Article

Applying Privacy as Trust in the Emerging Digital Welfare State

Yi-Chen Huang[*]

Abstract

With the emergence of the digital welfare state, social protection and assistance are increasingly driven by digital big data, artificial intelligence, and related technologies. The implementation of a conventional rights-based framework within the context of the digital welfare state involves examining the interaction between the state and its citizens from a human rights perspective. This approach emphasizes the importance of individual autonomy and the ability to make choices while adhering to the principles of accountability, non-discrimination, and equality.

The analysis of the 2020 Dutch SyRI case is the beginning of a rights-based judicial review in the digital welfare state in the Netherlands. Coincidentally, the Taiwanese Constitutional Court's recent 2022 judgment of the Taiwan National Insurance Health Database case relates to just these kinds of privacy concerns. Although the constitutional system and political structure of the Netherlands and Taiwan are quite different, both the Dutch SyRI case and the Taiwan NIHD approached the issue of privacy from the traditional, rights-based perspectives, highlighting the problems of focusing on invasion rather than creating values and existing asymmetrical information relationships.

This paper aims to contribute by incorporating the concept of trust as a

DOI：10.53106/181263242023061801003

[*] Ph.D. Candidate at College of Law, National Chengchi University; Edinburgh Law School. The draft of this paper has been presented at the 9th Asian Constitutional Law Forum, which took place on May 14, 2022. I would like to thank the Chair, Chien-Chih Lin, the Panelists, Chang-Chiang Hsieh and Pi-Chu Tsai, as well as all other participants of the panel "Digital Governance". Also, I am grateful to Han-Liang Chou for the comments and suggestions on the draft of this paper. Lastly, I would like to deeply thank the anonymous reviewers for their many insightful comments and suggestions, which helped improve and clarify this manuscript.

fundamental privacy value into the context of information relationships within the digital welfare state. It advocates for the introduction of a public trust model as well as the establishment of an independent supervision mechanism to carry out ex-ante risk assessments. This mechanism serves as an empowering tool to foster the creation of values and to address the information asymmetry that exists between individuals and the government in the digital welfare state.

Keywords: *Digital Welfare State, SyRI Case, Taiwan NIHD Case, Privacy as Trust*

CONTENTS

I. INTRODUCTION

Rapid advances in big data, artificial intelligence (AI), and related technologies have been widely used in multiple fields and industries, ranging from agriculture and manufacturing to health care. AI has been used in private-sector applications such as recruitment and employment[1] as well as by public authorities.[2] For instance, countries are increasingly relying on algorithmic decision systems (ADSs) to allocate public resources, especially in the field of social welfare.[3] The "digital welfare state" phenomenon has emerged through these technological advances.[4]

Because the welfare field accounts for a major share of national budgets, countries have been deploying "predictive policing" to predict potential risks and welfare fraud in order to reduce budgets and ensure efficiency. Nevertheless, previous studies and reports have suggested that implementing AI to allocate resources has brought about unintended consequences, especially in the form of discrimination.[5] For example, Virginia Eubanks identified that the impact of automated decision-making on public services in America discriminates against the poor more than non-digital tools.[6] Cathy O'Neil also pointed out that big data perpetuate bias, injustice, and inequality.[7]

In 2020, the Hague District Court ruled that *SyRI*, a Dutch fraud-detection system deployed in the welfare field, had failed to comply with Article 8(2) of the European Convention on Human Rights (ECHR).[8] That is, the *SyRI* legislation had failed to strike a fair balance between the legitimate aim of combating welfare fraud of the *SyRI* legislation and people's right to privacy. Coincidentally, the Taiwanese Constitutional Court

[1] Anna Lena Hunkenschroer & Christoph Luetge, *Ethics of AI-Enabled Recruiting and Selection: A Review and Research Agenda*, 178 J. BUS. ETHICS 977, 977-1007 (2022); Janneke Gerards & Raphaële Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law* 83 (EU Publications, 2021), https://data.europa.eu/doi/10.2838/544956.

[2] Gerards & Xenidis, *id.* at 87.

[3] *Id.*

[4] The concept of a "digital welfare state" seems to be first proposed by Alston Philip, United Nations Special Rapporteur on extreme poverty and human rights. Please *see* Philip Alston (Special Rapporteur), *Digital Welfare States and Human Rights, Report of the Special Rapporteur on Extreme Poverty and Human Rights*, at 4, U.N. A/74/493 (Oct. 11, 2019), https://documents.un.org/doc/undoc/gen/n19/312/13/pdf/n1931213.pdf?token=dSLhkZazlQbpqoIj5D&fe=true.

[5] Gerards & Xenidis, *supra* note 1, at 86-87.

[6] VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE POLICE AND PUNISH THE POOR 183-200 (2018).

[7] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 199-205 (2016).

[8] Rb. Den Haag Hague5 februari 2020, Case C-09-550982-HA ZA 18-388, ECLI:NL:RBDHA:2020:865 (NJCM et al. and FNV/The State of Netherlands) (Neth.).

heard arguments in the Taiwan National Insurance Health Database (NIHD) case relating to just these kinds of privacy concerns on 26 April 2022, with the main dilemma in this case being the secondary use of individuals' healthcare data.[9]

The selection of the Dutch *SyRI* case and the Taiwan NIHD case as case studies in this paper may pique the curiosity of readers. The Dutch *SyRI* case represents a significant legal precedent wherein the court examines the utilization of big data analytics for predictive analytics within the realm of welfare and social benefits, with a particular focus on human rights considerations. While the primary focus of the Taiwan NHIR Database case is on privacy rights rather than social security rights, it provides valuable insights into the potential difficulties surrounding the utilization of personal data by the Taiwanese digital welfare state, specifically in relation to social security rights. Despite the fact that the constitutional system and political structure of the Netherlands and Taiwan are quite different, the Dutch *SyRI* case and the Taiwan NIHD case share some similarities. Both cases approached the issue of privacy from the traditional, rights-based perspectives, highlighting the problems of focusing on invasion instead of creating values and existing asymmetrical information relationships.

The contribution this paper attempts to make is to borrow and introduce the idea of trust as a foundational privacy value into information relationships within the digital welfare state. This paper will first introduce the phenomenon of the digital welfare state in Section 2. Subsequently, this paper attempts to point out the problems of framing privacy as rights-based by examining and analyzing the Dutch *SyRI* case and the Taiwan NIHD case in Section 3. Finally, this paper in Section 4 argues that on the premise of privacy as trust is the social glue and bond, and further advocates establishing the independent supervision mechanism to conduct *ex-ante* risk assessments as an empowerment to create values and as a counterweight to the information asymmetry between people and government in the digital welfare state.

This paper aims to contribute by incorporating the concept of trust as a fundamental value of privacy into the context of information exchange within the digital welfare state. This paper will initially present the concept of the digital welfare state in Section 2. Subsequently, this paper critically attempts to evaluate the conceptualization of privacy as a right by investigating and evaluating two specific cases: the Dutch *SyRI* case and the Taiwan NIHD case. Section 3 will provide an in-depth analysis of these cases, highlighting the inherent flaws associated with defining privacy only

[9] *Constitutional Court to Hear NHIA Privacy Case* (Taipei Times, Apr. 6, 2022), https://www.taipeitimes.com/News/taiwan/archives/2022/04/06/2003776099.

as a right. Finally, this paper in Section 4 argues that on the premise of privacy as trust is the social glue and bond, and further advocates to establish the independent supervision mechanism to conduct ex ante risk assessments as an empowerment to create values and as a counterweight to the information asymmetry between people and government in the digital welfare state.

II. DEVELOPMENT OF THE DIGITAL WELFARE STATE

In recent years, welfare states worldwide have experienced digitalization transformation.[10] To reduce costs and improve efficiency, governments have integrated a degree of private participation into public administration, for example, when contracting private entities to design and implement AI systems for the management of welfare-recipient cases.[11] In these and many other ways, traditional welfare models have been challenged by transformations in the digital world.

