The Past, Present, and Future of the Right to Information Privacy: A Comparative Law Perspective

Liu, Ting-Chi*

I. Introduction

Not long ago, big data and the Internet of Things (IoT) had occupied the headlines, and now we are bombarded with advances in Artificial Intelligence (AI). The focus of our attention may be slightly shifted, but there is one thing in common behind all these concepts—they all involve the collection and analysis of huge amounts of data; most of which contains personal data.

These rapid advances in technology have forced us to rethink the right to information privacy, although different nations may reach different conclusions on the best approaches to tackle the problem. In Europe, the General Data Protection Regulation (GDPR),[1] which just went into effect in May, allows the European Union (EU) to set the new global standard for the protection of personal data, creating a ripple effect around the world.

Across the Atlantic Ocean, the opportunities and accompanying risks of big data had once let the Obama Administration review the U.S. patchwork privacy laws and respond with a Consumer Privacy Bill of Rights,[2] which fell far short of being enacted. But just three months ago, the U.S. Supreme Court in a 5-4 decision addressed the "seismic shifts in digital

* Associate Professor, College of Law, National Chengchi University.
[1] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1.
[2] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), *available at* https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf (last visited Aug. 28, 2018).

technology" and held that people can have a reasonable expectation of privacy in their historical cell-site location data, significantly limiting the application of the "third-party doctrine" in the modern era.[3]

It's an all-too- familiar story. The seminal article "The Right to Privacy" mentions the advance in photographic technology and the need for the law to catch up with it.[4] The development of the right to information privacy also closely traces the advent of computers and the internet.[5] Now as we enter the era of big data, IoT, and AI, the desire to process (personal) data is ever-growing, and the alleged benefits and potential risks are both hard to ignore.[6]

In Taiwan, the right to privacy is a relatively new concept. Interestingly, the right to *information* privacy was recognized prior to the right to privacy, by the Computer-processed Personal Data Protection Act of 1995 (CPDPA). Four years later, the Civil Code codified the right to privacy as one of the personality rights. It did not take long for these rights to be elevated and become constitutionally protected basic rights by the Taiwan Constitutional Court in 2004.

This article tries to explore the development of the right to information privacy from a comparative law perspective. Part II traces the past, examining the reason and process that such right took shape. Part III discusses the current status of the right and the challenges it faces. Relevant developments at the international level are also included and compared in this section. Part IV provides some observations and suggestions regarding the future of the right to information privacy and how to best to protect it. This article concludes that we in Taiwan should search for our own approach that can provide adequate protection to an individual's right to information privacy while allowing us to harness the potential benefits of big data, IoT and AI.

II. The past: recognizing a constitutional right to information privacy

In 1890, Samuel D. Warren and Louis Brandeis published the famous article "The Right to Privacy."[7] At that time, the goal was to urge the judiciary to recognize a new common law right, rooted in individuals' inviolate personality, so as to give people an opportunity to be left alone.[8]

In the United States, the right to privacy has gradually gained support in states' tort law.[9] However, at the federal constitution level, there are mixed developments in different aspects of the right to privacy. Decisional privacy, a right to be free from government intervention

---

[3] Carpenter v. United States, 138 S.Ct. 2206 (2018).
[4] *See* Samuel D. Warren Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-96 (1890).
[5] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 22-26 (2004).
[6] *See* e.g., Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, May 2014, *available at* https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf (last visited Aug. 28, 2018).
[7] Warren & Brandeis, *supra* note 4.
[8] *See id*. at 205.
[9] *See* SOLOVE, *supra* note 5, at 57-62.

when making important personal decisions (e.g., procreation, childrearing and sexuality) has been recognized by the U.S. Supreme Court in a series of cases.[10] Similarly, physical/bodily privacy, which protects the solitude of a person, has often been used in search and seizure cases.[11]

But it is not the case for informational privacy, which guarantees a person's right to control his/her personal data. Although the Congress had enacted the Privacy Act in 1974,[12] and the concept of informational privacy had found its way into the High Court's decisions,[13] the right to information privacy has not yet been explicitly accepted by the Court as a constitutional right. In *NASA v. Nelson*,[14] when the respondents challenged that some questions in the employment questionnaires intruded upon their privacy interest in avoiding disclosure of certain personal matters, the Court merely "assume[d] for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance."[15]

In Europe, however, the right to information privacy has a firm constitutional basis. For example, around the same period of time as its U.S. counterpart did, German Congress enacted its federal data protection act in 1977, which prohibits the processing of personal data unless it is required by law or data subjects give their consent.[16] Only six years later, the German Federal Constitutional Court, based on the constitutional provisions which protect human dignity and free development of one's personality, recognized a constitutional right of information self-determination in the famous *Census* case.[17] Such right "compels the State to organize data processing so that personal autonomy will be respected."[18]

Beyond the borders of individual European countries, the Council of Europe adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) in 1981.[19] According to privacy scholar Gloria González Fuster, Convention 108 is significant in three aspects: it moves the concept of data protection "beyond its previously strictly German context," it regards data protection as "rights and fundamental freedoms," and finally, "it articulates a special linkage of data protection with a 'right to privacy'."[20]

Later on, the European Union passed the *Directive 95/46/EC on the Protection of Individuals*

---

[10] *See e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003); Pierce v. Society of Sisters, 268 U.S. 510 (1925); Roe v. Wade, 410 U.S. 113, (1973).
[11] *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 52 (1997).
[12] Pub. L. No. 93-579, 88 Stat. 1896 (1974).
[13] *See* Whalen v. Roe, 429 U. S. 589, 599–600 (1977); Nixon v. Administrator of General Services, 433 U. S. 425, 457 (1977).
[14] 562 U.S. 134 (2011).
[15] Nelson, 562 U.S. at 147.
[16] *See* GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 59-61 (2014).
[17] *See* Paul M. Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 687-92 (1989).
[18] *See id*. at 690.
[19] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T.S. No. 108. *See* Francesca Bignami, *The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts*, 41 CORNELL INT'L L.J. 211, 220-23 (2008).
[20] *See* FUSTER, *supra* note 16, at 88-89.

with regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive).[21] The Directive provided a firm legal foundation for information self-determination across Europe. On the basis of the 1995 Data Protection Directive and various data protection statutes enacted in member countries, the *Charter of Fundamental Rights of the European Union* formally elevated personal data protection to the level of a fundamental right.[22]

It should be noted that this newly recognized right is independent from the traditional right to privacy, which guarantees "everyone…the right to respect for his or her private and family life, home, and communications."[23] The Charter provides a separate provision dedicated to the protection of personal data, prescribing the conditions for processing personal data and affording individuals certain substantive rights, such as a right to access and the right to rectify.[24]

Most importantly, and rather unconventionally, section 3 of said provision specifically states that "compliance with these rules shall be subject to control by an independent authority."[25] The issue of how to effectively protect personal data has itself been constitutionalized. It indicates that a constitutionally mandated organizational design that ensures independent oversight over day-to-day information practices is the key to safeguard personal data.

