An Analysis of Privacy Policy Research: From the Perspective of Rendition in Surveillance Capitalism Theory

Sachi Kuramoto

Abstract

Privacy policies dictate how data, including personal information, is used in digital services and how privacy is protected. However, data is being bought and sold through data brokers, and digital service providers are rapidly increasing their profits. S. Zuboff calls this situation "surveillance capitalism" and points out that it is based on the mechanism of "rendition," in which all human experience is converted into data, which is then handed over to service companies.

Therefore, in order to investigate how privacy policies work against rendition, it is necessary to organize how privacy policies have been analyzed in previous research and how rendition is or is not addressed. From there, we make recommendations on the state of privacy policy research with a focus on rendition. 75 research articles were included, and they were classified into five categories according to the nature of the research. It can be pointed out that existing privacy policy studies are mostly concerned with policy design and format and with content, and do not recognize rendition as a problem and therefore are insufficient for the protection of personal privacy.

Surveillance capitalism manipulates people's behavior by manipulating people from the level of desire, based on psychologist B.F. Skinner's mode of thinking. The current privacy protection system does not serve the purpose of protecting privacy to promote free will. Digital services manipulate people's behavior through rendition and deprive them of their self-manipulability, leading to the denial of human dignity. Privacy policies do not protect people's self-manipulability and may condone the manipulation of people's behavior.

1. INTRODUCTION

The manner in which personal information and data are used in digital services and the policies for privacy protection are defined by the privacy policies of digital service providers. Although there is no legal definition of privacy policies, the

Japan Advertising Agencies Association (JAA) defines a privacy policy as "a written policy regarding the collection, use, management, and protection of personal information"[1]. According to Jennifer Laird[2], a legal writer for PrivacyPolicies.com, a company that drafts privacy policies for companies' digital services, a privacy policy is a document that discloses what information is collected from users and why it is collected[3]. It specifically describes the collection and use of personal data, such as cookies, and restricts the data that users may share[4].

While these privacy policies are designed to protect personal information, the reality is that, the data generated by the use of digital services such as social networking sites and various applications - data that people provide without consciously or gratuitously[5]- is sold to data brokers by the companies and organizations that operate the digital services.

At the time it was purchased, it is nothing more than a jumble of information. However, data brokers, through their own organization and analysis, extract information on people's behavior and preferences from this data and process it into a usable form. The processed data is then sold to digital service companies that need the information. The digital service companies use the data to look into the

1 Japan Public Relations Association (Retrieved March 29, 2023, https://www.koho.or.jp/useful/qa/sonota/sonota03.html).

2 Assistant Professor of Sociology at Lehman College.

3 Privacy Policy.com, "What is a Privacy Policy?", (Retrieved February 15, 2023, https://www.privacypolicies.com/blog/what-is-privacy-policy/).

4 Digital services have terms of use that are separate from privacy policies. In some cases, the contents of the privacy policy are incorporated into the terms of use (Itakura 2013), but in general, they are created separately. Therefore, in this paper, terms of use and privacy policy are treated as different terms.

5 Rapid digitalization is increasing the influence of information and data in economic and social activities on modern society. Digital services are becoming increasingly popular in many fields, such as healthcare, education, retail, and communication. With the increased use of digital services, large amounts of data are being generated. Much of human behavior, both in the real world and online, is recorded in online services. For example, walking distance and physical activity are converted into health care data, while financial status and income/expenses are converted into data through cashless payment. A user's purchase history on a shopping site provides data on his or her purchasing habits; following a favorite account on a social networking service and "liking" its posts converts data on the person's entertainment and genre preferences; and the user's "likes" on a social networking service converts data on the person's interests and preferences into data.

preferences and usage trends of users, and provide services to individuals in line with them to gain profits. This manipulation of information transforms data, including personal information, into something so important that it has been called "the new oil of the 21st century"[6].

Digital services have thus rapidly increased their profits. This situation, Zuboff argues, is a kind of mutation of capitalism and named it "surveillance capitalism". Surveillance capitalism is "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales" (Zuboff 2019=2021: ii).

Zuboff says that the foundation of surveillance capitalism lies in the transformation (render) of people's experiences into data, which is then handed over (render) to digital service companies. She calls this mechanism "rendition".

What is even more remarkable is that the data people generate online is not only used to understand current preferences and trends. It is also being used as "prediction products" to predict possible behavior on digital services and to manipulate that behavior so that companies can profit from it. For example, companies that use them offer services to people who exhibit certain behavioral tendencies, based on predictions of their likely behavior. In doing so, however, these companies also manipulate the person through digital nudges[7] to make it easier for the person to choose the service[8]. In other words, through their digital services, companies are actually intervening in people's behavioral choices.

Zuboff insists that the basis of surveillance capitalism is a way of thinking that regards human beings not as "individuals" with dignity and personality, but as a group of organisms, or the "Other-One". This thought is derived from the psychologist B.F. Skinner (1971–2013), who based his theory on the idea that people do not choose their actions according to their own will. He argued that humans are

---

6 Ministry of Internal Affairs and Communications, "WHITE PAPER Information and Communications in Japan Year 2008".

7 It has gained attention in behavioral economics as a way to get people to take actions that are desirable for services. Hakuhodo Marketing Systems proposes digital marketing using digital nudges. (Retrieved March 29, 2023, https://www.hakuhodo-ms.co.jp/service/digital_nudge/)

8 Behavioral manipulation through rendition affects not only behavior in web-based services, but also behavior in the real world. As an example, Zuboff mentions the Pokémon Go craze. This application interferes with people's behavior in reality through their smartphones and applications.

always under the control of their surrounding environment, and therefore, all human behavior is merely the result of that control. Thus, he argued that through proper conditioning, human behavior is manipulable, and Zuboff noted that this mode of thinking is at the foundation of surveillance capitalism, which robs human beings of their free will and impairs their dignity.

And in reality, such rendition is quite common in digital services. If so, how do privacy policies function in response to rendition? Although there have been many previous studies on privacy policies, none of them have focused on rendition[9].

A study by S. Shinoda et al. (2017) is a good example of an analysis of various studies on privacy policies. This study reviews the various privacy policy research to date and categorizes them into four categories: "research on the design and format of presented texts," "research on the content of presented texts," "research on the timing of privacy policy presentation," and "correlations among trust, intention to start using services, and intention to acquire data. However, the study does not clarify whether these studies include analyses related to rendition, and there are many subsequent studies that they do not address, as five years have passed since the study was conducted.

Therefore, this paper reorganizes various privacy policy studies that they did not deal with, referring to the classification of Shinoda et al. In other words, I would like to analyze how rendition is or are not treated in various existing privacy policy studies, and then suggest the way of privacy policy research from the perspective of rendition.

2. REFERENCE SURVEY SUBJECTS AND METHODS

In this chapter, I survey various studies on privacy policies, and while focusing on how rendition is treated in these studies, I examine and reorganize the classification items indicated by Shinoda et al. This survey includes the studies on privacy policies mentioned by Shinoda et al. as well as those not mentioned by Shinoda et al. and the latest ones.

