Journal of Business Economics and Management
ISSN 1611-1699 / eISSN 2029-4433
2018 Volume 19 Issue 2: 253–267
https://doi.org/10.3846/jbem.2018.5200

THE DO NOT TRACK MECHANISM FOR DIGITAL FOOTPRINT PRIVACY PROTECTION IN MARKETING APPLICATIONS

Fa-Chang CHENG[1], Yu Shan WANG[2*]

[1]*Graduate Institute of Science and Technology Law, National Kaohsiung University of Science and Technology, No. 2, Juo-Yue Rd, Nantz District, Kahosiung 81164, Taiwan*
[2]*Department of Money and Banking, National Kaohsiung University of Science and Technology, No. 2, Juo-Yue Rd, Nantz District, Kahosiung 81164, Taiwan*

Received 17 November 2017; accepted 18 June 2018

Abstract. Serious concerns about the invasion of digital footprint information privacy due to intense commercial promotion through data mining has led to the emergence of privacy by design in the form of the Do Not Track (DNT) mechanism. This paper attempts to construct a theory to justify and find an appropriate solution to balance the different interests by implementing the DNT mechanism in the real-world marketing industry. The research method involves deduction in legal reasoning. This paper argues that digital footprint information privacy, which has high commercial value, should at least be awarded the status of a semi-fundamental human right. Additionally, when to adopt a DNT opt-out or default mechanism depends on the type of personal information involved. The practical implications suggest a compromise between digital footprint privacy protection and commercial applications in the marketing industry, to be achieved through technology. Since this important topic is relatively new in the area of marketing applications and no primary academic research has established a complete theoretical legal foundation, this article is among the first to do so. Beside its originality, this article also contributes to the literature by proposing a theoretically practical mechanism for both digital footprint privacy protection and marketing profits.

Keywords: information privacy, digital footprint, information protection, do not track, data mining, reasonable expectation, big data.

JEL Classification: K20, L81, M31.

Introduction

The issue of privacy protection on the Internet has been the subject of numerous disputes in recent years. Two technical reasons are worth mentioning. First, it is difficult to investigate alleged violations of information privacy because the identities of the customers are protected. Second, the trans-border nature of information privacy highlights the practical predicament of striking a balance between upholding the free flow of information while

*Corresponding author. E-mail: *yushan@nkust.edu.tw*

enforcing the law in the physical world. However, looking back at the more fundamental dispute on Internet privacy, the discussion focuses on the meaning of information privacy in the context of cyberspace. Cheng (2012) showed that the appropriate standard for defining the scope of information privacy is society's 'reasonable expectation'. This article argues that the concept of reasonable expectation is only supported by the seriousness of the invasion in the commercial sense.

The advancement of technology conceivably causes problems in defining and enforcing information privacy protection laws from the perspective of reasonable expectation. Disputes ultimately centre on the balance of interests through technological measures, especially given new kinds of cyber information, such as the digital footprint information discussed in this article. Therefore, research questions in digital footprint privacy protection should concern how to balance different kinds of interests and implement such a balance in the Internet marketing industry through technology.

In recent years, the application of big data through data mining technology has shown promising commercial capabilities. The trend of digital convergence has also contributed to the significant growth in the amount of information accessible through data mining. The aspects that affect digital convergence can be summarized as technology development, policy support, and acceptance in society. In terms of marketing applications, these aspects seem to point in a positive direction and move towards the ultimate goal of digital convergence. Therefore, different kinds of information have proliferated throughout cyberspace and digital footprint information has thus far functioned only as the missing link to these other kinds of information. The status quo of the Internet highlights the importance of the protection of digital footprints information in marketing applications, the primary focus of this article.

Just as one's digital footprint has come to be recognized as a subject of information privacy because of the unwillingness of Internet users to share this information with others (especially third-party data brokers), the trend to protect the privacy of online digital footprints, in addition to the seriousness of the invasion of such privacy, has led to the idea of privacy by design. Manshaei, Zhu, Alpcan, Basar and Hubaux (2011) indicated that game theory can be used to explain the need for a design mechanism to avoid free riders. Accordingly, a free rider is one who avoids contributing to the system, namely, digital footprint privacy protection in this case. If every participant were a free rider, the system would fail. Applying game theory, one can thus eliminate the free-rider effect through a design mechanism, that is, privacy-by-design legal requirements in this article.

The primary aim of this article is to propose a tentative model for implementing Do Not Track (DNT) in the legal infrastructure and reconciling digital footprint information privacy with the commercial interests of data mining businesses in a way that is both theoretically correct and practically feasible. The object of this article also applies to the Internet marketing industry in terms of achieving the best for the Internet environment and profits. The research method involves deduction in legal reasoning. Different approaches to general information privacy are introduced and the protection of digital footprint privacy should be inferable from the legal reasons behind these approaches. Since this important topic is relatively new in the area of marketing applications, no primary academic research has yet established a complete theoretical legal foundation and this article would be among the first to do so. Beside its originality, this article contributes to the literature by interpreting the legal rationale

behind the scenes, shedding light on current technological trends and the marketing industry, to pave the avenue towards a tentative solution to digital footprint privacy protection.