In Taiwan, personal data protection and the right to (information) privacy only emerged in the late 1990s. The CPDPA was enacted in 1995, which regulated computer-processed personal data within the public as well as certain private sectors. Although concerns about potential harm to individual privacy were one of the reasons for the legislation, the government's focus was really on clearing all the obstacles that might prevent/delay Taiwan from joining the World Trade Organization. According to one senior official, the fear that members of the European Union might take issue with Taiwan's failure to adequately protect personal data is what pushed the CPDPA through the legislative process.[26] As foreign trade was the main motivation of the CPDPA, personal data protection was not set in firm ground at the very beginning. Under-enforcement has become an issue since then.

Four years later, in 1999, the Civil Code was amended to include the right to privacy as one of the personality rights. The right to privacy, therefore, had gained a broader recognition in Taiwan's legal system. However, since the amendment and before the Constitutional Court ruled that the right to privacy is a fundamental right protected by the Constitution in 2004, there were very few cases in the civil courts that seriously discussed the contours of this new right.

Of the 22 civil judgments rendered by the Supreme Court that included the word "privacy"

---

[21] 1995 O.J. L 281/31.
[22] Charter of Fundamental Rights of the European Union, Dec. 7, 2000, 2000 O.J. (C 364) 1, 10.
[23] *Id*. art. 7.
[24] *Id*. art. 8.
[25] *Id*.
[26] *See* Zuo-Guo Liu & Shi-De Lee, GE REN ZI LIAO BAO HU FA SHI YI YU SHI WU: RU HE MIAN LIN GE ZI BAO HU DE HSIN SHI DAI [PERSONAL DATA PROTECTION ACT AND PRACTICE: HOW TO FACE THE NEW ERA OF PERSONAL DATA PROTECTION] 3-4 (2d ed. 2015).

from 1999 to 2004,[27] only one was committed to explaining what the right to privacy was. According to the judgment, the right to privacy is "a right which prevents others from unjustifiably intruding on one's private sphere," and "this personality right is to safeguard human dignity and is indispensable for the pursuit of happiness."[28] The Court, therefore, held that public disclosure of a legislator's home phone and cell phone numbers as well as his home address violated his right to privacy.[29]

The lack of meaningful privacy cases and serious discussion of the contours of the right to privacy in ordinary courts did not prevent the Constitutional Court from constitutionalizing the right in *Interpretation No.585*.[30] In this highly contentious case, the Court held that a law, which established a special commission with broad and rather unconstrained power to investigate the 319 shooting incident, intruded upon a constitutionally protected right to privacy. According to the Court:

> Although the right to privacy is not among those rights enumerated in the Constitution, it should nonetheless be protected under Article 22 of the Constitution in order to preserve human dignity, individuality, and the integrity of personality, as well as to protect the private sphere of an individual's personal life from intrusion and information self-determination.[31]

Due to the nature of the case, mainly regarding the issue of separation of powers, the Court did not elaborate on the exact denotations of the right to privacy.

The Constitutional Court encountered its first major information privacy case in 2005.[32] The issue was whether a then newly added provision in the Household Registration Act, which required applicants for new national identity cards to be fingerprinted, violated the Constitution. The Court explained in detail the meaning of the right of information self-determination, which it first recognized in *Interpretation No.585*. The Court stated:

> Informational self-determination, one aspect of information privacy, guarantees that individuals have a right to determine whether or not, to what extent, at what time, in what manner, and to whom to disclose their personal information. It also affords people a right to know and have control over the use of their personal information, as well as a right to rectify any errors contained therein.[33]

The right to information self-determination incorporates many aspects of the fair information practice principles (such as choice/consent, purpose specification/use limitation, individual

---

[27] These cases are: 88 Tai-Zai Zhi 22, 88 Tai-Shang Zhi 2924, 89 Tai-Shang Zhi 1899, 89 Tai-Shang Zhi 2134, 89 Tai-Shang Zhi 2267, 90 Tai-Shang Zhi 817, 91 Tai-Shang Zhi 202, 91 Tai-Shang Zhi 1495, 92 Tai-Shang Zhi 439, 92 Tai-Shang Zhi 870, 92 Tai-Shang Zhi 906, 92 Tai-Shang Zhi 1507, 92 Tai-Kang Zhi 544, 92 Tai-Shang Zhi 2671, 92 Tai-Shang Zhi 2676, 93 Tai-Shang Zhi 706, 93 Tai-Shang Zhi 1162, 93 Tai-Kang Zhi 558, 93 Tai-Shang Zhi 1681, 93 Tai-Shang Zhi 1805, 93 Tai-Shang Zhi 1979, 93 Tai-Shang Zhi 2014.

[28] 93 Tai-Shang Zhi 1979.

[29] *Id*.

[30] Interpretation No. 585 (Const. Ct., Dec. 15, 2004).

[31] *Id*. at para 25.

[32] Interpretation No. 603 (Const. Ct., Sept. 28, 2005). *See* Chung-Lin Chen, *In Search of a New Approach of Information Privacy Judicial Review: Interpretation No.603 of Taiwan's Constitutional Court as a Guide*, 20 IND. INT'L & COMP. L. REV. 21, 28-33 (2010).

[33] Interpretation No.603, at para 1.

participation), which form the backbone of many countries' data protection laws, including the CPDPA.[34] The focus of the right is to empower individuals, through a set of substantive rights (such as consent, right to access, right to rectify), giving them control over their personal data.