In 2019, the UN Special Rapporteur on Extreme Poverty and Human Rights, Philip Alston, introduced the notion of an emerging "digital welfare state" phenomenon.[12] The term "digital welfare state" refers to the utilization of technology and big data by the state to facilitate decision-making processes, particularly in the domains of social protection and social assistance systems.[13]

As social welfare has come to account for a major share of national budgets, governments in recent years have increasingly regarded it as an ideal experimental entry point for the ADS-induced reduction of budgets and improvement of efficiency.[14] At the same time, it would appear that the digital transformation of social welfare can help ensure better services for citizens.[15]

Alston's report identified several ways in which countries and public administrations have most prominently used big data and algorithms to govern social welfare: identity verification, eligibility assessment, welfare-benefit calculations and payments, risk scoring, and fraud prevention and detection.[16] However, a more recent welfare-oriented use of

[10] Aishwarya Narayan, *Digitisation and Privatisation in Social Protection Systems: International Trends* (Oct. 30, 2020), https://dvararesearch.com/digitisation-and-privatisation-in-social-protection-systems-international-trends/.

[11] *Id.*

[12] Alston, *supra* note 4, at 4.

[13] Rikke Frank Jørgensen, *Data and Rights in the Digital Welfare State: The Case of Denmark*, 26 INFO. COMMC'N & SOC'Y 123, 135 (2023).

[14] Alston, *supra* note 4, at 4-5.

[15] *Id.*

[16] *Id.*

data-driven analysis is "predictive policing." Authorities use predictive policing to control crime by predicting where crimes may occur or who may be involved in them.[17] In order to manage welfare resources cost- and time-efficiently and avoid welfare fraud, governments have become more and more reliant on available data and predictive algorithms as their regulatory mechanisms.

Alston refers to these predictive algorithms as "digital data and technologies that are used to automate, predict, identify, surveil, detect, target, and punish."[18] In today's modernized welfare system, the subject of decision-making has shifted from human caseworkers to big data, eliminating discretionary decision-making given on a case-by-case basis. In addition, governments have been applying big data and deploying algorithm systems to predict welfare fraud. Whatever approach a country takes to welfare, one issue remains crucial: how to determine who is--and who is not--entitled to receive social benefits.

As Terry Carney noted, the process of digitalization brings about significant transformation in the modes of interaction between citizens and the state, as well as the mode of governance in the social policy field.[19] The traditional model of the welfare state is more personalized, whereas the digital welfare state focuses on homogenization and standardization.[20] In the traditional welfare state, caseworkers will conduct in-personal meetings and interviews to verify cases' situations. The bottom-up approach enables caseworkers to assess the circumstances of all individuals involved while also providing them with discretion in accordance with their specific conditions. In the context of the digital welfare state, the government has implemented a uniform standard to assess eligibility via the algorithm, which has resulted in a reduction in discretionary and individual decisions.

Aligning with Terry Carney's observance, John Storm Pedersen claimed that the traditional welfare state is built on relationshipism, which is anchored in the trust-based relationship between citizens and public welfare caseworkers, but the digital welfare state is based on dataism.[21] That is, data rather than human beings are considered crucial elements in determining

[17] Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N. Y. U. L. Rev. 192, 198 (2019).

[18] Alston, *supra* note 4, at 4.

[19] Terry Carney, *The Automated Welfare State: Challenges for Socioeconomic Rights of the Marginalised*, *in* Money, Power, and AI: Automated Banks and Automated States 95, 110 (Zofia Bednarz & Monika Zalnieriute eds., 2023).

[20] Carney, *supra* note 19, at 111.

[21] John Storm Pedersen, *Chapter 15: The Digital Welfare State: Dataism versus Relationshipism*, *in* Big Data: Promise, Application and Pitfalls 301, 310 (John Storm Pedersen & Adrian Wilkinson eds., 2019).

social policy decisions.[22]

Although the state improves efficiency and reduces costs in the digital welfare state, limitations and challenges have been identified. The drawbacks of using standard criteria to determine eligibility for social benefits are that complexity and differences are overlooked. As Terry Carney indicated, taking Australia's experience as an example, the shift from in-person case meetings and interviews to algorithms has had negative consequences for the vulnerable and the trust between the citizens and the government.[23] In line with Terry Carney's observance, Cary Cogliance also emphasized that human beings must feel connection and empathy in order to build public trust in an automated state.[24]

III. THE PROBLEMS OF FRAMING PRIVACY AS RIGHTS-BASED THROUGH EXAMINING THE DUTCH *SYRI* CASE AND THE TAIWAN NIHD CASE

The application of the traditional rights-based approach to the digital welfare state entails approaching the relationship between the state and the people through the lens of human rights, which is guided by the principles of accountability, non-discrimination, and equality, etc.[25] In 2020, the Hague District Court ruled that *SyRI*, a Dutch fraud-detection system deployed in the welfare field, had failed to comply with Article 8(2) of the European Convention on Human Rights (ECHR).[26] It is a landmark judgment that touches upon the use of big data in the digital welfare state from a rights-based perspective and has attracted considerable international attention.[27]

The Hague District Court's decision to frame this issue from a rights-based perspective has garnered favorable acknowledgment.[28] However, this approach has also brought attention to the challenges associated with approaching privacy as rights-based. This Section will provide an introduction and overview of the context and the Court's ruling in the *SyRI* Case. It will subsequently examine the challenges associated with

[22] *Id.* at 310.

[23] Carney, *supra* note 19, at 114.

[24] Cary Coglianese, *Law and Empathy in the Automated State*, *in* MONEY, POWER, AND AI: AUTOMATED BANKS AND AUTOMATED STATES 173, 174 (Zofia Bednarz & Monika Zalnieriute eds., 2023).

[25] Jørgensen, *supra* note 13, at 128.

[26] Rb. Den Haag Hague 5 februari 2020, Case C-09-550982-HA ZA 18-388, ECLI:NL: RBDHA:2020:865 (NJCM et al. and FNV/The State of Netherlands) (Neth.).

[27] For example, the *SyRI* case received significant attention from the United Nations (UN). The UN Special Rapporteur on extreme poverty and human rights, Philip Alston, submitted an Amicus Brief.

[28] Adamantia Rachovitsa & Niclas Johann, *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case*, 22 HUM. RIGHTS L. REV. 1, 1-2 (2022).

adopting a rights-based approach to understanding privacy.

The constitutional recognition of the right to privacy was first recognized by the Taiwanese Constitutional Court in *JY Interpretation* No. 603 through the jurisprudence interpretation of Article 22 of the Constitution as one of the types of unremunerated rights.[29] Furthermore, it is worth noting that the Taiwanese Constitutional Court rendered judgment No. 13 of 2022 on the National Health Insurance Research (NHIR) Database case on August 12, 2022, addressing matters concerning privacy.[30]

This Section will introduce the Dutch *SyRI* Case and the Taiwan NIHD case, respectively, and then examine and analyze the Dutch *SyRI* case and the Taiwan NIHD case to highlight the challenges with framing privacy as a right.

A. *The SyRI Case in the Netherlands*

Prior to the *SyRI* case, the Administrative Jurisdiction Division of the Council of State (one of the three highest administrative courts of the Netherlands) in the *Aerius I* case declared that "the public agencies have an obligation to make the choices made and the data and assumptions used public in a full, timely and voluntary manner, allowing individuals to understand how they have been affected by an algorithm and to enable them to effectively contest that algorithm before a court."[31] The Supreme Court of the Netherlands has emphasized and confirmed the principle that "public administration must ensure the transparency and verifiability of decision-making process based on the algorisms program."[32]

[29] Please *see* Sifa Yuan Dafaguan Jieshi No.603 (司法院大法官解釋第543號) [Judicial Yuan Interpretation No. 603] (2005) (Taiwan).

[30] Summary of TCC Judgment 111-Hsien-Pan-13 (2022) 【Case on the National Health Insurance Research Database】, (Constitutional Court R.O.C. (Taiwan), Mar. 17, 2023), https://cons.judicial.gov.tw/en/docdata.aspx?fid=5248&id=347736.