1. Digital footprint, DNT, and privacy

Derikx, de Reuver, Kroesen and Bowman (2015) indicated that consumers might give up privacy because of economic incentives. Kim, Ly and Soman (2015) stated that governments and businesses should work together with consumer groups to build three pillars – that is, equipping the consumer, padding the environment, incentivizing businesses – to protect the safety of consumers in information privacy. Baesens, Bapna, Marsden, Vanthienen and Zhao (2016) showed that data applications have a profound influence on information privacy. Bhattacharyya and Chatterjee (2016) described the current phenomenon of social media collecting personal information. Stark (2016) removed information privacy protection from reality to state that the next frontier in privacy by design is to build up a user interface that exploits haptic and aromatic technologies alongside visual and auditory strategies. Lau (2017) noted that consumers like free services but many still believe there should be limits to online tracking. Markos, Milne and Peltier (2017) described sensitive information as the type that comprises the high-privacy segment (e.g. DNA profiles, credit card numbers) and is shared with unknown marketers and stated that policy makers should regulate the usage of such sensitive information. Yaprakli and Unalan (2017) verified smartphone users' concerns about personal information in big data applications. However, while these recent studies examined issues related to information privacy protection, none has discussed the relations between DNT mechanism and digital footprint privacy protection in marketing applications. This article therefore proposes the research framework illustrated in Figure 1 to study and review this gap in the literature.

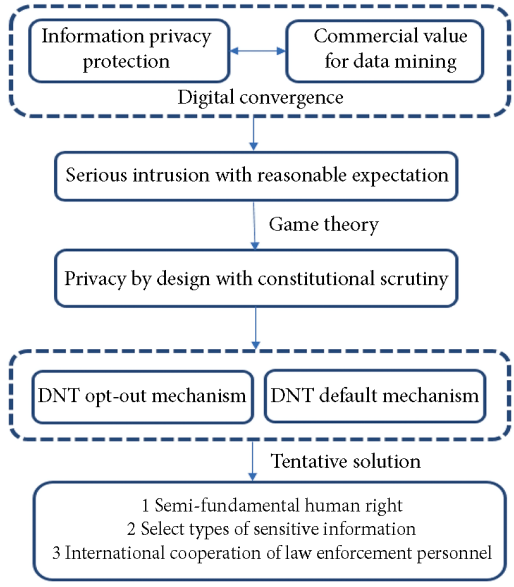

Figure 1. DNT mechanism in marketing applications (source: compiled by author)

In its broadest meaning, a digital footprint is the trace of anything recorded by a sensor. A congregation of digital footprints can form a big data set. The application of big data in data mining technology has shown promising commercial capabilities and has been extensively discussed. Data mining technology in the context of big data has raised numerous concerns about unreasonable surveillance, discrimination, and hard-to-trace invasion and law enforcement, which are detrimental to trust on the Internet. Jerome (2014) indicated that these legal concerns arise under the guise of information privacy in the protection of digital footprints. Therefore, the primary legal dispute in big data mining technology is based upon personal digital footprints, which are simply called digital footprints henceforth.

There are many sources of digital footprints. For example, to track Internet customers' activities on the Internet is to track their online digital footprints and the trend of the Internet of Things will ultimately connect almost every personal digital footprint to the Internet, including those of smartphones. Currently available technologies include cookies, mobile platforms, apps, RFID, and geolocation devices, which can be used in the broadest sense of the Internet, including the Internet of Things. Data mining technology based on digital footprints has different purposes, such as national security, public interests, and private commercial purposes. There could be few problems for the purpose of important public interests, compared with private commercial purposes which are the focus of this article. In particular, serious concerns arise when digital footprint information is used outside its original purpose, such as with advertisement networks and third-party data brokers[1].

The scope and concerns of such protection are also noted in the proposal for the Regulation on Privacy and Electronic Communications, as further mentioned in this paper[2]. Goodman (2015) showed that integrated personal information has become a valuable asset among data collectors and brokers, such as Google and Facebook. The convenience of the Internet has encouraged the public to give away its personal information in exchange for free services, without realizing how important this information is to the economic profit of Internet service providers (ISPs) and data collectors and brokers.

To perpetuate the huge economic profits generated by big data, traditional so-called privacy policy statements on websites do not serve to promote information privacy; instead, they eliminate any expectation a customer could have regarding privacy. Data brokers are selling integrated personal information to unknown third parties for large profits. People are thus gradually becoming controlled by cyber technology without recognizing the gravity of the situation or the potential harm to information privacy. The commercially driven forces shaping consumer habits through the use of integrated personal information are problematic and need to be curtailed. These problems could be nipped in the bud by protecting all personal information that can be traced and identified through digital footprints.