Interpretation No.603 marks one of the high points of the right to privacy in the Court's history. However, for the Constitutional Court, it was an easy case. In support of this massive, nation-wide fingerprinting scheme, the government only asserted several rather weak public interests (such as anti-counterfeiting, preventing false application or fraudulent use of identification cards, and making the identification of unconscious patients found on the streets, persons with dementia who get lost, and unidentified human remains). Relying on the principle of proportionality, the Court quickly dismissed these claims because collecting every citizen's fingerprints was neither the least restrictive means for some purposes, nor can it achieve the asserted interests. In some cases, it was disproportionate to the purposes it pursues.[35]

In other words, the Court was not confronted with a hard case where the government may raise an important or even compelling interest (e.g., anti-terrorism, prevention of crimes, public health) and try to justify the mass collection and/or use of personal data. Indeed, toward the end of *Interpretation No.603*, the Court explicitly left open the possibility for such mass collection and creation of a fingerprint database, subject to purpose specification and use limitation principles as well as other organizational and procedural safeguards.[36]

The Constitutional Court faced another major (information) privacy case in 2011.[37] At issue was the anti-stalking provision of the Social Order Maintenance Act, which was applied to the paparazzi's pursuit of celebrities in public places. The fact that the alleged privacy invasion activities happened on public roads did not prevent the Court from concluding that individuals can still have a reasonable expectation of privacy even in the public sphere where their behavior can be seen by others.[38]

In this case, the Court first articulated the link between information privacy and one's development of his/her personality, stating that "If individuals' private life and social activities have constantly been watched, monitored, eavesdropped or publicly disclosed, they cannot freely speak, act, and interact with others. The free development of their personality will, therefore, be impeded."[39] The Court then expressed its concerns about the erosion of privacy caused by the advance in technology. According to the Court, "recent development of information technology and easy access to all kinds of video/audio recording devices have greatly increased the possibility that individuals' private activities may be watched, monitored, eavesdropped, publicly disclosed, and the need for the protection of individuals' private activities and privacy, thus, has also increased."[40] In response to such circumstance, the Court concluded that "even in the public sphere, a person should, within the scope of

[34] *See* Chen, *supra* note 32, at 39-44.
[35] Interpretation No.603, at para 12.
[36] *Id*. at para 14.
[37] Interpretation No. 689 (Const. Ct., July 29, 2011).
[38] *Id*. at para 7.
[39] *Id*.
[40] *Id*.

social expectation, enjoy the legal protection of the freedom from the intrusion of his/her private sphere and information self-determination by not being constantly watched, monitored, eavesdropped, accessed, etc."[41]

Interpretation No.689 is significant in the evolvement of the right to privacy in Taiwan. It provides a concise but strong theoretical basis on why protection of (information) privacy is necessary in the information society. Moreover, by safeguarding individuals' privacy even in public places, the Constitutional Court makes it very clear that privacy is not equal to secrecy. Even if one's conduct and information have been exposed to the public eye, he/she can still enjoy privacy protection under some circumstances.

It is important to note that in modern society, total secrecy is hard to maintain. We constantly disclose our information to others (friends, employers, service providers, or the general public) and our information is also often being disclosed by other persons.[42] *Interpretation No.689*, therefore, forms a very good starting point for us to think about the issues we face today, such as the right to be forgotten—an issue involving when and how a person can request the erasure of his/her information even though that information is once (lawfully and) publicly available.

In the U.S., EU, and Taiwan, the fate of the right to information privacy is different. Although privacy is not an enumerated right in either the U.S., the German, or the Taiwan Constitution, the constitutional courts in the latter two countries embraced this right without hesitation. How can we explain this divergence?

When comparing the continental Europe and American concepts of privacy, Prof. James Q. Whitman observes that deeper social and political traditions might explain the difference.[43] According to Whitman, the European concept of privacy is founded on "rights to respect and personal dignity,"[44] whereas privacy in America is oriented toward the "values of liberty," which focus on freedom from intrusion by the state.[45] In addition, Europeans are more skeptical about free press and market power; in contrast, Americans believe in free speech and free market.[46] As the right to information privacy is about empowering individuals to control their information, the implications of such right on freedom of expression and the information market may prevent the U.S. courts from accepting it.[47]

Taiwan's experience is unique. On the one hand, the Constitutional Court has long held that our Constitution protects an individual's right to personality, and, on the basis of this right, the Court has recognized a broad range of other unenumerated rights, including the right to information privacy. On the other hand, freedom of expression is also strongly protected by

---

[41] *Id*.
[42] *See* SOLOVE, *supra* note 5, at 43.
[43] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004). *But cf.* Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better Than One Unitary Concept?*, 98 CALIF. L. REV. 1925, 1948-51 (2010).
[44] Whitman, *supra* note 43, at 1161.
[45] *Id*.
[46] *Id*. at 1171 & 1208.
[47] *See e.g.*, Sorrell v. IMS Health Inc., 564 U.S. 552 (2011). *See also* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 880 (2014).

the Constitution Court. A recent example is *Interpretation No.744*, which explicitly recognized the prior restraint doctrine and extended it even to commercial speech.[48]

Two factors may help to explain this result. First, the Constitutional Court's unenumerated rights decisions have been well accepted by the general public in Taiwan. Unlike its U.S. counterpart, the authority and legitimacy of the Court to identify unwritten rights have not been (seriously) questioned. Therefore, the Court is confident in taking a top-down approach by recognizing new constitutional rights even if there are few cases in ordinary courts.

Secondly, although we can trace U.S. influences in the Court's free speech interpretations, when the right to privacy clashes with freedom of expression, the Court does not give the same weight to free speech interests as the U.S. Supreme Court does, and it tries to search for a better balance between the competing interests. The best example also comes from *Interpretation No.689*. In considering which speech should be protected, public concerns and newsworthiness are not the only factors; the Court emphasizes that the Constitution protects only speech on matters of public interests.[49] By carefully screening the protected speech, the Court makes room for the right to information privacy.

III. The present: struggling to find the balance between information privacy and free flow of information

Today, our life depends on all kinds of digital devices (cell phones, smart watches, computers, etc.) that we can hardly live without it. In the era of IoT, even home appliances and our cars are connected to the internet. As a result, we create a huge amount of personal data from dawn to dusk (and even when we are sleeping at night if we wear a smart wrist device).[50] At the same time, traditional databases, which host medical records, household registration records, or tax records are regarded as potential treasure troves for big data analytics.

For companies and researchers, the collection and analysis of such data can provide individualized services, find new treatment for diseases, and train AI for more accurate decisions. For governments around the world, the retention and process of this information are for important purposes, such as anti-terrorism, prevention of crimes, or assisting in making better policies.[51]

The advance in information technology, however, brings new threats to privacy and also challenges the traditional model of protecting the right to information privacy. Take smart phones for example, we carry them wherever we go and the information generated from using these devices is enormous, from service-related data held by the telecommunication carriers to

[48] Interpretation No. 744 (Const. Ct., Jan. 6, 2017). In Central Hudson Gas & Electric Corp. v. Public Service Commission of New York, the U.S. Supreme Court stated that "[w]e have observed that commercial speech is such a sturdy brand of expression that traditional prior restraint doctrine may not apply to it." 447 U.S. 557, 571 n.13 (1980).