[31] Raad van State 17 mei 2017, ECLI:NL:RVS:2017:1259 (de Stichting Werkgroep Behoud de Peel/het college van gedeputeerde staten van Noord-Brabant) (Neth.) ¶ 14.4: "In order to prevent this unequal process position, the [public agencies] have the obligation to make public the choices made and the data and assumptions used, fully, timely and voluntarily, in an adequate manner so that these choices, data and assumptions for third parties. This complete, timely and adequate provision must make it possible to assess the choices made and the data and assumptions used, or to have them assessed and, if necessary, contested in a reasoned manner, so that real legal protection against decisions based on these choices, data and assumptions is possible, whereby the judge is able to test the legality of these decisions on the basis of this." Translated by Marlies van Eck, please *see* Marlies van Eck, *'Automated decisions and administrative law: the Netherlands,'* (Sept. 3 2018), https://automatedadministrativedecisionsandthelaw.wordpress.com/2018/09/03/automated-decisions-and-administrative-law-the-netherlands/; Gerards & Xenidis, *supra* note 1, at 113.

[32] HR 17 augustus 2018, ECLI:NL:HR:2018:1316 (van het college van burgemeester en wethouders van de gemeente Waalwijk te Waalwijk/[X] te [Z]) (WOZ), ¶ 2.3.3; translated by Marlies van Eck, please *see* Marlies van Eck, *Automated decisions and administrative law: the Netherlands*, (Sept. 3, 2018),
https://automatedadministrativedecisionsandthelaw.wordpress.com/2018/09/03/automated-decisions-a

SyRI was a Dutch fraud-detection system that relied on a large pool of invasively acquired personal data. In 2020, the Hague District Court ruled that *SyRI* had failed to comply with Article 8(2) of the ECHR. The landmark judgment marked the first time that a rights-based judicial review had targeted a state's foremost digital-welfare surveillance tool. Attracting considerable international attention, the *SyRI* case shined a light on the invasion of privacy and the potential risk of indirect discrimination in social welfare systems in the digital age. The cause of the discrimination in the *SyRI* case was likely biased data-collection processes, which tended to be deployed in low-income Dutch neighborhoods.[33]

Much of the *SyRI* case revolved around the lawfulness of the *SyRI* legislation. An attempt was made to review the *SyRI* legislation in relation to the aforementioned ECHR article. The claimants in the case were several civil society groups and two private individuals who initiated the legal proceedings against the government of the Netherlands. According to the claimants, *SyRI* was a digital tracking system that used deep learning and data mining to engage in risk profiling related to the country's social welfare system.[34]

The Hague District Court analyzed the *SyRI* case chiefly from the perspective of the right to respect for private life. The court recognized that the central objective of the *SyRI* legislation, namely combating welfare fraud in the interest of the state's economic integrity, constituted a compelling purpose--one that addressed a pressing social need.[35] Nevertheless, the court ruled that the *SyRI* legislation had failed to strike a fair balance between the legitimate aims of the *SyRI* legislation and people's right to privacy.

The court emphasized that Article 8 of the ECHR imposes on state legislators the special responsibility to ensure that new technologies such as *SyRI* respect human rights and political freedoms. During the proceedings of the case, the Dutch state declined to disclose the risk model that had served as the basis for *SyRI*; the absence of this important evidence prevented the court from checking or in any way properly assessing the Dutch state's contentions regarding *SyRI*.[36]

It is worth noting that the Hague District Court stated that the risk models run by *SyRI* may have had unintentional discriminatory effects.[37] The *amici curiae*, submitted by the Special Rapporteur on Extreme Poverty and Human Rights, noted that *SyRI* had been investigating neighborhoods

nd-administrative-law-the-netherlands/.

[33] Alston, *supra* note 4, ¶ 8.

[34] Rb. Den Haag Hague 5 februari 2020, Case C-09-550982-HA ZA 18-388, ECLI:NL: RBDHA:2020:865 (NJCM et al. and FNV/The State of Netherlands) (Neth.), ¶ 6.45.

[35] *Id.* ¶ 6.76.

[36] *Id.* ¶ 6.49.

[37] *Id.* ¶ 6.91.

that were known as "problem areas." Dutch citizens who were flagged by *SyRI* as being likely to commit benefits fraud tended to hail from low-income Dutch neighborhoods in cities such as Capelle aan den Ijssel, Eindhoven, Haarlem, and Rotterdam.[38] This observation was confirmed by the state at the hearings for the case.[39] In its ruling, the court expanded the ambit of the right to respect for private life enshrined in Article 8 of the ECHR: "The right to respect for private life in the context of data processing concerns the right to equal treatment in equal cases, and the right to protection against discrimination, stereotyping, and stigmatization."[40]

Last but not the least, although the Court has noticed that a National Intervention Teams Steering Group (Landelijke Stuurgroep Interventieteams--hereinafter: LSI) is responsible for advising the Ministry on the application of the *SyRI*,[41] the Court has found that the LSI is just the advisory body and its advice of LSI is non-binding.[42] More importantly, the Court has ruled that the LSI does simultaneously act as a player and referee in the *SyRI* case.[43] Therefore, the Court has concluded that "the *SyRI* legislation does not provide for a comprehensive review beforehand nor for a review by an independent third party, and it does not contain sufficient safeguards to protect the right to private life under Article 8(2) ECHR."[44]

B. *The Phenomenon of the Digital Welfare State in Taiwan*

In 2012 in Taiwan, the Ministry of the Interior established the Taiwan National Social Welfare Benefits Data Comparison System Database (全國社會福利津貼給付資料比對資訊系統),[45] which combines the tax information of the island's population with their social welfare information

[38] *Id.* ¶ 6.92.

[39] *Id.* ¶. 6.91-6.93.

[40] *Id.* ¶ 6.24.

[41] *Id.* ¶ 4.26.

[42] *Id.* ¶ 6. 101.

[43] *Id.* ¶ 6. 101: "What is more, the LSI is comprised of representatives of organs which also have an interest in combating and preventing abuse and fraud in the areas specified in Section 64 subsection 1 SUWI Act. Furthermore, the Social Affairs and Employment Inspectorate is not only represented in the LSI but can also be a participant in a collaborative alliance for the benefit of a *SyRI* project and is charged with analyzing data for the definitive risk selection based on which a risk report is submitted. The court is unable to assess if and to what extent the internal functional division between the various units of the Social Affairs and Employment Inspectorate (the investigation unit, the analysis unit, and possibly other units) is sufficiently safeguarded."

[44] *Id.* ¶ 6. 99, ¶ 6.106. Naomi Appelman, Ronan Ó Fathaigh & Joris van Hoboken, *Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands*, 12 JIPITEC 257, 258-69 (2021).

[45] Chu Mei-Chen (朱美珍), *Zixun Keji Dui Shehui Fuli Fuwu Yuesheng Zhuyi Zhi Tantao (資訊科技對社會福利服務躍升助益之探討)* [*Research on the Benefit of the Advancement of Social Welfare Services through Information Technology*], 161 SHEQU FAZHAN JIKAN (社區發展季刊) [COMMUNITY DEVELOPMENT JOURNAL QUARTERLY] 4, 7 (2018).

in a bid to reduce expenditures in money and time, particularly through the prevention of double-dipping and fraud.[46]

In addition, during the pandemic, the utilization of the NHIR Database and the customs and immigration data by the Taiwanese government to create profiles of individuals through the application of big data analysis techniques, taking into account factors such as travel history and clinical symptoms, Taiwan government can get hold of the latest situation and quickly manage the pandemic.[47] According to Hao-Yuan Cheng and Ding-Ping Liu's analysis, the attainment of an 88% detection rate in secondary cases can be ascribed to the implementation of comprehensive data collection methods, including self-reporting automatic text messages and the digital contact tracing system.[48] Through the combination of the cross-database data, the Taiwan government can quickly manage the pandemic at the early stage.[49] However, this welcomed criticism for intruding on the privacy rights, such as lacking explicit delegation and procedure safeguards.[50] As Chuan-Feng Wu noted, "the Central Epidemic Command Center (CCEC) fails to comprehensively disclose what personal data has been collected, how it was collected and processed, and for what purposes the data was used."[51] The erosion of trust between citizens and the government can be attributed to a lack of openness and transparency.

