Digital Development and Privacy: Is There a Way to Alleviate the Uneasy Tension?[*]

Wen-Tsong Chiou[**]

Contents

[*] 本文曾發表於2021法務部司法官學院線上國際研討會（2021年7月6日）。
中央研究院法律學研究所於2004年設立籌備處起，即以「科技發展與法律規範」作為其六大研究方向之一，而資訊法原即為「科技發展與法律規範」之研究範疇。隨著近年來資訊技術與資料科學的急速演進與發展，數位革命對社會帶來的衝擊既深且廣，更具有相當的急迫性。法律所於2016年底開始籌劃設立資訊法中心，並於2019年7月正式成立運作。資訊法中心一方面藉由與資訊科技及資料科學界的跨領域、跨學門合作對話，期能於資訊法研究的上游，在科學技術發展之始，即參與其目標與價值之論辯與設定；另一方面則藉由將傳統資訊法學術研究成果進一步轉譯為更貼近現實的政策語言，期能在資訊法研究的下游，更具體與實際地影響相關法政策之制訂與執行。時值法律所成立十週年之際，僅以數位發展與隱私一文誌之。

[**] Research Professor and Director of Information Law Center, Institutum Iurisprudentiae, Academia Sinica.

Online: http://publication.iias.sinica.edu.tw/91717012.pdf.

I. Digital Development: From a Technology-Oriented Project to the Building of a Data-Driven World

The rapid advance of information and communication technologies has revolutionized the society as a whole, including the way a state governs and how people interact with each other. While the degree of digital development is often measured by the coverage and accessibility of digital technologies and services in a given society,[1] the vision is not just to use and apply technology and digital tools for development (ICT4D) but to build a global network society in which information is strategically used to drive development.[2] In this way, not only are new business models formed and government decisions made through the use of digital technologies,[3] but values in the new economy are created and intelligent insights for governing purposes are informed by as much data as cutting-edge information technologies and analytic tools are now able to process effortlessly. The quest for a data-driven economy and data-driven governance begets growing hunger for data. It is against this backdrop that whether and how data should be collected and analyzed, normative questions rather than a purely technical matter, come to the fore in discussions about how digital development can be further realized.

Taiwan launched its first e-Government program in 1998 with a mission to set up a government internet infrastructure and the integration of its information systems to enable electronic exchange of data within the government.[4] Service-oriented elements were later added to the e-Government

---

1 INTERNATIONAL TELECOMMUNICATION UNION, MEASURING DIGITAL DEVELOPMENT: FACTS AND FIGURES 2020 (2020).

2 Jonathan Donner, *Keynote Remarks at the USAID Digital Development Forum: A Vision of Digital Development in 2028*, CARIBOU DIGITAL (Mar. 10, 2018), https://medium.com/caribou-digital/a-vision-of-digital-development-in-2028-43c8ff3c69e.

3 United Nation Conference on Trade and Development (UNCTAD), Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries (Sept. 4, 2019), https://unctad.org/system/files/official-document/der2019_en.pdf.

4 *See* RESEARCH, DEVELOPMENT AND EVALUATION COMMISSION OF EXECUTIVE YUAN, MID-RANGE PLAN FOR ELECTRONIC AND NETWORKED GOVERNMENT (1997).

infrastructure to provide electronic versions of government services in the second and the third phases of the e-Government program. Up to this point, digital development was only a tool for the government to do its usual business and provide existing services in a more expedient way. In 2016, Taiwan's "Digital Nation, Innovative Economy Development Plan (DIGI^{+}) 2017-2025" began to adopt a more comprehensive concept of digital transformation with an emphasis on a data-driven "innovative economy and digital governance." Enshrining the vision of crafting a "digital nation and smart island," DIGI^{+} put forth all sorts of policies and programs that can be fully realized only if large-scale data can be made available for analysis to generate insights for smarter governance and innovation, which ultimately contributes to higher economic growth.[5]