[49] *See* Chin-Yi Liu, Wei Der Bu Zu Der Shi Zi 689 [Interpretation No.689: An Unfinished Work], 184 Tai Wan Fa Xue Za Zhi [Taiwan Law Journal] 50, 51-53 (2011).

[50] *See* Article 29 Data Prot. Working Party, Opinion 08/2014 on Recent Developments on the Internet of Things, No. 14/EN, WP 223, 5-9 (Sept 16, 2014), *available at* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (last visited Sept. 10, 2018).

[51] *Cf.* Frederik Zuiderveen Borgesius et al., *Open Data, Privacy, and Fair Information Principles: Toward a Balancing Framework*, 30 BERKELEY TECH. L. J. 2073, 2080-86 (2015).

user-generated content information stored both in the cell phones and cloud servers in remote locations.[52] This information alone can put together a detailed profile about who we are (where we have been, what we think, who our friends are, etc.).[53] Furthermore, in the era of IoT and big data, as personal data is collected by all kinds of devices and the re-use of collected data becomes common practice, whether it is possible to maintain the traditional "notice-consent" model of the right to information self-determination becomes an issue.[54]

In this part, this paper will discuss three examples to illustrate the changes of laws in response to the development of technology as well as the challenges faced by the right to information privacy today.

A. Recognizing the potential threats to information privacy in the U.S.

As mentioned in Part II, in *NASA v. Nelson*, the U.S. Supreme Court rejected to recognize a constitutional right to information privacy. However, it does not mean that the Court is not concerned with the encroachment of technology on individuals' privacy.

In another line of cases involving the Fourth Amendment protection against unreasonable search and seizure, the U.S. Supreme Court seems to have gradually embraced a broader concept of privacy, which has an informational aspect in it. One year after *NASA v. Nelson* was decided, in *United States v. Jones*,[55] the Court unanimously held that installing a GPS tracking device on a vehicle to monitor the vehicle's movement constitutes a search under the Fourth Amendment.[56] However, the Justices were split, 5-4, in the reason of the decision. Justice Scalia's majority opinion relied on the trespass theory (attaching the GPS device to the suspect's car) to find the practice constituted a search.[57]

But Justice Alito's concurrence, which was joined by three other justices, took the reasonable-expectation-of-privacy approach, emphasizing that it is the detailed information revealed by the GPS tracking that deserves Fourth Amendment protection.[58] Distinguishing short-term and long-term surveillance, Alito believed that short-term monitoring of a person's movements on public streets did not impinge expectations of privacy; however, long-term and detailed surveillance is different. According to Alito, "society's expectation has been that law enforcement agents and others…could not…secretly monitor and catalogue every single movement of an individual's car for a very long period."[59]

The distinction makes sense. The aggregation of isolated travel information may let us gain insight into one's life, whether he/she is a religious person, lives a healthy lifestyle, supports a

---

[52] *See generally* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 26-27 (2017).
[53] *See* Carpenter v. United States, 138 S.Ct. 2206 (2018); Riley v. California, 134 S.Ct. 2473 (2014).
[54] *See* Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things*," 3-4 (Nov. 19, 2013), available at http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf (last visited Sept. 10, 2018).
[55] 565 U.S. 400 (2012).
[56] *Id*. at 404 & 429.
[57] *Id*. at 404-07.
[58] *Id*. at 418-19. Justice Sotomayor's concurring opinion supported both the trespass and reasonable expectation of privacy approaches. *Id*. at 413-14.
[59] *Id*. at 430.

particular political group, or has certain medical problems.[60] A rather thorough image of one's personality may be discerned from the long-term GPS tracking information, and therefore, it implicates the constitutionally protected privacy interests.

In addition to *Jones*, the Supreme Court again expressed its worry about the uneven balance between technology advancement and privacy protection. In *Carpenter v. United States*,[61] the Court ruled that people can have a reasonable expectation of privacy on historical cell-site location information (CSLI) generated when they use cell phone services.[62] The government, therefore, needs to apply for a warrant to obtain CSLI, instead of a simple court order under the *Stored Communications Act*, which only requires the government to show the records were "relevant and material to an ongoing investigation."[63]

This decision is significant in two aspects. First, unlike the *Jones* case, historical CSLI is protected even though there is no government trespass involved; the majority relies solely on the reasonable-expectation-of-privacy approach to justify its conclusion. Roberts observed that historical CSLI "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[64]

Secondly, the Court declined to extend the third-party doctrine, meaning that a person cannot have a reasonable expectation of privacy in information voluntarily disclosed to a third party, to CSLI.[65] Emphasizing the "unique nature of cell phone location records,"[66] which is "detailed, encyclopedic, and effortlessly compiled,"[67] the majority opinion held that such records had far greater privacy concerns than those considered in past third-party doctrine cases.[68] Moreover, Roberts rejected the argument that people *voluntarily* disclosed CSLI to their service providers. The indispensable nature of a cell phone in our everyday life gave us no choice but to carry it wherever we go.[69] And the telecommunication system automatically logged a cell-site record "without any affirmative act on the part of the user beyond powering up."[70]

It should be noted that in response to the issues regarding technology and privacy, the U.S. Supreme Court is very cautious. It is aware of the rapid development of technology and avoids laying down broad and general rules. Instead, it prefers to limit its holding to the specific facts of the case, making important decisions one step at a time. The *Carpenter* decision explicitly left the issue of real-time CSLI or other innovative surveillance techniques (such as "tower dump") undecided, and it did not address information collection techniques in the contexts of foreign affairs and national security.[71] As Chief Justice Roberts notes, when

---

[60] *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).
[61] 138 S.Ct. 2206 (2018).
[62] *Id.* at 2219-20.
[63] *Id.* at 2221.
[64] *Id.* at 2217.
[65] *Id.*
[66] *Id.*
[67] *Id.* at 2216.
[68] *Id.* at 2219-20.
[69] *Id.* at 2220.
[70] *Id.*
[71] *Id*.

deciding cases involving new innovations, "the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'"[72]

B. Setting a new world information privacy standard in the EU

In the field of protecting personal data, the EU has been a world leader. At the constitutional level, it recognizes both a right to the protection of personal data as well as a general right to privacy, and these rights have been rigorously enforced. For instance, the Court of Justice of the European Union (CJEU) invalidated Directive 2006/24/EC, which required member states to precautionarily store every person's telecommunications data for at least six months and up to 24 months on the grounds that the Directive's indiscriminate storage requirement was not necessary to achieve its goal of combating serious crimes.[73]

In addition to the fundamental rights, the EU had promulgated the 1995 Data Protection Directive (the predecessor of the GDPR), laying down specific rules to protect personal data. The 1995 Data Protection Directive and related judgments rendered by the CJEU firmly established the right to information self-determination, and they have great influences on the data protection legislations around the world.

