period of time and the combination of personal information with other information has the potential to shape a comprehensive personal profile.[212] The hot topic of big data technology is one of the applications of information aggregation technology.[213] The potential privacy harm related to information aggregation is that it is unpredictable and puts data subjects in fear of an unknown and uncontrollable risk of privacy harm.[214]

Information dissemination is the third type of act that could result in privacy harm. Examples include unauthorized disclosure of one's criminal records, making the person with such records unable to find a job or likely to be dismissed by his/her employer, and unauthorized disclosure of others' nude photos, which may cause a disturbance to the person's peace.[215]

---

[210] *See id*.

[211] "Information processing" contains subcategories of conduct relating to aggregation, identification, insecurity, secondary use, and exclusion. For a detailed explanation, *see id.* at 117-36.

[212] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1-7 (2004).

[213] VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6 (2013) ("There is no rigorous definition of big data. Initially the idea was that the volume of information had grown so large that the quantity being " examined no longer fit into the memory that computers use for processing, so engineers needed to revamp the tools they used for analyzing it all . . . . [O]ne way to think about the issue today—and the way we do in the book—is this: big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more"); *see also* Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 81 (2013) ("'Big data' can be defined as a problem-solving philosophy that leverages massive datasets and algorithmic analysis to extract 'hidden information and surprising correlations.'").

[214] *See* SOLOVE, *supra* note 168, at 118-19.

[215] "Dissemination contemplates" contains subcategories of conduct relating to breach of confidentiality, disclosure, exposure, increased accessibility of information, blackmail, appropriation, and distortion of information. For a detailed explanation, *see Id.* at 136-61; *see also* Hayley Tsukayama, *Toronto ""Police: There Have Been 'Hate Crimes' and Possible*

Invasion of a person's body or space is also recognized as an action that could endanger privacy because it is evident that intrusion into one's home would threaten the safety of the people who live there.[216]

C. Concept of Information Privacy Combining Privacy Harm and Privacy Interest

Privacy interest and privacy harm originate from different contexts but overlap in most of their content. The major reason is that where the interest exists is usually the place where privacy harm arises. Most of the time, privacy interest and privacy harm are addressed in different sequences. However, when privacy interest relates to subjective emotional feelings, such as whether one feels his personal affairs are disturbed, this subjective feeling is not necessarily regarded as an objective harm that is recognized by society. In this circumstance, the existence of privacy interest is not tantamount to privacy harm.

If a privacy concept is purely developed based on privacy interest, it is easier to draw a map that provides direction for clear concepts of privacy. The opposite side of this approach is that privacy interest may be broadly defined and therefore may sacrifice other human rights and public benefits. In contrast, a concept of privacy developed based on privacy harm without considering privacy interest is subject to the risk of sacrificing an individual's privacy interest in pursuit of social benefits because privacy harm may be invisible or ignored when there is a greater goal of protecting society's interest.

This article proposes that an integrated notion that contains both privacy interest and privacy harm is a better approach to comprehend privacy. Privacy harm and privacy

Suicides over the Ashley Madison Breach, WASH. POST, Aug. 24, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/08/24/toronto-police-there-have-been-hate-crimes-and-possible-suicides-over-the-ashley-madison-breach/ (The parent company of Ashley Madison, the adultery site, was hacked and a large number of users data were stolen. Thereafter, there have been "hate crimes" linked to the breach, as well as two unconfirmed reports of suicides).

216 "Invasion" contains subcategories of conduct relating to intrusion and decisional interference. For a detailed explanation, *see* SOLOVE, *supra* note 168, at 160-70.

interest must be viewed as a whole instead of as separate concepts.

Introducing privacy interest is a good way to explain the positive side of privacy and why privacy is important for individuals and society. This is a good approach to present the concept of privacy in a way that people can understand. Professor Solove introduced ten reasons why privacy requires protection so that the concept of privacy can be easily understood.[217] As far as privacy harm is concerned, it plays an important role in supporting the explanation that privacy protection should not be an interest based only on an individual's subjective expectation of privacy; privacy harm helps to determine whether privacy protection should be granted when considering the objective standard of the society.[218] Accordingly, the notion of privacy harm is an important element in comprehending information privacy because privacy harm must be viewed from the perspective of whether privacy protection will hamper technological advancement and the free flow of personal information. In summary, the concept of privacy originated from the presumption that privacy should be protected, and its content is shaped by the integration of privacy interest and privacy harm. When such an integrated concept of privacy applies to privacy controversies and the formation of privacy policies, the key issue is to determine whether privacy harm is caused after balancing the privacy value at issue with the conflicting rights or public interest.

For information privacy, it is true that the foundation of

---

[217] *See* Daniel Solove, *10 Reasons Why Privacy Matters*, LINKEDIN (Jan. 13, 2014), http://www.linkedin.com/today/post/article/20140113044954-2259773-10-reasons-why-privacy-matters?trk=eml-ced-b-art-M-0&ut=35ks2yPax8pC41 (Noting ten reasons why privacy matters: "1. Limit on Power; 2. Respect for Individuals; 3. Reputation Management; 4. Maintaining Appropriate Social "Boundaries; 5. Trust; 6. Control Over One's Life; 7. Freedom of Thought and Speech; 8. Freedom of Social and Political Activities; 9. Ability to Change and Have Second Chances; 10. Not Having to Explain or Justify Oneself.").