We have seen just in recent years that consumer behaviors and preferences revealed by past consumption records have become the Holy Grail for all sorts of companies. Businesses are looking for ways to create value by targeting the right customers for their products and services or developing new products or services to meet the needs of a niche market. As people are now well aware of social networking sites collecting "like and share" patterns of their users to produce filter bubbles, private vendors also clandestinely attach tags to websites that each user browses to create persona profiles for precision marketing. Smart meters are installed by the power company to record different users' electricity usage habits in order to arrange a more energy efficient power grid. These are but a few real-world examples of how data can generate more value in the economy. Under the DIGI^{+} plan and the following Smart Government 2.0 programs, the "data rush" seen in the private sector has also become a trendy fashion in the government's digital development strategies. Government policy and decision making, such as traffic management, prevention and response to disasters, crime control, allocation of

5 *See* NATIONAL DEVELOPMENT COUNCIL, SERVICE-BASED SMART GOVERNMENT PLAN: THE FIFTH PHASE OF E-GOVERNMENT PROGRAM (2018).

healthcare resources, and methods to combat wealth inequality, are expected to be sensibly informed by data already collected by the government. The government is also actively involved in "making data available for secondary uses" in roughly three ways: first, making government collected data available for private sector; second, making use of data collected by private sector for allegedly public purposes; third, creating more data for future uses.

II. Making Government-Collected Data Available for Value-Added Secondary Uses

As government is the single most active data collector in a modern society, those who consider data to be the driving force of the new economy naturally look to government databases for gold mining opportunities. For example, retailers are asking for government-held demographic and public transportation data, to identify the best new store locations; real estate agencies use fuzzy transaction price data released by the Ministry of the Interior to develop price prediction algorithms based on types and locations of properties. However, pressure to open government data for value-added secondary uses is not limited to aggregate or statistical data. Microdata that contain much more detailed information about individuals are the real trophy for both profit-seeking entrepreneurs and curious researchers. Under the banner of inclusive financing, Fintech start-up companies have already tried hard to gain access to individual credit information. They expect to use credit reporting data, which can only be collected by the government-approved Joint Credit Information Center (JCIC) and be shared among its member institutions, as a stepping stone to compete with traditional big commercial banks by introducing specific financial products and services to people with particular risk profiles. Individual health records statutorily required to be collected by the National Health Insurance Administration (NHIA) for insurance claim review are now considered by many to be treasure that should be open for exploration with big data analytic tools for either academic or commercial purposes. However, the

ways in which Taiwan's government handles demands for access to individual credit information and health insurance records of the entire population represent two very different models of data sharing to pursue digital development.

A. Model 1: Autonomy-based Approach

Despite the fact that individual credit information is currently open only to financial institutions that are tightly regulated and that no such regulation yet applies to Fintech companies, the government seems to be willing to give the green light to unregulated novel uses subject to each individual's consent. The rhetoric of the data subject's autonomy compliments coincidentally the policy goal of promoting digital transformation in finance.[6] Similarly, people who use a private service that requires submitting certain personal information now can authorize the transmission of their data to the service provider from a government database via the MyData platform, a digital service portal sponsored by the Taiwan government. Thus, an applicant for a personal loan can authorize the provision of his or her own income tax data as proof of earnings directly from the National Taxation Bureau to the bank.

Touted as "secured data transaction based on voluntary consent," the autonomy-based approach to data sharing has been welcomed and promoted as an important tool for digital development.[7] However, Taiwan's government seems to allow this approach so far only for cases that involve individuals making secondary uses of their own data. When the scenario comes to the third-party uses of large-scale data that involve a huge number of data subjects, the government may think that the costs of an autonomy-based approach would be too daunting.

---

6 FINANCIAL SUPERVISORY COMMISSION, FINTECH DEVELOPMENT ROADMAP (Aug. 27, 2020), https://www.fsc.gov.tw/userfiles/file/FinTech%20Development%20Roadmap.pdf.