However, as Recital 6 of the GDPR states, "[r]apid technological developments and globalization have brought new challenges for the protection of personal data,"[74] the EU was forced to consider whether the existing data protection scheme was still sound in the era of big data and IoT. After several years' in depth discussion, the EU passed the GDPR. In its essence, the GDPR reaffirms the existing "individual control" model of personal data protection by enhancing the notification requirements, laying down the conditions for a valid consent, and affording data subjects with new substantive rights, such as the right to be forgotten and data portability.[75]

To be sure, these new rights are not without controversies. For example, the right to be forgotten had been seen as "precipitat[ing] the Internet Age's most dramatic conflict between European conceptions of privacy and American conceptions of free speech."[76] The concerns are especially acute when such a right applies to truthful information that is already in the public domain. The worries are that by affording this ultimate control to individuals, the right to be forgotten will affect the free flow of information.[77]

On the other hand, some scholars are more optimistic. They view the right to be forgotten as

---

[72] *Id.* (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
[73] *See* Judgment of the Court (Grand Chamber), 8 April 2014 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C- 293/12 and C- 594/12. *See also* ORLA LYNSKEY THE FOUNDATIONS OF EU DATA PROTECTION LAW 161-66 (2015).
[74] 2016 O.J. L 119/2.
[75] *See* Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 632-34 (2013).
[76] Jeffrey Rosen, The Right to Be Forgotten, Atlantic (June 19, 2012), http://www.theatlantic.com/magazine/archive/2012/07/the-right-tobe-forgotten/309044 (last visited Sept. 10, 2018).
[77] *See e.g.*, M. Margaret McKeown, *Challenges and New Frontiers: National Courts as the Frontline International Law*, 32 AM. U. INT'L L. REV. 763, 768-69 (2016).

providing a tool for "digital redemption."[78] At its most abstract form, a common ground exists in different cultures across the globe that under certain circumstances, people deserve a second chance.[79] Indeed, in some scenarios, the right to be forgotten may help to foster free speech. Teenagers can speak freely and not to worry that some ill-advised, stupid and regrettable words/pictures they post on social media pages will come to haunt them in the future. They will have a chance to escape from embarrassing moments of past mistakes and be able to reinvent themselves. Similarly, for victims of revenge porn, a convenient and effective way to decrease accessibility to troubling and uncomfortable pictures will allow them to regain control of their lives, making them more willing to participate in the online world.[80] The right to be forgotten is therefore not a nightmare for free speech advocates; it only requires us to carefully re-weight and re-balance the competing interests.[81]

Beyond substantive rights, organizational and procedural safeguards are the focal point of the GDPR as well. When a type of data processing, especially using new technologies, is likely to have a high risk to data subjects' rights, a data protection impact assessment should be carried out by the data controller.[82] Prior consultation with supervisory authority is also mandatory if the assessment indeed indicates such a high risk.[83]

Furthermore, public authorities and other data controllers who conduct regular and systematic monitoring of data subjects on a large scale or process sensitive data of a large scale should designate a data protection officer (DPO).[84] According to the GDPR, DPOs should have the expertise in data protection laws and practices;[85] they should be independent and armed with enough resources to perform their tasks, which include providing necessary advice and monitoring compliance with the GDPR.[86]

These procedural and organizational safeguards try to shift the burden of protecting personal data from data subjects to data controllers.[87] Instead of requiring individuals to make difficult decisions on whether to allow the processing of their data, data controllers should be responsible for assessing and mitigating the risks as well as justifying their operations. Such

---

[78] MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 9 & 21 (2016).
[79] *See generally* W. Gregory Voss & Céline Castets-Renard*, Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A Study on the Convergence of Norms,* 14 COLO. TECH. L.J. 281 (2016). *See also* Amy Gajda, *Privacy, Press and the Right to be Forgotten in the United States*, 93 WASH. L. REV. 201 (2018).
[80] S*ee* Lillian Edwards, Revenge Porn: *Why the Right to be Forgotten is the Right Remedy*, The Guardian (July 29, 2014), http://www.theguardian.com/technology/2014/jul/29/revenge-porn-right-to-be-forgotten-house-of-lords (last visited Sept. 10, 2018).
[81] *See* JONES, *supra* note 78, at 138.
[82] *See* GDPR, *supra* note 1, art. 35, at 53.
[83] *Id*. art. 36, at 54.
[84] *Id*. art. 37(1), at 55.
[85] *Id*. art. 37(5), at 55.
[86] *Id*. arts. 38 & 39, at 55-56.
[87] *Cf.* Fred H. Cate et. al., Data Protection Principles for the 21st Century: Revising the 1980 OECD Guideline 10 (2014), *available at* http://download.microsoft.com/download/D/F/6/DF6849D9-00D6-4E60-889F-BB74D4CA3CC8/Data-Protection-Principles-for-the-21st-Century.pdf (last visited Sept. 10, 2018) (stating that "The existing focus on notice and consent has tended to shift responsibility for data protection to the data subject; moving away from a focus on data collection and the related notice and consent requirements can shift responsibility for data protection to data users").

measures ease the concerns, under the current individual control model, that individuals lack the motivation and resources to exercise their substantive rights.[88] The preventive nature of these requirements also ensures that data protection issues are properly considered and handled at the earliest stage, helping to avoid downstream harm.

Most importantly, the GDPR has several provisions which are directly in response to the issues raised by big data and with an eye on promoting digital economy. For example, the GDPR creates a concept of pseudonymization, which means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information."[89] Pseudonymization is regarded as a technical measure to protect the rights of the data subjects. Pseudonymized data is still personal data subject to the GDPR;[90] however, if data is pseudonymized, it may be stored for longer periods beyond what is necessary for the purposes for which it was originally collected.[91]

In addition, the GDPR also relaxes the purpose limitation principle, meaning that personal data can only be used for the purposes specified at the time when they are collected.[92] Under the GDPR, if personal data are further processed for certain purposes (e.g., scientific or historical research purposes) and appropriate safeguards are employed (e.g., pseudonymization), it may not be regarded as violating the purpose limitation principle.[93]

These provisions indicate that the EU aims to reconcile the interests of protecting personal data with the need of exploring the value of the same.[94] The fact that the GDPR backs off over long held data protection principles, such as storage limitation and purpose limitation, also indicates that big data analytics and other technology developments do challenge the traditional data protection regime. The individual control model may still have its value, but in the era of big data, IoT, and AI, we also need to search for other possibilities in order to strike a better balance between privacy protection and the use of personal data.