[218] SOLOVE, *supra* note 168, at 78 ("[P]rivacy value differs depending upon the type of problem it protects against. Privacy problems impede certain activities, and the value of privacy emerges from the value of preserving these activities. Its value must be worked out as we balance it against opposing interests.").

privacy interest is one's right to control information about oneself, but we cannot ignore the fact that the secrecy and intimacy of different types of personal information represent different degrees of interest in information privacy.[219] Society's perspective on the secrecy and intimacy of certain personal information leads to the determination of whether privacy harm would be caused and the seriousness of such privacy harm. Therefore, to construct a concept of information privacy, the starting point should be the basic interest that requires protection of information privacy, in which the focus is the individual right to control over personal information. Based on the above foundation, the next step is to examine other people's privacy interests, such as secrecy and intimacy. With this understanding of multiple information privacy interests, the focus then moves to privacy harm to shed light on the related social context to determine whether the subjective information privacy interest, despite involving one's right to control over personal information, would truly suffer privacy harm and deserves privacy protection from society's perspective.

We cannot ignore the social value of privacy rights.[220] As Professor Solove contends, "Privacy isn't the trumpeting of the individual against society's interests but the protection of the individual based on society's own norms and values. Privacy isn't simply a way to extricate individuals from social control; it is itself a form of social control that emerges from a society's norms."[221] The above-mentioned Arab Spring proved that privacy has an important function in fostering democracy; therefore, the genuine value of privacy must include its social aspect. The protection of privacy rights has a social value that fosters democracy because people with privacy protection may communicate with each other and express their views of the government without concern about revenge or abuses of government power.[222] In Taiwan, the Criminal Investigation Bureau ("CIB") sought access to Taiwan's nationwide highway

---

[219] J.Y. Interp. No. 603, *supra* note 157, at reasoning ¶ 8.

[220] *See generally* Chang, *supra* note 191, at 147-50.

[221] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 50 (2011).

[222] *See* REGAN, *supra* note 190, at 225-27; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1658 (1999).

electronic toll collection ("ETC") system database, which functions as a massive vehicle surveillance program that captures drivers' location data.[223] The CIB asked the ETC operator to turn over toll records in the name of crime prevention.[224] If the CIB's indiscriminate gathering of personal information is prone to abuse, such as attacks on political foes, it will ultimately endanger democratic society. When the social value of privacy is considered, the CIB's desire to access all drivers' data should be prohibited unless the CIB can demonstrate that the claimed public interest is greater than the social value of democracy.[225]

This multi-faceted concept of information privacy combined with the privacy harm approach wherein the respective social contexts are evaluated form a complete concept of information privacy to provide a practical solution for privacy disputes arising from new technologies. In *Tsai*, where health information is involved, if the spotlight is on the individual right to control his personal health information, whether one has lost his control over his/her own data represents the entire concept of information privacy protection. When one's right to control is deprived, under the control-based privacy theory, the individual's privacy right is also deprived. Under the constitutional regime in the continental law system, human rights can only be restricted for statutory reasons but cannot be deprived.[226] Applying this logic, one of the plaintiffs' claims is

---

[223] *See* 林志青 [Lin Zhi Qing], *Yuǎn tōng 2 cì bàojià yōu gè zī fǎ dǎzhù xíngshì jú chíxù xiétiáo* (*遠通 2 次報價憂個資法打住　刑事局持續協調*) [*PDPA Concerns Halted FE-Toll Two Offers to CIB, Negotiation Continues*], PÍNGGUǑ RÌBÀO (蘋果日報) [APPLE DAILY], Jan. 11, 2014, http://www.appledaily.com.tw/realtimenews/article/new/20140111/324266/.
See Ye Zhi Jian (葉志堅), *ETC Chéng jiānkòng xìtǒng?! Jǐng zhèng shǔ fāwén jiānkòng quánmín* (*ETC* 成監控系統？！ 警政署發文監控全民) [*ETC Turns to Be a Surveillance System?! The Criminal Investigation Bureau Sent Notice to Monitor All Citizens*], JĪNRÌ XĪNWÉN (今日新聞) [NOWNEWS] (Jan. 10, 2014), http://www.nownews.com/n/2014/01/10/1085265.

[225] *See* Chen-Hung Chang, *Eyes on the Road Program in Taiwan—Information Privacy Issues under the Taiwan Personal Data Protection Act*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 145, 170-85 (2015).

[226] J.Y. Interp. No. 567, at reasoning ¶ 3 (Oct. 24, 2003) (Taiwan) ("While the state may impose more restrictions on individual rights during extraordinary periods and due to necessity under extraordinary circumstances, such restrictions must nevertheless not exceed the boundaries

reasonable—even if the defendant is allowed to reuse their personal data, the plaintiffs may assert their right to information control to demand that the defendant stop using the data without their consent after discovering that their health data were used in a manner to which the data subjects did not consent.[227] If we agree that the plaintiffs' right to control over their personal health data is an absolute right, there is no possibility that the NHIA may disclose health data to other government agencies and academic institutions without the data subjects' consent. The NHIA cannot use these personal data despite these data are used to conduct medical research to provide more value for the society, such as generating aggregated information to improve public health services and to form better healthcare policies. The *Tsai* case has illustrated that if information privacy is observed purely from the perspective of individuals' subjective interest in retaining control over their personal information without considering the likelihood of causing privacy harm, such a conception of privacy will impede the development of information technology and the pursuit of greater public welfare.

This article proposes that the multi-faceted information privacy value combined with the affirmation of privacy harm can serve as an improved concept of privacy. This improved concept can be helpful of balancing conflicts with other people's interests or public interest, providing a legal foundation in the reform of current privacy laws and regulations, and responding to the new privacy threats produced by new technologies.

---

of minimum human rights protection. Freedom of thought must be upheld to safeguard the spiritual activities of the people, the root of human civilization and the foundation of freedom of expression, and the most fundamental human dignity the Constitution intends to protect. Given its particularly crucial meaning to freedom, democracy and the continuance of the constitutional rule of law, no government agencies may encroach upon [this fundamental right] in the name of emergencies. Even in times of extraordinary nature, and regardless of whether in the form of a statute, invasion of the scope of minimum human rights is prohibited, be it with the means to compel revelation or rehabilitation.), *translated in* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=567.