2.1. Studies to be investigated

In this paper, I used Google scholar to extract privacy policy research. I

9 The rendition mechanism has existed since before Zuboff pointed it out.

searched for articles using the words “privacy policy” or “privacy policy” (search date: February 1, 2023)[10]. I collected studies that were available online in order of relevance to the search term. Furthermore, I excluded from our survey those studies that did not focus on privacy policies per se. For example, I excluded studies in which privacy policy was only treated as one of the survey items when investigating people’s privacy awareness[11], studies on the technical aspects of developing privacy policy-compliant systems and applications[12], and studies that propose the use of technological mechanisms during policy development to ensure that privacy policies are consistent with privacy laws and regulations[13].

As a result, the remaining 65 research papers (25 in Japanese and 40 in English) were selected for this survey[14]. Of course, this is not an exhaustive list, and the possibility of bias cannot necessarily be ruled out, but on this basis, the survey aims to understand the current trends in this type of research.

2.2. Research methods

Shinoda et al. classify existing studies on privacy policy into the following four categories based on the nature of their research content: “(1) Research on the design and format of presented texts.” “(2) Research on the content of presented texts.” “(3) Research on the timing of privacy policy presentation.” “(4) Correlations among trust, intention to start using services, and intention to acquire data.”

Shinoda et al. do not, however, establish detailed criteria for classification.

---

10 Use only this term in the search as multiple keywords yield very few hits in the literature. For example, in Google Scholar, a search for literature on privacy policies of a particular company by combining the names of specific companies turned only a small number of research that briefly mentioned a paticular company’s privacy policy in the context of an analysis of privacy policies.

11 Tabata, Akio, 2014, “<Research Note> Privacy Awareness of Kwansei-Gakuin University Students: in regard of “Privacy Paradox”, *Bulletin of the Faculty of Sociology, Kwansei Gakuin University*, 118: 89–101.

12 Kojima, Takao, and Yukio Itakura, 2008, “The Automatic Analyzing Method of a Privacy Policy Matching Engine,” *Computer Security Group (CSEC)*, 21 (2008–CSEC–040), 91–96.

13 Backes, Michael, Markus Durmuth, and G. Karjot, 2004, “Unification in privacy policy evaluation-translating EPAL into Prolog.”, *Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2004).*

14 The reason for the small number of Japanese-language references compared to English-language references is that I could not find more than 30 papers on the subject of privacy policy that were available for review.

Moreover, in their classification, they merely describe the essence of the studies included in each category in a simplified manner. Therefore, I will reexamine the contents of the papers to which Shinoda et al. to refers to and elaborate the criteria for classification.

First, in "(1) Research on the design and format of presented texts," Shinoda et al. classify the studies by Y. Pan et al. (2006), I. Adjerid et al. (2013), J. Gluck et al. (2016), and P. G. Kelly et al. (2009).

Pan et al. found that the amount of text in a privacy policy has no effect on users' sense of trust. Adjerid et al. and Gluck et al. rather find that short privacy policies are effective in communicating information. Kelly et al. made a comparison table of privacy policy designs of financial institutions and investigated the extent to which different designs affect users' understanding of the policies.

All of these studies, which Shinoda et al. chose for classification (1), consider the relationship between the form and quantity of the policy and users' understanding of the policy rather than the content of the privacy policy itself. In other words, it can be said that Shinoda et al. assumed that the criterion for classification (1) was whether the study focused on the quantity, textual expression, and structure of privacy policies.

Next, as "(2) Research on the content of presented texts," Shinoda et al. cite the studies by Takasaki et al. (2014) and B. Brendt et al. (2005). Takasaki's study suggests that the degree of transparency in the explanation of how data is used influences privacy concerns.

Brendt et al. investigated whether a difference in willingness to provide data to a website occurs between groups that read policies written in accordance with EU data protection regulations and those that do not, and found that no significant difference occurs. These are studies on the content of privacy policies and the impact of their content on users, and Shinoda et al. include in category (2) studies that focus on the content of privacy policies, rather than on the amount of text or format of the privacy policy.

Next, "(3) Research on the timing of privacy policy presentation" includes studies by H. Takasaki et al. (2010), I. Adjerid et al. (2013), J. Lin et al. (2012), R. Balebako et al. (2013) and R. Balebako et al. (2015). According to Takasaki et al.'s study, obtaining prior consent from users to use data and other information through privacy policies does not affect users' intentions to use services or to disclose information.

Adjerid et al. found that 15 seconds after a privacy policy is presented, people who read the policy forget its content; Lin et al. found that whenever an application accesses a mobile device's internal resources, informing the user of the access status improves the user's privacy awareness by informing the user each time the application accesses the internal resources of the mobile device. Lin et al. also suggest that clearly communicating the purpose of data use can increase user trust in the service provider and reduce user anxiety, benefiting both the user and the service provider.

Balebako et al. (2013) conducted an experiment in which users were presented with the individual details of their privacy policy, such as the transmission of data to external parties and access to data by applications, at the appropriate time (just-in-time), and found that users were not fully aware of how their data was shared with third parties. It became clear that users were not fully aware of how their data was shared with third parties. Therefore, I point out that it is undesirable to assume that users understand the trade-offs between applications and data sharing.

Furthermore, according to Balebako et al. (2015), displaying a privacy notice each time a smartphone application is being used improves recall compared to displaying it in the app store. Thus, making privacy policies more memorable can help people make well-informed decisions about privacy.

Shinoda et al. labeled these studies as "research on the timing of privacy policy presentation," but this includes studies that focus not only on the timing but also on the effects that the presentation method causes on users. For this reason, the classification name in this paper is changed from that set by Shinoda et al. and is now "(3) Research on how privacy policies are presented."

Next, "(4) Correlations among trust, intention to start using services, and intention to acquire data" includes studies by M.J. Metzger et al. (2006) and H. Takasaki (2010). Metzger et al. found that certain trust and assurance mechanisms, including privacy policies, e-retailers' reputation, and concerns about personal privacy and data security on trust in commercial websites and disclosure of personal information, and concluded that the content of privacy policies have no effect on trust in or disclosure of information to retailers via the Internet.

Takasaki et al. also found that the higher the concern for privacy protection, the lower the willingness to disclose data and use services. Based on the inclusion of such studies, it can be said that studies analyzing the impact of privacy policies on users' sense of trust fall under this category.

Shinoda et al. classify these studies as "correlations among trust, intention to start using services, and intention to acquire data", but the studies categorized there rather explore the nature of privacy policies that promote people's use of services. Therefore, for the classification in this paper, I use the classification name of "(4) Research on the relationship between privacy policies and intention to use services," which is different from the classification name of Shinoda et al.

So far, we have organized the four classifications by Shinoda et al. and attempted to review the criteria for the literature review conducted in this paper. However, there are various privacy policy studies other than those discussed by Shinoda et al., and not a few of them do not fall under any of the classifications. For this reason, a fifth classification, "(5) Others," is proposed in this paper. In the next section, we will classify and organize previous privacy policy research based on these five categories.

3. CLASSIFICATION RESULTS

In this chapter, the studies selected in Section 1 of Chapter 2 are classified according to the classification criteria in Section 2.2. First, the number of eligible papers by classification is shown below. In reviewing the classification results for both Japanese and English literature, it can be seen that "(1) Research on the design and format of presented texts" and "(2) Research on the content of presented texts" and "(5) Others" are common to both researches written in either language. In particular, the fact that (1) is more common than the other items is also common to both Japan and other countries.

From these findings, it can be assumed that privacy policy research in Japan and research in other countries are in a similar direction. Based on these results, the reviewed studies under study were categorized and are shown in Table 1. The number of research used in the study by Shinoda et al. is shown in parentheses <>. The research papers subject to classification are also listed in Table 2 at the end of this paper.