C. Struggling with "old" laws and new technology in Taiwan

In recent years, Taiwan's PDPA had been updated twice. Unfortunately, the development of new information technologies, such as big data, IoT, or AI, had not been taken into account during the legislative process. At the same time, the government made the pursuit of a digital economy a priority. Different open data and big data projects have been successively carried out. How to implement the right to information self-determination specified in *Interpretation No.603* in the era of big data becomes a thorny issue. The dispute over the use of (personal) information generated from the National Health Insurance program is a good example.

At the risk of oversimplifying the fact of the case, the National Health Insurance Administration (NHIA) has collected over twenty year's worth of medical records of

---

88 *See e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885 (2013).
89 *See* GDPR, *supra* note 1, art. 4(5), at 33.
90 *See* GDPR, *supra* note 1, recital 26, at 5.
91 *See* GDPR, *supra* note 1, art. 5, at 36.
92 *Id*. at 35
93 *Id*.
94 *See* Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, 17 COLUM. SCI. & TECH. L. REV. 315, 323 & 329-31 (2016).

everyone in Taiwan during the course of implementing the mandatory National Health Insurance program. In recent years, the NHIA has transferred these records to its supervisory agency, the Ministry of Health and Welfare (MHW), which, combining these records with other health and welfare related information, establishes a health and welfare information database.[95] The MHW then encrypts these records and, through an application and review process, allows eligible government agencies and research institutions to use these encrypted data to conduct scientific research.[96]

The Taiwan Association for Human Rights (TAHR) believes that such use of the records is against the PDPA and impinges upon the constitutionally protected right to information self-determination on several grounds. It claims that both the NHIA and the MHW are beyond their statutory authority to transfer such data or establish the database.[97] The TAHR also contends that the encryption method employed by the MHW is not sufficiently secured and that an individual data subject might still be identified from the encrypted data set, which does not meet the requirement of the PDPA for using collected data beyond their original purpose.[98] Lastly, the TAHR claims that in order to respect individuals' right to information self-determination, the NHIA and the MHW should permit persons who are against such use to opt-out.[99]

Both the Taipei Administrative High Court and the Supreme Administrative Court sided with the government, holding that the NHIA's and the MHW's organizational statutes, which empower these agencies to promote public health, can be the legal basis to process these records.[100] Moreover, both courts were satisfied with the level of protection provided by the encryption method used by the NHW, even though the Supreme Administrative Court correctly pointed out that the encryption is reversible.[101] Finally, both courts rejected the contention that individuals should have the right to opt-out under such circumstance because the PDPA did not explicitly afford this right.[102]

Putting aside the soundness of the courts' reasoning, this case vividly illustrates the challenges faced by the traditional data protection regime in the era of big data. When the public interests are important enough (e.g., medical research, public health), the temptation for allowing the processing the personal data will be very high. The balance is easily tipped to the interests of the public at large when the other side of the scale is an individual's subjective privacy interest.[103]

Moreover, current laws allow the NHIA and the MHW to use these records without formal

---

[95] Supreme Administrative Court, 106-Pan-54 (Jan 25, 2017). For a detailed account of the case, *see* Chen-Hung Chang, *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)*, 28 PACE INT'L L. REV. 27, 37-40 (2016).
[96] Supreme Administrative Court, 106-Pan-54.
[97] *Id*.
[98] *Id*.
[99] *Id*.
[100] Taipei Administrative High Court, 103-Su-Geng-Yi-120 (May 19, 2016); Supreme Administrative Court, 106-Pan-54.
[101] 103-Su-Geng-Yi-120, at reasoning ¶ (7); 106-Pan-54, at reasoning ¶ 2(2).
[102] 103-Su-Geng-Yi-120, at reasoning ¶ (8); 106-Pan-54, at reasoning ¶ 2(2).
[103] *Cf*. Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 345 (2008).

privacy risk assessment, and the transparency of the practice is also an issue. Under the PDPA, individuals need to actively exercise their right to access in order to find the details, and they may then use their right to object to stop the data processing. However, the practice may already cause damage to individuals' information privacy. Data subjects are just closing the stable door after the horse has bolted.

Thirdly, the traditional "individualized notice/consent" scheme may be a poor fit for big data analytics. By its very nature, big data analytics involve unintended secondary use, which is not foreseen at the time of data collection. The volume of data involved may prevent the data controllers to seek individualized consent.[104]

In the past, data anonymization was a way to protect data subjects and allow further uses of data without consent. By completely severing the link between data and the data subject, data anonymization ensures that subsequent use of anonymized data will not cause any harm on the original data subject. However, the advance in information technology has made data anonymization more and more difficult.[105] Big data analytics' ability to find hidden correlations of data also hold true for re-identification of anonymized data. If the risks of re-identification cannot be ruled out, should a right to opt-out be recognized as a safeguard?

Lastly, modern information privacy issues often involve complicated technical questions, such as encryption, de-identification, and the risk of re-identification. Whether the administrative courts have the relevant expertise to decide such matter is highly questionable.

Unfortunately, current laws may not provide us with satisfactory answers to all of the questions mentioned above. How should the right to information privacy adapt to the era of big data, IoT and AI? This paper will outline some suggestions in the next part.

IV. The future of the right to information privacy in Taiwan

Two factors make the traditional human right protection paradigm, which emphasizes substantive rights and post-hoc remedies, difficult to apply to the right to information privacy. First, the constant change of technology has made the right to information privacy hard to grasp. The right is developed in response to the changes of information technology and the threats to one's personality. However, information technology evolves so quickly that a rigid substantive right approach can hardly catch up with it.

Take the core concept of information privacy, the meaning of personal data, as an example. The type of data that can be regarded as identifiable to a particular person is constantly changing. It is determined not only by data anonymization technology but also re-identification technology. Most of the time, there is no black and white answer to the question; as privacy scholars Denial Solove and Paul Schwartz aptly describe: the key to think about personally identifiable information is the risk level of identification, and the concept of

[104] *See* Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 73-74 (2016).
[105] *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 708-09 (2016).

identifiability is "a continuum of risk rather than [] a simple dichotomy."[106]

Secondly, in today's digital world, the sheer volume of personal data collected and processed by both the public and private sectors is unfathomable, which makes it impossible for individuals to monitor all the information practices and take appropriate (legal) actions accordingly.[107]

To compound the problem, questionable information practices often happen behind the scenes since personal data can be easily collected, processed and shared in secret. Therefore, individuals may not be aware of them. In addition, even if people do notice the potentially unlawful practices, information privacy harms are typically non-tangible and often involve uncertain future risks, which may not be worth the trouble to bring formal legal action against the wrongdoers.[108]

Due to these problems, a new paradigm may be warranted to protect the right to information privacy in the future. This paper discusses some of the possibilities below.