[227] Tsai v. NHIA, 2014 FĂ YUÁN FĂLÜ WĂNG (法源法律網) [LAWBANK], No. 102-Su-36 at reasoning ¶ iii (Taipei High Admin. Ct. May 14, 2014) (Taiwan).

V. Applying the Modified Information Privacy Concept to *Tsai*

In *Tsai*, the plaintiffs argued vigorously that they should have the right to control over their personal health data. It was difficult for them to accept the court's judgement that the NHIA may freely use their health data although they had expressly voiced their privacy concerns and raised objections against the NHIA's disclosure of their data. When the plaintiffs gave their consent to the NHIA for the latter to collect their personal health data, they were informed that the health data were provided to receive the national health insurance services. The NHIA did not inform them that the health data would be used for medical research, and the plaintiffs did not give consent to allow the use of the data for these medical research purposes. The defendant NHIA did not contest the absence of the plaintiffs' written consent for the data reuse and did not deny the fact that health data were used for a purpose other than the purpose stated when the data were collected. The NHIA's main argument was that it was using the health data for medical research, with the data duly encrypted to the extent that it did not identify individuals directly or indirectly.

The HIPAA Privacy Rule specifies three occasions on which a data controller may disclose a natural person's health data for research purposes. First, a data controller may use or disclose personal health data with authorization from the data subject. If the data subject's authorization is unavailable, the second scenario is that the health data should be de-identified. In this case, the data controller is not bound by the restrictions of the Privacy Rule in using the personal data. When it is necessary to retain health data as personally identifiable, the available option is to obtain approval from an IRB or privacy board. This article notes some problems in applying the three conditions to the use of health data.

A. Unconditionally Requiring the Data Subject's Authorization will Become an Impediment to Medical Research Rather than a Pathway for Privacy Protection

If privacy is viewed purely from the perspective of the

individual's right to control his own data, it offers little help in protecting privacy and may undermine medical research. Most information privacy protection legal systems in the main jurisdictions were developed under the control–driven notion, which focuses on the autonomy of the data subject in deciding whether and how his data are used. One primary privacy principle has been declared and complied with for decades, which emphasize the notice-and-choice (informed consent) doctrine to ensure that data subjects have full control over their own data.[228] When modern technologies make it impossible for a data subject to know when and how his data are collected and used, it becomes questionable whether the notice-and-choice approach is still workable and meaningful for the benefit of privacy protection and innovation in technology.[229] The following paragraphs will explain why the informed consent principle falls short of protecting the privacy of personal health data in medical research projects.

1. Shifting the Burden of Privacy Protection to the Data Subject Would Cause an Adverse Impact on Privacy Protection

There are drawbacks to universally requiring an individual's choice and consent for the use of health data for research purposes. The first and foremost is that medical research involves highly professional knowledge and is not an easy concept for the general public to comprehend. It is also very unlikely that anyone, after reading a few lines of a single page of a privacy notice, can immediately detect the privacy risks associated with the medical research in which the health data will be used. Even though a privacy notice may be thoroughly presented at length for several pages, no one is likely to bother to read it. Even if some people attempt to read the notice, the complicated and professional terms and conditions are usually too difficult for people with no professional background to understand. If it is not reasonably

[228] *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011); Cate, *supra* note 6, at 1766 ("Many data protection laws enacted since then have followed suit, relying on choice-often together with notice necessary to support choice-as the key tool for protecting privacy, or even as the goal of those laws").

[229] *See* Chang, *supra* note 191, at 141-45.

expected that the message of privacy risks can be fully communicated and understood by data subjects, consent by data subjects means very little in relation to protecting the data subjects' privacy right. On the contrary, if the data controller can use health data in any manner as long as the data subject has given consent, a "blind" authorization will endanger privacy protection.[230]

The notice-and-choice principle fails to consider situations in which health information involves the personal privacy interest of the data subject as well as the privacy interest of other people or a specific group, especially genetic information. In January 2007, a Taiwanese hospital (Mackay Memorial Hospital) collected salivary samples from twenty-nine persons who belonged to the Kavalan, one of Taiwan's aboriginal tribes, for biological research on the Taiwanese tribes and to examine how the tribes are biologically related to each other.[231] The collection of salivary samples was conducted with the authorization of the test subjects.[232] However, many of the Kavalan people (except for those who were willing to provide their salivary samples for the research) have vigorously contested the research project, alleging that this project seriously violated the Indigenous Peoples Basic Act of Taiwan.[233] The battle came to an end after the hospital agreed to stop the project and destroy all the salivary samples it had obtained.[234] In the Kavalan case, the Kavalan tribe had strong standing to object to the biological research, for which twenty-nine Kavalan persons had given their consent, due to the important factor that the salivary samples not only represent the bodily features of the twenty-nine people but could also reveal the biological information of all people with Kavalan

---

[230] *See* Cate, *supra* note 6, at 1775-76.

[231] *See* Chen Hui Hui (陳惠惠) and Chang Bo Dong (張柏東), *Zūnzhòng jīyīn chǎnquán mǎ xié xiāohuǐ yuán mín jiǎn tǐ* (*尊重基因產權 馬偕銷毀原民檢體*) [*To respect the individuals' right on genetic data, Mackay agreed to destroy the indigenous peoples' test samples*], LIÁNHÉ BÀO (聯合報) [UNITED DAILY NEWS] (Apr. 2, 2007), http://biobankforum.blogspot.tw/2009/05/blog-post_9724.html.