7 NATIONAL DEVELOPMENT COUNCIL, ABOUT MYDATA, https://mydata.nat.gov.tw/sp/about (last visited July 12, 2021).

B. Model 2: De-identification Approach

As the rhetoric of autonomy is deemed inappropriate for governance of large-scale secondary data uses, a model that relies instead on means of de-identification has become more dominant. In the case of National Health Insurance (NHI) data, for example, not only was consent not sought before health data belonging to individuals were put to secondary uses, but the government also rejected, primarily on the ground that pseudonyms have been used to prevent disclosure of direct identifiers, data subjects' requests to cease processing their NHI data for unspecified secondary research uses. As the pseudonyms, which remain universally unique identifiers scrambled from national identity numbers, still allow data belonging to a specific person within the NHI database to be linked among different datasets and to other databases, the risk of indirect identification is never completely ruled out. It is therefore highly questionable that unconditionally depriving data subjects of autonomy over their health data would be in compliance with the constitutional principle of proportionality, especially when what the data subjects claimed is merely a right of *ex post* opt-out. Other examples of pseudonymized but potentially linkable microdata in government databases, which are also made available for secondary uses without consent or prior knowledge of data subjects, include at least household income tax, electronic toll collection data, registry of motor vehicles, and education records.[8] Sharing of microdata in this manner allows researchers to explore whether there is any hidden link between, say, performance in past education and current earnings, or commuting routes and car types. It nevertheless threatens to allow production or reconstruction of personal profiles and thus touches exactly on the core of the right to "privacy as independence".

---

8 Zong-Shi Liu, *Introduction to the Promotion of Using Government Data for Big Data Analysis*, 341 GOVERNMENT INFORMATION BULLETIN 1, 1-9 (2016)（in Mandarin：公務機關巨量資料分析應用推動簡介）。

C. Yet Another Paradigm Shift: Empowerment Approach

While the resolution of the legal issue regarding the scope of individual autonomy over data is currently pending in Taiwan's Constitutional Court, a paradigm shift from relying upon a convenient but elusive standard of de-identification as a proper legal ground for secondary data uses to enlisting the power of information technology or institutional arrangements to better assist with individual control over personal data has been witnessed in many places elsewhere in the world.

As early as 2008, the concept of "dynamic consent" (DC) has been proposed in the context of biobanking. As a new approach for consent, DC allows individuals to revisit and review consent decisions and preferences over time, as and when they choose, by drawing on digital technologies to support and enhance an ongoing relationship between researchers and participants.[9] Later, the concept of "meta consent," which also rely on modern information technologies to empower individual control over future data uses, extends the scope of application to all kinds of data, new or old, and beyond the context of biomedical research.[10] In addition to technological solutions, new social institutions also contribute to the paradigm change in data governance. For example, California's Consumer Privacy Act (CCPA) explicitly recognizes the right to opt out of the sale of individuals' personal information. It also strongly supports the technical standard of user-enabled global privacy control (GPC) to help online consumers exercise their rights.[11] Data subjects in Switzerland can

---

9 ENCORE — ENSURING CONSENT AND REVOCATION: THE ENCORE PROJECT, http://www.hpl.hp.com/breweb/encoreproject/index.html (last visited July 9, 2021); Jane Kaye et al., *Dynamic Consent: A Patient Interface for Twenty-first Century Research Networks*, 23 EUR. J. HUM. GENET. 141, 141-46 (2015); Harriet J. A. Teare, Megan Prictor & Jane Kaye, *Reflections on Dynamic Consent in Biomedical Research: The Story So Far*, 29 EUR. J. HUM. GENET. 649, 649-56 (2021).

10 Thomas Ploug & Søren Holm, *Meta Consent — A Flexible Solution to the Problem of Secondary Use of Health Data*, 30(9) BIOETHICS 721, 721-32 (2016).

11 GLOBAL PRIVACY CONTROL, https://globalprivacycontrol.org/#about (last visited July 9, 2021).

join MiData, a data cooperative, and entrust it to manage secondary uses of their data in accordance with their preferences. Japan's "Databank" similarly plays a dual role of a data chamberlain commissioned by data subjects and a database manager which provides data for secondary uses.