A. A constitutionally-mandated independent supervisory mechanism

First, to effectively safeguard the right to information, a constitutionally-mandated independent supervisory mechanism must be in place.[109] The Charter of Fundamental Rights of the European Union has embraced this idea, and Section 3, Article 8 specifies that "[c]ompliance with these rules shall be subject to control by an independent authority." Indeed, there are good reasons for this provision.

As mentioned above, due to the special characteristics of information privacy harms (covert intrusion and non-tangible, uncertain future harms), we can hardly expect people to take action to protect their rights. In addition, the government itself is the single biggest personal data holder, often initiating different data sharing and open data projects, and entrusting the supervisory role to ordinary administrative agencies may not be a feasible and realistic choice. In fact, from Taiwan's own experience, the under-enforcement of the CPDPA and PDPA, has fully illustrated the shortcomings of letting agencies police their own information practices.

Therefore, the constitution should require the establishment of an independent supervisory mechanism, possibly an independent data protection agency (board). This agency should be free from executive control and be tasked with overseeing the implementation of the PDPA in both the public and private sectors.

In the past, the Constitutional Court has not imposed this kind of obligation on the legislature. However, from the Court's existing interpretations, such an obligation may not be so far-fetched. In *Interpretation No.603*, the Court has recognized that "*organizational* and

---

[106] Paul M. Schwartz & Denial J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1879 (2011).
[107] *See* Allen, *supra* not 104, at 73-74.
[108] *Cf.* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 7754-56 (2018); Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361-62 (2014).
[109] *Cf.* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 565 (1995) (stating that "independent monitoring of information processing is necessary. Such an institution of data protection oversight plays three critical roles").

procedural safeguards" are important in order to protect personal data.[110] True, the organizational safeguards mentioned above are limited in scope; it's an obligation imposed on a particular data controller regarding the personal data it collected. Nevertheless, it clearly demonstrates that proper organizational arrangement is key to the protection of information privacy.

Another decision of the Court, *Interpretation No.613*,[111] is also illuminating here. The decision is concerning communication freedom. The court emphasizes that

> the meaning of the constitutionally-protected freedom of communications is not limited to passively prevent the intrusion from public authority. It also imposes an affirmative obligation on the legislature to enact various *organizational*, procedural, and substance laws so as to avert information monopoly and ensure society's diversified opinions can be voiced out and distributed through communication platforms, creating a free zone of public discourse.[112]

In the era of big data, both public and private sectors routinely process vast amounts of personal data. Some of the information practices are necessary and legitimate, but others are not. As government agencies and companies alike rely on personal data to fulfill their functions, passively preventing all the parties from processing our data is not a feasible option. What we need is a properly designed organization that can proactively monitor these information practices and provide necessary guidelines. This organization will ensure the creation of a trusted atmosphere where we can harness the benefits of processing personal data while respecting individuals' right to information privacy. Similar to *Interpretation No.613*, the Court should declare that the legislature has a constitutional duty to protect information privacy through an appropriate organizational design.

B. Establishing data protection due process

Currently, the right to information privacy emphasizes empowering individuals by providing a set of substantive rights to data subjects. For example, in *Interpretation No.603*, the Constitutional Court declares that information privacy guarantees "individuals have a right to determine whether or not, to what extent, at what time, in what manner, and to whom to disclose their personal information; it also affords people a right to know and have control over the use of their personal information, as well as a right to rectify any errors contained therein."[113]

However, many information practices happen without the knowledge of the data subjects. Relying on data subjects to actively assert their right to know in every occasion is not practical. Furthermore, current information privacy issues often involve complex technical problems and difficult interest balancing. Under such circumstances, to require an individual data subject, who lacks the relevant expertise, to meaningfully exercise his/herright is both unrealistic and unfair.

---

[110] Interpretation No.603, at para 14.
[111] Interpretation No. 613 (Const. Ct., July 21, 2006).
[112] *Id*. at para 4.
[113] Interpretation No.603, at para 8.

Therefore, requiring data controllers' to actively inform individuals concerned as well as the general public, and give them an opportunity to participate when important information policies are taking shape is crucial.[114] It will not only shift the burden of justifying the legality of the information practice to those who need to process personal data, but it will also allow data subjects as well as outside experts to meaningfully examine the relevant issues.

It should be noted that openness and individual participation are traditional data protection principles. Currently, however, these principles are more passive or abstract. According to the OECD privacy guidelines, it only affords data subjects some substantive rights (such as right the make inquiries, right to access, and right to rectify or erasure) and requires a "general policy of openness about developments, practices and policies with respect to personal data."[115]

In contrast, the concept of data protection due process focuses on procedural rights.[116] It will impose a constitutional-based notification obligation on those who wish to engage in important or major information practices (such as those involving large-scale or sensitive personal data). It will provide data subjects and the general public with a right to be heard; in some instances, a written/paper hearing may suffice, but other instances may require a formal oral evidentiary hearing where issues like anonymization, pseudonymization, re-identification or the asserted public interests can be carefully scrutinized.

Recent interpretations of the Constitutional Court indicate that the justices embrace procedural due process in order to protect substantive rights, at least in cases regarding property rights. In *Interpretation No.763*,[117] an eminent domain case, the Court imposed a constitutional obligation on the government to notify the original property owners regarding the status of the property after the title of the property is transferred to the government so as to allow them to exercise the right to purchase back their lands.[118] In *Interpretation No.709*,[119] a case concerning the constitutionality of several provisions of the Urban Renewal Act, in addition to holding that interested parties have a right to receive necessary information, the Court declared that a formal hearing is required by the Constitution before the government can make important urban renewal decisions.[120]

Information privacy cases share similar characteristics of the property rights cases mentioned above. Like the original property owners in the eminent domain case, data subjects seldom have knowledge regarding how their personal data is processed. How can we expect them to exercise their substantive right? In addition, some information practices do involve important public interests but at the same time may affect the right to information privacy of a large number of people. A constitutionally-mandated hearing, which allows data subjects and/or the

---

[114] *See* Milda MaCenaite, *The "Riskification" of European Data Protection Law through a Two-Fold Shift*, 8 EUR. J. RISK REG. 506, 530-32 (2017).
[115] Organization for Economic Co-Operation and Development, Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80) 58 Final (Oct. 1, 1980).
[116] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 124-28 (2014).
[117] Interpretation No. 763 (Const. Ct., May 4, 2018).
[118] *Id*. at para 4.
[119] Interpretation No. 709 (Const. Ct., Apr. 26, 2013).
[120] *Id*. at para 4.

general public to participate, will not only ensure that the information practice can indeed achieve asserted public interests and comply with relevant laws but also help to form a consensus and increase the acceptance of such information practice.