[232] *Id.*

[233] The Indigenous Peoples' Basic Law (2015) (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL034022.

[234] *See* Chen (**陳**) and Chang (**張**), *supra* note 234.

blood. If the research results indicate certain genetic diseases or disorders of the Kavalan tribe, once these results are published, not only will the twenty-nine test subjects be affected in many aspects of their lives, financially (such as a possible increase in health insurance premiums) or emotionally (such as carrying the reputation of being part of an unhealthy tribe), but these adverse impacts will also affect the entire Kavalan tribe.[235]

2. Ensuring Individuals' Autonomy Right to Their Own Data Does Not Guarantee Privacy Protection

The plaintiffs in *Tsai* alleged that the only legitimate way to use personal health data in medical research is to obtain authorization from the data subjects. The multi-dimension privacy interest theory has demonstrated that an individual's right to make a decision about personal data represents only one of the faces of privacy protection. Putting the entire emphasis on an individual's control over his personal information fails to consider other dimensions of privacy interests and cannot guard information for privacy protection.

Based on the pluralistic interest privacy theory that this article has proposed, in the matter of information privacy, it is not only the right of individual control over personal data that deserves attention; it is also equally important to ensure the secrecy and intimate relationships of personal data. Protecting an individual's right to control over personal data does not guarantee protection of an individual's information privacy.[236] For example, one may give consent based on his own decision that a hospital may use his health data; however, the hospital may fail to establish and implement a data security system, creating a loophole for hackers to compromise the hospital's database and steal the personal data. This situation demonstrates that an individual's privacy right is not fully protected simply because the individual has full control in deciding who may collect and use his personal data.

When a person' s right to control his data conflicts with the public interest or other rights, the remedy is not to regain

[235] *See* Gostin, *supra* note 2, at 489-92.
[236] *See* Cate, *supra* note 6, at 1769.

control over the data but to ensure that other parts of the privacy interest are enhanced. The HIPAA Privacy Rule allows the data controller to use health data for medical research by obtaining approval from the IRB or privacy board in lieu of the data subject's consent. This is a step back for an individual's control over his data to make room for conflicting interests. In the meantime, there should be proper measures to ensure that other privacy interests are well protected. Although not expressly indicated in the Privacy Rule, it is important that the IRB and privacy board's review processes should ensure the secrecy of the data at issue. For example, to the greatest extent possible, the data that will be used should be processed in a manner that removes any personally identifiable information as much as possible. It is also reasonable to impose an enhanced data security standard on the data controller considering that the data controller has been exempted from the difficulty of obtaining the data subject's consent and the data subject is giving up his control over his personal data. In particular, if the personal data have been de-identified to be exempted from the obligation to obtain individual consent pursuant to the Privacy Rule, a balanced privacy policy would require that the research institution should be prohibited from recovering the de-identified personal data into identified data.

3. A Balance Check Between Public Interest of Medical Research and Threats to Privacy Protection

The notice-and-choice principle is impractical in an internet-connected world. If the informed consent principle must be adhered to in all matters, it is costly and time-consuming to ensure that everyone has full control over the flow of his personal information.[237] When considering the benefits of protecting privacy, we should also take into account the costs incurred and the lost opportunities for medical research. An individual's consent usually limits the scope and manner in which the data controller may use or disclose the data because the informed consent principle requires that the notice cannot be too general and should clearly state the

[237] *See id*. at 1776.

specific purpose regarding the data collection and use. This one-topic or one-time consent or authorization, even if obtained, cannot serve as a pathway for the use of the same data for other research topics. This consent requirement appears unrealistic for medical research because a research topic is often inspired or derived from other research topics that may not closely relate to the original purpose of collecting the personal data. If it is mandatory for the data controller to obtain new consent from the data subject to use or disclose personal data for a new research project, this will inevitably undercut the efficiency of medical research.[238]

In *Tsai*, at the time when the NHIA collected patients' health data, the plan to establish a national health insurance data center had not yet been proposed. If the informed consent requirement were strictly complied with, the NHIA could not use the patients' health data in medical research projects because the patients' consent was limited to the provision of medical services. Therefore, if the NHIA intends to establish a national health insurance data center and it is necessary that new consent is obtained from the patients as required by the informed consent principle, the notice-and-consent process would involve millions of people and incur enormous time and expenses.

Moreover, if an individual's consent is treated as the only way for the data controller to use health data, a selection bias of the data would lead to the failure of the research because the data with consent may not be representative.[239]

To resolve the limitations the informed-consent requirement has caused to the use of health data in medical research, a possible solution is to compromise the self-decision interest while offering individuals enhanced protection for other parts of their privacy interest. This could be a balanced approach in which the benefits contributed by medical research outweigh the importance of protecting individuals' control over their data. The multi-faceted privacy theory supports this approach. When one portion of the privacy interest cannot

---

[238] *See id*. at 1789-90.

[239] *See id*. at 1791; Sharona Hoffman & Andy Podgurski, *Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research*, 65 SMU L. REV. 85, 114-18 (2012).

receive full protection (i.e., a loss of control over personal data), a reasonable remedy could be to require the data controller, who benefits from the use of personal data, to provide enhanced protection for other portions of privacy interest, such as data security. The privacy law may be improved to require the data controller to implement a best practice to protect the secrecy of the data it uses and to operate a safe and secure environment for data storage to prevent data misuse or theft.

B. Applying a Privacy Harm Approach in Categorizing Personal Data and Suitable Privacy Protection Standards

1. What Type of Personal Data are Protected in PDPA and HIPAA?

In both Taiwan PDPA and the U.S. HIPAA, whether personal data are personally identifiable serves as a jurisdiction trigger. As far as health data are concerned, the protected information in the Privacy Rule and the PDPA are similar and refer to personally *identified* information and personally *identifiable* information.