Although there have not yet been case laws relating to predictive

[46] *See* Tseng Chung-Ming (曾中明), *Weisheng Fulibu Zixun Yewu Tuizhan Gaikuang (衛生福利部資訊業務推展概況)* [*Overview of the Information Service Promotion of the Ministry of Health and Welfare*], 312 ZHENGFU JIGUAN ZIXUN TONGBAO (政府機關資訊通報) [GOVERNMENT OFFICES INFORMATION NOTICES] 1, 7 (2013); Tseng Chung-Ming (曾中明), Cheng Wen-Yi (鄭文義) & Chiu Kuo-Kuang (邱國光), *Neizhengbu Shezheng Zixun Xitong De Xiankuang Yu zhanwang* (*內政部社政資訊系統的現況與展望*) [*The Current Situation of and Prospects for the Social Affairs Information System of the Ministry of the Interior*] 111 SHEQU FAZHAN JIKAN (社區發展季刊) [COMMUNITY DEVELOPMENT JOURNAL QUARTERLY] 4, 9 (2005).

[47] Melyssa Eigen, Flora Wang & Urs Gasser, *Country Spotlight: Taiwan's Digital Quarantine System* (Berkman Klein Center, July 31, 2020), https://cyber.harvard.edu/story/2020-07/country-spotlight-taiwans-digital-quarantine-system.

[48] Hao-Yuan Cheng & Ding-Ping Liu, *Early Prompt Response to COVID-19 in Taiwan: Comprehensive Surveillance, Decisive Border Control, and Information Technology Support*, 23 J. OF THE FORMOSAN MED. ASS'N 1, 3-4 (2022).

[49] The Covid-19 first appeared in China in December 2019. Given its geographic proximity to China, it is foreseeable that Taiwan will experience a serious outbreak of the Covid-19 pandemic during the early stages of period 2020-2021. Surprisingly, the number of daily confirmed cases remained below 100 cases until May 2021, when the first major outbreak occurred. Please refer to *Timeline COVID-19* (Ministry of Health and Welfare, Apr. 30, 2023), https://covid19.mohw.gov.tw/en/sp-timeline0-206.html.

[50] Ching-Fu Lin, Chien-Huei Wu & Chuan-Feng Wu, *Reimagining the Administrative State in Times of Global Health Crisis: An Anatomy of Taiwan's Regulatory Actions in Response to the COVID-19 Pandemic*, 11 EUR. J. OF RISK REG. 256, 266 (2020); Chuan-Feng Wu, *Covid-19 and Data Privacy Challenges in Taiwan* (Lex-Atlas: Covid-19, June 28, 2021), https://lexatlas-c19.org/covid-19-and-data-privacy-challenges-in-taiwan/.

[51] Lin, Wu & Wu, *supra* note 50.

analytics caused by algorithm decision-making, the Taiwanese Constitutional Court heard arguments and delivered judgment in the TNHID case relating to just these kinds of privacy concerns in 2022,[52] with the main dilemma in this case being the secondary use of individuals’ healthcare data.

The case in question centers on Taiwan’s National Health Insurance, which is a compulsory insurance program for which the Taiwanese government established the National Health Insurance Research (NHIR) Database. In essence, this database facilitates the mass collection of the country’s health-related data. Because the database is so rich in content, the government has leveraged the resource by allowing third parties to access it for academic research. However, criticism about potential infringements on information privacy and privacy autonomy has been voiced by the Taiwan Association for Human Rights (TAHR). This non-governmental organization has accused the National Health Insurance Administration of providing the personal data of the NHIR Database to third parties for purposes other than legitimate collection. Some people have argued that this “secondary” use of the NHIR Database by third parties is inconsistent with Taiwan’s constitutional protections covering the right to information privacy. Thus, the TAHR advocacy group filed a petition with the Constitutional Court in 2017.[53]

The Taiwanese Constitutional Court rendered judgment No. 13 of 2022 on the NHIR Database case on 12 August 2022.[54] The Taiwanese Constitutional Court has declared that Article 6(1)(4) of the Personal Data Protection Act, 2016[55] does not violate the right to privacy enshrined in Article 22 of the Constitution. In addition, the Constitutional Court declared that the lack of regulations permitting people to exercise their rights of “opt-out” is incompatible with Article 22 of the Constitution.

Nevertheless, it is worth noting that the Taiwanese Constitutional Court has also stated that lacking an independent monitoring mechanism for the protection of personal data in the present legal framework of the Personal

[52] *Constitutional Court to Hear NHIA Privacy Case*, *supra* note 9.

[53] *See* Ching-Yi Liu, Wei-Ping Li & Yun-Pu Tu, *Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan’s Open Data Policy and Practices*, 30 WASH. INT’L L.J. 545, 567-76 (2021).

[54] Summary of TCC Judgment 111-Hsien-Pan-13 (2022) 【Case on the National Health Insurance Research Database】 (Constitutional Court R.O.C. (Taiwan), Mar. 17, 2023), https://cons.judicial.gov.tw/en/docdata.aspx?fid=5248&id=347736; Wu Cheng-feng & William Hetherington, *Health Data Access Partly Unconstitutional: Court* (Taipei Times, Aug. 13, 2022), https://www.taipeitimes.com/News/taiwan/archives /2022/08/13/2003783452.

[55] Article 6(1)(4) of the Personal Data Protection Act states, “Data pertaining to a natural person’s medical records, healthcare, genetics, sex life, physical examination and criminal records shall not be collected, processed or used unless on any of the following bases: [. . .] 4. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for the purpose of healthcare, public health, or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject.”

Data Protection Act is inadequate, which might be unconstitutional.[56] The Taiwanese Constitutional Court asked the relevant authorities to enact relevant laws within three years from the date of the announcement of the judgment by making the EU General Data Protection Regulation a reference for the establishment of an independent supervisory authority.[57]

However, in terms of lacking an independent supervisory authority, several Justices in their dissenting in part opinions have criticized that the majority simply give a warning, and point out the majority should straightforwardly declare it unconstitutional.[58] Chief Justice Tzong-Li HSU's dissenting in part opinion explained that the rationale behind the dissenting opinions is that people who are the data subjects do not know or have no way of knowing that their personal data are obtained and used in the NHIR Database case. Under the circumstances, only by the establishment of an independent supervisory authority that evaluates and controls the usage of personal data, the people's right to privacy can be protected, and the requirement of the due process laid out in the Constitution of Taiwan should be met.[59]

[56] Summary of TCC Judgment 111-Hsien-Pan-13 (2022) 【Case on the National Health Insurance Research Database】, (Constitutional Court R.O.C. (Taiwan), Mar. 17, 2023), https://cons.judicial.gov. tw/en/docdata. aspx?fid=5248&id=347736.

[57] Indy Liu, *Ruling on NHIA Data Reveals a Larger Issue* (Taipei Times, Aug.19, 2022) https://www.taipeitimes.com/News/editorials/archives/2022/08/19/2003783770.

