Article

New Technology, New Information Privacy: Social-Value-Oriented Information Privacy Theory

Chen-Hung Chang *

ABSTRACT

Today's innovative technologies offer remarkable advantages in our daily lives, but they also give rise to concerns that these technological advancements will adversely impact individuals' privacy. The traditional notions of information privacy were based on personal control over data about oneself, an antiqued notion in a time where pervasive surveillance has rendered it nearly impossible for individuals to protect information privacy on their own. Key privacy concerns arise because it is nearly impossible to be left out of the intertwined digital and Internet world. Those who choose not to use the Internet, smartphones, tablet computers, electronic mail and online social network platforms, nevertheless remain trapped in the inescapable digital net, with others able to track their personal data.

This essay includes suggestions for reconstructing traditional privacy theories. The traditional notice-and-choice principle has failed to protect the information privacy. Privacy should be determined by both individuals' subjective feelings and objective social norms. The government has a constitutional obligation to protect the right to privacy by constructing basic information privacy protection principles. Furthermore, this essay proposes an approach to constructing a

DOI：10.3966/181263242015031001004

* S.J.D. Candidate, American University Washington College of Law. Email: chihshein@gmail.com. The author gratefully acknowledges the constructive comments of two anonymous reviewers and would like to thank Michael Carroll, Amy Tenney, and Leesa Klepper at American University Washington College of Law for their valuable comments and guidance on author's research and writing of this paper. The author would also like to extend the gratitude to the production staff of NTU Law Review for their assistance in preparing this paper for publication.

social-value-oriented information privacy theory. Among others, in determining the context of privacy, if no social precedents are available, the particular social activity's consequences, purposes, and values may first be identified, and then these results may be used to trace back to the starting point and consider how to regulate social activities.

Keywords: *Information Privacy, Right to Privacy, Big Data, Online Privacy, Notice-and-Choice Principle*

CONTENTS

I. INTRODUCTION

The development of new technologies has changed the way governments and businesses operate, and has tested the definitions of certain fundamental notions of privacy. Before the Internet was introduced, perception of privacy protection was rather simple: Just keep personal matters to oneself, and the secrets are safe with him/her. Even where someone managed to obtain another's personal information, the circulation of information was relatively limited in scope, and it was not that difficult to track the flow of information.

In the initial stage of the digital era, the Internet was regarded as a tool to better protect privacy than the non-digital world. The predominant view at the time was that cyberspace would enhance privacy protection because numerous activities could be completed through cyberspace instead of face-to-face contact. Commercial activities were facilitated by the Internet especially in certain areas of an individual's intimate matters (such as purchasing products for sexual intimacy). The Internet provided an alternative for consumers to conduct such activities with vendors through an online connection without facing the embarrassment and awkwardness of revealing personal matters during an in-store purchase.[1]

However, when digital technology and telecommunications rapidly advanced and transformed, the presumed benefit of privacy protection on the Internet disappeared. The Internet is losing its privacy-safe status. When individuals attempt to hide behind the shield of the Internet to engage in activities without revealing their identities—unavoidable in the off-line world, they are actually subject to another privacy risk. The emerging information technology has created an almost pervasive surveillance system, wherein it is nearly impossible for people to be left alone. Due to less expensive data storage media, any activity, even those which occur only once, can be recorded instantly and permanently, never to be forgotten. Broader network access means that personal data is kept not only in private homes, but also in an Internet cloud, where data owners cannot exercise proper control over their own data. Moreover, the use of fast aggregation and disclosure tools threatens safeguards for personal data, and when such tools are combined with advanced statistic and analytic methods, businesses possess more power to systematically collect and analyze vast quantities of data in order to predict consumer behavior.

These developments offer remarkable advantages in our daily lives, but they also give rise to concerns that these technology advancements will

1. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 197 (2000).

adversely impact individuals' privacy. If the pervasive surveillance system is inescapable, it would be reasonable for the individual to change his or her living habits in pursuit of privacy. Individuals may choose to be isolated, be silent or become suspicious or guarded when they cannot predict how and when their personal data will be used by whom for what purpose, and they fear that any unwanted use might interfere with their future.

This essay proposes that a modern notion of information privacy is needed to respond to the new privacy concerns raised by new technologies. Where the information technologies are more advanced, the data controllers have greater power. Individuals are too weak to resist the tide, and they are losing control over personal data uploaded into the maze of the Internet. In today's innovative technology environment, personal data is utilized in ways which are unpredictable and beyond the individual's control. There appears to be no limit for companies and nations in growing ever larger databases. The traditional notions of information privacy were based on personal control over data about oneself, which has become an antiqued notion when pervasive surveillance has rendered it nearly impossible for individuals to protect information privacy on their own. Sticking to the traditional notions of information privacy overemphasizes the individual dimension, and does not actually reflect the modern needs of privacy.

The next question is how to modify the tradition notions to form a modern one. Several methodologies will be introduced in constructing the notion of information privacy. This essay notes that a modern theory has to accommodate the inherent difficulties of exercising personal control over data due to technological changes, something not taken into consideration when the traditional privacy theory was developed. This essay provides a view that a viable approach to resolve the lack-of-control problem is to recognize the social value of privacy. People live within a social context, and any new privacy theory must be able to adapt to societal changes brought about by technologies. The societal context elements are essential to accurately perceiving the value of information privacy and determining a balance for data protection.

The concept of privacy is described in various terms in different contexts and typically refer to three areas of privacy: decisional privacy (the right to make personal decisions, e.g., contraception, abortion, marriage, procreation, child rearing, and sexual intimacy without interference), physical (or spatial) privacy (the right to be free from unreasonable searches and seizures) and information privacy (the right to control information about oneself).[2] This essay primarily focuses on information privacy because this

2. Fred H. Cate & Beth E. Cate, *The Supreme Court and Information Privacy*, 2 INT'L DATA

area is most relevant to the effect on data collection, use, disclosure and storage as a result of changing technologies. Physical privacy will be addressed via relevant information privacy problems, such as police use of Global Positioning System (GPS) devices to track movements of suspected criminals. Decisional privacy issues are outside the scope of this essay.

II. INFORMATION PRIVACY IMPLICATIONS OF NEW INFORMATION TECHNOLOGIES

A. *The Impact of Technology on Privacy*

Technological evolution has shaped notions of privacy throughout history. In the 1890s, when Louis Brandeis and Samuel Warren published the landmark essay *The Right to Privacy*,[3] which inspired numerous future privacy theories, it was an era when cutting-edge photographic devices, allowing for convenient photo shooting, were newly invented.[4] When the new devices were criticized for leaving people open to invasions of privacy, the two prominent thinkers set forth the definition of privacy as "the right to be let alone" to advocate a respect for privacy in the wake of technological evolution.[5] Later on, the invention of the telephone pioneered long distance electronic communication, arousing vigorous debate over whether government wire-tapping of phone lines constituted an unreasonable search and seizure under the Fourth Amendment to the United States Constitution. This issue was decided by the United States Supreme Court in *Olmstead v. United States,* which held that placing taps on telephone wires did not constitute a search under the Fourth Amendment, because it did not involve a physical entry.[6] *Olmstead* mainly considered whether government interception of private phone conversations was legitimate and did not specifically address privacy issues. In its reasoning, *Olmstead* seemed to declare that an individual had no right to privacy over a telephone conversation, which Justice Brandeis dissented that this notion failed to reflect the core value of privacy in technological changes.[7] Forty years later,

---

PRIVACY L. 255, 256 (2012), http://idpl.oxfordjournals.org/content/2/4/255.full.pdf+html (last visited Mar. 31, 2015); COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 2-6 (2008).

3. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

4. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 11 (4th ed. 2011) ("In 1884, the Eastman Kodak Company introduced the 'snap camera,' a handheld camera that was small and cheap enough for use by the general public. The snap camera allowed people to take candid photographs in public places for the first time.").

5. Warren & Brandeis, *supra* note 3, at 193.

6. Olmstead v. United States, 277 U.S. 438, 457-66 (1928).

7. *Id*. at 478-79 (Brandeis, J., dissenting) ("The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness . . . . [T]hey conferred, as against the Government, the

in *Katz v. United States*, the Court embraced Brandeis's dissent opinion in *Olmstead*, holding that government eavesdropping on telephone booth conversations violates a reasonable expectation to privacy, which, thus, constituted a "search and seizure" within the meaning of the Fourth Amendment.[8] The Court took forty years to adapt the privacy notion to take telephone technology into account.[9]

It has been over a century since *The Rights to Privacy* was presented. Privacy protection has developed extensively since then, and new issues continue to arise. It is time to examine if the existing privacy protection regimes are sufficient to cope with changing technology. The available legal remedies for invasion of privacy appear to fall short in dealing with new types of privacy invasion caused by new technologies. For example, tort claims in the United States are unlikely to protect individuals' privacy, as tort claims are based on actions that intrude into one's private life; the victim shall present an objectively reasonable expectation of privacy in terms of the place, conversation, or activity upon which the defendant intruded.[10] As the considerations would mostly focus on the nature of the relevant place, conversation, or activity and its accessibility to the public in a tort claim,[11] this regime cannot offer privacy protection if the alleged intrusion occurs in a place that was accessible to the public or on private property in public view.[12] The public/private dichotomy standard is probably a clear-cut approach when a line could be easily drawn between private territory and public space; however, new devices for videotaping, audiotaping or photographing in a networked world have blurred this line.[13]

Another era of information technology innovation began in the 1950s upon the advent of computers and magnetic tape technology that

---

right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment . . . [A]pplying to the Fourth and Fifth Amendments the established rule of construction, the defendants' objections to the evidence obtained by wire-tapping must, in my opinion, be sustained. It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.").

8. Katz v. United States, 389 U.S. 347, 350-53 (1967).

9. ROBERT GELLMAN & PAM DIXON, ONLINE PRIVACY: A REFERENCE HANDBOOK 17 (2011).

10. Anonymous, *Privacy, Technology, and the California "Anti-Paparazzi" Statute*, 112 HARV. L. REV. 1367, 1370 (1998).

11. *Id*.

12. *Id*. at 1371.

13. Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 17-20 (2013).

significantly enhanced information storage.[14] Since this time, information technology has continued to develop, and the rise of the Internet in the 1990s brought rapid technological developments in information privacy.[15] As the world entered the Internet age, people began to observe privacy changes: Physical interaction was no longer necessary for information transmission, and data flowed in a virtual world composed of a worldwide system of interconnected computer networks. Innovations in digital technology prompted the expansion of the Internet. Combined with broadband applications and fiber optic communication networks, the world's capacity to store, aggregate, and transmit data has grown radically, facilitating instant and high-quantity data transmission across borders, and beyond territorial boundaries. Furthermore, revolutions in wireless Internet service and mobile devices have dramatically changed the global communication landscape, facilitating human connection anytime and anywhere.

In the last century, the invention of the telephone marked a historical step in communications technology and culture, but the Court took forty years to adapt privacy protection to this new development. The Court's delay in keeping up with changes in technology was perhaps tolerable because the use of the telephone as a tool to invade privacy was relatively random. Now we are in the midst of an unprecedented tidal wave of technological revolution. The immense power of widespread digital and Internet technology does not offer mankind the luxury of passively watching and waiting. Failure to establish a countervailing privacy theory and legal system will leave individuals prone to overwhelming privacy attacks by emerging technology until information privacy is weakened, and, ultimately, heavily diminished.

B. *Common Features of Privacy Concerns Arising from Emerging Technologies*

Before we examine how the traditional notions of privacy shall be transformed to a modern one to reflect the changes of emerging technologies, it is essential to identify the relevant factors of privacy concerns due to emerging technologies. The wide use of internet-connected networks and electronic mobile devices has brought significant conveniences for the individual. At the same time, corporations are eager to take advantage of improvements in technology in order to obtain extensive information about consumers (such as shopping behaviors and preferences), and there is

14. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 14 (2004).

15. *See id*. at 15.

an increasing investment in research and development for techniques that enable useful computation of consumer data.

Online behavioral advertising is a major topic in the area of privacy protection[16] involving the issue of whether an individual's data, when stored on a mobile device, should be treated differently in terms of data protection.[17] This is another area where new technologies empower companies to conduct wider and deeper information gathering with the downside of exposing consumer data to unknown and unlimited uses. Businesses can now obtain users' geo-location data via mobile devices and analyze the users' movement patterns to produce behavioral advertisements targeted at the individual based on the physical location observed, and likewise, track the user digitally, using website based "cookies," which provide information from data files placed on the user's computer when that user visits an affiliated website.[18] A more advanced technology, deep packet inspection (DPI), enables Internet service providers (ISPs) to collect all Internet communications to and from a consumer, analyze their web traffic, and compile a "record of Web use to develop an advertising profile for a particular customer or group of customers."[19] This danger of data being used in unexpected ways is not unique to the online world. Grocery stores are preparing to launch a new high-tech device, smart shelves, to gather information on consumers' shopping habits and to make real-time purchase recommendations through sensors that examine the facial features of shoppers.[20] The problem of privacy creep is expanding, no longer limited to those members of society who elect to use new technologies.

Many other new technologies are coming into use, and different technologies may trigger different privacy implications. A fundamental

---

16. FEDERAL TRADE COMMISSION, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: TRACKING, TARGETING, AND TECHNOLOGY (2009), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf; FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

17. FEDERAL TRADE COMMISSION, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

18. Andrea N. Person, *Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May be Limiting the Online Experience*, 62 FED. COMM. L.J. 435, 442 (2010).

19. *See id.* at 441.

20. Travis Gettys, *Snack Maker Mondelēz Readying 'Smart Shelves' to Track and Influence Shopper Behavior*, RAW STORY, Oct. 15, 2013, http://www.rawstory.com/rs/2013/10/15/snack-maker-mondelez-readying-smart-shelves-to-track-and-influence-shopper-behavior/.

question that should be asked is the following: What are the common challenges to information privacy that arise due to new information technologies? Has the character of information privacy changed, or has a new type of privacy been created due to technological changes? Only when the privacy threats under the new information technology age are correctly perceived are we in a better position to evaluate whether the existing laws are sufficient to regulate the privacy threats identified or whether a new approach must be developed for problems caused by new technologies.

Several information privacy features have been identified as a result of the widespread use of the Internet. First of all, more detailed and extensive personal preferences and interests are collected from online activities, such as the history of Internet search terms and websites visited. [21] Second, ever more affordable data storage media[22] and faster aggregation and transfer of information provide great tools for business in the reuse of personal data.[23] When online communications are stored on a public network server or in the cloud, the line between public and private information is blurred.[24] Lastly, various pieces of personal information can be easily aggregated from different sources and linked to a single individual.[25]

Some observations have been made in relation to the characteristics of online communication as compared to offline information flows. They include: 1. Information Processing: Information is processed and disseminated faster and at higher quantities;[26] 2. Persistence: "Messages posted online have 'persistence,' in that messages can be replicated, archived, and essentially made permanent through cheap digital copies;"[27] 3. Quick and Efficient Searches: Third parties can "quickly and efficiently 'search' a public database, through a keyword search" via the Internet;[28] and 4. Audience Invisibility: "When sharing a post or tweet online, we have a general idea who will see our content, but we cannot know if our message will be seen by unanticipated audiences."[29]

It has also been pointed out that online privacy differs from offline privacy in several dimensions: online privacy lacks traditional national borders; digital and internet technology have greater memory capacities due to longer and higher quantity data retention, as well as easier access to information, and networked technology makes it harder to identify the owner

21. PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 625 (4th ed. 2010).
22. *Id*.
23. *Id*. at 626.
24. *Id*.
25. *Id*.
26. *See* Hartzog & Stutzman, *supra* note 13, at 10.
27. *Id*.
28. *Id*.
29. *Id*.

of data contained within.[30]

To summarize, emerging technologies have facilitated the collection, access and use personal data without restrictions in location and time. But the flip side of this convenience is an increasing threat to privacy protection. It will only become more difficult for one to know if his personal data is being gathered and how such data will be utilized. The current privacy laws and policies were designed under the assumption that one should be able to fully control his own data and decide how the data can be used. If the emerging technologies are shifting in the direction where individuals are less likely to be informed of and to control the information flow of their own data, a modern privacy notion will be needed to fix the privacy problems created by the above identified features of privacy in the era of new technologies.

C. *Privacy Concerns are Further Magnified Due to Big Data and Mobile Technologies*

"Big Data" technology brings up a new privacy issue.[31] The definition of "Big Data" is not uniform,[32] but according to Microsoft's definition, "big data is the term increasingly used to describe the process of applying serious computing power—the latest in machine learning and artificial intelligence—to seriously massive and often highly complex sets of information."[33] The "Big" feature of "Big Data" is used in two different senses. "It is big in the quantity and variety of data that are available to be

30. *See* GELLMAN & DIXON, *supra* note 9, at 4-9; Andrea Peterson, *We are Drowning in a Sea of Data. And Data Insecurity*, WASH. POST, Feb. 20, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/20/we-are-drowning-in-a-sea-of-data-and-data-insecurity/ ("Vast amounts of our lives are measured or recorded in ways that just were not possible before the advent of modern computing. When you buy groceries, your store discount card is creating a profile of your shopping habits. Some stores even physically track you with the wireless from your phone. When you visit your doctor, the information likely ends up in an electronic records system. Signing up for car insurance? There's your driving record pulled.").

31. Anonymous, Symposium, *Privacy and Big Data*: *Making Ends Meet*, STAN. L. REV. ONLINE (Sept. 3, 2013), http://www.stanfordlawreview.org/online/privacy-and-big-data.

32. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6 (2013) ("There is no rigorous definition of big data. Initially the idea was that the volume of information had grown so large that the quantity being examined no longer fit into the memory that computers use for processing, so engineers needed to revamp the tools they used for analyzing it all . . . . [O]ne way to think about the issue today—and the way we do in the book—is this: big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more"); *see also* Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 81 (2013) ("'Big data' can be defined as a problem-solving philosophy that leverages massive datasets and algorithmic analysis to extract 'hidden information and surprising correlations.'").

33. Microsoft News Center, *The Big Bang: How the Big Data Explosion is Changing the World*, (Feb. 11, 2013), https://www.microsoft.com/en-us/news/features/2013/feb13/02-11bigdata.aspx.

processed. And, it is big in the scale of analysis (termed 'analytics') that can be applied to those data, ultimately to make inferences and draw conclusions."[34] The "Google Flu Trends" case is a good example for explaining how "Big Data" is being created using new computing technology and what new privacy concerns are raised.[35] Google Flu Trends is a project launched by Google in 2008 to test the theory that "one might predict the parts of the world suffering from flu outbreaks by watching the symptoms people type into the Google search engine."[36] Google attempted to prove that "it can detect likely flu outbreaks a week or two faster than the physician-reporting surveillance efforts of the Centers for Disease Control and Prevention."[37] However, the project was done at the expense of breaching information privacy and betraying the public's trust. Failing to comply with the notice-and-choice and transparency principles,[38] Google did not offer people the choice to decide whether to trade their sensitive data (medical symptoms) to help save lives.[39]

Big Data technology is not merely a tool for businesses to analyze consumer preferences based on historic data. It can also be used to influence consumers' behaviors without their awareness. The giant online social network Facebook released research results in June 2014 from an experiment indicating that the Facebook News Feed can affect emotional states, as

34. PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY (PCAST), BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE ix, (May, 2014), http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

35. Another good example of the privacy concern of big data, s*ee* Andrew Leonard, *How Netflix is Turning Viewers into Puppets: "House of Cards" Gives Viewers Exactly what Big Data Says We Want. This won't End Well*, SALON.COM (Feb. 1, 2013), http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/ ("For at least a year, Netflix has been explicit about its plans to exploit its Big Data capabilities to influence its programming choices. 'House of Cards' is one of the first major test cases of this Big Data-driven creative strategy. For almost a year, Netflix executives have told us that their detailed knowledge of Netflix subscriber view preferences clinched their decision to license a remake of the popular and critically well regarded 1990 BBC miniseries. Netflix's data indicated that the same subscribers who loved the original BBC production also gobbled down movies starring Kevin Spacey or directed by David Fincher. Therefore, concluded Netflix executives, a remake of the BBC drama with Spacey and Fincher attached was a no-brainer, to the point that the company committed $100 million for two 13-episode seasons . . . . [F]or years Netflix has been analyzing what we watched last night to suggest movies or TV shows that we might like to watch tomorrow. Now it is using the same formula to prefabricate its own programming to fit what it thinks we will like. Isn't the inevitable result of this that the creative impulse gets channeled into a pre-built canal?").