All of the above examples share a common goal: to reduce transaction costs for data subjects in exercising their rights. Costs for communicating with data subjects and ascertaining their preferences are no longer an obstacle or excuse for taking an easy path of de-identification that results in denying individual autonomy. More importantly, the new paradigm of data governance contributes to laying a trustworthy foundation for digital development. Overlooking this paradigm shift would be a costly mistake and would frustrate the ideal of building a data-driven world that continues to respect human rights and democratic value.

III. Government Making Use of Data Collected by Private Sector

In addition to making government collected data available for private secondary uses, Taiwan's government is also engaged in making use of data originally collected by private sector for allegedly public purposes. The requisition of data by the government is usually made in the name of public interest and is most evident in a time of emergency, such as the Covid-19 pandemic we've just encountered. Government use of data in private sector is praised by some as a smart application of the fruits of digital development. Its exceptional yet sometimes impregnable nature, however, also raises the concerns of unruly power expansion.

As personal information is continuously created as digital footprints of human activities in private life, the law assures in principle that those data would stay private unless it is expressly required by law or is necessary for

furthering public interests among others.[12] Such assurance, however, proves to be tenuous.

During the Covid-19 pandemic, the government requisitioned from private third parties several forms of personal data originally collected for purposes entirely irrelevant to disease control. For example, credit card transaction records, mobile phone registration and geolocation data were taken to map the footprints of possible cases and potential contacts.[13] While the Communicable Disease Control Act (CDC Act) only authorizes the public health authority to conduct epidemic investigation "to ascertain the origin of a disease," the government alleges that the power of "tracing potential contacts" is also within the authorization of the law. The government further argues that the same legal provision not only allows the authority to compel all sorts of third parties to provide identifiable information for epidemic investigation, but gives it the power to employ high-tech methods used mainly in criminal investigation, such as obtaining mobile phone signals of hundreds of thousands of people from their mobile phone companies without their knowledge and consent, to trace potential contacts as well. That is probably because the Constitutional Court had admitted in a previous case a weaker form of due process protection to individuals and stopped short of allowing the government to do whatever it takes to end a pandemic.[14] The government is now more inclined to expand the statutory interpretation of the law to its greatest extent and to adopt measures that are not clearly authorized.

When the line between normality and a state of exception becomes blurred, government making secondary uses of privately collected data may

---

12 Article 20 of Personal Data Protection Act (2015).

13 Chi-Mai Chen et al., *Containing COVID-19 Among 627,386 Persons in Contact With the Diamond Princess Cruise Ship Passengers Who Disembarked in Taiwan: Big Data Analytics*, 22(5) J. MED. INTERNET RES. 1170, 1173 (2020); MINISTRY OF HEALTH AND WELFARE, KEY SUCCESS FACTORS: SMART COMMUNITY TRANSMISSION PREVENTION, https://covid19.mohw.gov.tw/en/cp-4775-53739-206.html (last visited July 9, 2021).

14 Interpretation No. 690 of the Constitutional Court, Judicial Yuan (2011).

become a new normal. It raises the worries about "function creep," a phenomenon in which information collected for one purpose tends to be used for ever-expanding and very often undisclosed purposes,[15] and casts another shadow over the future of digital development.

IV. Government Engaged in Creating More Data for Future Uses

It is in the above atmosphere that the government policy to issue an electronic version of national identity cards (eID) faces challenges and doubts.

The first Taiwan national identity card was issued in 1948 as a tool accompanying household regulation. It also served as a means to verify identity before government agencies assigned public obligations or conferred rights. The national ID card has begun to carry a lifelong one-person-one-number UID in 1965 as an anti-counterfeit measure. When it became mandatory in 1973, the function of the national ID card remained limited to identity verification in the course of public agencies performing statutory duties.

However, the law that authorized the mandatory national identity card does not clearly prohibit the use of the card beyond its statutorily sanctioned purposes. The vague language of the law breeds extremely broad uses or even abuses of the cards and the ID numbers. Businesses taking a person's ID number as a direct identifier in their information systems is a common practice. Handing over one's national ID card to others as proof of identity in exchange for private services is also regularly seen in our daily life. The paper-based nature of the card and the analog nature of identity information on the card nevertheless restrain the proliferation of data.