Table 1　Classification table of the reviewed research

Classification	Number of research (Japanese)	Number of research (English)	Number of research (Japanese and English)
(1)	9	23 <4>	32 <4>
(2)	6 <1>	15 <1>	21 <2>
(3)	3 <1>	1 <1>	4 <2>
(4)	3 <1>	2 <1>	5 <2>
(5)	7	6	13
Total	28 <3>	47 <7>	75 <10>

Note: (1) Research on the design and format of presented texts
(2) Research on the content of presented texts
(3) Research on how privacy policies are presented
(4) Research on the relationship between privacy policies and intention to use services
(5) Others
The numbers in parentheses <> are the number of references that were included in the study by Shinoda et al. (2017) in the research that are the subject of analysis in this paper.

3.1. (1) Research on the design and format of presented texts

(1) is a group of studies that focus on the difficulty and complexity of the text and structure of privacy policies as factors that hinder users' understanding and propose improvements. Studies categorized here include F. Liu et al. (2018), K. Takemori et al. (2013), S. Kanamori et al. (2017), K. Kawaguchi (2019), and Y. Shvartzshnaider et al. (2019). Users do not understand privacy policies, let alone read them, as Liu et al. (2018) noted. Shvartzshnaider, Kanamori, and Kawaguchi cited expressions that were difficult or ambiguous as reasons for this. Kanamori also pointed out that privacy policies for paid services are more likely to be read than those for free services. Liu and Takemori suggested the need to construct a clear privacy policy, for example, a system that automatically arranges the important information that each company should include in its privacy policy. M. Bergmann (2009) presents a proposal to display privacy policy items that are relevant to the use of the service, noting that such a display method would increase users' privacy awareness.

A. Besmer et al. (2010), E. Costante et al. (2012), F. Liu et al. (2014), and K. Ghazinour et al. (2016) have raised measures to devise privacy policy design and format. Besmer et al. propose incorporating social navigation[15] features into privacy

15　Social navigation is the sharing and use of knowledge and information among users on the Internet for decision making and problem solving in the use of digital services (Aragaki and

policy displays to facilitate people's understanding of privacy policy content and to assist them in decision making.

Costante et al. and Liu et al. (2014) suggest that using machine learning techniques to analyze and categorize the content of privacy policies can help create policies that make it clear what part of the data used by digital services the policy covers. Ghazinour et al. also examined the usability impact of policy simplification using a Privacy Policy Visualization Model (PPVM) as a measure to facilitate the reading of privacy policies, noting that it enables users to make informed decisions.

However, if when we consider that understanding privacy policy also means understanding that using a service means being taken in by the rendition mechanism, then this group of studies in this classification is also indirectly related to rendition.

The purpose of these studies is to improve users' understanding of privacy policies, not to focus directly on rendition. However, studies on the design and format of privacy policies increase the probability that users will read privacy policies and contribute to a better understanding of privacy policies by users, so that users can make decisions about using services based on a more accurate understanding of the contents of privacy policies. And this is the reason why I can say that this category of studies is intended to. Therefore, it can be said that this group of studies in this category is also indirectly related to rendition.

3.2. (2) Research on the content of presented texts

Studies focusing on privacy policy content are diverse. First, there are studies by A. Alabduljabbar (2022), S. Cockcroft et al. (2016), and L.B. Movius et al. (2009) that compare privacy policy content. Alabduljabbar examined privacy policies for paid and free content and found that policies for paid content were relatively transparent regarding data protection and other issues, while free content did not differ much in policy content despite the different content. Cockcroft et al. and Movius focused on cultural differences and found that these differences were reflected in privacy policy content.

In another studies, Md. Moniruzzaman et al. (2010) pointed out that controlling access to data through policies is what privacy is all about, and privacy can be protected by clearly stating the control of data access within privacy policies.

Yasumura 2014).

B. Andow et al. (2019) also analyzed 11430 application privacy policies using PolicyLint[16] and noted that 14.2% of them contained inconsistencies that could indicate misleading statements.

Thus, the analysis of privacy policy content includes a comparison of policy content and pointing out problems that current privacy policies have. Since there are studies that suggest changing the contents of privacy policies in a way that limits the collection of data, it can be said that studies are included to deter the progression of rendition.

3.3. (3) Research on how privacy policies are presented

Research on privacy policy presentation includes those by V. Bannihatti Kumar et al. (2020), S. Ichinose et al. (2013), A. Takenouchi et al. (2020), and F. Shinbo (2003).

Kummer et al. propose a presentation method that extracts only the opt-out portion of the privacy policy. Ichinose et al. propose a presentation method that extracts only the opt-out part of the privacy policy. Ichinose et al. point out that few applications properly post privacy policies. According to Takenouchi et al., devising a method of presenting privacy policies and other terms of use did not promote users' reading of the terms. Shinbo points out that privacy policies need to be posted in appropriate situations in administrative services as well.

Although these research does not focus on rendition, they can improve users' awareness of privacy policies by studying the appropriate presentation of policies. Therefore, it can be said that these studies promote the users' understanding of the existence and content of privacy policies for digital services before using them, and these studies can be said to have a deterrent effect on the progression of rendition.

3.4. (4) Research on the relationship between privacy policies and intention to use services

Research by S. Shinoda et al. (2017), H. Takasaki (2016), L.J. Strahilevitz et al. (2016), and H.M. LaMonica et al. (2021) analyzed the relationship between privacy policy and intention to use services.

Shinoda et al. propose a survey method to analyze whether changes in users'

16 PolicyLint is a lint tool designed to identify inconsistencies within privacy policies. A lint tool is a checking tool that can verify the description of source code in a programming language against various rules.

intentions and behavior due to the presentation of privacy policies benefit service providers.

Takasaki analyzes how people's privacy concerns affect their intention to use the service, and points out that there are various types of privacy concerns, including latent anxiety, resistance to information disclosure, and concern about secondary use infringement. He then points out the need to address each type of concern, since the problematic factors differ for each type of concern. He then points out that the perception of privacy policy by people may cause a decrease in their willingness to use the service.

Strahilevitz et al. point out that even if users of a service read the privacy policy, it does not affect their trust in the service. LaMonica et al. point out that the lack of transparency in privacy policies undermines users' trust that steps are being taken to protect the privacy of their personal information.

Although these studies do not deal directly with rendition, given the development of each study that the way privacy policies are presented creates a sense of trust in digital services and encourages their use, it can be said that the study in category 4 differs from (1), (2), and (3) in that it considers privacy policies as something that facilitates rendition.

3.5. (5) Others

In this section, I will organize studies that are not included in the above four categories. First, as a survey of the status of personal information protection, there is the study by S. Hashimoto (2002), who found that the Personal Information Protection Law did not fully protect personal information in the 2000s, when the formulation of privacy policies had not progressed. Even with progress in policy formulation, A.M. Arellanop et al. (2018) pointed out that personal information was not sufficiently protected, using medical information as an example.

In addition to M. Numao (2006) and A. Aljeraisy et al. (2022), who pointed out the inadequacy of privacy protection regulations as a whole, not just privacy policies, and advocated the creation of a privacy protection system. M. Warkentin et al. (2011) analyzed what influences firms' compliance with privacy policies.