36. Paul Ohm, Response, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. ONLINE 339, 341 (2013).

37. *But see id*. at 342 (Questioning that the benefits Google claimed might not be real benefits—"Has a traveler ever avoided boarding a plane to a city on a distant coast because of the relative difference in the shading of the oranges between home and destination?" The project's primary mission was to market Google.).

38. *See infra* Part III. A.

39. *See* Ohm, *supra* note 36, at 339.

reflected in users' posting behaviors.[40] Facebook conducted an emotional contagion experiment on 689,003 Facebook users by monitoring how hundreds of thousands of users react when they are exposed to carefully moderated content in their news feeds.[41] One Facebook researcher stated that the goal of the experiment was to "investigate the common worry that seeing friends post positive content leads to people feeling negative or left out. At the same time, we were concerned that exposure to friends' negativity might lead people to avoid visiting Facebook."[42] Similar to the Google Flu Trends project, the Facebook emotional experiment campaign indicates the real possibility that consumer behavior can be manipulated by businesses through Big Data technology.[43]

In addition to the common features of privacy concerns that have been observed, there is another key factor: It is nearly impossible for anyone to be left out of the intertwined digital and Internet world. The traditional control-driven approach would not be effective for information privacy protection in a world where, even if a person chooses not to use the Internet, mobile devices or online social network platforms, he remains trapped in the inescapable digital net where others remain able to track his personal data.

We have to face the fact that in this highly technologically developed era, people do not have a real choice to escape from surveillance from government and private sectors. The Internet and mobile devices combine and form a pervasive surveillance world that is nearly impossible to escape from. Businesses have a greater ability to track, maintain and analyze data to generate a digital dossier on individuals. New technologies can link location data with identity and significantly reduce the chances for individuals to be truly left alone. Individual choice is no longer a valid form of privacy protection. Through broader network access, people gradually lose control over their own data, and it is more difficult for individuals to keep their data secret.[44] Therefore, the architecture of privacy protection in the new era of information technology should not only retain the traditional theory of personal control or rely on the shaky public/private standard, but should instead adapt to real 21st century privacy needs.

Unlike in the non-digital age, online users do not know who has their data, nor can they prevent and stop unwanted intrusions. How others gather and use personal data is unknown and invisible to the affected persons. Life

40. Gail Sullivan, *Facebook Responds to Criticism of its Experiment on Users*, WASH. POST (June 30, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/06/30/facebook-responds-to-criticism-of-study-that-manipulated-users-news-feeds/.

41. *See id*.

42. *Id*.

43. *Id*.

44. Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 249-50 (2008).

will be full of unknown and uncertain exposures to privacy attacks, and individuals will gradually lose their autonomy over personal information.[45] A major threat from new technologies is that the Internet enables a far more detailed collection of information than that possible in the offline world.

A significant privacy problem that has not been fully addressed in this era of emerging technology is that individuals are less likely to know who is collecting, using, or controlling their personal data. In the offline world, when individuals subscribe to a newspaper or shop at malls, they know who possesses their contact information and transaction history. Modern technologies, on the other hand, have one thing in common: Online users are unlikely to know their data is being collected when they click on or scroll down a web page. The invisibility feature is the most significant difference between online and offline information privacy. Individuals are less likely to know exactly how their data are used due to the dynamic and global nature of the Internet. These "invisibility" and "unknown" features should be included as important privacy considerations when addressing how to design a baseline privacy protection regime.

The invisibility and unknown features present another question. If people do not know that their privacy rights have been infringed, they cannot stop the damaging activities or present a claim for compensation. Historically, the basis for an injured party's privacy invasion claim is how the intruder illegally collected or used the subject's personal data and the damage that was caused. However, in the digital era, the privacy harm is unlikely to be detected the moment that the data is collected or used, and the major harm might occur long after the privacy breach. The flip side of embracing powerful technologies to enhance management of complex data is a reduced ability for data subjects to control circulation of their data. The tendency of new computing and mobile technologies to expand into the major aspects of our lives fosters growing fears of unknown and invisible invasions of privacy. These unpredictable breaches of privacy are eroding the individual's freedom to be left alone. Without a proper response to expanding innovative technology development in terms of privacy protection, a great concern for future privacy is that data subjects will gradually lose the capacity to protect the privacy of their information.

---

45. New information technologies form a digital surveillance society. This kind of society is like a "Panoption—an architectural design for a prison," originally conceived by Jeremy Bentham in 1791. By setting up an observation tower at the center of the Panoption, all prisoners are watched by a supervisor in the tower at anywhere, any time. "By always being visible, by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be watched. This fear alone is sufficient to achieve control." *See* SOLOVE, *supra* note 14, at 30-31.

III. AN APPROACH TO RESPOND TO NEW INFORMATION PRIVACY IMPLICATIONS

Most information privacy protection legal regimes in the world were developed under the control-driven notion, which focuses on the autonomy of the subject in deciding whether and how data can be used. Privacy laws and policies are constructed on several principles, primarily the fair information practice principles (FIPPs), which emphasize notice-and-choice (informed consent), as well as the transparency of data collection and processing, to ensure that the subject of the data has full control over his own data.[46] These principles can be described as the "privacy self-management" approach.[47] However, when information gathering and use through new technologies have largely become invisible and unknown to subjects of data, notice-and-choice is not a pragmatic approach in allowing both protection of privacy and innovation in technology.

A. *Problems with the Notice-and-Choice Principle*

The FIPPs first officially appeared in a 1973 report by the U.S. Department of Health, Education, and Welfare[48] to "address concerns about the increasing digitization of data."[49] The notice-and-choice and transparency principles are constructed on two theories. First, privacy is a right to control information about oneself. Under the transparency-and-choice approach the subject of the data can determine, based on the information provided by data controller in the course of data collection and use, whether to agree to such collection and use of their data, which should be an effective method in protecting the subject's right to control data about himself.[50] Second, in a completely free market, where all relevant information is fully available, the subject of the data, data

46. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011).

47. Daniel J. Solove, Symposium, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

48. SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS xx-xxi (1973), http://www.justice.gov/opcl/docs/rec-com-rights.pdf. (The Fair Information Practice rests on five basic principles: 1."There must be no personal data record keeping systems whose very existence is secret." 2. "There must be a way for an individual to find out what information about him is in a record and how it is used." 3. "There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made other purposes without his consent." 4. "There must be a way for an individual to correct or amend a record of identifiable information about him." 5. "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.").

49. *See* Solove, *supra* note 47, at 1882.

50. *See* Nissenbaum, *supra* note 46, at 34.

controllers and data users will naturally find an agreeable balance of data privacy protection.[51]

The FIPPs largely centered on procedural safeguards to promote the individual's rights in determining their own data's being collected and used. However, the rationale for why personal data must be protected has not been frequently addressed. For instance, FIPPs do not provide explanation on the prohibition of any data collection and use when certain categories of personal data are involved. FIPPs now face a tougher challenge as to whether the transparency-and-choice approach is adequate for online privacy protection.[52] The main concern is whether the theoretical condition that the subject of data can always be given full information, and accordingly, make an informed decision holds true in the real world. Under this principle, the subject must be clearly told what he or she is consenting to. However, many consumers pay little attention to privacy notices or policies written by companies, and cannot fully comprehend the content even if they read the terms.[53] Certain consumers have the mislead notions of privacy, for example, that their privacy is automatically assured as long as there is a "privacy policy" label displayed on the webpage of the businesses that they are interacting with, though they do not investigate the terms of the privacy policy.[54]

Moreover, the idealized assumptions of a free market and rational choice by individuals fail to consider the complex structure of the modern online economy, wherein multiple third parties, including both private sector (such as data brokers, data processors and advertising companies) and public sector (such as a government agency requesting that businesses grant access to consumer data) play a role in information collection and processing, which may significantly change the theoretical model.[55]

Problems have occurred in online social networks, illustrating that the notice-and-choice principle is insufficient to protect information privacy. LinkedIn is a social network and online platform for professionals;[56] it is "the world's largest professional network with 225 million members in over 200 countries and territories around the globe."[57] In September 2013, four individuals filed a lawsuit against LinkedIn alleging that the company had

51. *Id*.

52. Solove, *supra* note 47, at 1883-93 (There are two broad types of problems according to Professor Solove's discussion: " (1) cognitive problems, which concern challenges caused by the way humans make decisions, and (2) structural problems, which concern challenges arising from how privacy decisions are designed.").

53. *See id*. at 1885-86.

54. *Id*. at 1886.

55. Nissenbaum, *supra* note 46, at 34.

56. LINKEDIN, https://www.linkedin.com/ (last visited Mar. 31, 2015).

57. Peter S. Vogel, *Is LinkedIn Being Sued for Doing Just What It Says It Will Do?*, E-COMMERCE TIMES (Nov. 8, 2013), http://www.ecommercetimes.com/story/79383.html.

been breaking into their users' email accounts, downloading their contacts' email addresses and sending emails to their contacts to join LinkedIn.[58] The complaint alleged that the invitations appeared as they were sent by LinkedIn members, but were in fact sent by the company itself.[59] LinkedIn denied that the emails were sent without the users' consent, defending itself with a provision in its privacy policy, reading: "We collect information when you sync non-LinkedIn content—like your email address book, mobile device contacts, or calendar—with your account. We use this information to improve your experience and allow you and your network to be better connected. You can remove your address book and any other synced information whenever you'd like."[60] It is possible that, similar to most consumers using commercial websites or online services, LinkedIn users might not pay attention to the privacy notices. Moreover, even if they read the clauses, the vagueness of the above provision does not seem to offer a clear indication that when one checks the box to agree to the terms of use and join as a LinkedIn member, he has agreed that LinkedIn may collect and use his email address book and mobile device contacts.

The FIPPs provide no resolution if the data being collected or used relates to a third party who is not in a position to learn the existence of data processing. Even if we assume that all LinkedIn members understand and agree to grant LinkedIn a right to use all their email address books and mobile service contacts, based on the current notice-and-choice approach, the consent is only effective between the member and LinkedIn and does not extend to third parties. However, under the default LinkedIn settings, any person on a LinkedIn member's email or phone contact list is brought to the attention of LinkedIn without his knowledge. This case clearly runs afoul of the notice-and-choice principle because the subject of the data neither knows that his personal information has been disclosed to LinkedIn nor has a chance to object to the disclosure.