To create a perfect commercial promotion using data collected on the Internet, advertisers must obtain the following three types of information from data brokers: who the potential

[1] Committee on Commerce, Science, and Transportation – Office of Oversight and Investigations Majority Staff, 'A review of the data broker industry: collection, use, and sale of customer data for marketing purposes' http://educationnewyork.com/files/rockefeller_databroker.pdf [accessed 2 May 2017].

[2] Proposal for a Regulation of the European Parliament and of the Council-concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM(2017) 10 final, 2017/0003 (COD), 10/1/2017.

customer is, what the potential customer wants, and where the potential customer is physically located. Data brokers are usually able to provide this information and satisfy advertisers' needs (Goodman, 2015). In addition, the notion of having 'nothing to hide', which generally suggests there is no privacy on the Internet, further encourages the general public to give up even more of its personal information. In the meantime, ironically, free speech advocates are ardently trying to prevent their own information privacy from being invaded. Goodman (2015) also argued that self-regulation in lucrative business activities may not be a realistic goal under the current circumstances.

Whether our society requires law enforcement to intervene in information privacy protection or just education so that people can learn how to maintain their information privacy on the Internet remains a matter of debate. Guffin, Glover and Benjamin (2014) showed that law enforcement is required in addition to supplementary education to both businesses and Internet customers. This article argues that the time for government enforcement has come, for the reasons mentioned. Strong concerns about losing the battle for the protection of cyber information privacy due to the seriousness of the intrusion have led to the concept of privacy by design. For purposes of commercial online data collection (i.e. digital footprint tracking), the method of implementing privacy by design is embodied in the DNT mechanism, as explained later in this paper.

Two types of DNT mechanisms can be deployed on the Internet: one is the DNT opt-out mechanism and the other is the DNT default mechanism. Implementing the opt-out mechanism means that an Internet customer will be tracked in the digital world through an ISP's own procedures unless the customer demonstrates the clear intent of not wanting to be tracked. By contrast, the default mechanism, with its original settings, does not track an Internet customer on the Internet unless the customer clearly expresses that desire. Choosing the appropriate DNT mechanism reflects the conflict that arises when attempting to strike a balance between digital footprint privacy protection and marketing applications that use the information for Internet commerce profits.

2. Different approaches to embracing DNT in the era of information privacy by design

The EU Data Protection Directive (Directive 95/46/EC) treats information privacy as a fundamental human right under Article 1 and only the exceptional circumstances it stipulates can serve as legitimate grounds to override this information privacy protection. Most of those legal grounds are well delineated (e.g. unambiguous consent, legal obligations, and the vital interests of the data's subject), especially in situations with sensitive information (e.g. explicit consent, requirements of employment law and union activities). Despite citing exceptions to the concept of balance of interests, the Data Protection Directive lays down the fundamental principle that a digital footprint should be treated seriously, even under the constitutional balance of interests.

The Directive on Privacy and Electronic Communications (Directive 2002/58/EC) directly applies information privacy issues to the cyberspace context and develops specific rules to implement cyberspace information privacy. Given the privacy by design concept,

the 25th legislative reason for this directive stipulate that cookies and similar devices should be used only under when the information provider is aware of their existence and purpose. Since cookies gather traffic data, Article 6 of the directive requires the information provider's consent before such data can be processed. Based on the definition in Directive 95/46/EC, *consent* means that the information provider must give 'specific and informed indication of his wishes by which the data subject (information provider) signifies his agreement to personal data relating to him being processed'. There was a case in which a national court, referring questions for preliminary ruling – one of which related to Article 7, concerning data processing exceptions of Directive 95/46/EC – used the phrase *express consent* and thus acquired the EU court's acquiescence[3]. The EU Cookie Directive (2009/136/EC) amends Directive 2002/58/EC by directly stating 'has given his or her consent'. In Directives 2009/136/EC and 2002/58/EC, express consent would allow two exceptions: technical storage or access to carry out transmissions and required services. Generally speaking, these two types of use would not be covered in the customer's expectation of privacy, due to the functionality explicitly requested by the customer.

The most recently enacted General Data Protection Regulation (GDPR) (Regulation 2016/679), which took effect in April 2018, generally overhauls Directive 95/46/EC and proffers enhanced personal information protection; implanting the ideas of transparency, privacy by design, and accountability; improving security breach notification processes; introducing integrated supervisory regimes, and so forth. For the purpose of discussing the DNT mechanism, in GDPR, the European Commission defines *consent* as 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data'. Abbamonte (2014) showed there is no room for the enforcement of implied consent under the EU directives and regulations. Regarding online behavioural advertising, the 2010 Working Party, clearly indicated that DNT opt-out is insufficient to protect information privacy in behavioural advertising[4]. The most appropriate solution under the above-mentioned EU directives and regulations would therefore be to apply the DNT default mechanism on the Internet.