These studies, however, like the ones I have seen in the previous sections, do not focus on rendition. Currently, people's personal information is supposed to be protected in writing by privacy policies. On the other hand, rendition mechanisms that convert such personal information into data and buy and sell it have been

established and continue to operate without restrictions. And an analysis of existing research in this chapter reveals that no research has been conducted on such a current situation.

The studies included in (1), (2), (3), and (4), which are related to improving users' understanding of privacy policies and thereby improving their intention to use services, are not necessarily unrelated to promoting rendition. Nevertheless, not only are they not targeted at rendition, but they are also not designed with rendition in mind. This suggests that existing privacy policy studies have not even recognized rendition as an issue. If this is the case, then they were only extremely inadequate studies for the protection of individual privacy.

4. NECESSARY PERSPECTIVES: INSTRUMENTALISM, FREE WILL AND SELF-MANIPULABILITY

Then what perspective should privacy policy research focused on rendition take? As indicated in Chapter 1, rendition is the process by which digital service companies transform people's experiences into data and hand it over to other companies. In this chapter, I organize Skinner's "Other One" mode of thinking, which underlies surveillance capitalism, to identify clues for conducting privacy policy analysis focused on rendition. I will then examine the perspectives needed to conduct privacy policy research.

4.1. Operant conditioning and free will

Skinner's thought is that if the manipulator, whose goal is to manipulate people as intended, views people not as individuals with personalities but as "others," or groups of "organisms," and manipulates human behavior from the level of desire, the manipulator can elicit the intended behavior. In this section, I will introduce this mode of thinking presented by Skinner, with particular focus on its relation to free will.

Skinner's theory was inspired by the work of I.P. Pavlov[17], who discovered the

17 Dogs salivate under the unconditional stimulus of being fed, but when a conditioned stimulus of ringing a bell is added before feeding, they salivate just by hearing the bell, even if they are not shown the food. Pavlov discovered the mechanism of this "conditioned reflex" (Fukumoto 2019).

mechanism of conditioned reflexes, J.B. Watson[18], who studied reflex behavior with a focus on conditioned reflexes in the field of psychology, and E.L. Thorndike, who discovered the "law of effects," which states that among the responses animals make to stimuli, responses that have some form of effect tend to occur in association with the stimulus (Kanahara 2011: 3).

All of these studies took the position that all human behavior is not caused by man's own will, but by external stimuli; Skinner placed the behavioral reflexes pointed out by Pavlov in the context of classical conditioning theory, and in particular, he developed "operant conditioning," which developed from Thorndike's study. Operant conditioning is a type of conditioning in which a specific stimulus is applied to a subject to induce a spontaneous behavior other than the direct response to the stimulus, so that the behavior can always be elicited when the stimulus is applied. Skinner argues that by manipulating the behavior produced in response to a stimulus, it is possible to induce people to voluntarily perform a behavior that is desirable to the operator.

Zuboff calls this surveillance capitalism, in which companies that provide digital services interfere with people's actions and thoughts, manipulating them into choosing behaviors that increase the provider's profits. She points out that the system of surveillance capitalism uses what Skinner calls an "operant conditioning" approach. Zuboff's point that "Skinner's vision is brought to life in the relentless pursuit of surveillance capitalism's economic imperatives and the ubiquitous digital apparatus that surveillance capitalism creates and harnesses to its novel aims." (Zuboff 2019=2021: 428) is that through digital devices like smartphones, people to act in ways that benefit the corporations under surveillance capitalism, a system of operant conditioning is being used.

Regarding the implementation of Skinner's vision in surveillance capitalism, Zuboff further argues that people's actions in digital services are not the result of their own free will choices, but are the result of the addition of external factors, including digital nudges. Nevertheless, she says that in these services, people are "*made to appear*" as if they themselves are freely choosing their actions. In other words, she strongly criticizes surveillance capitalism as an erosion of people's free

18 Watson argued that for psychology to be a science, it should not focus on something as vague as the mind, and that research should focus on conditioned reflexes (Kanehara 2011).

will[19].

Behaviorist psychology, including Skinner's theory, has been criticized since its publication for its dehumanizing effect, with A. Kohn (2001) claiming that Skinner's theory uproots humanity and removes the elements that make human beings human. On the other hand, psychologist S. Pinker (2004), science journalist M. Brooks (2010), and O. Miyagi (1968), among others, argued in defense of Skinner, claiming that it is an illusion to believe that humans act by free will in the first place (Kanehara 2011). Miyagi, in particular, points out that what people consider to be freedom is merely a "sense of freedom. For example, if a child tries to eat what he or she wants to eat and is scolded by his or her parents, the child will stop eating for fear of punishment. In this case, the child would feel as if he or she voluntarily made the choice not to eat, but in reality, the child is only making the choice out of fear of punishment. This is not a true act of free will, but merely the formation of a sense of freedom.

Thus, even before Zuboff's theory, there were arguments against Skinner's theory, such as whether operant conditioning undermines free will, and whether free will exists in the first place[20]. In response to these arguments, Zuboff points out that free will is the human condition and the root of human nature. She also makes the following interesting point about free will and privacy protection. She states that in a system of surveillance capitalism based on operant conditioning, "There is ... only the steady displacement of the will to will that has been embodied in self-determination, enpressed in the first-person voice, and nourished in the kind of sanctuary that depends upon the possibility of private life and the promise of public freedom." (Zuboff 2019=2021: 436). This "new will" is action and thought through operant conditioning. And as surveillance capitalism permeates, the supposedly free will of the individual is being "replaced" by this "new will".

Zuboff believes that privacy protection promotes free will. Therefore, she believes that privacy protection is closely related to opposing surveillance capitalism, which denies individual free will. However, she notes that the current

19 And Zuboff adds that this own idea is by no means "not an indulgence in nostalgia or a random privileging of the pre-digital human story as somehow more truly human" (Zuboff 2019=2021: 380).

20 Regarding free will, Zuboff notes that people can influence the future through their own free will and that "*the assertion of freedom of will also asserts the right to the future tense as a condition of a fully hunan life*." (Zuboff 2019=2021: 381).

privacy institutions and laws are not designed to protect privacy. The problems with existing privacy policy research that we have seen so far are also indicative of this very thing. In other words, privacy policy researchers have completely overlooked the very areas that Zuboff sees as the keystone of privacy protection.

Unfortunately, however, Zuboff does not go into the specifics of the relationship between privacy protection and free will, and thus surveillance capitalism, and her discussion remains abstract. Therefore, I will now focus on the relationship between privacy protection and free will in order to examine what perspectives are needed for privacy policy research that incorporates a rendition perspective.

4.2. Free will and privacy: deprivation of self-manipulability

In considering the concept of privacy, while the majority of research has been conducted from the perspective of victims of the invasion of privacy, T. Sakamoto (2009) has raised the importance of considering privacy from the perspective of the "assailant" of the invasion of privacy, that is to say, he pointed out the importance of considering privacy from the perspective of the "infringing" party. He argued that the privacy issue should be considered not from the perspective of the party whose personal secrets or hidden things are revealed or whose personal information is leaked, but also as an issue of information production, in which personal information is produced regardless of the facts or will of the individual and used for the producer's own benefit[21].

Sakamoto bases this argument on the theories of E. Goffman (1961=1984), who conducted fieldwork with inpatients in psychiatric wards and the staff who treat and care for them, as well as the organizational, institutional, and institutional environments for diagnosis, treatment, and care ("*Asylum*"). In these institutions, inmates are indeed under total "surveillance" and are not free to make their own choices about their behavior. Nevertheless, at least some of them there engage in "secondary coordination," trying to circumvent institutional rules and conspiring with institutional staff, which, according to Goffman, leads to a sense that the patients still retain some of their dignity.