The PDPA distinguishes personal information into three categories: personally directly identified (identified) information, personally indirectly identified (identifiable) information, and non-personally identifiable information (Non-PII).[240] Only the first two types of personal information (PII) are protected by the PDPA, whereas Non-PII is excluded.

Similar to the PDPA, the HIPAA Privacy Rule limits its protection to PII and further specifies the types of PII that are protected in the Privacy Rule. The Privacy Rule defines personally identifiable health information as follows: "Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual" and such information identifies the individual or can be used to identify the individual.[241]

---

[240] Personal Information Protection Act art. 2, cl. 1 (2010) (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627.

[241] 45 C.F.R. § 160.103 (definition of individually identifiable health information).

The PDPA defines personally directly identified information as follows: "Information refers to an identified person when it singles out a specific individual from others."[242] Citizenship ID card numbers and passport numbers are listed as examples of identified information. Personally indirectly identified information is defined as "other information which may be used to identify a natural person indirectly" and information that "cannot directly identify a specific person without comparing to, combining with or connecting to other information."[243] The Taiwanese court previously ruled that cell phone users' service provider information, as shown in communication apps, should be regarded as personal information in the PDPA. The court held that although the phone service provider information alone cannot identify a specific person, the service provider information combined with the user's cell phone number can identify a specific cell phone user.[244]

To explain why the PDPA and HIPAA expressly excluded Non-PII,[245] the harm-based approach to information privacy theory could serve as the theoretical basis[246] because the use or disclosure of Non-PII is unlikely to cause privacy harm; therefore, it is unnecessary to offer privacy protection for non-PII. A side issue this article has noted is that technological advances have greatly increased the possibility of identifying personal features from certain data.[247] Whether a piece of information should be regarded as Non-PII might change from time to time. The excluded Non-PII might be used to identify a certain person with the help of modern information

---

[242] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the U.S. and EU*, 102 CALIF. L, REV. 877, 905 (2014).

[243] Enforcement Rules of the Personal Information Protection Act art. 3 (2012) (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid =FL010628.

[244] Liu v. Taiwan Mobile, No. 103-Bei-Hsiao-1360, at reasoning ¶ iii (Taipei Dist. Ct. Oct. 20, 2014) (Taiwan).

[245] Schwartz & Solove, *supra* note 237, at 879.

[246] *See* Fred H. Cate, *Principles for Protecting Privacy*, 22 CATO J. 33, 53-54 (2003) (asserting that health privacy protection should focus on privacy harm, not individual control over health data).

[247] *See* Ohm, *supra* note 127, at 1716-27; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1841-45 (2011).

technology. [248] This represents another issue related to controversies in defining Non-PII.

2. How PII Is Regulated in PDPA and HIPAA Privacy Rule

The PDPA and HIPAA stipulate that both *identified* and *identifiable* data are protected in both laws but fail to differentiate the protection for these two main types of personal data. Not all personal information is subject to equal privacy risk. For instance, it is unreasonable to apply the same privacy rules to an individual's social security number (identified information) and his phone carrier information printed on a phone bill (identifiable information). When personal information is categorized into several types—directly identified, indirectly identified at low costs, indirectly identified at high cost, and non-identifiable—this is an acknowledgement of different privacy harms associated with the respective types of data. The next issue is how to determine the appropriate degree of privacy protection for *identified* information compared to *identifiable* information.

To protect information privacy, the Organization for Economic Co-operation and Development (OECD) declared in the "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data" eight principles, which are known as FIPPs: 1. Collection Limitation Principle;[249] 2. Data Quality Principle;[250] 3. Purpose Specification Principle; [251] 4. Use Limitation

---

[248] *Id.* at 1704 ("reidentification science exposes the underlying promise made by these laws-that anonymization protects privacy-as an empty one, as broken as the technologists' promises. At the very least, lawmakers must reexamine every privacy law, asking whether the power of reidentification and fragility of anonymization have thwarted their original designs.").

[249] Org. for Econ. Co-operation *&* *Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* OECD Doc. C(80)(58)/FINAL, as amended on 11 July 2013 by C(2013)79, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf ("There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.").

[250] *Id*. ("Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.").

[251] *Id*. ("The purposes for which personal data are collected should be

Principle;[252] 5. Security Safeguards Principle;[253] 6. Openness Principle; [254] 7. Individual Participation Principle; [255] 8. Accountability Principle.[256] These eight principles were re-categorized by Professors Schwartz and Solove as follows:

> (1) limits on information use; (2) limits on data collection (also termed "data minimization"); (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date ("data quality principle"); (5) notice, access, and correction rights for the individual; (6) creation of processing systems that the concerned individual can know about and understand (transparent processing systems); and (7) security for personal data.[257]

The FIPPs fail to differentiate rules for identified and identifiable information.[258] This one-size-fits-all approach is likely to impede business development and does not enhance privacy protection. Again, this article adopts the privacy harm-

---

specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.").

[252] *Id*. ("Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.").

[253] *Id*. at 5 ("Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.").

[254] *Id*. ("There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.").

[255] *Id*. ("Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii.at a charge, if any, that is not excessive; iii.in a reasonable manner; and iv.in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.").

[256] *Id*. ("A data controller should be accountable for complying with measures which give effect to the principles stated above.").

[257] Schwartz & Solove, *supra* note 237, at 909.