The EU seems to be more concerned, however, about potential privacy disputes in digital footprints and is inclined to be conservative in permitting exceptions. The infrastructure design of the DNT default mechanism should be mandated by the above-mentioned EU directives and regulations to apply the consent exception. However, the 2012 Working Party suggested that first-party analytic cookies be considered the third exemption to consent[5]. This suggestion reveals the EU's intent to consider adopting the DNT opt-out methodology under limited circumstances.

In the recent development of the Proposal for a Regulation on Privacy and Electronic Communications to complement GDPR, the European Commission made it clear that the regulated entity 'providers of electronic communications services' has the broadest meaning, which consists of all providers of services for remuneration via electronic communications

[3] Volker und Markus Schecke GbR v. Land Hessen, Celex No. 609CC0092, EU: Case C-92/09 (2010).

[4] Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP171, 22/6/2010.

[5] Opinion 04/2012 on Cookie Consent Exemption, 00879/12/EN, WP194, 7/6/2012.

networks. Electronic communications services process electronic communications data containing two types of personal information: electronic communications content and electronic communications metadata. The regulation also covers providers of public online directories and software allowing electronic communications. The EU thus clearly intends to fully protect electronic communications information privacy, despite its compromise on the concept of first-party analytic cookies and allowing for exemptions from consent, and encourages the development of more detailed requirements for the DNT default regime[6].

The scenario for information privacy protection in digital footprints observed in the EU would be incompatible with the legal infrastructure in the United States. The U.S. Supreme Court has never recognized information privacy as a fundamental human right that would withstand strict constitutional scrutiny. Cheng (2010) and Shelton (2014) have shown that federal legislation focuses on either the legal dispute of government search and seizure or specific types of information protection. Even federal wiretap laws, which regulate unauthorized transmission interception, may not prohibit ISP advertising behaviour. In addition, Nizio (2014) showed that federal regulation is not involved with first- or third-party tracking, which is the traditional focus of digital footprint privacy protection. Generally, information privacy for digital footprints would not be protected by the above-mentioned federal legislation. Although the Supreme Court has recognized that physical location tracking can be covered under one kind of information privacy, privacy ultimately rests on state laws and federal administrative advice (i.e. the Federal Trade Commission) if the appropriate digital footprint protection is not covered under federal legislation[7].

Generally, the policy strategy for digital footprint privacy protection in the United States (when it does exist) for adhering to the privacy by design principle is the DNT opt-out mechanism described in this article. At the state level, Maxwell (2013/2014) showed that some states, such as California, have legislative policy strategies for digital footprint privacy protection, but there is no remedy or penalty for violations, rendering the legislation meaningless[8]. Additionally, as of yet, no legal case has directly related to digital footprint privacy protection with consent exemption in the United States. The Federal Trade Commission report 'Suggestions for Mobile Platforms' has advised mobile platforms to consider adopting the DNT opt-out mechanism (McKinnon, 2014).

Hayes (2014) indicated that there has been a strong voice in favour of federal regulations in the digital footprint privacy protection field because of intense customer concerns about being tracked on the Internet and consistent failure to enact DNT federal legislation. Koponen and Mangiaracina (2013) showed that industrial standards of self-regulation with the DNT opt-out mechanism could raise concerns about unfair competition if these standards are detrimental to digital footprint privacy protection. Strauss (2014) also showed that the majority of U.S. academics have suggested that the federal government has an obligation to

[6] In Article 8(d) of the proposed Regulation, the first party analytic practice is exempted from the regulation. And under the description of (25) of the proposed Regulation, the customers could have different default setting options for cookie, ranging from high (for example, never accept cookies) to lower (for example, always accept cookies) and intermediate (for example, reject third party cookies or only accept first party cookies).

[7] U.S. v. Jones, 132 S. Ct. 945, 949 (2012).

[8] The regulation is codified under the title of 'Internet Privacy Requirements' cited as California Business and Professions Code 22 § 22575 (2013).

respect customers' choices through the DNT opt-out mechanism, as opposed to the DNT default mechanism, which is mandatory in respecting digital footprint privacy protection. Table 1 summarizes the different policy attitudes between the United States and European Union to digital footprint protection through the privacy by design principle.

Table 1. Different policy attitudes to digital footprint protection through the privacy by design principle between the United States and European Union (source: compiled by authors)

Digital footprint protection through privacy by design	The United States	European Union
Constitutional hierarchy	Non-fundamental human right	Fundamental human right
Legal authorities for consent	The federal trade commission report 'Suggestions for mobile platforms' only required implied consent	Directive 95/46/EC Directives 2009/136/EC and 2002/58/EC GDPR Required express consent
Commercial use without express consent	Allowed	Not allowed
DNT mechanism	DNT opt-out mechanism	DNT default mechanism

We assume that the United States' stronger commercial orientation and the U.S. government's subsequent greater deference to business interests, compared to the EU's human rights approach, have resulted in an opt-out regime. In the United States, academic disputes as to whether or not customer data are protected within the scope of the right to freedom of speech have potentially influenced the constitutional hierarchy of information privacy and commercial data collection, thus further complicating the issue of which kind of DNT mechanism should be applied. Kaminski and Witnov (2015) showed that information privacy may have nothing to do with or even directly conflict with freedom of speech in the sense of commercial promotion. From that perspective, data collection does not constitute expression, which represents the substance of freedom of speech protection (Bambauer, 2014). Besides, even in recognizing that data collection has an influence on the free flow of information, as well as an impact on freedom of speech, the U.S. courts would tend to explain data collection as either an indirect influence on freedom of speech or one category of commercial speech, thus receiving only intermediate constitutional scrutiny.