Failure to resolve the notice-and-choice loopholes in privacy protection has a negative impact on businesses. Some might say that the aforementioned situation is not a serious privacy problem because the email invitation simply offers the third party a chance to join the LinkedIn network; if the party receiving the invitation is not interested in the network, he can just ignore the email. However, one person's ordinary may be other's extraordinary. Those who care about information privacy may feel embarrassed and annoyed when LinkedIn has free access to their email contacts and sends emails to those they have not been in touch with for a

58. *Id*.
59. *Id*.
60. *Your Privacy Matters: 1.4. Address Book and Other Services that Sync with LinkedIn*, LINKEDIN, http://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv (last visited Mar. 31, 2015).

long time, have a bad history with, or were only briefly contacted. For persons who receive invitations from LinkedIn to join the network, one invitation may be tolerable, but most people are annoyed if they are bombarded with hundreds of emails. Most seriously is the chilling effect to LinkedIn members and their friends, who may begin to fear that their personal information is out of their control and do not know what type of privacy harm they will incur in the future.

This LinkedIn case presents a unique concern generated by modern technologies: Individuals, whether social network users or third parties, are losing control over their data, and there does not seem to be an easy way to prevent or predict when and how information privacy invasion occurs.

A stronger notice-and-choice privacy policy does not aid in privacy protection if the changing factors of privacy in the modern technology age are not taken into consideration. In response to the above defect, and to rectify the flaws of the notice-and-choice principle, some have proposed that an enhanced transparency principle should be implemented, mandating that data controllers shall provide subjects of the data with more information on the ways in which the personal data is collected, stored and shared.[61] These methods include requiring companies that collect personal data through commercial websites to post a clear and conspicuous privacy policy, as well as take steps to ensure that individuals are informed about data processing. The methods may go further and set the default position as "opt-in" (controllers cannot send out marketing messages before individuals expressly agree) instead of "opt-out" (controllers can send marketing messages until the recipient objects).

However, merely adding more procedural requirements is not a viable approach to achieve privacy protection goals.[62] In the emerging world of technology, consumers not only interact with businesses that engage in commercial transactions or online activity with consumers, multiple parties participate in data collection, exchange, and use, and often these parties are unknown to the consumers (e.g., data brokers). There are practical difficulties to enforcing the notice-and-choice policy in this situation. Even if a transparency policy is strictly enforced and requires full disclosure of all parties who have access to personal data, consumers will be flooded with privacy notices, too numerous and burdensome for the average consumer to digest.[63] Swamping the world with privacy notices is not a remedy for the information privacy issue, as such messages would be as annoying as

61. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTION INNOVATION IN THE GLOBAL DIGITAL ECONOMY 47-48 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

62. Nissenbaum, *supra* note 46, at 35.

63. Solove, *supra* note 47, at 1888.

nonstop pop-up advertisements, leading most consumers to simply ignore them.

Likely, using resources to require compliance with the notice-and-choice policy is not a meaningful and feasible option in today's technology environment. The primary challenge comes from bulk data collection for reuse in the future, which may include purposes outside the scope of consent originally given by the data subject. The improved technology tools allow business to conduct data mining, storage and analysis for purposes that were not predicted by either the data controllers or subjects of the data. "Google Flu Trends" is one example. Google stipulates in its privacy policy that the Google search engine service and Gmail service will collect user information to improve Google services, such as enhancing Google search results and blocking spam messages.[64] While the original idea underlying Google's collection of user information was to improve the search engine and electronic email services, the collected data was later used for another purpose—to predict the parts of the world suffering from flu outbreaks.

B. *Suggestions for the Reconstruction of Information Privacy Theories*

This essay proposes that adding more procedural notice-and-choice requirements will be of little help in protecting information privacy in the 21st century. In this era, livelihoods rely on free flowing data and data-intensive applications on a global scale. A viable approach in the emerging world brought by new technologies must provide more substantial results where privacy laws or policies are constructed to balance between protecting information privacy and allowing the uninterrupted flow of data for international trade. We must return to our basic issue: Why does information privacy deserve protection? From here, we may examine how to cope with new information privacy challenges, as well as whether privacy theories should be modified. This essay includes suggestions for reconstructing the traditional privacy theories below and proposes that privacy should be determined by both individuals' subjective feelings and objective social norms. Moreover, the government has a constitutional obligation to protect the right to privacy by constructing basic information privacy principles.

64. Hayley Tsukayama, *Google Explains Itself after E-mail Scanning Backlash*, WASH. POST, (Apr. 15, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/15/google-explains-itself-after-e-mail-scanning-backlash/.

1. *Individual Value of Privacy*

Historically, the concept of privacy has been understood from the subject's personal perspective, feelings and beliefs. Professor Fred H. Cate sets out the following aspects of privacy:

> (1) individual autonomy (the right to make decisions about marriage or family without government interference); (2) solitude and intimacy (the desire to limit access to a place or to oneself); (3) confidentiality (trade secrets and information disclosed subject to a promise of confidentiality); (4) anonymity (the desire not to be identified); (5) security (for oneself or one's information); (6) freedom from intrusion—whether physical (a trespasser) or technological (a hidden camera or microphone); (7) control of information about oneself.[65]

Professor Daniel J. Solove provides the following definitions of privacy: (1) "the right to be let alone;"[66] (2) "limited access to the self;"[67] (3) "secrecy;"[68] (4) "control over personal information;"[69] (5) "personhood" (the protection of one's personality, individuality, and dignity);[70] (6) "intimacy" (control over or limited access to one's intimate relationships or aspects of life).[71] These notions of privacy originate from individualistic values of privacy rights.[72] "Intimacy" may not be strictly limited to an individual's inner feelings or thoughts, but may also be constructed on outside perceptions of their relationships with others.[73]

The above dimensions of privacy fall short of modern needs forced by new information technologies. Among other technologies, the Internet has created a virtual world that facilitates robust information exchange over which individuals have little control. All information uploaded to publically accessible areas of the Internet leaves the original information owner's control. No attempt to thoroughly enforce the control-based theory, in

65. FRED H. CATE, PRIVACY IN PERSPECTIVE 3-4 (2001).
66. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 15-18 (2008).
67. *See id*. at 18-21.
68. *See id*. at 21-24.
69. *See id*. at 24-29.
70. *See id*. at 29-34.
71. *See id*. at 34-37.
72. *See id*. at 89.
73. James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323, 326 (1975) ("[T]he value of privacy [is] based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people."), http://www2.warwick.ac.uk/fac/soc/philosophy/undergraduate/modules/ph212/2014-15/rachels_james_-_why_privacy_is_important.pdf.

opposition to the direction in which the Internet operates, will aid in online information privacy protection, and would likely impinge on the considerable advantages of efficient personal data transfer.

Further, mobile electronic devices have changed the notion that a right to privacy is a right of seclusion or secrecy. When cameras are pervasive in smart phones or tablets, they can be easily used to secretly shoot high-resolution photos, making it more difficult for individuals to be let alone and keep their privacy. Individuals' geographic location can be tracked to within a few meters using the GPS function of cell phones. When this information may be accessed without the individual's knowledge, it becomes nearly impossible to limit access to oneself. If privacy protection standards are developed to enhance an individual's control over data and ensure secrecy and confidentiality in all aspects, the flip side is losing the advantages of these advancements. In fact, as technological advancement has become an unstoppable and accelerating force, insisting on the control theory will adversely create deadlock and decrease the availability of feasible solutions to harmonize the interests of personal information privacy and supporting technology innovations.

2. *Social Value of Privacy*

Traditional privacy theory is largely centered on the individual's subjective values. But if we recognize that privacy notions must evolve with societal changes, the social value of privacy may also be taken into consideration. This essay proposes that, under new technologies, privacy issues are no longer limited to strictly personal matters, and individuals are too weak to defend against privacy invasions from powerful technology giants. The individual's granular interest in privacy cannot be considered in the same league as the sweeping benefits claimed by businesses or government. As further explained below, a viable approach is to take into account both the individual value and the social values of privacy. This will be important to a new notion of privacy suitable for the modern technological era, and will make it possible for privacy to stand on an equal footing with interest in a free flow of information.[74]

A key piece of the privacy puzzle is that privacy is a notion generated in the course of a social life; therefore, the value of privacy cannot be correctly perceived without considering the social context.[75] Individuals and society

74. DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 47-50 (2011).

75. Julie E. Cohen, Symposium, *What Privacy is For*, 126 HARV. L. REV. 1904, 1905 (2013) ("[L]iberal privacy theory's descriptive premises about both the self and the nature of privacy are wrong. The self has no autonomous, precultural core, nor could it, because we are born and remain

are inseparable. Reputation and credibility are legitimate rights and are protected by laws because a person's reputation is an opinion from the public and is shaped by society. Reputation is essential to a person's social life, but it would be meaningless to a man sailing alone on the sea for his entire life. Similarly, if one is living alone, it is meaningless to talk about privacy protection because there are no fears of eavesdropping, prying eyes, or secret collection and use of personal data.

In line with the contention that the value of privacy is built upon a social life, the approach to define privacy and make privacy policy must consider relevant societal factors, without the limitation of individual perspective. Such an approach will complicate the balance between privacy and technology, as different circumstances involving diverse factors will fill each evaluation with uncertainties. As opposed to this approach, another option is to identify a commonly accepted value of privacy that can universally apply to all situations. However, offering a nominal and abstract definition of privacy is unlikely an effective solution to the problem of precisely determining the value of privacy, if the definition does not contain privacy factors relevant to the society.[76] For instance, a classic definition of privacy is that it is a right to be let alone.[77] However, no one can claim that his privacy includes the right to be let alone anytime and anywhere. Imagine you are having a long-waited romantic gateway with your loved one and are enjoying a candle light dinner at a high-end restaurant. Unfortunately, a large crowd in the restaurant, chatting and laughing loudly, ruins the romantic atmosphere. As upset as you may be, it is unrealistic to claim a right to be let alone against the loud crowd. In this example, the abstract concept of privacy as a right to be let alone does not offer a guideline to resolve real life problems without examining how to realize privacy in the real world during interactions with a society's interests. One's right to be left alone will inevitably conflict with the ability for others to engage in the infringing social activity. This conflict is why the United States Supreme Court developed the reasonable expectation of privacy doctrine[78] for determining

situated within social and cultural contexts.").