[258] *See id*.

based approach to review this issue. Unlike *identified* personal data (e.g., social security numbers), *identifiable* personal data (e.g., phone carrier information printed on a phone bill) cannot directly identify a certain person and is not subject to the same risk of privacy harm as identified information. It is therefore unnecessary to impose the full set of FIPPs restrictions on the use of identifiable information in view of the lower privacy risks and to balance the benefits of the free flow of information. With regard to the question of which privacy principles should apply, the point should be that if personal information has a higher likelihood of identifying a person and an individual is subject to a higher risk of privacy harm if such information is improperly used or disclosed, more privacy protection measures should be offered to protect the person's control over his personal data. For example, the use limitation principle or the purpose specification principle, which was devised to ensure that an individual can decide whether and how his data can be used and makes sense in the case of identified personal data, may be relaxed for identifiable information.[259] The reason is that the benefits for a person's control over his personally identifiable information are not as great as they are for his personally identified information.

The Google Flu Trends project is an example that demonstrates the need to lift certain FIPPs restrictions to benefit social welfare through the massive collection and use of personal health data. Google Flu Trends is a project that was launched by Google in 2008 to test the theory that "one might predict the parts of the world suffering from flu outbreaks by watching the symptoms people type into the Google search engine."[260] When launching the project, Google attempted to prove that "it can detect likely flu outbreaks a week or two faster than the physician-reporting surveillance efforts of the Centers for Disease Control and Prevention."[261] Google failed

---

[259] *See id*. at 909-10 (holding a similar opinion).

[260] Paul Ohm, Response, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. ONLINE 339, 341 (2013).

[261] *Id*. at 342 (questioning that the benefits Google claimed might not be real benefits—"Has a traveler ever avoided boarding a plane to a city on a distant coast because of the relative difference in the shading of the oranges between home and destination?" The project's primary mission was to market Google.).

to comply with the informed consent principle and did not offer people the choice to decide whether to trade their health data (i.e., medical symptoms) to help save lives.[262] Google stipulates in its privacy policy that the Google search engine service and the Gmail service collect user information to improve Google services, such as enhancing Google's search results and blocking spam messages. [263] Although the original idea underlying Google's collection of user information was to improve the search engine and electronic email services, the collected data were later used for another purpose: to predict the parts of the world suffering from flu outbreaks. Applying Taiwan's PDPA to the "Google Flu Trends" project, Google would have violated the informed consent and use limitation principle when using personal data for purposes to which the subjects did not agree. The Google Flu Trends project shows that when the data controller violates the informed consent principle, it cannot use personal data in any manner, no matter what types of data it wants to use. If privacy rules can be differentiated depending on the respective types of data, Google might contend that the medical symptoms it has collected, processed and used are identifiable information. Accordingly, the informed consent principle, use limitation principle, purpose specification principle or other individual participation right may not be applicable.

The multi-faceted information privacy theory supports a differentiated privacy protection regime for personally identifiable information. Although it is inevitable that an individual's control over his personal data is reduced to protect other people's rights or to pursue public interests, the individual's privacy right can still be protected from other angles of privacy, such as the secrecy and safety of the personal data. The HIPAA Privacy Rule allows the data controller to use or disclose PHI in research without obtaining the data subject's authorization if such use or disclosure of PHI is conducted with an IRB waiver. Evidently, the data subject has lost his decision-making right when providing his PHI. In the meantime, the remedy to protect the data subject's privacy is to ensure that his data are kept confidential by the data

[262] *See id*. at 339.

[263] *See* Cate, *supra* note 6, at 1794.

controller. It is therefore reasonable that in the IRB's review process, the IRB should ascertain that the data controller has complied with other FIPPs requirements, such as the review of practicability and minimal risk.[264]

3. A Suggested Approach to Regulating Identifiable Health Information in the Use of Medical Research

A possible approach to aid medical research is to lift certain FIPPs restrictions for the data controller to use PII. Medical research requires a substantial volume of personal information. When more efficiency and flexibility are offered to researchers to collect and use personal data without abiding by stringent data use restrictions, certain part of the information privacy right is compromised. The *privacy harm* approach would be helpful to evaluate what types of data and which parts of privacy rights may be compromised in exchange for the benefits to medical research. For example, personally *identifiable* information involves less privacy harm risk than personally *identified* information, and the data use restrictions applicable to personally *identified* information may be lifted in the case of personally *identifiable* information.

Among personally *identifiable* information, health data would require greater privacy protection than other types of *identifiable* information. For an AIDS patient, the exposure of his sensitive health information "can be stigmatizing, and can cause embarrassment, social isolation, and a loss of self-esteem."[265] This situation illustrates that identifiable health information is subject to a higher risk of privacy harm compared to other kinds of identifiable personal information and therefore requires a higher degree of privacy protection. As such, although personally *identifiable* information may be subject to fewer restrictions on data use when compared to personally *identified* information, it should be noted that personally *identifiable health* information requires a higher level of privacy protection than other general identifiable personal information.

Based on the multi-faceted privacy theory and the risk of

---

[264] *See* Gostin, *supra* note 2, at 490.

[265] 45 C.F.R. § 164.514(e)(2) (2015).

harm approach that this article has proposed, FIPPs should be flexible to balance the various conflicting privacy interests and the possible risk of privacy harm. Below is an analysis of one of the FIPPs' widely known principles, the informed consent principle.

According to the HIPAA Privacy Rule, one of the means of using a natural person's data is by obtaining the data subject's consent, which is known as the informed consent principle. The informed consent principle comes at a price; it is costly for the data controller to comply with the informed consent principle. In view of the difficulties for a data controller to obtain subjects' consent, especially when millions of data subjects are involved, the Privacy Rule offers two more alternatives. One is to obtain an IRB's (or privacy board's) waiver after the IRB's review of the research proposal. The other option is to prove that the data at issue are non-identifiable information (Non-PII) and that there is no need to obtain the data subjects' authorization.