For Goffman, society is nothing more than a social situation brought about by

21 In this regard, Sakamoto noted that secrets and concealments may also be communicated to others depending on the situation, and personal information may also be registered as needed, and that the content of the information is not the issue.

face-to-face interaction. From this sociological perspective, in every social situation, people live by creating their own selves "outside" of the society, that is, "outside" of their individual social situation, through which they manipulate their selves toward the society. That is to say, in every social situation, people live by creating their own self for each situation and presenting it to others in the situation. In doing so, the place where the self is created is always outside of the social situation, and that is where the self is generated. This way of life is a way of relating people to society that is unique to modernity, and here I can see the connection between the dignity, autonomy, or sanctity of the modern individual and dramaturgy in Goffman's sociology.

Even in mental hospitals (asylums), which seem to be completely supervised institutions, the inmates who are committed there generate themselves differently from that required by the institution in the form of "secondary adjustment" and attempt to manipulate the social conditions of the institution in various ways. Moreover, they are to some extent successful in their attempts. Through these observations, Goffman reveals the dignity and meaning of the individual that can exist even in these environments. That is, even in an environment of total surveillance, people behave in such a way that they find their own dignity through having an outside of the social situation and finding cracks here they can behave manipulatively in some way toward society.

In other words, the place where the self is created is always outside of the social situation, and that is where information about the self is produced. He pointed out that human dignity lies in "self-manipulability," in which people create a desirable self for themselves by deciding how they behave and act, and by manipulating themselves to disclose or conceal information about the self.

From this, Sakamoto says that the meaning of privacy lies in the fact that each individual can manipulate his or her own self and have a self outside of the social situation that he or she can create for himself or herself. In other words, he pointed out that each individual is able to create his or her own self which is suitable for each social situation, and that the ability to create and maintain one's own social face through this process is what brings about the dignity of the human being in modernity.

He then stated that the place where the self is generated was in the private sphere in modern society, but in modern society, it has shifted to the information system. In modern society, where the status system has been eliminated, people

are now free to create and perform themselves. Individuals are now in a position to manipulate themselves in the private sphere. However, in today's data-driven information society, the place where the individual self is created has shifted to the information system, which is "outside" the self. For example, driver's licenses and credit cards, which serve as proof of identity, have been converted into data, and information about one's inner self, such as personal preferences, has been converted into data in the form of purchase histories.

In this changing site of self-production, many of today's digital services predict people's behavior through rendition and manipulate their behavior to increase their profits. In other words, it is no longer possible for individuals to freely direct themselves. In other words, people lose their self-manipulability through the use of digital services.

The loss of self-manipulability means that people are deprived of their free will to freely create themselves. In the case of digital services, if people can select information to be provided to the information system from among information about themselves, or if there is room for manipulation of personal information consisting of data, self-manipulability can be said to be barely preserved. However, today, most services do not have such a mechanism[22]. Therefore, users provide data brokers with all information generated through the use of digital services, whether they like it or not, but they are not involved in the production process of new information that is created from such information.

Not only that, people are manipulated in their behavior through rendition using data collected by digital services. This means that people today are no longer able to direct themselves based on their free will and have lost their self-manipulability. Thus, it can be pointed out that rendition is a denial of human dignity since intervening and manipulating human free will leads to the deprivation of human self-manipulability.

As the previous research organized in Chapter 3 points out, existing privacy policy research does not include a perspective on rendition, with Zuboff accusing privacy policies of not explicitly stating that users' data will be handed over to third parties, even within the rendition mechanism, privacy policies are "*surveillance policies*" and a "baroque and perverse" entity that infiltrates rendition

22 Although "Personal Data Trust Bank" systems exist, in which people can choose what they want to offer from the data they generate and sell it for a fee, it is not yet widespread enough.

without users' knowledge (Zuboff 2019=2021: 53)[23].

Therefore, it can be pointed out that privacy policies may not protect people's self-manipulability. However, as I have noted in the previous chapters, existing privacy policy research has not addressed this point. In order to conduct research focused on rendition, it is necessary to note that privacy policies do not protect people's self-manipulability, but allow the manipulation of people's behavior for the expansion of economic benefits.

5. CONCLUSION: PRIVACY POLICY AND SELF-MANIPULABILITY

This paper pointed out that rendition, which Zuboff identifies as the mechanism that forms the basis of surveillance capitalism, is also an important perspective in privacy policy research, and I argued that existing privacy policy research has not focused on rendition.

Digital service companies use the data obtained through rendition to manipulate the behavior of digital service users. This destroys the self-manipulability potential that people are supposed to have, and threatens their dignity. In other words, the rendition mechanism is the root of this problem. However, it is clear that current privacy policy research has not focused on rendition.

Therefore, future privacy policy research should focus on whether and in what way each digital service company's privacy policy permits rendition. In other words, there is a need to analyze the content of privacy policies from the perspective of rendition.

In future research, I plan to conduct a content analysis of privacy policies as they are actually presented to the public. Zuboff argues that "Individual privacy is a casualty of this (surveillance capitalism) control, and its defense requires a reframing of privacy discourse, law, and judicial reasoning." (Zuboff 2019=2021: 217), but the various existing studies mentioned in this paper suggest limitations in pointing out problems with policies. Therefore, there is a need to go beyond the existing privacy policy research frameworks to properly identify the problems of surveillance capitalism.

---

23 In particular, Zuboff criticizes the rendition process by which policies tacitly allow users' data to be sold to third parties, stating that "privacy policies are more aptly referred to as *surveillance policies*" (Zuboff 2019=2021: 285).

Table2　List of references classified in Chapter 3

classification (1) Research on the design and format of presented texts

Angulo, Julio, et al., 2012, "Towards usable privacy policy display and management," *Information Management & Computer Security*, 20.1: 4–17.

Bardus, Marco, et al., 2022, "Data management and privacy policy of COVID-19 contact-tracing apps: Systematic review and content analysis," *JMIR mHealth and uHealth*, 10.7: e35195

Bergmann, Mike, 2009, "Testing privacy awareness," *The Future of Identity in the Information Society: 4th IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School, Brno, Czech Republic, September 1–7, 2008, Revised Selected Papers 4*. Springer Berlin Heidelberg.

Besmer, Andrew, Jason Watson, and Heather Richter Lipford, 2010, "The impact of social navigation on privacy policy configuration," *Proceeding of the Sixth Symposium on Usable Privacy and Security*.

Brodie, Carolyn A., Clare-Marie Karat, and John Karat, 2006, "An empirical study of natural language parsing of privacy policy rules using the SPARCLE policy workbench," *Proceeding of the second symposium on Usable privacy and security*.

Costante, Elisa, et al., 2012, "A machine learning solution to assess privacy policy completeness: (short paper)," *Proceeding of the 2012 ACM Workshop on Privacy in the Electronic Society*.

Gandy Jr, Oscar H., 2003, "Public opinion surveys and the formation of privacy policy," *Journal of social issues*, 59.2: 283–299.

Ghazinour, Kambiz, Maryam Majedi, and Ken Barker, 2009, "A model for privacy policy visualization," *2009 33rd Annual IEEE International Computer Software and Applications Conference*. Vol. 2. IEEE.