76. SOLOVE, *supra* note 66, at 13-14.

77. Warren & Brandeis, *supra* note 3, at 193.

78. The United States Supreme Court in *Katz v. United States* held that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *See* Katz v. United States, 389 U.S. 347, 351 (1967). In his concurring opinion of *Katz*, Justice Harlan set out both the subjective and objective requirement under the Fourth Amendment: "a person have exhibited an actual (subjective) expectation of privacy" and "the expectation be one that society is prepared to recognize as 'reasonable'." *See also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., Concurring). This twofold test laid out the foundation of the widely cited reasonable expectation of privacy test and formed the major consideration when the Court determined the Fourth Amendment claim.

Fourth Amendment claims and privacy torts. When one exposes himself to a public place to engage in his social life, he is prepared to give up the right to be left alone, and does not expect privacy. Under this standard, one's privacy is not absolutely protected when it runs into conflict with others' interests such as the right to free expression in public places.

The society one is living in influences how privacy is perceived. Therefore, privacy protection should include the subjective expectation of individuals as well as objective elements from society.[79] This proposition is supported by certain academic opinions that recognize the social value of privacy.[80] Professor Julie E. Cohen proposes that "[s]ubjectivity, and hence selfhood, exists in the space between the experience of autonomous selfhood and the reality of social shaping."[81] This notion recognizes the social value of privacy and ensures a harmonious link between personal selfhood and societal norms. In other words, privacy "enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making."[82] As Professor Solove contends, "[p]rivacy isn't the trumpeting of the individual against society's interests but the protection of the individual based on society's own norms and values. Privacy isn't simply a way to extricate individuals from social control; it is itself a form of social control that emerges from a society's norms."[83]

Additionally, privacy has an important function in fostering democracy and therefore the genuine value of privacy must include its social aspect. Political scientist Priscilla M. Regan analyzes privacy in a social context and contends that benefits from privacy protection include resisting abuse of government power and fostering democracy.[84] Professor Paul M. Schwartz echoes this position that "[t]he maintenance of a democratic order requires both deliberative democracy and an individual capacity for self-determination."[85] Accordingly, one value of privacy is to ensure that the

79. Cohen, *supra* note 75, at 1927 ("Privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing, and those purposes must be taken into account when making privacy policy.").

80. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 85-86 (2010); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 968-78 (1989); ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 19-20 (2011) ("The question of how to reconcile the ideal of privacy rights with the need for information, surveillance, and social cohesion is an unquestionably importance one, the subject of frequent debates . . . . [W]e need to extend debates—common in feminist literatures—about balancing freedom from unwanted privacy rights, on the one hand, with duties of privacy, on the other.").

81. Cohen, *supra* note 75, at 1909.

82. *Id*. at 1911.

83. SOLOVE, *supra* note 74, at 50.

84. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225-27 (1995) ("Privacy has value not just to individuals as individuals or to all individuals in common but also to the democratic political system.").

85. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1658

individual can exercise his right of self-determination, thereby preserving the overall social value (e.g., democracy).[86] Professor Neil M. Richards also supports privacy as a social aspect and presents the notion of "intellectual privacy," that is, "[t]he ability to freely make up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy. In this respect, intellectual privacy is a cornerstone of meaningful First Amendment liberties."[87]

3. *A Modified Privacy Theory and Its Application to the Taiwanese Drivers' Data Collection Case*

The control-driven information privacy theory cannot deal with the privacy problems emerging in the 21st century. With the help of technological improvements, data collection, processing and use are significantly advancing in terms of speed, quantity and location. One accompanying effect of this is an increasing difficulty for people in controlling their personal data. This fundamental change has become a major challenge to the existing data protection regime which is largely centered on individual control over their data. The current and dominant individual-value based data protection regime is designed to protect the individual's control over personal data. As mentioned above, this theory appears to have become impractical in the protection of individuals' privacy as technological improvements have made it nearly impossible for individuals to retain control over personal data. If this theory is not modified, it will be of no help in protecting privacy and will adversely hinder technological advancement.

The notion of privacy needs to be enhanced with a concept of social value in order to compete with the interests of the free flow of information on an equal footing. We cannot ignore the benefits to the general public brought by technological advancement which heavily relies on the free flow of personal data. In many situations, the public interest may outweigh the affected individual value of privacy. In the above mentioned Google Flu Trend Project, Google used the collected personal data for the purpose of predicting and preventing the spread of infectious disease. While the project may have affected the privacy rights of the data subjects, this may be acceptable because the project's goals are to protect a greater societal interest. It is important to note that, if the privacy theory used to analyze issues in conflict is one that contains only the single (individual value) element to protect the individual's control over personal data, such a theory would fail to protect personal interest, as personal interest can hardly prevail

(1999).

86. *Id*. at 1660.

87. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

when it is compared with public interest. Likewise, if the privacy theory has only this single element, the government does not usually have the authority to intervene in personal matters even where personal data are threatened by private entities. For example, in a contract wherein individuals have assented through contractual arrangements to a business' use of personal data to build up a family tree, the government is unlikely to take the initiative to raise privacy concerns and take actions to change the contractual arrangements. To remedy the shortcomings of the individual-value based information privacy theory, this essay proposes a solution in including the social value of privacy as an enhancement to the privacy theory. This enhanced theory immediately offers a legitimate ground for the government to step in to protect privacy interests when the affected individuals lack the power in resisting privacy right infringement supported by public interest.

It is important however to note that the social value of privacy is not a replacement for the fundamental individual value of privacy. Undoubtedly the nature of privacy is that of a personal human right, and it is not at all the position of this essay that privacy is rooted in social value. But it should be recognized that privacy is a spiritual right which has an important social dimension. The value of privacy for the individual cannot be separated from the value of the individual in a society. Privacy benefits both individuals and society, and these two dimensions work together in an interlocked, symbiotic fashion. Given this, the evaluation of the individual value of privacy has to consider the factors in the society as a whole. For example, to draw a line of the free flow of personal data, the social norms need to be considered in evaluating under what circumstances the flow of personal data would constitute an infringement upon privacy rights. This essay will, in the following paragraphs, examine this modified theory's workability by attempting to apply it in an outstanding case in Taiwan.

In January 2014, Taiwan officially launched a nationwide highway electronic toll collection (ETC) system, which is a distance-based electronic toll collection system aimed at allowing highway users to drive through the toll plaza without having to slow down to pay the toll. The system works using radio-frequency identification (RFID) technology,[88] implemented through the use of an electronic tag ("eTag") installed on the user's vehicle.

88. Oleg Kobelev, *Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance through the Use of Radio Frequency Identification Technology and the Need for Legislative Response*, 6 N.C.J.L. & TECH. 325, 326 (2004) ("RFID is a technology that allows companies and governments to implant tiny and virtually undetectable microchips or 'tags' with antennas into almost any product or animal, including humans. Predicted by MIT researchers to become the most pervasive computer technology in history, most RFID tags do not require any external power source and can transmit information via radio waves when the tag enters the reception field of the nearest scanner. RFID tags are commonly used to store an Electronic Product Code ('EPC') that assigns a unique identifier to every RFID chip, thereby allowing fast, efficient, and cost-effective inventory tracking.") (footnote omitted).

Although the original goal of the ETC was to shorten travel times on highways by employing a stable and efficient electronic toll collection method across the country, unexpected privacy concerns were raised due to the widespread data collection made possible by the ETC system. Numerous electronic gates are being installed on the highway to conduct electronic surveillance on all vehicles that enter the highway for 24 hours a day, 365 days a year.

A news report revealed that Taiwan's Criminal Investigation Bureau (CIB) sought access to the ETC database.[89] The CIB requested the ETC operator to turn over toll records in the name of crime prevention. If we weigh the conflicting interests between the purely individual value of privacy and public interest in crime prevention, one can hardly claim that he will suffer concrete privacy harm, let alone that such harm is significant to preempt the public interest claimed by the CIB. As a result, the government's indiscriminate gathering of personal information is prone to abuse, such as attacks on political foes, ultimately endangering democratic society. This example illustrates that a notion of privacy which incorporates the social value of privacy significantly impacts privacy protection compared with a notion based purely on an individual value of privacy. When the social value of privacy is considered, the CIB's desire to access all drivers' data should be prohibited unless the CIB can demonstrate that the claimed public interest is greater than the social value of democracy.

C. *An Approach to Constructing a Social-Value-Oriented Privacy Theory and Its Application to Policy Making*

1. *Dignity-Based Privacy Theory: A Notion to Better Safeguard the Social Value of Privacy*

When the social value of privacy is recognized, we understand privacy in its social context. Privacy is not individual freedom or liberty. Freedom is an independent, stand-alone human right that should not be compromised, regardless of outside elements. Privacy, however, is a dynamic notion that is shaped by changing circumstances.[90] The current privacy policy

89. Lin Zhi Qing (林志青), *Yuan Tong Laing Ci Baojia You Ge Zi Fa Da Zhu Xing Shi Ju Chi Xu Xie Tiao (遠通2次報價憂個資法打住　刑事局持續協調)* [*PDPA Concerns Halted FE-Toll Two Offers to CIB, Negotiation Continues*], PING GUO RI BAO (蘋果日報) [APPLE DAILY] (Jan. 11, 2014), http://www.appledaily.com.tw/realtimenews/article/new/20140111/324266/.

90. Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2092 (2000) ("[P]rivacy presupposes persons who are socially embedded, whose identity and self-worth depend upon the performance of social norms, the violation of which constitutes 'intrinsic' injury.").

overemphasizes the individual's right to self-determination, while failing to consider another aspect of privacy (its social context). The next issue is the methodology used to consider social value with regard to privacy protection.