C. Leaving enough room for the legislature and ordinary courts to develop new information privacy norms

Information technology is constantly changing. An entrenched and rigid constitutional right will forbid the legislature to develop information privacy norms in order to adapt to such changes and strike a proper balance between competing interests. Moreover, information privacy issues are highly contextualized and so should the statutes governing these issues.[121]

Some categories of personal data may require different sets of rules. For example, in the EU, personal data generated in the context of providing electronic communications is subject to the regulation of a separate directive.[122] Moreover, the purpose of processing may also be determinative. Law enforcement, national security, and medical research purposes, to name a few, may warrant tailor-made data protection norms in order to accommodate the complex interest-balancing in those special contexts.

Therefore, the constitutional right to information privacy should leave enough room for the legislature to fine-tune data protection laws in different contexts if needed. Taking individual consent as an example, although consent is the backbone of information self-determination, the form of consent (e.g., opt-in or opt-out consent) should not be constitutionalized. If consent is indeed necessary in a given context, legislature should be able to determine whether opt-in or opt-out or a mixed option is the best approach. The Court should generally respect the legislative discretion in this regard.

Similarly, the constitutional court may wish to take a "wait-and-see" approach on recently recognized information privacy rights, such as the right to be forgotten and right to data portability. The Court should not hastily accept these rights as fundamental rights protected by the Constitution. The legislature may be in a better position to assess relevant factors, including the development of information technology, and determine whether and how to establish these rights on the statutory level. Ordinary courts and certain administrative agencies with relevant expertise may play an important role as well.

Take the right to be forgotten as an example, relying on existing laws, such as articles 18 and 195 of the Civil Code as well as the right to erasure of the PDPA, ordinary courts may decide, on a case-by-case basis, whether to require data controllers to remove personal data in a given context.[123] These courts routinely handle disputes involving conflict between freedom of

---

[121] *Cf.* Schwartz & Solove, *supra* note 106, at 1880 (stating that "no single information privacy statute contains all [fair information practice] principles in the same fashion or form. The precise content of the resulting obligations will often differ based on the context of data processing, the nature of the information collected, and the specific legislative, regulatory, organizational environment in which the rules are formulated.")

[122] Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications), 2002 OJ (L 201) 37.

[123] *Cf.* Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to the Forgotten, and the Construction of the Public Sphere*, 67 Duke L.J. 981, 1057-61 (2018) (discussing the application of the tort liability of public disclosure of private facts as a means to realize the right to be forgotten).

expression and right to privacy. There are good reasons to believe that they are capable of striking an appropriate balance among competing interests in accordance with specific facts of the case.

The approach proposed above will ensure we have a better understanding of the impact of these new information privacy rights on relevant parties and the development of information technology. The one-case-at-a-time/trial-and-error method allows us to carefully evaluate the benefits and costs of these new rights and reach a solution that is best for our own needs and legal culture.

V. Conclusion

Information technology is evolving, and so should be a right that is developed in response to the threats caused by such technology. In the past, Taiwan had recognized a broad constitutional right to information privacy, emphasizing individuals' control over their information. However, the traditional approach has its limitations. We should learn from local experiences of implementing CPDPA and PDPA over the past twenty years. When facing the challenges caused by big data, IoT, and AI, Taiwan should strive to find a suitable approach that can effectively protect individuals' rights to information privacy while allowing the people to harness the potential benefits of advancements in technology.

資訊隱私權的過去、現在與未來—比較法的觀點

劉定基*

中文摘要

在不久之前，大數據及物聯網才佔據各大頭條，現在人工智慧的議題又充斥媒體版面。我們關注的焦點或許稍有不同，但在這些概念背後其實有其共通之處—均涉及大量資料的蒐集與分析，而這其中，絕大多數的資料都屬於個人資料。

這些快速發展的科技迫使我們必須重新思考資訊隱私權的意義與內涵，縱然不同國家對於解決問題的最佳方法可能有不同的結論。在歐洲，於今年五月正式生效的「一般資料保護規則」，使歐盟得以制定新的個人資料保護國際標準，並在全球引起漣漪效應。

而在大西洋的彼端，大數據所帶來的風險與機會，也一度讓歐巴馬政府重新審視美國散見在各個領域的隱私規範，並提出整合性的「消費者隱私權利法案」，可惜該法案最後並未成功完成立法程序。然而，就在三個月前，美國聯邦最高法院以 5 比 4 的票數，處理了一項被多數意見認為涉及「數位科技巨大變動」的案件，認定人民對其行動通信基地台的歷史位置紀錄擁有合理的隱私期待，大幅限縮了所謂「第三方原則」的適用範圍。

上述一系列的發展，其實一點都不陌生。在具有深遠影響力的「隱私權」一文中，就提及了攝影技術的進步使得法律必須跟隨改變；相同地，資訊隱私權概念的提出也與電腦及網際網路的發展亦步亦趨。在進入大數

* 國立政治大學法學院副教授

據、物聯網與人工智慧的時代，人們對於利用（個人）資料的渴求不斷地成長，然而，這其中所潛藏的利益與風險，也值得我們重視。

在臺灣，隱私權相對而言是較新穎的概念。有趣的是，資訊隱私權因1995 年制定的「電腦處理個人資料保護法」，而先隱私權一步被承認；四年之後民法的修正，才正式將隱私權納為人格權的一環；而在 2004 年，臺灣司法院大法官更進一步將這些權利提升為憲法基本權利。

本文嘗試探究資訊隱私權發展的進程。第二部分首先追溯過往，檢視此一權利形成的理由及過程；第三部分則討論此一權利現在的內涵與所面臨的挑戰；第四部分則就資訊隱私權的未來發展及保障問題，提出本文的觀察與建議。最後，本文認為臺灣應在兼顧實現大數據、物聯網及人工智慧潛在利益，以及保障個人資訊隱私權的前提下，設法在法律上走出自己的路。