Ghazinour, Kambiz, and Tahani Albalawi, 2016, "A usability study on the privacy policy visualization model," *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. IEEE.

Kanamori, Sachiko, et al., 2017, "Categorization based on the Ambiguity and Amount of Information Associated with a Named Entity of Privacy Policy A Study on Transparency in Privacy Policies," *Proceeding of the Computer Security Symposium 2017*, 2.

Kanamori, Sachiko., et al., 2019, "Cross-Cultural Analysis for Constructing a User Support Tool to Understand Privacy Policies," *Proceeding of the Computer Security Symposium 2019*: 222–228.

Kanamori, Sachiko, et al., 2020, "Categorization based on the Ambiguity and Amount of Information Associated with a Named Entity of Privacy Policies -A Study on Transparency in Privacy Policies," *The 34th Annual Conference of the Japanese Society for Artificial Intelligence*.

Karat, John, et al., 2005, "Privacy in information technology: Designing to enable privacy policy management in organizations," *International Journal of Human-Computer Studies* 63.1–2: 153–174.

Karjoth, Günter, and Matthias Schunter, 2002, "A privacy policy model for enterprises," *Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15*. IEEE.

Kawaguchi, Kanako, 2019, "What is it like "the plain explanation to the general public" for their privacy preserving?," *Chiba University Graduate School of Humanities and Studies on Public Affairs. Research Project Reports*, 342: 16–24.

Kumaraguru, Ponnurangam, et al. 2007, "A survey of privacy policy languages," *Workshop on Usable IT Security Management (USM 07): Proceeding of the 3rd Symposium on Usable Privacy and Security, ACM*.

Lipford, Heather R., et al., 2010, "Visual vs. compact: A comparison of privacy policy interfaces," *Proceeding of the SIGCHI Conference on Human Factors in Computing Systems*.

Liu, Fei, et al., 2014, "A step towards usable privacy policy: Automatic alignment of privacy statements," *Proceeding of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers*.

Liu, Frederick, et al., 2018, "Towards automatic classification of privacy policy text," *School of Computer Science Carnegie Mellon University*.

Magata, Fumihiko, et al., 2019, "A connotative framework for optimizing system implementation of purposes of processing of personal information applied to reorganization of NTT DOCOMO privacy policy," *IPSJ SIG Technical Report*, 3: 1–8.

Meier, Yannic, Johanna Schäwel, and Nicole C. Krämer, 2020, "The shorter the better? Effects of privacy policy length on online privacy decision-making," *Media and Communication* 8.2: 291–301.

Najmeh, Mousabi N., et al., 2020, "Establishing a strong baseline for privacy policy classification," *ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia*, September 21–23, 2020, Proceedings 35. Springer International Publishing.

Pardo, Raúl, and Gerardo Schneider, 2014, "A formal privacy policy framework for social networks," *Software Engineering and Formal Methods: 12th International Conference, SEFM 2014, Grenoble, France*, September 1–5, 2014, Proceedings 12. Springer International Publishing.

Sathyendra, Kanthashree M., et al., 2017, "Identifying the provision of choices in privacy policy text," *Proceeding of the 2017 Conference on Empirical Methods in Natural Language Processing*.

Shinoda, Shiori, 2020, "Users Evaluation of Expression and Representation of Privacy Policy's Contents," *Information Processing Society of Japan*, 61(6): 1146–1174.

Shvartzshnaider, Yan, et al., 2019, "Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis," *Proceeding of the AAAI Conference on Human Computation and Crowdsourcing*, 7.

Takemori, Keisuke, et al., 2013, "Third party review framework for privacy policy of application/contents," *Research Report Computer Security (CSEC)*, 62: 1–8.

Tesfay, Welderufael B., et al., 2018, "PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation," *Proceeding of the Fourth ACM International Workshop on Security and Privacy Analytics*.

Wilson, Shomir, et al., 2016, "The creation and analysis of a website privacy policy corpus," *Proceeding of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*.

Yatsugawa, Naonobu, 2015, "Appropriate Handling of Personal Data based on Privacy-by-Design," *Unisys technology review*, 34(4): 221–240.

Yu, Le, et al., 2015, "Autoppg: Towards automatic generation of privacy policy for android applications," *Proceeding of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*.

Yuriyama, Madoka, Yuji Watanabe, and Masayuki Numao, 2003, "A Method for Partitioning Privacy Policy Definition Based on ID Type for Virtual ID System," *IEICE Conferences Archives*, The Institute of Electronics, Information and Communication Engineers.

classification (2) Research on the content of presented texts

Alabduljabbar, Abdulrahman, and David Mohaisen, 2022, "Measuring the privacy dimension of free content websites through automated privacy policy analysis and annotation," *Companion Proceeding of the Web Conference 2022*.

Andow, Benjamin, et al., 2019, "PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play," *USENIX Security Symposium*.

Andrade, Eduardo B., Velitchka Kaltcheva, and Barton Weitz, 2002, "Self-disclosure on the web: The impact of privacy policy, reward, and company reputation," *ACR North American Advances*.

Antón, Annie I., et al., 2007, "A roadmap for comprehensive online privacy policy management," *Communications of the ACM*, 50(7): 109–116.

Brown, Michael, and Carrie Klein, 2020, "Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents," *The Journal of Higher Education*, 91(7): 1149–1178.

Chowdhury, Omar, et al., 2013, "Privacy promises that can be kept: a policy analysis method with application to the HIPAA privacy rule," *Proceeding of the 18th ACM symposium on Access control models and technologies*.

Cockcroft, Sophie, and Saphira Rekker, 2016, "The relationship between culture and information privacy policy," *Electronic Markets*, 26: 55–72.

Hyman, David A., and William E. Kovacic, 2018, "Implementing Privacy Policy: Who Should Do What," *Fordham Intell. Prop. Media & Ent. LJ*, 29: 1117.

Ikigai, Naoto, 2010, "Online privacy and self-regulation: Behavioral targeting advertising regulations in EU and U.S.," *Journal of The Japan Society of Information and Communication Research* 28.3: 105–113

Isohara, Takamasa, et al., 2013, "Privacy Policy Generation Assistant-mechanism based API and External Module detection for Android Application," *IPSJ SIG Technical Report 2013*. 63: 1–8.

Itakura, Yoichiro, 2017, "A Consideration of Privacy Contracts (1)," *Journal of Law and Information System*, 1: 28–35.

Itakura, Yoichiro, 2018, "A Consideration of Privacy Contracts (3)," *Journal of Law and Information System*, 3: 73–76.

Itakura, Yoichiro, 2019, "A Consideration of Privacy Contracts (6)," *Journal of Law and Information System*, 6: 69–74.

Linden, Thomas, et al., 2020, "The privacy policy landscape after the GDPR," *Proceedings on Privacy Enhancing Technologies*, 2020(1): 47–64.