[58] Please *see* Xianfa Fating (憲法法庭) [Constitutional Court R.O.C. (Taiwan)], Xianfa Fating 111 Nian Xianpanzi Di 13 Hao Panjue Xu Dafaguan Zongli Tichu zhi Bufen Butong Yijianshu (憲法法庭111年憲判字第13號判決許大法官宗力提出之部分不同意見書) [Dissenting in Part Opinion Delivered by Justice Hsu Tzong-Li of TCC Judgment 111-Hsien-Pan-13 (2022)], 3-4, https://cons.judicial. gov.tw/download/download.aspx?id=460751; Xianfa Fating (憲法法庭) [Constitutional Court R.O.C. (Taiwan)], Xianfa Fating 111 Nian Xianpanzi Di 13 Hao Panjue Huang Dafaguan Zhaoyuan Tichu, Xu Dafaguan Zongli, Xu Dafaguan Zhixiong, Xie Dafaguan Mingyang, Yang Dafaguan Huiqin Jiaru zhi Bufen Butong Yijianshu (憲法法庭111年憲判字第13號判決黃大法官昭元提出，許大法官宗力、許大法官志雄、謝大法官銘洋、楊大法官惠欽加入之部分不同意見書) [Dissenting in Part Opinion Delivered by Justice Jau-Yuan Hwang, Joined by Justice Hsu Tzong-Li, Justice Hsu Zhi-Xiong, Justice Shieh Ming-Yan, and Justice Yang Hui-Chin of TCC Judgment 111-Hsien-Pan-13 (2022)], 14-17, https://cons.judicial.gov.tw/download/download.aspx?id=460753; Xianfa Fating (憲法法庭) [Constitutional Court R.O.C. (Taiwan)], Xianfa Fating 111 Nian Xianpanzi Di 13 Hao Panjue Xie Dafaguan Mingyang Tichu zhi Bufen Butong Yijianshu (憲法法庭111年憲判字第13號判決謝大法官銘洋提出之部分不同意見書) [Dissenting in Part Opinion Delivered by Justice Shieh Ming-Yan of TCC Judgment 111-Hsien-Pan-13 (2022)], 14-17, https://cons.judicial.gov.tw/download/download.aspx?id=460754; Xianfa Fating (憲法法庭) [Constitutional Court R.O.C. (Taiwan)], Xianfa Fating 111 Nian Xianpanzi Di 13 Hao Panjue Yang Dafaguan Huiqin Tichu zhi Bufen Butong Yijianshu (憲法法庭111年憲判字第13號判決楊大法官惠欽提出之部分不同意見書) [Dissenting in Part Opinion Delivered by Justice Yang Hui-Chin of TCC Judgment 111-Hsien-Pan-13 (2022)], 12-13, https://cons.judicial. gov.tw/download/download.aspx?id=460755.

[59] Xianfa Fating (憲法法庭) [Constitutional Court R.O.C. (Taiwan)], Xianfa Fating 111 Nian Xianpanzi Di 13 Hao Panjue Xu Dafaguan Zongli Tichu zhi Bufen Butong Yijianshu (憲法法庭111年憲判字第13號判決許大法官宗力提出之部分不同意見書)

On May 16, 2023, the Legislative Branch has passed the Amendment to the Taiwan Personal Data Protection Act, stipulating that the Personal Data Protection Commission as the exclusive competent authority for personal data protection in order to compatible with the request of the Taiwanese Constitutional Court.[60]

C. *Analysis*

The Dutch *SyRI* case examined the phenomenon of data discrimination that emerges as a result of employing big data in decision-making processes, whereas the Taiwan NIHD case focuses on the secondary use of personal data. Notwithstanding the disparities witnessed in the two instances, it is imperative to recognize their resemblances. Both the Dutch *SyRI* case and the Taiwan NIHD case examine the concept of privacy from a conventional, rights-oriented perspective, and both provide light on the difficulties and obstacles involved with understanding privacy as a rights-based framework within the arena of big data decision-making: (1) Rather than creating value, the emphasis is on defense against invasion. (2) An unbalanced relationship exists between individuals and the government. This will be explained more in the Section that follows.

1. *The Prioritization of Defense against Invasion Over the Creation of Values*

As we have seen through the *SyRI* case, the information relationship between the Trusters(individuals) and entrustees (the government) is unstable and fragile. On the one hand, people do not believe and trust the government, thus they share little, bad or even inaccurate information. On the other hand, the government harbors suspicious that people might submit wrong information and engaged in welfare benefit fraud. This distrust prompts the government to implement the *SyRI* mechanism to detect fraud,

[DISSENTING IN PART OPINION DELIVERED BY JUSTICE HSU TZONG-LI OF TCC JUDGMENT 111-HSIEN-PAN-13 (2022)], 3-4, https://cons.judicial.gov.tw/download/download.aspx?id=460751. In addition, experts appointed by the Constitutional Court have pointed out in the oral argument that the impugned act associated with the NHIR Database (i.e., the Personal Data Protection Act, 2016) violated the due process right to privacy. The impugned act does not require the establishment of such due-process procedures as risk evaluation, public participation, and the involvement of independent public authorities. The absence of these procedures in the Personal Data Protection Act would appear to be a violation of the "due process of law" provisions laid out in the Constitution of Taiwan.

[60] Grace Shao & Sean J.C. Shih, *Taiwan: Amendment to the Taiwan Personal Data Protection Act* (Global Compliance News, June. 1, 2023), https://www.globalcompliancenews.com/2023/06/01/https-insightplus-bakermckenzie-com-bm-data-technology-taiwan-amendment-to-the-taiwan-personal-data-protection-act-increased-fines-for-data-breaches-and-establishment-of-the-personal-data-protection/.

especially targeting "problem areas." Stereotypes result in discrimination, deepening the distrust between people and government.

Furthermore, upon examining the Taiwan NIHD case, the claimants put out the argument that the absence of restrictions governing the exercise of the "opt-out" right infringes against their privacy rights. [61] This contention was upheld by the Constitutional Court. The underlying assumption of this argument is that privacy, which encompasses the concepts of autonomy and choice, is a fundamental entitlement that safeguards individuals from encroachment. However, this viewpoint overlooks how engagement and transparency could contribute to the process of public policymaking.

This phenomenon corresponds to the issue of "the harm fixation" that arises from framing privacy in a negative manner, as highlighted by Neil Richards and Woodrow Hartzog.[62] As previously stated, the court ruled that the *SyRI* legislation had failed to strike a fair balance between the legitimate aims of the *SyRI* legislation and people's right to privacy, which is incompatible with Article 8(2) of ECHR. The court's ruling is underpinned by the idea that "privacy is an injury to be remedied,"[63] namely through the lens of a rights-based understanding of privacy.

Nevertheless, this approach and comprehension fall short of properly grasping the crux of the issue and the underlying rationales contributing to this outcome. The privacy intrusion and collateral unintended discriminatory consequences stemming from the fraud-detection system are attributable to its erroneous reliance on biased data-collection processes. This bias stems from a lack of trust between the people and the government. Citizens frequently believe that governments are prone to encroaching on their privacy, which leads to a reluctance to share thorough and correct information. The government also posits that individuals, particularly within a specific demographic, may deliberately furnish inaccurate data. The government disguises its bias by employing seemingly unbiased artificial intelligence technologies. The aforementioned situation not only demonstrates a failure to generate societal advantages or social values and make appropriate decisions by using big data, but it also perpetuates a continuous loop of negative consequences. This predisposition may run counter to the objectives and goals of the digital welfare state, which leverages big data to enhance the provision of services and decision-making processes.

[61] *See* XIANFA FATING (憲法法庭) [CONSTITUTIONAL COURT R.O.C. (TAIWAN)], CAI JI-XUN DENG QIREN 1061204 XIANFA JIESHI SHENGQINGSHU (蔡季勳等7人1061204憲法解釋聲請書) [THE 1061204 PETITION FOR CONSTITUTIONAL INTERPRETATION OF JI-XUN CAI AND OTHER 7 PETITIONERS], 51-57, https://cons.judicial. gov.tw/docdata. aspx?fid=38&id=309956.

[62] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 442 (2016).

[63] *Id.* at 441.

Rather than using an atomic and individual approach, big data analytics may provide macro and systematical insights instantly, providing big-picture evidence and allowing the policymakers to make decisions from a holistic perspective.[64] Fighting COVID-19 is a good example of how big data assists policymakers in facilitating decision-making, as mentioned in Section 3.2. Furthermore, according to McKinsey Global Institute's research, the potential benefits of big data across the OECD-Europe public sector are creating EUR €150 billion to €300 billion in new value annually over ten years, deriving from operational efficiency, reduction in fraud and error and increase in tax collection.[65]

In summary, the mindset of prioritization of defense against invasion overlooks the potential benefits and values that big data may offer the public governance.

2. *Information Asymmetry between People and Government*

In accordance with the rationale of conceptualizing privacy as a right, anyone expressing a claim must establish the existence of harm. This pertains to how the burden of proof is distributed in legal proceedings involving litigation brought against the government.

In the *SyRI* case, the claimants argued that *SyRI* carried with it a significant risk of discrimination targeting people of lower socioeconomic backgrounds, including immigrants. However, the Dutch government refused to provide key information related to *SyRI*, so the Hague District Court was unable to conclude decisively whether the system was unjustifiably discriminatory. Therefore, the Hague District Court ruled that the government was required by Article 8 of the ECHR to reveal how AI had been operating in *SyRI*. That is to say, the legal burden of proof was found to rest on the government, which would thus have to demonstrate that *SyRI* did not result in discrimination.[66]

The Hague District Court framed the case around the issue of the right to privacy, ultimately ruling that the use of *SyRI* to target certain vulnerable regions and populations was disproportionate to the system's intended goal.