The *limited data set* information principle in the Privacy Rule offers another possibility for a data controller to use personal data without an individual's consent. Applying the *limited data set,* it is not mandatory that all eighteen enumerated personal identifiers are removed; personal information such as town or city, state, and zip code, the birth date and month of the data subject may be retained.[266] The disclosure and use of *limited data set* information, compared to other types of identifiable information, is subject to a different set of rules. The covered entities may disclose or use the limited data set information, which is *identifiable* information, without obtaining authorization from the data subjects.[267] In summary, a certain flexibility has been implemented in the Privacy Rule to accommodate the interest of using personal data in medical research.

Although the Privacy Rule does not explicitly offer different requirements for informed consent depending on whether the personal data at issue are personally identified or identifiable information, the *limited data set* principle has

[266] *Id.*

[267] *Id.* at (e)(4)(ii)(C).

inspired such a possibility. Specifically, when establishing the *limited data set* information principle, legislators have observed that there is a higher risk for *limited data set* information to identify a specific person than Non-PII. Given that certain informed consent requirements are exempted, the Privacy Rule requires a higher degree of data security to ensure the secrecy of the data, including requiring the data controller to commit to the safe use of the data and to ensure that it will not take any measures to re-identify the data subjects.[268]

For medical research, it is worth considering whether the widely used key-coded medical data may be exempted from the informed consent requirements while other protections are enhanced. Key-coded medical data are one type of classic identifiable information used in the medical community.[269] In *Tsai,* the NHRI alleged that the health data had been encrypted and stored in the data center in the form of key-coded data. The personal health data were stored in the National Health Insurance Research Database center in the format of key-coded data, which does not directly identify a specific person.[270] Key-coded data, when de-coded, may re-identify a specific person and should be regarded as identifiable Information. Pursuant to the Privacy Rule, the data controller should obtain the data subjects' authorization before it may

---

[268] *See* Schwartz & Solove, *supra* note 237, at 907.

[269] Tsai v. NHIA, FǍ YUÁN FǍLÙ WǍNG (法源法律網) [LAWBANK], No. 102-Su-36 at reasoning ¶ v (Taipei High Admin. Ct. May 14, 2014) (Taiwan) http://www.lawbank.com.tw.

[270] *See* Schwartz & Solove, *supra* note 237, at 909; Suzanne M. Rivera, *Privacy v. Progress: Research Exceptionalism Is Bad Medicine*, 24 HEALTH MATRIX: J. L.-MED. 49, 62 (2014) ("Disqualifying the use of de-identified data originally collected for research purposes unless subjects are re-consented would be a mistake for three reasons. First, it is illogical. How can you obtain consent from people when you do not know their identities? Secondly, not using existing data would require collection of new data, meaning more people than necessary must be studied to answer important questions. This is wasteful (an injustice, with regard to the distribution of limited resources) and unnecessarily exposes more people to the risk of harm (a violation of beneficence). Finally, it seems to ignore common sense. While patients may have no knowledge (outside of the standard HIPAA warning) that their data can be used for research, subjects who previously have consented to participate in research actually know and agreed that their data can be used for science (and presumably would be more agreeable for further study usage).").

provide key-coded data for others in medical research. However, because the risk and possible privacy harm for the key-coded data are relatively low if the data are not re-identified, it is worth reexamining whether it is necessary to apply the informed consent requirements to the key-coded data. It is even worth considering whether it is possible that identifiable information may be exempted from the informed consent principle. Without the difficulty of obtaining the required informed consent, this approach might not increase the risk of privacy harm and might provide enhanced privacy protection. For example, if it is mandatory that the covered entity comply with the informed consent principle before it may disclose key-coded data for others to conduct research, this approach forces the covered entity to re-identify the individuals by transferring the identifiable information to identified information. Without the re-identified data to know who should be informed about the contemplated research, it is not possible for the data controller to obtain the data subjects' consent. The re-identification process itself actually increases the risk of privacy harm.[271]

This article proposes that if information is identifiable, the unnecessary FIPPs that are only essential for an individual's right to make decisions may be relaxed. The remedy of the relaxed restrictions is the enhanced protection of other parts of privacy interests, including the security and secrecy of the personal information. Furthermore, in view of the sensitive nature of health data, a higher degree of privacy protection should be provided. Lifting certain restrictions to facilitate data use for identifiable health information is unlikely to undercut the protection of the privacy of health information while making it possible to uphold the public interest through medical research. It is also true that identifiable health information requires a higher degree of privacy protection compared to other kinds of identifiable personal information. A compromise and a balance check mechanism could require a neutral and professional body to verify that there is a public interest behind the contemplated research and to guard the privacy rights of individuals. It is important that this review

[271] PDPA, *supra* note 17, at § 16(5).

process is intended to ensure that there is public interest for the medical research. This is different from the HIPAA Privacy Rule, in which the use and disclosure of identified/identifiable health information is acceptable with the IRB's (or privacy board's) approval of a waiver of authorization in lieu of the data subject's authorization.

This suggestion may help with the review process of the IRB or privacy board. Pursuant to the Privacy Rule, identified and identifiable health information are subject to the same rules. In other words, in the absence of the data subject's consent, the disclosure and use of identifiable health information for research should comply with the same IRB review process as the process that applies to identified health information. It is inevitable that the IRB will be overloaded, undercutting the efficiency of the review process. Given this situation, this article has proposed that identifiable health information may be subject to a simplified IRB review process so that the data controller may use health data in research as long as the IRB has confirmed that the proposed research is for medical research to pursue public interest.