Compared with the above-mentioned detachment of the freedom of speech approach, some scholars have instead moved towards the anti-information privacy extreme and analogized data collection to freedom of speech through the catalyst of the right to knowledge. According to Bambauer (2014), cyber information privacy could clash directly with freedom of speech and require strict constitutional scrutiny. Cohen (2015) used the term *zombie-free speech jurisprudence* to describe free speech protection in the service of economic power. If the declaration of such an opinion becomes a reality, this article expects that much of information privacy legislation will be deemed unconstitutional, as would the DNT opt-out mechanism. Bartholomew (2014) showed that the U.S. Supreme Court is still on the path towards reconciling the contradiction between information privacy and freedom of speech on the Internet with commercial data mining technology. However, in current U.S. judicial

practice, the legal interests of digital footprint privacy will most likely be deemed to balance with other non-fundamental competing legal interests, such as the interests of commercial data collection, also inciting a range of academic opinions due to uncertainty about the constitutional hierarchy.

In contrast with the constitutional hierarchy in the United States, the EU treats legal interests in digital footprint privacy as a fundamental human right, which defeats most constitutional challenges from other legal interests. Even if the United States and the EU have their own constitutional attitudes in the dispute over digital footprint privacy protection under the privacy by design trend, this article would argue that evolving Internet commercial strategy and Internet globalization also raise concerns about altering the constitutional hierarchy for information privacy on the Internet. Tom Wheeler, ex-chairperson of the FCC, announced that, because the relationship between consumers and their telecommunication carriers differs from that between consumers and the websites they visit (i.e. consumers have less choice with their telecommunication carrier), the DNT mechanism should be more restrictive for data collectors and brokers under the telecommunication carrier regime (Wheeler, 2016). Under Wheeler's theory, the DNT opt-out mechanism should be deployed to market other communication; otherwise, the appropriate method for protecting information privacy in digital footprints is the DNT default mechanism.

The FCC's differential treatment of telecommunication carriers and websites indicates that telecommunication carriers are highly regulated. Their different treatment also suggests that the FCC is willing to reinforce digital footprint privacy protection by strictly interpreting the meaning of 'approval of the customer' in the 1934 Communications Act. In addition, the Congressional Bipartisan Privacy Caucus has expressed its intention to promote the DNT default mechanism (Doty & Mulligan, 2013).

U.S. policy around digital footprint privacy protection thus once shifted, to some extent, from the DNT opt-out mechanism towards the DNT default mechanism. However, under Trump, that path was discarded, because the DNT default mechanism would place a large burden on backbone service providers, compared with website owners[9]. We believe that giving more attention to the DNT default mechanism than is being done under Trump's administration would be beneficial to the Internet environment. As previously mentioned, the article would further dispute that Internet globalization and evolving Internet commercial strategy will probably make both legal infrastructures meet halfway. Therefore, it boldly suggests and expects that the EU will also compromise and approach the predicted scheme of digital footprint privacy protection due to the realities of commercial practice. The potential exemption previously noted to first-party analytics through the application of cookies seems to support this prediction. If states work together to implement digital footprint privacy protection, then the law enforcement authorities in different sovereign states could work together more efficiently in addressing digital footprint privacy violations.

[9] The White House Office of the Press Secretary, 'S. J. Res. 34–Disapproving the Federal Communications Commission's rule on privacy of customers of broadband services' https://www.whitehouse.gov/the-press-office/2017/03/28/statement-administration-policy-sjres-34-%E2%80%93-disapproving-federal [Accessed 26 August 2017].

3. Confusion in the personal information protection act in Taiwan and a milestone digital footprint privacy protection case in Mainland China: a tentative solution for the future of the DNT regulation scheme

The previous sections have demonstrated that the constitutional hierarchy of information privacy is a key consideration in deciding whether the DNT opt-out or default mechanism would be suitable to a nation's legal system. This is exactly why confusion occurred in both Taiwan and Mainland China when they attempted to implement the DNT default mechanism in their legal system. Taiwan enacted the Personal Information Protection Act to indicate the government was paying attention to the need for information privacy protection. This legislation imitates Directive 95/46/EC in the way it structures information privacy protection. Although the Constitutional Court of Taiwan has interpreted the right to receive a Nationality Certificate plus fingerprint privacy as a fundamental human right, the Constitutional Court never recognized information privacy as a fundamental human right. Whether constitutional theory is solid enough to support the Personal Information Protection Act is debatable when compared to the fundamental human dignity upheld in the EU.