[64] *Big Data Analytics for Policy Making, Report, A Study Prepared for the European Commission DG INFORMATICS (DG DIGIT)* 47-48, 55-56 (EC, 2016), https://joinup.ec.europa.eu/sites/default/files/document/2016-07/dg_digit_study_big_data_analytics_for_policy_making.pdf.

[65] James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh & Angela Hung Byers, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* 61-62 (McKinsey Global Institute, May, 2011), https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20for%20innovation/mgi_big_data_full_report.pdf.

[66] Jack Maxwell & Joe Tomlinson, *Proving Algorithmic Discrimination in Government Decision-Making*, 20 OXFORD UNIVERSITY COMMONWEALTH L.J. 352, 353, 359 (2020).

Thus, the Dutch government had failed to strike a satisfactory balance between the right of privacy and the public interest in detecting welfare fraud; thus, *SyRI* was not in compliance with Article 8(2) of the ECHR. In the end, the State Secretary for Social Affairs and Employment decided not to appeal the judgment,[67] and the judgment of the Hague District Court became the final word on the matter. *SyRI* would cease to operate.

As to the Taiwan NIHD case, the disagreement surrounding the right to opt out can be linked to the existence of an asymmetrical information relationship among the parties concerned. The government exercises authority over all algorithms and processes pertaining to big data information. Individuals have limited awareness of how their data is utilized, leading to their inability to provide their data with confidence.

According to Neil Richards and Woodrow Hartzog, the regulation of privacy should not be confined to the mere prevention of harm but should also aim to generate value rather than only alleviate harm.[68] The Hague District Court has determined that the doctrine of burden of proof on the government is a crucial legal recourse for addressing unjust discrimination within the digital-welfare state.[69] However, it is important to note that this approach is still entrenched in the conventional, rights-based perspective on privacy. Despite the government's provision of algorithmic disclosure and big data processing knowledge, a significant portion of the population lacks the requisite competence to comprehensively comprehend these concepts. The absence of comprehensive knowledge in this domain may pose significant challenges for society in determining whether a given algorithm exhibits discriminatory characteristics or produces discriminatory outcomes. The alteration in the allocation of the burden of proof possesses the capacity to partially mitigate the knowledge asymmetry that exists between private citizens and the governing authorities. Nevertheless, it is crucial to acknowledge that this persistent information disparity persists.

This paper will now proceed to incorporate the concepts of privacy as trust into the context of the digital welfare state, with the aim of addressing the issues associated with an excessive focus on harm.

[67] Marvin van Bekkum & Frederik Zuiderveen Borgesius, *Digital Welfare Fraud Detection and the Dutch SyRI Judgment*, 23 Eur. J. of Soc. Security 323, 337 (2021).

[68] Richards & Hartzog, *supra* note 62, at 443.

[69] Philip Alston, *Brief by the United Nations Special Rapporteur on Extreme Poverty and Human Rights as Amicus Curiae in the Case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of the Hague (case number: C/09/550982/HA ZA 18/388)* 9 (United Nations Human Rights: Office of the High Commissioner, 2019), https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf; Rachovitsa & Johann, *supra* note 28, at 11-12.

IV. APPLYING PRIVACY AS TRUST IN THE EMERGING DIGITAL WELFARE STATE

As mentioned previously, the digital welfare state has transformed the mode of governance in the social security field. The digital welfare state uses algorithms to assess who is eligible for social security protection, making identity verification one of its most important responsibilities.[70] However, privacy concerns have arisen, particularly in the context of amassing types and categories of data in order to properly and promptly identify identities and grant benefits.[71] The digital welfare state, which is operated by algorithms rather than humans, has lost human connection and empathy, as well as trust. Following this logic, restoring and reinforcing trust in the digital welfare state would be a major concern. In the following section, this paper will attempt to put forward the idea of privacy as trust and illustrate how it might be applied in the digital welfare state.

The Dutch *SyRI* case has confirmed the importance of transparency and accountability in the automated decision-making process. It is the precondition that allows the Court to have the capacity to evaluate whether the automated decision-making process has discriminatory effects. Furthermore, both the Dutch *SyRI* case and Taiwan NIHD cases emphasize the significance of implementing an independent monitoring mechanism. As mentioned, the proposal for establishing an independent mechanism is founded on the assumption of understanding privacy as a rights-based perspective and as a shield against invasions. However, individuals continue to be hesitant to provide comprehensive and accurate information due to a lack of confidence. In this scenario, the results and outputs obtained through the use of big data processes would be deemed erroneous, obstructing the fulfillment of the intended goal of establishing a digital welfare state. The anticipated reduction in costs was not achieved; rather, there was an increase in costs.

The examination and analysis of the Dutch *SyRI* case and the Taiwan NIHD case reveal the difficulties of framing privacy as a rights-based issue. This section will present an idea proposal for using the concept of privacy as trust within the context of the digital welfare state. In order to address the information asymmetry between individuals and the government in the context of the digital welfare state, this paper proposes the establishment of an independent supervision mechanism to conduct *ex-ante* risk assessments. The underlying premise of this proposal is the reliance on trust-based privacy as a social bond.

[70] Jonathan McCully, *Blog Explainer: What is the "Digital Welfare State"?* (Apr. 27, 2020), https://digitalfreedomfund.org/explainer-what-is-the-digital-welfare-state/.

[71] *Id.*

A. *Privacy as Trust as the Social Bond in the Digital Welfare State*

In contrast to the conventional rights-based approach to privacy, the concept of "privacy as trust" was initially proposed by Neil Richards and Woodrow Hartzog[72] and subsequently developed upon by Ari Ezra Waldman.[73] The concept of privacy as trust is justified by the fact that the view of privacy as a right fails to acknowledge and properly appreciate the underlying power dynamics between data subjects and data controllers or processors.[74] The conceptualization of privacy as a right is predicated on the principles of autonomy and choice. The disclosure of data in our daily lives is deemed necessary; nonetheless, the entities in charge of managing or processing this data operate under the assumption that such disclosure is an outcome of our voluntary decision-making, personal autonomy, and implicit consent.[75] Furthermore, the data controller or data processor may exploit our data for the purposes of behavioral targeting, predictive analytics, and automated decision-making.[76] In this particular setting, which features a pronounced asymmetry in power dynamics, privacy has been conceptualized as a protective barrier against encroachment.

Examining the concept of privacy within the framework of trust may serve as a potential solution to the limitations. According to the observations made by Neil Richards and Woodrow Hartzog, "in the context of information relationship, trust means the willingness to become vulnerable to a person or organization by disclosing personal information."[77] Despite the potential risks associated with trust and disclosure, such as misuse and unauthorized disclosure, individuals are nonetheless prepared to assume these risks on the basis of trust.[78]

The primary claim is that, throughout history, the notion of privacy has been traditionally perceived as a safeguard against encroachment from a rights-oriented standpoint, focusing on cost-cutting rather than benefit-generating, thus contradicting the inherent positive attributes of social rights. In light of the current scenario, I posited that viewing privacy as a matter of trust could potentially offer a viable strategy for managing the dynamics of information exchange within the context of the digital welfare state.

Taking Taiwan as an example, social rights are stipulated in Article 15

[72] *See* Richards & Hartzog, *supra* note 62, at 472.

[73] *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 61-62 (2018).

[74] *Id.* at 66.

[75] *Id.* at 66-67.

[76] *Id.* at 66-67.

[77] Richards & Hartzog, *supra* note 62, at 449-50.