The United States and continental Europe perceive privacy differently. The fundamental difference is that Europeans view privacy as an aspect of "dignity,"[91] while Americans view privacy as an aspect of "freedom"[92] (or "liberty").[93] Professor Robert C. Post shares the opinion of sociologist George Herbert Mead: "The 'I' is the response of the organism to the attitudes of the others; the 'me' is the organized set of attitudes of others which one himself assumes. The attitudes of the others constitute the organized 'me,' and then one reacts toward that as an 'I',"[94] and he says:

> Privacy as dignity protects the "me"; privacy as freedom protects the "I." Privacy as dignity safeguards the socialized aspects of the self; privacy as freedom safeguards the spontaneous, independent, and uniquely individual aspects of the self. . . . Privacy as dignity seeks to eliminate differences by bringing all persons within the bounds of a single normalized community; privacy as freedom protects individual autonomy by nullifying the reach of that community.[95]

The notion of dignity closely links to the most basic rights, such as the rights to one's image, name, and reputation. Founding privacy on the notion of dignity inherently yields broader protection because it protects against infringements not only from the State but also private entities, such as the media.[96] By contrast, the American "Freedom" basis is much more oriented toward values of liberty against the State.[97] In the European notion of privacy, the right to privacy is integrated and interacts with a society. Historically, this has meant the government has a duty to protect such rights, as the benefits to a society often outweigh the disadvantages to individual

---

91. *Id.* ("Dignity, by contrast, refers to 'our sense of ourselves as commanding (attitudinal) respect.' Unlike autonomy, dignity depends upon intersubjective norms that define the forms of conduct that constitute respect between persons. That is why modem legal systems so often set autonomy and dignity in opposition to each other.") (footnote omitted).

92. *See id*. at 2095 ("[P]rivacy as freedom is an almost exact inversion of the concept of privacy as dignity. Privacy as freedom presupposes difference, rather than mutuality. It contemplates a space in which social norms are suspended, rather than enforced. It imagines persons as autonomous and self-defining, rather than as socially embedded and tied together through common socialization into shared norms.").

93. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151, 1161-62 (2003).

94. GEORGE HERBERT MEAD, ON SOCIAL PSYCHOLOGY 239 (1964).

95. Post, *supra* note 90, at 2095-96.

96. *See* Whitman, *supra* note 93, at 1162-63.

97. *See id*. at 1161.

citizens.

The European Union (EU) and United States (U.S.) may hold differing notions of privacy due to different political histories and citizens' opinions on the role of government. Generally speaking, Europeans believe that the government was established to protect people against intrusions from private parties; on the other hand, Americans have greater trust for private entities, viewing government as the greatest enemy of liberty. This conflict explains the different approaches to regulating online privacy problems in the EU and United States. Under EU privacy law, government regulation is used to restrict collection, use and sharing of personal data, while the current bills proposed in the U.S. seem more inclined to rely on self-regulation by industry.[98]

The (American) liberty-based privacy protection approach emphasizes individual autonomy, and regulations are formed based on its core value–the individuals' control over personal matters. Regulations designed based on this approach often aim to prevent government intrusion and tend to be more conservative with regard to restricting activities of private enterprise. On the other hand, human dignity is the cornerstone of the EU privacy protection policy, which uses a dignity-based approach.[99] Any collection or use of certain information (such as sensitive information) that is likely to impair dignity is banned, even if the affected person has exhibited an intention to give up the right. The EU uses this approach because its dignity-based privacy involves both an individual's and society's norms, and nations are not regarded as an enemy of the people, but as a guardian against the invasion of privacy by private parties.

As Professor Post comments, "Privacy as dignity locates privacy in precisely the aspects of social life that are shared and mutual. Invading privacy causes injury because we are socialized to experience common norms as essential prerequisites of our own identity and self-respect."[100] Therefore, if one has injured another's dignity, the State has an obligation to take an active stance in protecting peoples' dignity, and in this case, the State becomes the peoples' ally in its role protecting their privacy. In sum, at most, a liberty-enshrined privacy theory can passively prevent intrusions by the government, whereas the counterpart, a dignity-initiated privacy theory, preserves citizens' right to resist government while also obligating the state to provide for protection and effective realization of human rights, fostering

98. FEDERAL TRADE COMMISSION, *supra* note 16.

99. *Cf.* Spiros Simitis, *Privacy: An Endless Debate*, 98 CAL. L. REV. 1989, 1993 (2010) ("The German Courts . . . made a conscious choice to ground privacy in both concepts [dignity and liberty]. Besides, precisely because of the importance of both dignity and liberty, the European Union and its Member States are obliged to protect privacy in both their internal regulations and external agreements.").

100. *See* Post, *supra* note 90, at 2094.

the civil liberties that are needed to sustain meaningful democracies.[101]

This is the look of a modified and improved privacy theory. It will develop from a dignity-based privacy theory to encompass elements of individual privacy. This individual privacy is the core of a privacy notion based on individual autonomy. Surrounding this core are multiple layers of dignity-based privacy elements that represent social privacy, which is supported by the common good and human dignity.

With a dignity-based privacy theory, the government will be empowered to protect privacy when individuals are too weak to resist privacy invasions fueled by rapidly evolving technologies. Currently, business is the main threat to privacy rights, compiling considerable personal information on a scale that trumps the public sector in both quantity and diversity. Businesses are profit motivated and naturally eager to collect as much personal information as possible in order to seize the business opportunities it presents. Giant corporations have substantial data mining power, exceeding that of the government. Thus, in privacy protection, the individual's exercise of his right to self-privacy (in the freedom-based privacy theory, against the government) is no longer a meaningful way of resisting. When individuals cannot deter, detect, stop or escape from information privacy invasions by large, transnational corporations with power beyond any single person's control, it is imperative that the government should shoulder the responsibility of protecting citizens' information privacy.

Some might doubt that data collection and use by a firm is an activity by a private party, a situation in which the government should typically not intervene. This contention overlooks an important feature of privacy: privacy protection for the individual is not only a private matter, but must instead rise to the level of public policy and social good. Accordingly, privacy rights should not be exercised at the individual's discretion[102] when

---

101. Sifa Yuan Dafaguan Jieshi No. 603 (司法院大法官解釋No. 603) [Judicial Yuan Grand Justice Interpretation No. 603], at holding ¶ 1 (Sept. 28, 2005) (Taiwan) ("To preserve human dignity and to respect free development of personality is the core value of the constitutional structure of free democracy. Although the right of privacy is not among those rights specifically enumerated in the Constitution, it should nonetheless be considered as an indispensable fundamental right and thus protected under Article 22 of the Constitution for purposes of preserving human dignity, individuality and moral integrity, as well as preventing invasions of personal privacy and maintaining self-control of personal information."),
http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603.

102. ALLEN, *supra* note 80, at 13 ("The foundational goods are the sorts of human resources liberal philosophers and political theorists since John Rawls have often referred as 'primary goods.' Rawls's own long list of primary goods featured the following: basic rights and liberties; freedom of movement and free choice of occupation against a background of diverse opportunities . . . and the social bases for self-respect . . . . My view is that for the sake of foundational human goods, liberal societies properly constrain both government coercion and individual choice, including the choice to forgo privacies we will typically need for a lifetime of self-respect, trusting relationships, positions of responsibility, and other forms of flourishing.").

it contradicts societal norms. For instance, if personal data are shared to enhance or reproduce a social hierarchy which preserves unfair advantages for certain groups of people, harming the common good in a way which should be discouraged by a democratic society, the way one manages his data should be limited. For example, Ancestry.com offers services to create family trees for free, which requires that participants enter not only their own personal information, but those of their relatives as well.[103] Hypothetically, such service provider could also compile certain genetic and ethnic data from participants and sell such data to a biometrics company. Fueled by the large genetic and ethnic database provided by this service, a biometrics company creates a map of human genetic variations that details the genetic histories of different populations across the world. The biometrics company might have various motivations for creating this genetic map, such as treating a disease, which is probably acceptable to the general public. However, if the same genetic map is used for racial discrimination, to sustain the interests of certain ethnic races or to diminish other ethnic groups, the collection and transfer of such biometrics data should be restricted. This is one example to illustrate why, in many regimes, such as the EU, certain categories of personal data that involve sensitive information are subject to stringent limits on data collection and use, such as personal data showing racial or ethnic origin and those concerning one's health or sex life.[104] Abuse of this type of information will thwart social justice and should be subject to merely the individual's contractual discretion. It is important that government be urged to take a strong, active stance in preventing, deterring and stopping invasions of privacy, as is encouraged by the dignity-based privacy theory.

2. *The Importance of Context in Privacy Protection: A Concrete-to-Abstract Approach*

It is customary to consider context when making policy and interpreting laws. In criminal law, consideration for the accused's intention or state of mind when committing the act that causes injury or death, such as self-defense, provocation, or diminished capacity, may lead to different criminal liabilities. Similarly, in making privacy protection policies, the relevant conditions underlying an invasion of privacy should be considered, especially in the attempt to keep up with ever-evolving technology. For

103. ANCESTRY.COM, http://trees.ancestry.com/ (last visited Mar. 31, 2015).

104. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 40, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

privacy, context is not easy to construct using a simplified definition. Rather, we may discern the context by deconstructing the different types of privacy conditions into their various elements. By comparing and categorizing these elements and recognizing the harms created, policy makers can determine the logic necessary to decide whether and how to consider such situations with respect for privacy protection in context.

The scope of the context can be extended or reduced, depending on the conditions considered. If societal norms as a whole are regarded as the context, other societies with different norms require different privacy protection policies. For instance, most commentators opine that Europeans take privacy rights more seriously than Americans. A French article describes the U.S. as a place where strangers share their private activities and information, such as salaries, in a way that is difficult to imagine for northern Europeans.[105] Europeans take pride in Article 8 of the European Convention on Human Rights which states that "Everyone has the right to respect for his private and family life, his home and his correspondence." [106] The European Union's new Charter of Fundamental rights[107] protects not only this right of respect for one's private and family life but for personal data as well.[108] On the other hand, the United States Constitution does not contain an abstract privacy context. In the United States, privacy is generally protected through piecemeal legislation and the common law system, which differs from the more systemic protection offered in the EU.

The same society may have different privacy contexts, requiring different protection policies. For instance, Internet technology could constitute a specific context based on its unique status as a globally connected network. In this context, activities using online data and interactions on the Web, as well as the accompanying privacy implications, may need to be treated under different privacy protection policies than those used for offline activities.

If the context is narrowed down to being determined from the perspective that information technologies facilitate the free flow of information, which allows businesses to deliver products and services more effectively and efficiently, other online activities that do not involve significant productivity gains and are operated for other functions, such as online social networks (OSNs)[109] and big data technology,[110] will require

105. Whitman, *supra* note 93, at 1155.

106. Convention for the Protection of Human Rights and Fundamental Freedom, art. 8, para. 1, Jan. 1, 1990, 213 U.N.T.S. 222.