Under Articles 15 and 19 of the Personal Information Protection Act, a government or non-government agency can acquire consent from a personal data provider as an exception in data collection and processing. Articles 16 and 20 additionally regulate how a government or non-government agency can acquire consent as one exception if the information is used outside the specific purpose of data collection. Furthermore, written consent is required to collect, process, or use personal information categorized as sensitive through the consent exception.

The Electronic Signatures Act of Taiwan satisfies the consent requirement in electronic documents. Generally, the consent must ensue from informed notification about collecting, processing, or using personal information. From the perspective of privacy by design, the consent exception shall require the DNT default mechanism for data collection, processing, and use in the act. However, Article 20 of the Personal Information Protection Act states that, if a non-government agency uses personal information for marketing pursuant to the consent exception and is turned down by the information provider, the agency shall cease such action. To say that the DNT default mechanism is required to prove informed consent would be incompatible with the concept that marketing by personal information is presumed legitimate unless the information provider refuses such commercial marketing.

The confusion surrounding the legal hierarchy of information privacy observed in Taiwan can also be found in Mainland China. A fairly recent case handed down to the Nanjing Intermediate People's Court in 2015, the first case reviewing an information privacy dispute caused by cookies, caught the attention of academics and practitioners[10]. In this case, the plaintiff accused Baidu, a search engine, of collecting information about his personal inclinations and engaging in commercial promotion using this information. The Nanjing Intermediate People's Court overthrew the decision of the Nanjing Gulou District People's Court for two reasons. First, the intermediate court did not accept the plaintiff's argument that the information collected in this case infringed upon his information privacy. The intermediate

[10] Nanjing Intermediate People's Court Civil Judgement No. Ningminsanchuzi 5028/2014.

court treated cookies as a communication broker between users' computers and the ISP (Baidu in this case). It found no direct connection between the digital footprint and the plaintiff's identity. Second, Baidu's privacy statement on its website and the plaintiff's implied consent were sufficient to fulfil the national public policy objective of protecting privacy in the information industry and respecting a customer's right to choice and right to knowledge.

The court's explanation in this case contradicted the guidelines of information security technology and information protection in public or commercial information service systems. In those guidelines, Mainland China defines personal information contained within computer data as related to a specific individual and it can be used independently or combined with other types of information to identify the individual. The information contained in cookies could certainly be combined with the personal identity stored by telecommunication providers to recognize people. In this case, on the one hand, the judges stated that Baidu maintained the customer's right to choice and right to knowledge, which are part of the information privacy protection scheme. On the other hand, they argued that the anonymous information collected by cookies is not identifiable personal information. The statement is inherently paradoxical. The above-mentioned guidelines also reinforce the protection of sensitive personal information in a manner that is similar to the EU's. The case reflects the reality that even regulations seem to greatly value information privacy; however, the judicial decision indicates the opposite and circumvents the predicament of determining where information privacy falls within the constitutional legal hierarchy by insisting that cookie-collected information is not identifiable and, therefore, not protected information.

By reviewing Taiwan's current information privacy protection and the milestone case of alleged cookie information privacy infringement in Mainland China, this article demonstrates how digital footprint privacy protection depends on the constitutional hierarchy of information privacy. Confusion arises whenever this constitutional hierarchy of information privacy is uncertain and government authorities boldly move towards the type of legislation the EU has adopted on the issue. While the different approaches remain in dispute and the above-mentioned confusion still applies, the fact that countries are paying serious attention to protecting information privacy in digital footprint is undeniable and the trend continues. The practical experiences of Taiwan and Mainland China prove the crucial link between the constitutional hierarchy of information privacy and the type of DNT mechanism deployed on the Internet.

As suggested earlier in this article, the policy choice between the DNT default and opt-out mechanisms depends substantially on where information privacy is situated within the constitutional hierarchy. By noting the serious and formidable issue of information privacy in digital footprints, as well as any potential manipulation by commercial data collectors and brokers, this article suggests that information privacy should be granted, at the very least, the status of a semi-fundamental human right. To limit the exercise of a fundamental human right will require a more restrictive constitutional check, compared with an ordinary human right. The purpose of defining information privacy as a semi-fundamental human right, in between fundamental and ordinary human rights, is to create flexibility of interpretation. This flexibility could then explain the differentiation between the DNT default and opt-out mechanisms.

Willis (2013) argues that certain types of sensitive digital footprints, such as online pharmacy information, require the enforcement of DNT default mechanism regulations to protect Internet customers. However, other kinds of digital footprints require only the DNT opt-out mechanism, which must also embody a customer-friendly privacy policy. A consensus as to what kinds of digital footprints fall under the definition of sensitive information should be reached by way of public consultation to collect opinions from all relevant fields. For example, this article expects individuals' political affiliation information to make the list, because the Taiwanese are rather conservative and tend not to disclose this information in their daily lives.