[78] *Id.* at 450.

of Taiwan's Constitution[79] and Article 10, Paragraph 8 of the Amendment to the Constitution regarding "fundamental national policies."[80] In 2009, Taiwan successively enacted the enforcement Acts of the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR).[81] The incorporation of these international human rights treaties into Taiwanese domestic law was a major step forward for the democratic nation. Under Article 9 of the ICESCR, the state should recognize the right of everyone to social security, including social insurance. The Committee on Economic, Social, and Cultural Rights further elaborated that "qualifying conditions for benefits must be reasonable, proportionate, and transparent. The withdrawal, reduction or suspension of benefits should be circumscribed, based on the grounds that are reasonable, subject to due process, and provided for in national law."[82] Moreover, "All persons should be covered by the social security system, especially individuals belonging to the most disadvantaged and marginalized groups, without discrimination on any of the grounds prohibited under article 2, paragraph 2, of the Covenant."

The allocation of social security benefits is inextricably linked to the digital welfare state. A potential tension exists in the sphere of the digital welfare state regarding the portrayal of privacy as both a fundamental right and as both adverse and protective characteristics, which could potentially undermine the beneficial dimensions of social rights. In contrast to the emphasis on individual autonomy in negative rights, social rights should be advocated for as a subset of positive rights.[83] Viewing privacy in a negative light implies that it functions as a protective barrier against intrusion. Hence, antagonism was visible in the dynamic between the governing authorities and the public. In this particular scenario, the creation of societal values is deemed unattainable.

Nevertheless, the fulfillment of social rights necessitates the proactive involvement of the state rather than passivity. By reconceptualizing privacy as trust, the dynamics of the interaction between individuals and the state

[79] ZHONGHUA MINGUO XIANFA (中華民國憲法) [CONSTITUTION OF R.O.C.] § 15 (1947) (Taiwan): "The right of existence, the right of work, and the right of property shall be guaranteed to the people."

[80] ZHONGHUA MINGUO XIANFA ZENGXIU TIAOWEN (中華民國憲法增修條文) [ADDITIONAL ARTICLES OF THE CONSTITUTION OF THE R.O.C.] § 10, para.8 (2005) (Taiwan): "The State shall emphasize social relief and assistance, welfare services, employment for citizens, social insurance, medical and health care, and other social welfare services. Priority shall be given to funding social relief and assistance, and employment for citizens."

[81] JIUNN-RONG YEH, THE CONSTITUTION OF TAIWAN-A CONTEXTUAL ANALYSIS 234 (2016).

[82] UN Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 19: The Right to Social Security (Article 9), U.N. Doc. E/C.12/GC/19, ¶ 24 (Nov. 23, 2007).

[83] Cécile Fabre, SOCIAL RIGHTS UNDER THE CONSTITUTION: GOVERNMENT AND THE DECENT LIFE 7 (2000).

shift from one of confrontation to one of cooperation. The establishment of a cooperative connection between the government and its citizens is a fundamental requirement for the achievement of social rights and the formation of social ideals. Individuals place their trust and confidence in the government based on the principle of privacy as trust, prompting them to willingly divulge accurate personal information. In a framework characterized by mutual trust, the government seeks to optimize the utility of decision-making processes, including big data. Consequently, it is able to arrive at more informed and improved decisions by leveraging the outcomes of big data processing.

B. *Recommendation: Importing the Data Trust Model*

In the framework of the digital welfare state, privacy is framed as trust, with disclosure and transparency serving as the preconditions and foundations for the trust in the information relationship. This paper aims to import the new data governance model of data trust in the digital welfare state in order to implement the idea of privacy as trust. As Sylvie Delacroix and Neil D. Lawrence noted, the model of data trust employs a bottom-up method, allowing data subjects a voice and the opportunity to participate in the process.[84] The negative repercussions experienced by marginalized individuals subjected to discrimination, in particular, can be attributed to the homogeneity and standardization principles rooted in dataism within the context of the digital welfare state. Using the data trust model is nothing more than a feasible solution to mitigating the consequences through citizen involvement and participation.

The data trust paradigm is based on the assumption that all data are components of the public interests, with the goal of maximizing social interests through data sharing and aggregation from different sources.[85] Disclose and transparency offers a solution to escape the problem of harm fixation. "Trust can be accountable."[86] In order to earn the trust of the data subjects, public authorities should invite data subjects and stakeholders to participate in the consultation process, allowing the government to explain

[84] Sylvie Delacroix & Neil D. Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIVACY L. 236, 240 (2019).

[85] Craglia Massimo, Scholten Henk J., Micheli Marina, Hradec Jiri, Calzada Igor, Luitjens Steven, Ponti Marisa & Boter Jaap, *Digitranscope: The Governance of Digitally-Transformed Society* 47 (JRC Publications Repository, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3801710; Liu Ching-Yi （劉靜怡）, *Cong "Yinsibaohu dao "Ziliaozhili"* (*從「隱私保護」到「資料治理」*) [*From "Protection of Privacy" to "Data Governmence"*], 23 RENWEN YU SHEHUI KEXUE JIANXUN (人文與社會科學簡訊) [HUMANITIES AND SOCIAL SCIENCES NEWSLETTER QUARTERLY] 13, 16 (2022).

[86] Richards & Hartzog, *supra* note 62, at 459.

and disclose how they collect, process their personal data. Additionally, this serves as a means to demonstrate their accountability by identifying the party to whom the legal obligation is attributed. Furthermore, public authorities introduce third parties and independent supervision mechanisms to serve as neutral intermediaries in determining what personal data has been collected, how it was collected and processed, and for what purposes the data was used.[87] Importing the data trust model allows the principles of disclosure and transparency to be operationalized while also presenting a feasible strategy for mitigating the effects of information asymmetry and mitigating the limitations of the digital welfare state mentioned in Section 3.2.

As Ching-Yi Liu noted, a legal expert involved in the Taiwan NIHD case, it was advised that privacy as trust should be the foundation of sharing and reusing the personal data, as well as the core of establishing the legal framework of information and privacy law in Taiwan.[88] The establishment of trust is a crucial factor in facilitating the public sector's ability to gather and analyze personal data, enabling improved decision-making in the realm of social policy and yielding societal benefits. The implementation of the data trust model compelled the government to require the disclosure of information, thereby fostering the development of mutual trust in the informational exchange.

In today's digital welfare states, opaque automated decision-making systems might restrict people's access to social benefits, thereby constituting a violation of social rights.[89] The unrelenting technological advances can result in situations where multiple actors, including third parties with only an indirect stake in a given trove of data, can access the information, including information on social security. A potential outcome of increasingly unfettered access to data can be the discrimination and stigmatization of the poor and of other marginalized and dispossessed people--those who often receive social-security benefits and are therefore often those people least capable of insisting on their rights.[90]

Given that social rights might be unduly violated by automated decision-making systems in the digital welfare state, this paper argued that public authorities establish legal frameworks to implement the data trust model that allows stakeholders to be involved in the decision-making

[87] Massimo et al., *supra* note 85, at 49.

[88] Xianfa Fating (憲法法庭) [Constitutional Court R.O.C. (Taiwan)], Liujingyi Jiaoshou 1110418 Yijianshu (劉靜怡教授1110418意見書) [Legal Opinion of Professor Ching-Yi Liu], 25 (2022), https://cons.judicial.gov.tw/download/download.aspx?id=460801.

[89] Rachovitsa & Johann, *supra* note 28, at 8; Alston, *supra* note 69, ¶ 19-27.

[90] Alston Philip (Special Rapporteur on Extreme Poverty and Human Rights), *Report of the Special Rapporteur on Extreme Poverty and Human Rights*, at 4-5, U.N. DOC A/74/493 (2019), https://documents.un.org/doc/undoc/gen/n19/312/13/pdf/n1931213.pdf?token=dSLhkZazlQbpqoIj5D&fe=true=

process that ensures their data is securely used, and their privacy protected as it applies to social rights in the context of digital welfare states. Furthermore, this paper will argue that the data trust model has the potential to indirectly alleviate other trust-related concerns beyond data in the context of the digital welfare state. Undeniably, algorithms are unable to replace the level of trust and security that is established through face-to-face interactions and contacts. While algorithms cannot fully replace face-to-face meetings, the government could demonstrate its sincerity and commitment by implementing the data trust model, which promotes transparency, disclosure and accountability, as mentioned above. Through this process, the citizens progressively establish trust and confidence in the social welfare system, leading them to engage and provide their data to ensure the effective operation of the social welfare system. Overall, the data trust model could serve as a compromise to alleviate the trust-related issue that arises from the absence of in-person interaction. Only when the mechanism is in place will the data subjects be confident and willing to share their data in order to create and maximize the public value of data.