C. Analysis of *Tsai*

The core issue of *Tsai* relates to the evaluation of the plaintiff's privacy rights in medical research. The defendant NHIA exercised its official duty — performing health care services—when collected citizens' health data, including those of the eight plaintiffs. The NHIA then disclosed and transferred these health data to the NHRI and CCHIA to process the health data to establish a National Health Insurance Research Database center, which is obviously a new purpose other than the one for which the data were collected. The data stored in the data center were accessible by the public upon application. The plaintiffs argued that based on their right to information privacy, the defendant should cease using their personal health data. The plaintiffs further claimed that although the NHIA argued that the data were encrypted and transformed into key-coded data, these data could be de-coded to link to their personal identity.

The HIPAA Privacy Rule does not allow the NHIA to use the plaintiffs' personal data without their consent. Assuming

that the NHIA is the covered entity under the Privacy Rule, the encrypted data at issue did not qualify as non-PII or "limited data set" information because the key-coded information could be used to identify the individuals. Pursuant to the Privacy rule, without the plaintiffs' consent or the IRB's waiver, the data controller cannot disclose or use the health data for medical research. When the NHIA transferred the plaintiffs' health data to the NHRI and CCHIA, no IRB review process was conducted. Given this situation, had the court ruled on *Tsai* pursuant to the Privacy Rule, the defendant would have lost the case.

On the contrary, the Taiwan court ruled in favor of the NHRI because the NHRI qualified for the safe harbor element for the data controller to use personal data without the data subjects' consent. Item 5, Article 16 of the Taiwan PDPA provides that a data controller may use personal data for medical research if and when such data are processed to the extent that they cannot be used to identify a specific person.[272] This is one of the exceptions where the data controller may use personal data without the data subjects' consent. It is evident that this exception should not apply to personally *identified* information. The next issue is whether the NHIA's allegedly encrypted data should be regarded as identifiable information or Non-PII. The plaintiffs alleged the former because encrypted data can be re-identified and claimed that defendant did not enjoy the safe harbor of Non-PII. It is difficult to deny that there is a possibility for *identified* information to be re-identified. Nonetheless, the *privacy harm* approach may come into play to evaluate how such encrypted data should be protected. The encrypted key-coded information, as identifiable information, indicates the likelihood that such information may be used to identify a certain person. However, there is no imminent danger or threat that personal identity will be exposed as soon as the information is disclosed or used. We cannot ignore the fact that the disclosure or use of key-coded information does not result in the same privacy risk as personally identified information. As such, it is unnecessary to

[272] Tsai v. NHIA, FĂ YUÁN FĂLÜ WĂNG (法源法律網) [LAWBANK], No. 102-Su-36 at reasoning ¶ v (Taipei High Admin. Ct. May 14, 2014) (Taiwan), http://www.lawbank.com.tw.

apply the informed consent requirement to key-coded information. This article proposes that a reasonable interpretation of "processed to the extent unable to identify a certain person" in Item 5, Article 16 of the PDPA should include Non-PII and personally *identifiable* information. In other words, it is unnecessary for the data to be processed to the extent that it is "not personally identifiable" to qualify for the exception. Based on this interpretation, the key-coded health information may qualify for the exception of Item 5, Article 16 of the PDPA. Furthermore, with reference with other articles of the PDPA, it makes no sense to limit the Item 5, Article 16 exception to "not personally identifiable" information only. Pursuant to Item 1, Article 2 of the PDPA, "not personally identifiable" information was excluded from the PDPA at the outset. The data controller may freely use "not personally identifiable" information without qualifying for the Item 5, Article 16 exception. In other words, Item 5, Article 16 of the PDPA would be meaningless if it were interpreted to refer to solely to "not personally identifiable" information.

The NHRI argued that the plaintiffs' health data were encrypted and that these data were not personally identifiable and should be exempted from the PDPA.[273] This argument was accepted by the court, which held that the encrypted data were not indirectly or directly identifiable to the plaintiffs. The court also accepted the defendant's argument that Item 5, Article 16 of the PDPA would allow the defendant to use the health data for medical research without the plaintiffs' consent.[274] This article notes that the NHRI, NHIA and the court erred in treating key-coded information as non-identifiable information when they contended and ruled that the defendant may use the data without the plaintiffs' consent.

The analysis in this article leads to the same conclusion that the defendant may use the plaintiffs' health data without their authorization, but the reasoning is different. This article takes the position that to qualify for the exception in Item 5, Article 16 of the PDPA, "personally identifiable information" would suffice. The encrypted health data should be regarded

[273] *Id*. at reasoning ¶ vii.
[274] *Id*. at reasoning ¶ vi.

as identifiable information. Moreover, because the personal data at stake were reused for public interest and the data were processed to the extent that they were not directly identifiable for any specific person, the plaintiffs had no legal standing to object to the defendant's disclosure of their data. If such *identifiable* health information is re-identified to become *identified* health information, the data controller is still bound by the restrictions of the use of *identified* health information, as provided in the IRB review process.[275]

VI. Conclusion

Information technology has played an important role in the evolution of information privacy theory. The recently developed big data technology greatly transformed the way health information is used in medical research. Investments are increasingly made to develop big health data centers, of which the Taiwan National Health Insurance Database center is one example. Traditional privacy theory has fallen short of reconciling privacy conflicts between information privacy and medical research arising from new technologies, and it is time to consider a modified approach to properly address privacy concerns. By analyzing the issues associated with *Tsai,* this article proposed a multi-faceted privacy theory and a harm-based information privacy approach to address the privacy concerns caused by modern technology. With the rapid pace of technological development, privacy theory may need to be modified from time to time. The modified privacy theory proposed in this article may serve as a starting point and basis for future discussion when future technology changes call for further amendments to privacy theory.

[275] *Id*. at reasoning ¶ vi.