This article would argue that pushing for full-scale implementation of the DNT default mechanism needs further review. Any slight discrepancies between the tentative model and the EU model could be compensated for by two options. First, the business industry can voluntarily adopt the DNT default mechanism through self-awareness. Second, a Safe Harbour mutual agreement between the EU and other sovereign states or codes of conduct and certifications designed in GDPR can also be used. Transparency and accountability are also part of the tentative proposal as a supplementary measure. The concept of transparency means that data collectors and brokers should handle the personal information of Internet customers in a transparent manner, with a customer-friendly privacy policy, and customers should be educated in how to assert their information privacy rights. The concept of accountability will educate data collectors and brokers to be responsible with handling customers' personal information.

Conclusions

The trend of digital convergence has led to significant growth in the amount of information accessible through data mining. Personal information has gradually been transformed into a commodity in the eyes of enterprises. Nevertheless, serious concerns about legal information privacy disputes have not subsided, solely because of the commercial convenience created by big data mining technology. On the contrary, the voice of privacy by design has emerged from recognition of the seriousness of the invasion in the commercial sense. The privacy by design concept embodied in digital footprint privacy protection is the DNT technical setting. This setting can be applied using two different approaches: the DNT opt-out mechanism and the DNT default mechanism. The discrepancy in deployment between the DNT opt-out and default mechanisms focuses on where information privacy lies in a state's constitutional hierarchy. Theoretically speaking, the higher the constitutional hierarchy of information privacy in a given legal system, the more appropriate it is to apply the DNT default mechanism. The EU seems to be adopting the DNT default mechanism, while the United States tends to favour the DNT opt-out approach, leading to many controversies. Confusion occurs whenever the constitutional hierarchy of information privacy is uncertain and governmental authorities boldly push towards the type of legislation observed in the EU to protect digital footprint information privacy.

In considering how serious and formidable the issue of information digital footprint privacy invasion is, as well as any potential manipulation by data collector and brokers, this

article suggests that information privacy deserves at least the status of a semi-fundamental human right. This article further argues that certain types of sensitive digital footprints, such as online pharmacy information or individuals' political affiliation information in Taiwan, require DNT default mechanism regulations to protect Internet customers, whereas other kinds of digital footprints require only the DNT opt-out mechanism, including a customer-friendly privacy policy. Consensus as to what kinds of digital footprints fall under the definition of sensitive information should be reached by way of public consultations to collect viewpoints from all relevant fields. After all, business activity profits and customer trust are both crucial to the health of the cyberspace environment.

This article observes that, while the United States and the EU have their own policy attitudes regarding digital footprint privacy protection under the privacy by design trend, Internet globalization will probably make both legal infrastructures meet halfway. The FCC's decision in the Verizon case indicates that U.S. policy thinking concerning digital footprint privacy protection has somewhat shifted from the DNT opt-out mechanism towards the scheme put forth by this article. This article also expects the EU to compromise and converge towards the suggested digital footprint privacy protection scheme due to the realities of commercial practice. If states cooperate with one another in providing digital footprint privacy protection, then the law enforcement authorities in different sovereign states could work together more efficiently to address digital footprint privacy violations.

In sum, the tentative proposal of the DNT mechanism for digital footprint privacy protection in marketing applications suggests the following five steps to implement such a mechanism. 1) Step one is to recognize the legal status of digital footprint as one kind of information privacy. 2) Step two is to establish digital footprint privacy as a semi-fundamental human right. 3) Step three is to delineate the scope of sensitive information through public consultation. 4) Step four is to promote the concept of privacy by design in terms of implementing the DNT mechanism in the market, supplemented by transparency and accountability, where sensitive information is protected under the DNT default mechanism while other kinds of digital footprints would require only the DNT opt-out mechanism. 5) Step five is to enforce digital footprint privacy violations through the international cooperation of law enforcement agencies. Implementing the DNT mechanism would require lawmakers and law enforcement personnel around the world to cooperate with one another and for ISPs to abide by the law. Marketing applications following this five-step tentative proposal would achieve the goals of both protecting digital footprint privacy and, ultimately, market profits. This article thus provides valuable theory that can be applied to the online marketing industry and substantiated through marketing industry practices.

This paper is limited in that it focuses on the theoretical grounds for implementing a DNT mechanism for only marketing applications. Future research could gather quantitative data to examine the presumption that the proposed tentative DNT mechanism would best strike a balance between digital footprint privacy protection and the marketing application of such information to maintain Internet profits. Future research could use large-scale questionnaires to evaluate the effectiveness of the hypotheses discussed in this article.

Compliance with ethical standards

This article does not contain any studies with human participants or animals performed by any of the authors.

References

Abbamonte, G. B. (2014). The protection of computer privacy under EU law. *Columbia Journal of European Law*, *21*, 71-88.

Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2016). Transformational issues of big data and analytics in networked business. *MIS Quarterly*, *40*(4), 807-818. https://doi.org/10.25300/MISQ/2016/40:4.03

Bambauer, J. (2014). Is data speech. *Stanford Law Review*, *66*, 57-120.