107. Charter of Fundamental Rights of the European Union, arts. 7-8, 2000 O.J. (C364) 1, 10.

108. Whitman, *supra* note 93, at 1157.

109. Heng Xu, Symposium, *Reframing Privacy 2.0 in Online Social Network*, 14 U. PA. J. CONST. L. 1077 *passim* (2012).

110. Cohen, *supra* note 75, at 1924-25 (According to Professor Julie E. Cohen, there are three

different privacy protection policies.

It is not easy to precisely determine the context for privacy considerations, particularly if the context is based on abstract concepts on the value of privacy. Regardless of whether privacy is conceptualized as the right to control one's personal information or to secrecy, a conceptual discussion will mechanically apply the same notion to all situations regardless of the context involved. As a result, it cannot distinguish the different contexts of privacy. For instance, if privacy is defined as a right to be let alone, the doctrine of a reasonable expectation of privacy would be used, and then the private/public dichotomy would be the guiding principle used to determine whether one has a right to privacy protection. However, in the modern world, even in public places, different contexts can arise calling into question whether one has actually exhibited an intention to give up his expectation of privacy. For instance, different privacy considerations should govern when: (1) *John* tags his colleague *Jane* in a photo on Facebook[111] to discuss a shared trip and (2) *John* tags a photo sent to him by *Jane* seeking treatment advice for serious skin problems.

Certain scholars stress the importance of the context for privacy considerations. Professor Solove claimed that a more meaningful approach would be to focus on privacy harms in the context of society because "the value of privacy should be understood in terms of its contribution to society."[112] According to Professor Helen Nissenbaum, privacy should be understood based on the notion of "contextual integrity", stating that privacy "is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones."[113] Professor Nissenbaum proposes specific contexts for information privacy protection and contends that

---

distinct but mutually reinforcing problems of Big Data: 1. Hidden research: "Big Data in the private sector neither pretends nor aspires to transparency; research agendas and data sets are typically kept secret, as are the analytics that underpin them." 2. Underlying ideology: Someone may say that "Big Data is the ultimate expression of a mode of rationality that equates information with truth and more information with more truth, and that denies the possibility that information processing designed simply to identify 'patterns' might be systematically infused with a particular ideology." However, "the denial of ideology is itself an ideological position. Information is never just information: even pattern identification is informed by values about what makes a pattern, and why the pattern in question is worth noting." 3. Constructed subjectivity: "[t]he techniques of Big Data subject individuals to predictive judgments about their preferences, and the process of modulation also shapes and produces those preferences.").

111. FACEBOOK, https://www.facebook.com/ (last visited Mar. 31, 2015).

112. SOLOVE, *supra* note 66, at 173.

113. NISSENBAUM, *supra* note 80, at 231.

"[c]ontext-relative informational norms are characterized by four key parameters: contexts, actors, attributes, and transmission principles."[114]

The context for privacy should be constructed using a bottom-up and concrete-to-abstract approach. An important reason a meaningful approach needs to focus on the privacy threats in a society is primarily that "[p]rivacy is not just freedom from social control but is in fact a socially constructed form of protection."[115] The bottom-up approach to categorization is useful for recognizing the harms created by privacy problems and reminds us that balancing the conflicting interests between an individual and society is important.[116]

More precisely, this approach reminds us that the value of protecting individual privacy emerges from its contribution to society; the value of protecting individual privacy is a social value.[117] Thus, different types of privacy in different social contexts may generate different privacy concerns and social benefit considerations. The harm results from balancing cost and benefit within the social context. For example, the benefits of online advertising are far greater than offline advertising, but the harms to privacy from online advertising are more unpredictable than offline advertising.[118] Therefore, the bottom-up approach appears to be a more meaningful model.

Certain scholars suggest that in the online world, balance is the foremost consideration when contemplating protection of both information privacy and the benefits from the free flow of information.[119] Open information flow is not only essential to self-governance but also aids businesses in delivering the correct products and services to the correct customers, at the correct time, effectively, and at a low cost.[120] Professor Cate asserts that "the open flow of information gives consumers real choice."[121] He opines that we cannot overemphasize individual control over personal data; the notion of online privacy should be more focused on the balancing approach and, in particular, should not ignore the interests of free flowing information.[122]

---

114. *Id*. at 140-47.
115. SOLOVE, *supra* note 66, at 174.
116. *Id*.
117. SOLOVE, *supra* note 74, at 49-50.
118. An empirical statistics of the cost and benefits of online privacy regulation, *see* Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.
119. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 881 (1999).
120. *Id.*
121. *Id.* at 884.
122. *Id.* at 881-84.

3. *An Approach to Determine the Precise Context for Privacy Protection*

In today's world, we are surrounded by Internet services, and enjoy the benefits of online banking, digital media and online shopping, but the online world is not so different from the offline world in terms of substance. Web 2.0 technology[123] significantly helped YouTube and online social networks, such as Facebook and Twitter, change the way people interact with each other. This does not imply, as Professor Nissenbaum mentions, that Internet technology creates a new society. People continue to manage assets, shop, read, watch movies and engage in their social lives offline. The Internet and associated technological advancements serve as new (not replacement) conduit for these various activities.[124] Internet technology's integration into society, forming a social system with an Internet backbone, is described by Professor Nissenbaum as the "socio-technical system" and "the Net."[125] In simple terms, these conduits do not divide the world into two parts, and there are not two different social systems. Rather, these different conduits have been simultaneously adopted into peoples' social lives, forming a single, unified system.

A fundamental solution should be to determine the online context and apply the context to existing privacy policy to tailor standards for online privacy. The interest in conflict with information privacy is the free flow of information. This conflict lies within both offline and online activities. To address online privacy, the context of the online environment must be determined.[126] Consider the example of movie rental. How is renting a DVD different from using online streaming services? For mail, how does physical delivery by the postal service differ from electronic delivery via email services? If the services do not differ, the existing privacy laws should be sufficient, and if the services include certain variations, perhaps slight changes to reflect the slight differences would suffice.[127] For instance, *Jill* sends her personal printed photos to *Jack* as a memento of their romantic trip to Europe, and *Jack* shared the photos with friends visiting his home. Similarly, *Jill* sends her digital photos (using OSNs technology) to *Jack*, and *Jack* uploads the photos to his Facebook. If there is no invasion of privacy in

123. Lisa Veasman, *Piggy Backing on the Web 2.0 Internet: Copyright Liability and Web 2.0 Mashups*, 30 HASTINGS COMM. ENT. L.J. 311, 314 (2008) (Web 2.0 is "a new and improved version from the Web of the past ('Web 1.0'). Web 2.0 is the term commonly used to refer to 'technology that encourages sharing, user input and community.' Specifically, it is a second generation of Web-based services, including blogs, social networking sites, RSS feeds, podcasts, Web APIs, and mashups. Such applications involve the end-user, more than the previous Web 1.0 applications era.").

124. Nissenbaum, *supra* note 46, at 37-38, 43.

125. *See id*. at 37.

126. *See id*. at 38-39.

127. *See id*. at 43.

the former case, should there be different information privacy considerations in the latter case? If there are different privacy considerations, what is the rationale?

In determining the context of privacy, if no social precedents are available, the particular social activity's consequences, purposes, and values may first be identified, and then these results may be used to establish a starting point for the consideration of how to regulate social activity.[128] The United States Supreme Court took this approach in *Riley v. California*, which was decided on June 25th, 2014.[129] The mutual issue in the two cases *People v. Riley*[130] and *United States v. Wurie*[131] was "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[132] The California courts' opinion in *People v. Riley* stated that a modern cell phone does not differ from other physical possessions, and "the Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person" (the search incident to arrest doctrine).[133] In *United States v. Wurie*, the First Circuit held the opposite: "cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests."[134]

The opposing court opinions in these two cases exhibit a critical difference. In the search incident to arrest, should Fourth Amendment protection apply differently when the search object is modern cell phone or other physical possessions, such as cigarette pack, wallet, or purse? After identifying the context for privacy in this case, as well as the purposes, functions, and value associated with modern cell phones, the Supreme Court concluded that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[135] The Court noted several important features of mobile phones that support affording a higher level privacy protection against government search of cell phones. First, a smart phone is not simply a device used to call or receive calls, but rather it functions as a computer, with immense storage capacity, which can also connect to its owner's information stored on the Internet. The privacy concerns associated with the data stored in cell phones differs

128. *See id*. at 44.
129. Riley v. California, 134 S. Ct. 2473 (2014).
130. People v. Riley, No. D059840, 2013 Cal. LEXIS 3714 (Cal.App. 4 Dist. May 1, 2013).
131. United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).
132. Riley v. California, 134 S. Ct. 2473, 2480 (2014).
133. *Id*. at 2481.
134. *Id*. at 2482.
135. *Id*. at 2489.

significantly from other physical records.[136] The digital records in cell phones can reveal nearly every aspect of the cell phone user' life "from the mundane to the intimate."[137] As the Court noted, "A cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record;"[138] "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[139] The Court correctly identified that the privacy concerns associated with a cell phone exceed the device; the digital data stored in the phone requires more extensive privacy protection.

The Court further recognized that no search incident to arrest precedent could have applied to a cell phone found on a person arrested because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[140] No devices or physical possessions offer similarly high levels of information as a modern cell phone and in the past, a pocket-size computer was unimaginable. The next step of the approach is to determine the context for privacy protection in the cell phone search, including the purpose and benefit of allowing the search-incident-to-arrest, as well as the associated impact on the cell phone users' privacy and social activities. Because social precedents are unavailable, it is feasible to first identify the particular social activity's consequences, purposes and values, and then use these results to return to the starting point and consider how to regulate the social activity. The Court explained that the search-incident-to-arrest doctrine can be justified on two grounds: the protection of officer safety and the prevention of destruction of evidence.[141] However, unlike possession of a gun or knife by an arrested person, a cell phone or the data stored in the phone does not implicate safety concerns.[142] As to the second ground to preserve evidence by allowing the government to search a person's cell phone upon arrest, two types of evidence destruction are unique to digital data: remote wiping and data encryption.[143] There are actually other, less privacy-invasive methods that can be adopted instead. For example, police officers can turn the phone off or remove its battery, or "if they are concerned about encryption or other

136. *Id.*
137. *Id.* at 2490.
138. *Id.* at 2489.
139. *Id.*
140. *Id.* at 2488-89.
141. *Id.* at 2484-85.
142. *Id.* at 2485.
143. *Id.* at 2486.

potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves."[144]

Cell phones can store a great deal of evidence on the arrestee, but a considerable amount private information unrelated to the accused offense would also be subject to any search. As the Court noted, modern cell phones can reveal personal data and activities that cannot be found even in a search of the accused's residence:

> [A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[145]

Therefore, allowing cell phones searches in a search-incident-to-arrest will endanger individuals' privacy and inevitably change people's cell phone use habits and affect social activities. Unlike other physical possessions that are allowed in the search-incident-to-arrest without a warrant, the government interest should be heightened to search cell phones in a manner that is less invasive of privacy.[146]

D. *Applying the Context-Relative Approach in the M+App Case*

A recent Taiwanese court decision reveals the importance of identifying the context of privacy when modern technologies are involved. The Taipei District Court handed down a decision on December 24th, 2014 that Taiwan Mobile Co., Ltd. ("Taiwan Mobile"), one of the major cell phone service providers in Taiwan, had violated the Taiwan Personal Data Protection Act (hereinafter "PDPA") by illegally using personal data.[147] The crux of the dispute arises from Taiwan Mobile's communication application software—M+Messenger ("M+App")—which has a unique function to help users identify whether their contacts are using the same telephone service network or not (different minute rate for phone communication would apply). As part of the function, in addition to the phone number of the user's contacts, M+App displays all contacts' telephone service providers next to their phone numbers. The plaintiff was a user of another cell phone

144. *Id*. at 2487.