Once the national ID card is embedded with an RFID microchip and the

---

15 Evelina Manukyan & Joseph Guzzetta, *How Function Creep May Cripple App-based Contact Tracing*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (May 27, 2020), https://iapp.org/news/a/how-function-creep-may-cripple-app-based-contact-tracing/.

identity information becomes digitalized, everything will not be the same. eID is a game changer in that it substantially increases the risks of unwanted data collection and undisclosed information proliferation if left unregulated. Even more troublesome in Taiwan's case is that individuals would be forced, even without a valid legal authorization, to carry certain electronic identity information on the card, which is deliberately designed to be accessible by anyone, and not only authorized agencies; this is beyond its statutorily designated purposes. No opt-out opportunity is given to allow those who have concerns about digitalization to choose a deactivated version of the eID card. Without a law that properly regulates the collection, storage and uses of electronic identity information, the use and abuse of eID would bring about a world in which digital footprints proliferate at a speed beyond imagination and become ready prey for surveillance capitalism.[16] It is through the risk of function creep, again, that exploitation of digital footprints, rather than real surveillance by the government, becomes a real threat to the evangelic vision of digital development enthusiastically promised by the government's eID program.

V. Conclusion

While digital development seems to promise an unconditionally bright future, it involves a challenging choice between rushing to the goal unscrupulously and going forward with a load of democratic values. A competition between liberal democracy and autocracy is clear and intense. While an authoritarian regime can easily provide a fast-track approach to digital development at the expense of due process of law and protection of human rights, steps of a democracy are often mired in debates over values and goals of a good society. It is always tempting to accomplish the dream of a data-driven world by submitting whatever data are available for analysis to

16 Shoshana Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 28(1) NEW LAB. F. 10, 10-29 (2019).

generate allegedly generous surplus without asking who bears the burdens and who actually benefits in such a society. Luckily, examples from the authoritarian regime have reminded us that the road to digital development without human rights is not the one that we should take.

References

Chen, Chi-Mai, Hong-Wei Jyan, Shih-Chieh Chien, Hsiao-Hsuan Jen, Chen-Yang Hsu, Po-Chang Lee, Chun-Fu Lee, Yi-Ting Yang, Meng-Yu Chen, Li-Sheng Chen, Hsiu-Hsi Chen, and Chang-Chuan Chan. 2020. Containing COVID-19 Among 627,386 Persons in Contact With the Diamond Princess Cruise Ship Passengers Who Disembarked in Taiwan: Big Data Analytics. *Journal of Medical Internet Research* 22(5):1170-1178.

Donner, Jonathan. 2018. Keynote remarks at the USAID Digital Development Forum: A Vision of Digital Development in 2028. Available at https://medium.com/caribou-digital/a-vision-of-digital-development-in-2028-43c8ff3c69e.

International Telecommunication Union (ITU). 2020. *Measuring Digital Development: Facts and Figures 2020*. Switzerland: International Telecommunication Union.

Kaye, Jane, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare, and Karen Melham. 2015. Dynamic Consent: A Patient Interface for Twenty-first Century Research Networks. *European Journal of Human Genetics* 23:141-146.

Liu, Zong-Shi. 2016. Introduction to the Promotion of Using Government Data for Big Data Analysis. *Government Information Bulletin* 341:5-13.

Manukyan, Evelina, and Joseph Guzzetta. 2020. How Function Creep May Cripple App-based Contact Tracing. In *The International Association of Privacy Professionals.* https://iapp.org/news/a/how-function-creep-may-cripple-app-based-contact-tracing/.

Ploug, Thomas, and Søren Holm. 2016. Meta Consent — A Flexible Solution to the Problem of Secondary Use of Health Data. *Bioethics* 30(9):721-732.

Teare, Harriet J. A., Megan Prictor, and Jane Kaye. 2021. Reflections on Dynamic Consent in Biomedical Research: The Story So Far. *European Journal of Human Genetics* 29:649-656.

United Nation Conference on Trade and Development (UNCTAD). 2019. *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. Switzerland: United Nations Publications.

Zuboff, Shoshana. 2019. Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum* 28(1):10-29.