V. CONCLUSION

By analyzing the Dutch *SyRI* case and the Taiwan NIHD case, the aforementioned cases shed light on the challenges associated with a rights-based privacy approach. These challenges include an emphasis on protecting against privacy infringements rather than fostering value creation, as well as an inherent power imbalance between individuals and the government. This inclination is incongruous with the affirmative essence of social rights and the goals of the digital welfare state. In light of the aforementioned context, the primary contribution of this paper lies in its endeavour to include and introduce the concept of trust as a fundamental value for privacy into the realm of information exchange within the digital welfare state. Moreover, the introduction of public a trust model and the establishment of an independent monitoring system are recommended in this study. This is based on the understanding that disclosure and openness serve as prerequisites and foundations for fostering trust in the information connection. By reframing privacy as a matter of trust rather than solely emphasizing intrusion, it becomes possible to harness privacy as a means to foster societal benefits within the context of the digital welfare state.

REFERENCES

Alston, P. (2019). *Brief by the United Nations Special Rapporteur on Extreme Poverty and Human Rights as Amicus Curiae in the Case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/HA ZA 18/388)*. United Nations Human Rights: Office of the High Commissioner. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

Appelman, N., Fathaigh, R. Ó. & van Hoboken, J. (2021). Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, *12*(4) 257-271.

Big Data Analytics for Policy Making, Report, A Study Prepared for the European Commission DG INFORMATICS (DG DIGIT) (2016). European Commission. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2016-07/dg_digit_study_big_data_ analytics_for_policy_making.pdf.

Carney, T. (2023). The Automated Welfare State: Challenges for Socioeconomic Rights of the Marginalised. In Z. Bednarz & M. Zalnieriute (Eds.), *Money, Power, and AI: Automated Banks and Automated States* (pp. 95-115). England, U.K.: Cambridge University Press.

Chu, M.-C. (朱美珍) (2018). Zixun Keji Dui Shehui Fuli Fuwu Yuesheng Zhuyi Zhi Tantao (資訊科技對社會福利服務躍升助益之探討) [Research on the Benefit of the Advancement of Social Welfare Services through Information Technology]. *Shequ Fazhan Jikan* (*社區發展季刊*) [*Community Development Journal Quarterly*], *161*, 4-19.

Coglianese, C. (2023). Law and Empathy in the Automated State. In Z. Bednarz & M. Zalnieriute (Eds.), *Money, Power, and AI: Automated Banks and Automated States* (pp. 173-188). England, U.K.: Cambridge University Press.

Cheng, H.-Y. & Liu, D.-P. (2022). Early Prompt Response to COVID-19 in Taiwan: Comprehensive Surveillance, Decisive Border Control, and Information Technology Support. *Journal of the Formosan Medical Association*, *23*(1), 2-7.

Delacroix, S. & Lawrence, N. D. (2019). Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. *International Data Privacy Law*, *9*(4), 236-252.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile*

Police and Punish the Poor. New York, U.S.: St Martin's Press.

Fabre, C. (2000). *Social Rights under the Constitution: Government and the Decent Life*. England, U.K.: Oxford University Press.

Hunkenschroer, A. L. & Luetge, C. (2022). Ethics of AI-Enabled Recruiting and Selection: A Review and Research Agenda. *Journal of Business Ethics*, *178*, 977-1007.

Jørgensen, R. F. (2023). Data and Rights in the Digital Welfare State: The Case of Denmark. *Information, Communication & Society*, *26*, 123-138.

Lin, C.-F., Wu, C.-H. & Wu, C.-F. (2020). Reimagining the Administrative State in Times of Global Health Crisis: An Anatomy of Taiwan's Regulatory Actions in Response to the COVID-19 Pandemic. *European Journal of Risk Regulation*, *11*(2), 256-272.

Liu, C.-Y., Li, W.-P. & Tu, Y.-P. (2021). Privacy Perils of Open Data and Data Sharing: A Case Study of Taiwan's Open Data Policy and Practices. *Washington International Law Journal*, *30*(3), 545-597.

Liu, C.-Y. (劉靜怡) (2022). Cong "Yinsibaohu dao "Ziliaozhili" (從「隱私保護」到「資料治理」) [From "Protection of Privacy" to "Data Governance"]. *Renwen Yu Shehui Kexue Jianxun* (*人文與社會科學簡訊*) [*Humanities and Social Sciences Newsletter Quarterly*], *23*(3), 13-18.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. & Byers, A. H. (2011). *Big Data: The Next Frontier for Innovation, Competition, and Productivity*. McKinsey Global Institute. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions /mckinsey%20digital/our%20insights/big%20data%20the%20next%20 frontier%20for% 20innovation/mgi_big_data_full_report.pdf.

Maxwell, J. & Tomlinson, J. (2020). Proving Algorithmic Discrimination in Government Decision-Making. *Oxford University Commonwealth Law Journal*, *20*(2), 352-360.

Richards, N. & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law, S*tanford Technology Law Review*, *19*, 431-472.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York, U.S.: Crown Publishing Group.

Pedersen, J. S. (2019). Chapter 15: The Digital Welfare State: Dataism versus Relationshipism. In J. S. Pedersen & A. Wilkinson (Eds.), *Big Data: Promise, Application and Pitfalls* (pp. 301-324). England, U.K.: Edward Elgar Publishing.

Rachovitsa, A. & Johann, N. (2022). The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case. *Human Rights Law Review*, *22*(2), 1-15.

Richardson R., Schultz J. M. & Crawford K. (2019). Dirty Data, Bad Predictions: Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review*. *94*, 192-233.

Tseng, C.-M. (曾中明) (2013). Weisheng Fulibu Zixun Yewu Tuizhan Gaikuang（衛生福利部資訊業務推展概況）[Overview of the Information Service Promotion of the Ministry of Health and Welfare]. *Zhengfu Jiguan Zixun Tongbao* (*政府機關資訊通報*) [*Government Offices Information Notices*], *312*.

Tseng, C.-M. (曾中明), Cheng, W.-Y. (鄭文義) & Chiu, K.-K. (邱國光) (2005). Neizhengbu Shezheng Zixun Xitong De Xiankuang Yu zhanwang（內政部社政資訊系統的現況與展望）[The Current Situation of and Prospects for the Social Affairs Information System of the Ministry of the Interior]. *Shequ Fazhan Jikan* (*社區發展季刊*) [*Community Development Journal Quarterly*], *111*, 4-17.

van Bekkum, M. & Borgesius, F. Z. (2021). Digital Welfare Fraud Detection and the Dutch SyRI Judgment. *European Journal of Social Security*, *23*(4), 323-340.

Waldman, A. E. (2018). *Privacy as Trust: Information Privacy for an Information Age*. England, U.K.: Cambridge University Press.

Yeh. J.-R. (2016). *The Constitution of Taiwan-A Contextual Analysis*. England, U.K.: Hart Publishing.

「信任」作為數位福利國之隱私和資料治理基礎

黃怡禎

摘　要

隨著因大數據、人工智慧的興起，相關技術逐步應用於社會福利決策領域，數位福利國在此背景下應運而生。本文以2020年荷蘭首次從基本權利觀點對於數位福利國隱私和資料治理進行司法審查的*SyRI*案和2022年臺灣憲法法庭的健保資料庫案為比較分析案例，兩者皆從基本權利觀點出發，作為其司法審查基礎與切點。透過兩則案例分析，凸顯此取徑過於著重消極抵禦侵害面向，而忽略以創造福祉的面向，思考隱私與資料的治理和管制，以及在數位福利國中既存的資訊不對稱關係。本文主張應以「信任」作為數位福利國的隱私和資料治理基礎，並在此基礎上建立資料信任模式，透過獨立監督機制進行事前風險評估，藉此作為在數位福利國創造資料治理福祉最大化和試圖消弭資訊不對稱的可能解方。

關鍵詞：數位福利國、*SyRI*案、健保資料庫案、信任作為隱私基礎