Moniruzzaman, Md, Md Sadek Ferdous, and Roksana Hossain, 2010, "A study of privacy

policy enforcement in access control models," *2010 13th International Conference on Computer and Information Technology (ICCIT)*. IEEE.
Movius, Lauren B., and Nathalie Krup, 2009, "US and EU privacy policy: Comparison of regulatory approaches," *International Journal of Communication*, 3: 19.
Sadeh, Norman, et al., 2013, "The usable privacy policy project," *Technical report, Technical Report, CMU–ISR–13–119*, Carnegie Mellon University.
Slavin, Rocky, et al., 2016, "Toward a framework for detecting privacy policy violations in android application code," *Proceeding of the 38th International Conference on Software Engineering*.
Such, Jose M., and Michael Rovatsos, 2016, "Privacy policy negotiation in social media," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 11(1): 1–29.
Takasaki, Haruo, 2016, "A Study on Consumer Preferences for Personalized Services: An Empirical Analysis Focusing on the Diversity of Privacy Concerns," *Journal of The Japan Society of Information and Communication Research*, 34(3): 25–39.
Wishart, Ryan, et al., 2010, "Collaborative privacy policy authoring in a social networking context," *2010 IEEE International Symposium on Policies for Distributed Systems and Networks*. IEEE.

classification (3) Research on how privacy policies are presented

Bannihatti Kumar, Vinayshekhar, et al., 2020, "Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy text," *Proceeding of The Web Conference 2020*.
Ichinose, Sayo, et al., 2013, "Survey on the Current Status of Application Privacy Policy Posting in Smartphone Apps," *CSEC: Computer Security Group (CSEC)*, 61: 1–6.
Shinbo, Fumio, 2003, "Significance and Current Status of Privacy Policy Posting in Administrative Agencies: Focusing on the Efforts in the U.S. Federal Government Agencies," *Information Media Research*, 2(1): 29–43.
Takenouchi, Asahi, and Koji Yatani, 2020, "A Comparative Study of Display Methods Aimed at Promoting Reading of Terms of Service," *FIT*, 3: 57–64.

classification (4) Research on the relationship between privacy policies and intention to use services

LaMonica, Haley M., et al., 2021, "Privacy practices of health information technologies: privacy policy risk assessment study and proposed guidelines," *Journal of Medical Internet Research*, 23(9): e26317.
Nishimura, Yoichi, 2014, "Internet privacy concerns: Reactions to privacy policy and behavioral targeting advertising," *Proceeding of the 78th Annual Meeting of the Japanese Psychological Association*.
Shinoda, Shiori, et al., 2017, "Basic Consideration for the Impact of Online Privacy Policies on Consumer Trust," *Research Report Security Psychology and Trust (SPT) 2017*, 5: 1–6.
Strahilevitz, Lior J., and Matthew B. Kugler, 2016, "Is privacy policy language irrelevant to consumers?," *The Journal of Legal Studies*45. S2: S69–S95.
Takasaki, Haruo, 2016, "The Study on User Preferences of Personalized Services an Empirical Analysis Assuming Plurality of Privacy Concerns," *Journal of The Japan*

Society of Information and Communication Research, 34(3): 25–39.

classification (5) Others

Aljeraisy, Atheer, et al., 2022, "Exploring the relationships between privacy by design schemes and privacy laws: a comparative analysis," *arXiv preprint arXiv: 2210.03520*.

Arellano, April Moreno, et al., 2018, "Privacy policy and technology in biomedical data science," *Annual review of biomedical data science*, 1: 115–129.

Hashimoto, Seishi, 2002, "Policy Framework for Consumer Protection in the Networked Society: from the Viewpoint of Online Privacy Protection," *Doshisha University policy & management review* (3)73–94: 73–94.

Itakura, Yoichiro, and Mosuke Terada, 2015, "The Impact of Terms of Use and the Privacy Policy stated in the Proposals of Amendments for the Act on the Protection of Personal Information and the Civil Code (Monetary Claims Act) towards the Provisions of Privacy Related Clauses," Research Report *Electronic Intellectual Property (EIP)* 2015(14): 1–6.

Itakura, Yoichiro, and Mosuke Terada, 2018, "The Significance and Context of the Establishment of California Consumer Privacy Act of 2018," *Research Report IPSJ SIG Technical Report (DPS) 2018*, 2: 1–7.

Komukai, Taro, 2014, "Consumer Privacy Policy Developments at the U.S. FTC," *Information and Communications Policy Review*, 8: e100–e108.

Murata, Kiyoshi, and Yoko Orido, 2013, "Who Invades Privacy?," *The National Research and Presentation Conference of the Japan Society for Management Information Sciences 2013*, 0: 306–309.

Numao, Masayuki, 2006, "Privacy and AI (<Special Issue> Information Security and AI)," *Artificial Intelligence*, 21(5): 593–601.

Phillips, David J., 2004, "Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies," *New Media & Society*, 6(6): 691–706.

Rosmaini, Elly, et al., 2018, "Insights to develop privacy policy for organization in Indonesia," *Journal of Physics: Conference Series*, 978(1), IOP Publishing.

Sakuma, Jun, et al., 2015, "Function Evaluation to Ensure Privacy Policy Enforcement," *Proceeding of the Computer Security Symposium 2015*, 3: 40–47.

Wang, Xiaoyin, et al., 2018, "Guileak: Tracing privacy policy claims on user input data for android applications," *Proceeding of the 40th International Conference on Software Engineering*.

Warkentin, Merrill, Allen C. Johnston, and Jordan Shropshire, 2011, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems*, 20(3): 267–284.

REFERENCES

Adjerid, Idris, et al., 2013, "Sleights of privacy: framing, disclosures, and the limits of transparency," *Proceeding of the Ninth Symposium on Usable Privacy and Security - SOUPS'13*, New York, USA, ACM Press: 1.

Alabduljabbar, Abdulrahman, and David Mohaisen, 2022, "Measuring the Privacy Dimension of Free Content Websites through Automated Privacy Policy Analysis and Annotation," *Companion Proceeding of the Web Conference*.

Aljeraisy, Atheer, et al., 2022, "Exploring the relationships between privacy by design schemes and privacy laws: a comparative analysis," *arXiv preprint arXiv*: 2210.03520.

Aragaki, Noriko, and Michiaki Yasumura, 2014, "Social navigation: its impact and potential for support," *Cognitive Science*, 11. 3: 163–170.

Arellano, April Moreno, et al., 2018, "Privacy policy and technology in biomedical data science," *Annual review of biomedical data science*, 1: 115.

Balebako, Rebecca, et al., 2013, ""Little brothers watching you": raising awareness of data leaks on smartphones," *Proceeding of the Ninth Symposium on Usable Privacy and Security SOUPS '13*, New York, USA, ACM Press: 1.

Balebako, Rebecca, et al., 2015, "The Impact of Timing on the Salience of Smartphone App Privacy Notices," *Proceeding of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices SPSM*, 15: 63–74.

Bannihatti Kumar, Vinayshekhar, et al., 2020, "Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy text," *Proceeding of The Web Conference 2020*.

Berendt, Bettina, et al., 2005, "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, 48(4): 101–106.

Bergmann, Mike, 2009, "Testing privacy awareness," *IFIP Summer School on the Future of Identity in the Information Society*, Springer, Berlin, Heidelberg.

Besmer, Andrew, Jason Watson, and Heather Richter Lipford, 2010, "The impact of social navigation on privacy policy configuration," *Proceeding of the Sixth Symposium on Usable Privacy and Security*.

Brooks, Michael, 2010, *13 things that don't make sense: the most intriguing scientific mysteries of our time*, Profile Books. (Translated by Koichi Nirei, 2010, *Mada kagaku de tokenai 13 no nazo*, Soshisha.).

Cockcroft, Sophie, and Saphira Rekker, 2016, "The relationship between culture and information privacy policy," *Electronic Markets*, 26(1): 55–72.