Bartholomew, M. (2014). Intellectual property's lessons for information privacy. *Nebraska Law Review*, *92*, 746-798.

Bhattacharyya, M., & Chatterjee, U. (2016). A study on people's concerns on social media analysis for online audience identification and its impact on new media advertising. *Amity Journal of Media & Communication Studies*, *6*(1), 124-130.

Cheng, F. A. (2010). Electronic medical records in U.S. and the inspiration to Taiwan. *Journal of Law & Medicine (Taiwan)*, *17*(1), 9-23.

Cheng, F. A. (2012). Commentary on the protection of information privacy. In T. K. Buckner & B. L. Knowles (Eds.), *Privacy: management, legal issues and security aspects* (pp. 125-130). New York: Nova Science Publishers Inc.

Cohen, J. E. (2015). The zombie first amendment. *William & Mary Law Review*, *56*(4), 1119-1158.

Derikx, S., de Reuver, M., Kroesen, M., & Bowman, H. (2015). Buying-off privacy concerns for mobility services in the Internet-of-things era: a discrete choice experiment on the case of mobile insurance. In *BLED 2015 Proceedings*, 7-10 June (pp. 228-238). Slovenia

Doty, N., & Mulligan, D. K. (2013). Internet multi-stakeholder processes and techno-policy standards initial reflections on privacy at the world wide web consortium. *Journal on Telecommunications & High Technology Law*, *11*, 135-182.

Goodman, M. (2015). *Future crimes: everything is connected, everything is vulnerable and what we can do about it* (pp. 44-104). New York: Doubleday.

Guffin, P. J., Glover, K. J., & Benjamin, S. M. (2014). Foreword (in) symposium: who is governing privacy? Regulation and protection in a digital era. *Maine Law Review*, *66*(2), 369-371.

Hayes, A. S. (2014). The USPS as an ops: a remedy for users' online privacy concerns. *Common Law & Policy*, *19*, 465-507. https://doi.org/10.1080/10811680.2014.955770

Jerome, J. (2014). Big data: catalyst for a privacy conversation. *Indiana Law Review*, *48*, 213-242.

Kaminski, M. E., & Witnov, S. (2015). The conforming effect: first amendment implications of surveillance beyond chilling speech. *University of Richmond Law Review*, *49*, 465-518.

Kim, M., Ly, K. M., & Soman, D. (2015). A behavioural lens on consumer privacy. In *Rotman School of Management* (pp. 1-40). Toronto, University of Toronto.

Koponen, J., & Mangiaracina, A. (2013). No free lunch: personal data and privacy in EU competition law. *Competition Law International*, *9*(2), 183-195.

Lau, A. (2017). The privacy box: enabling consumer choice and meaningful consent in online privacy. In *The Public Interest Advocacy Centre* (pp. 1-58). Ottawa, ON, Canada.

Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J. P. (2011). Game theory meets network security and privacy. *ACM Computing Surveys*, *45*(3), 1-45.

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information sensitivity and willingness to provide continua: a comparative privacy study of the United States and Brazil. *Journal of Public Policy & Marketing*, *36*(1), 79-96. https://doi.org/10.1509/jppm.15.159

Maxwell, K. (2013/2014). Online behavioral advertising: the pros and cons of regulation and suggestions for adherence to California's constitutional right to privacy. *Nexus: Chapman's Journal of Law & Policy*, *19*, 51-76.

McKinnon, A. (2014). Sacrificing privacy for convenience: the need for stricter FTC regulations in an age of smartphone surveillance. *Journal of National Association of Administrative Law Judiciary*, *34*(2), 484-526.

Nizio, A. (2014). Taking matters into its own hands: why congress should pass legislation to allow the FTC to regulate consumer online privacy with a 'do not track' mechanism. *University of Illinois Journal of Law, Technology & Policy*, 283-306.

Shelton, A. (2014). A reasonable expectation of privacy online: 'do not track' legislation. *University of Baltimore Law Forum*, *45*(1), 35-56.

Stark, L. (2016). The emotional context of information privacy. *The Information Society*, *32*(1), 14-27. https://doi.org/10.1080/01972243.2015.1107167

Strauss, B. (2014). Online tracking: can the free market create choice where none exists. *Chicago-Kent Journal of Intellectual Property*, *13*(2), 539-570.

Wheeler, T. (2016). *Chairman Wheeler's proposal to give broadband consumers increased choice, transparency & security with respect to their data*. Retrieved from http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0310/DOC-338159A1.pdf.

Willis, L. E. (2013). When nudges fail: Slippery default. *The University of Chicago Law Review*, *80*, 1155-1229.

Yaprakli, T. S., & Unalan, M. (2017). Consumer privacy in the era of big data: a survey of smartphone users concerns. In *2nd World Conference on Technology, Innovation and Entrepreneurship*, *Press Academia Procedia, 12-14 May, 2017*. Istanbul, Turkey. https://doi.org/10.17261/Pressacademia.2017.509