Costante, Elisa, et al., 2012, "A machine learning solution to assess privacy policy completeness: (short paper)," *Proceeding of the 2012 ACM Workshop on Privacy in the Electronic Society*.

Fukumoto, Ichiro, 2019, "Study of Hybrid Therapy with Peripheral Nerve Stimulations and Biofeedback— Hybrid BF Enforces both Conditioned and Unconditioned Stimulus?—," *Journal of Japanese Society of Biofeedback Research*, 46(1): 39–47.

Ghazinour, Kambiz, Maryam Majedi, and Ken Barker, 2009, "A model for privacy policy visualization," *2009 33rd Annual IEEE International Computer Software and Applications Conference*, 2.

Gluck, Joshua, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, Yuvraj Agarwal, 2016, "How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices," Proceeding of the Twelfth Symposium on Usable

Privacy and Security (SOUPS 2016).

Goffman, Erving, 1961, *Asylums: Essays on the Social Situations of Mental Patients and Other Inmates*, Anchor Books, Doubleday & Company. (Translated by Takeshi Ishiguro, 1984, *Asylum——shisetsu shūyōsha no nichijō sekai*, Seishin Shobo.).

Hashimoto, Seishi, 2002, "Policy Framework for Consumer Protection in the Networked Society: from the Viewpoint of Online Privacy Protection," *Doshisha University policy & management review*, 3: 73–94.

Ichinose, Sayo, et al., 2013, "Survey on the Current Status of Application Privacy Policy Posting in Smartphone Apps," *CSEC: Computer Security Group (CSEC) 2013*, 61: 1–6.

Itakura, Yoichiro, 2013, "The Study of Terms of Use Relating to Processing of Personal Information," *Research Report of Electronic Intellectual Property and Infrastructures (EIP) 2013*, 4: 1–6.

Kanamori, Sachiko, et al., 2017, "Categorization based on the Ambiguity and Amount of Information Associated with a Named Entity of Privacy Policy A Study on Transparency in Privacy Policies," *Proceeding of the Computer Security Symposium 2017*, 2.

Kanehara, Shunsuke, 2011, "The Life of B. F. Skinner," *Bulletin of Faculty of Contemporary Social Studies Nagasaki Wesleyan University*, 9(1).

Kawaguchi, Kanako, 2019, ""What is it like?" the plain explanation to the general public for their privacy preserving?," *Chiba University. Graduate School of Humanities and Studies on Public Affairs. Research Project Reports*, 342: 16–24.

Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor, Robert W. Reeder, 2009, "A "nutrition label" for privacy," Proceeding of the 5th Symposium on Usable Privacy and Security SOUPS '09, New York, New York, USA, ACM Press: 1.

Kohn, Alfie, 1999, *Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, As, Praise, and Other Bribes*, Mariner Books. (Translated by Hidebumi Tanaka, 2001, *Hōsyū syugi wo koete*, Hosei University Press.).

LaMonica, Haley M., et al., 2021, "Privacy practices of health information technologies: privacy policy risk assessment study and proposed guidelines," Journal of medical Internet research, 23(9): e26317.

Lin, Jialiu, et al., 2012, "Expectation and purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing," *Proceeding of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, New York, USA, ACM Press: 501.

Liu, Fei, et al., 2014, "A step towards usable privacy policy: Automatic alignment of privacy statements," *Proceeding of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers*.

Liu, Frederick, et al., 2018, "Towards automatic classification of privacy policy text," *School of Computer Science Carnegie Mellon University*.

Metzger, Miriam J., 2006, "Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure," *Communication Research*, 33(3): 155–179.

Miyagi, Otoya, 1965, *Ningen no kokoro*, KADOKAWA.

Moniruzzaman, Md, Md Sadek Ferdous, and Roksana Hossain, 2010, "A study of privacy policy

enforcement in access control models," *2010 13th International Conference on Computer and Information Technology (ICCIT). IEEE.*

Movius, Lauren B., and Nathalie Krup, 2009, "US and EU privacy policy: Comparison of regulatory approaches," *International Journal of Communication*, 3: 19.

Numao, Masayuki, 2006, "Privacy and AI (<Special Issue>Information Security and Artificial Intelligence)," *Journal of The Japanese Society for Artificial Intelligence* 21(5): 593–601.

Pan, Yue, and George M. Zinkhan, 2006, "Exploring the impact of online privacy disclosures on consumer trust," *Journal of Retailing*, 82(4): 331–338.

Pinker, Steven, 2002, *The Blank Slate: The Modern Denial of Human Nature*, Penguin Books, New York (Translated by Atsuko Yamashita, 2004, *Ningen no honshō wo kangaeru—kokoro ha kūhaku no sekiban ka*, NHK Publishing, Inc.).

Sakamoto, Toshio, 2009, *Post Privacy*, Seikyusha.

Shinbo, Fumio, 2003, "Significance and Current Status of Privacy Policy Posting in Administrative Agencies: Focusing on the Efforts in the U.S. Federal Government Agencies," *Information Media Research*, 2(1): 29–43.

Shinoda, Shiori, et al., 2017, "Basic Consideration for the Impact of Online Privacy Policies on Consumer Trust," *Research Report Security Psychology and Trust (SPT) 2017*, 5: 1–6.

Shvartzshnaider, Yan, et al., 2019, "Going against the (appropriate) flow: A contextual integrity approach to privacy policy analysis," *Proceeding of the AAAI Conference on Human Computation and Crowdsourcing*, 7.

Skinner. Burrhus F., 1971, *Beyond freedom and dignity*, New York: Alfred Knopf. (Translated by Hiroo Yamagata, 2013, *Jiyuu to Songen wo koete*, Shumpusha.).

Strahilevitz, Lior J., and Matthew B. Kugler, 2016, "Is privacy policy language irrelevant to consumers?," *The Journal of Legal Studies*, 45(S2): S69–S95.

Takasaki, Haruo, et al., 2010, "Kojin jōhō wo bēsu toshita pāsonaraizēshon sābisu riyō no shōhisha senkō ni kansuru kenkyū," *Proceeding of the 27th Annual Conference of The Japan Society of Information and Communication Research*.

Takasaki, Haruo, Teppei Takaguchi, and Hisaya Sanezumi, 2014, "A Study on Causes for Privacy Concerns about Personalized Services on Mobile Devices," *Journal of public utility economics*, 66(2), 25–34.

Takasaki, Haruo, 2016, "A Study on Consumer Preferences for Personalized Services: An Empirical Analysis Focusing on the Diversity of Privacy Concerns," *Journal of The Japan Society of Information and Communication Research*, 34(3): 25–39.

Takemori, Keisuke, et al., 2013, "Third party review framework for privacy policy of application/contents," *Research Report Computer Security (CSEC) 2013*, 62: 1–8.

Takenouchi, Asahi, and Koji Yatani, 2020, "A Comparative Study of Display Methods Aimed at Promoting Reading of Terms of Service," *FIT*, 3: 57–64.

Warkentin, Merrill, Allen C. Johnston, and Jordan Shropshire, 2011, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems*, 20(3): 267–284.

Zuboff, Shoshana, 2019, *The Age of Surveillance Capitalism: The Fight for the Future at the New*

Frontier of Power, Profile Books. (Translated by Kayoko Nokata, 2021, *Kanshi shihon shugi*, Toyo Keizai Inc.).

（蔵本紗知, 南山大学大学院社会科学研究科博士後期課程, E-mail: d20ce001@m.nanzan-u.ac.jp）