145. *Id*. at 2491.

146. *Id*. at 2488 ("The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody.").

147. Liu Zuo-Guo v. Taiwan Mobile, No. 103-Bei-Hsiao-Shang-155, at holding (Taipei Dist. Ct. Dec. 24, 2014) (Taiwan).

company—Far EasTone Telecommunications ("FET")—who alleged that Taiwan Mobile's use of his personal data through M+App was illegal and has infringed upon his privacy rights.[148] The dispute is largely centered on whether Taiwan Mobile may legitimately use the data for purposes differing from those given when the data were first collected. The Taipei District Court ruled against Taiwan Mobile, holding that it had exceeded the scope of necessity in using the data in question, and no public interest can be found to justify its use of the data.[149] This decision has aroused a lot of attention in both academic and industry circles concerned with information privacy, with worry that this decision is likely to impede technological advancement.[150]

Back in October 2005, the Taiwan government launched a nationwide Number Portability Centralized Database Administration Center ("NPAC") to enable mobile phone users to retain their mobile telephone numbers when switching from one mobile network operator to another. A total of twelve Taiwanese fixed-line and mobile phone carriers, including Taiwan Mobile and FET, participate the NPAC plan and submitted their respective users' data to the Telecom Technology Center, a state-sponsored enterprise.[151] According to NPAC, their database holds a total of 13 million fixed line and 28 million mobile phone subscribers' phone number data.[152] It was intended that this elimination of a significant barrier to switching would increase competition among the service operators.

When the plaintiff signed up for FET's mobile phone service, he agreed that FET may collect, process and use his data for purpose of providing such phone service. FET is the original collector of his data, who, in turn, uploaded and provided same to NPAC, making the data available to all NPAC participants. The purpose of FET's collection of its users' data was to facilitate provision of phone services. Therefore, FET's forwarding of its users' data to NPAC was within the original purpose of data collection. Taiwan Mobile, as a participant to the NPAC, is also allowed to access and use the personal data, as long as such access and use falls within the scope claimed necessary to fulfill the purpose of collection.

The question is whether it was permissible for Taiwan Mobile to apply the data from NPAC in its M+App application, allowing its users to identify

148. Liu Zuo-Guo v. Taiwan Mobile, No. 103-Bei-Hsiao-1360, at reasoning ¶ i (Taipei Dist. Ct. Oct. 20, 2014) (Taiwan).

149. *See id.* at reasoning ¶ iv.

150. Hong Sheng-Yi (洪聖壹), *M+Messenger Zao Pan Wei Fan Ge Zi Fa Tai Ge Da: Guan Nian Cuo Wu Jiang Shang Su* (M+Messenger遭判違反個資　台哥大：觀念錯誤、將上訴) [*M+Messenger is Ruled by the Court to Have Violated the Personal Data Protection Act; Taiwan Mobile: the Judgment is Incorrect and it will File an Appeal*], DONG SEN XIN WEN YUN (東森新聞雲) [ETTODAY] (Oct. 28, 2014), http://www.ettoday.net/news/20141028/418979.htm.

151. NPAC OVERVIEW, http://www.npac.org.tw/eng/ (last visited Mar. 31, 2015).

152. *See* TELECOM TECHNOLOGY CENTER, http://www.ttc.org.tw/index.php?apps=pgarticle&action=index&cat_id=8 (last visited Mar. 31, 2015).

the phone service carrier of their contacts. Taiwan Mobile's use of the data (potentially allowing users to save or monitor phone costs) is unlikely to be regarded as within the original purpose given for data collection. Therefore, Taiwan Mobile must justify that it is using the data in accordance with an exemption under the PDPA.[153] One of the most relevant exemptions is for data reuse conducted out of a public interest.[154] The PDPA does not entirely prohibit the use of data outside the scope of the purpose of collection, and has certain enumerated exemptions. It is out of the scope of this essay to evaluate the adequacy of these statutory exemptions. Nonetheless, these exemptions are based on a policy believing that the benefit of data free flow in certain situations outweighs the benefit of keeping the data private. Therefore, it is important to identify the privacy harm in the specific social context so that a balance can be made to evaluate whether to protect the value of information free flow or the value of privacy protection. Unfortunately, no such arguments were raised or debated in the court decision.

What makes this case complex is that when the plaintiff agreed to surrender his personal data to FET, he had no expectation that his data would also be used by Taiwan Mobile. This is a perfect example of one of the reasons the notice-and-choice principle has been criticized for being impractical. As technology is developed and advanced to reuse old data for new purposes, there are ever more occasions where this reuse will be done by a third party. Data use is not limited to data controller who obtains data directly from individuals. Since the data reuse occurs after the data is collected and involves an enormous number of people, it is nearly impossible to inform the individual about the possible reuse of data, let alone obtain consent. However, such data reuse could be hugely beneficial for society at large, if it is permitted. This real-life example illustrates how new technology has made the FIPPs impractical and there is an imperative need to modify the traditional notice-and-choice privacy standard.

As mentioned above, it is vital to identify the context for privacy under which the data are being used. Unfortunately, the Taipei District Court did not identify the specific purpose, function, and value associated with M+App. The court's reasoning only focused on a single element—whether

153. Ge Ren Ziliao Baohu Fa (個人資料保護法) [Personal Information Protection Act] (2010) (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (The PDPA is originally in Taiwanese. The PDPA is also called Personal Information Protection Act in some Taiwan law databases when said law is English. There is no official English version or translation of PDPA in Taiwan.).

154. Ge Ren Ziliao Baohu Fa (個人資料保護法) [Personal Information Protection Act], art. 20, ¶ 1, cl. 2, (2010) (Taiwan), http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627.

the data were used outside the scope of the original purpose of collection. It is true that when the data were collected for one purpose, to which the data owner has given his consent, but are used for another purpose, the latter is not within the original expectation of the data owner regarding how the data will be treated. This is forbidden by the notice-and-choice principle declared in Article 20 of the PDPA, which states that uses of such data for other purpose are prohibited.[155] However, there are certain contexts that do not fit within this principle, wherein the use of data is causing no true privacy harms and should be permitted. These are the numerated exceptions given in the same article, which permit the use of data outside the scope of the purpose originally given for data collection.[156] In this case, to properly determine if there was a privacy harm, there are certain elements for the privacy context that have to be considered: whether the information is sensitive data,[157] and whether the data owner has a reasonable expectation of how the data will be used.[158]

If the approach in *Riley v. California* were adopted, the M+App judgment could have a critical difference. Without precedent to rely on, the Taipei District Court should first identify the specific features of the data at issue. In the past, when phone numbers were not portable, different network operators were assigned different ranges of numbers. The first four numbers of a consumers' phone number represented a specific network operator. At that time, no one claimed that such an arrangement presented any privacy issues. Likewise, it is still current practice for telecommunication companies to print their logo and names on the envelope of phone bills sent to consumers, visible in non-private contexts. No concerns were expressed that this data should be considered private or sensitive, or that this practice would infringe on anyone's privacy. If there was no invasion of privacy by disclosure of service provider through bills or the phone number itself, there should be no different information privacy considerations when the same data is disclosed by a modern technology (M+App) and there is no reason to

155. *Id*. at art. 20, ¶ 1.

156. *Id*. at art. 20, ¶ 1 (Under the Article 20, ¶ 1 of the PDPA, personal data may be used only for the purposes for which it was collected except for the followings: 1. It is in accordance with law; 2. It is to promote the public interest; 3. It is to prevent harm to the data subject's life, body, freedom or property; 4. It is to prevent harm to other persons' vital rights and interests; 5. It is necessary for a government agency or a research institution to conduct statistical data analysis or academic research, provided that the data, after being processed by the data provider or disclosed by the data collector, can no longer be connected with a person's identity; and 6. Written consent has been given by the data subject.)

157. Sifa Yuan Dafaguan Jieshi No. 603 (司法院大法官解釋No. 603) [Judicial Yuan Grand Justice Interpretation No. 603], at reasoning ¶ 8 (Sept. 28, 2005) (Taiwan), http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603.

158. Sifa Yuan Dafaguan Jieshi No. 689 (司法院大法官解釋No. 689) [Judicial Yuan Grand Justice Interpretation No. 689], at reasoning ¶ 6 (July 29, 2011) (Taiwan), http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=689.

require a higher level of privacy protection.

Next are the social activity's consequences, purposes and values of the data reuse. The M+App identifies and displays the name of the network operator of the person who is on the contact list of the M+App. Before this information is provided to M+App user, their contact list already contains the name and phone number of the individual concerned. It is difficult, in this context, to comprehend why the name of the data subject's phone company would cause more harm, when the user must already have more sensitive information. The user of M+App is most likely using the App to determine the cost of calls he may place. It is hard to imagine what kind of privacy harm to the data subject would arise from the use of this information.

Lastly, one may argue that individuals have a reasonable expectation to data privacy (i.e. which company is providing phone service to him). However, it is hard to imagine one never talks about which company he is receiving phone service from, much less one who attempts to keep such information confidential. As such, if the data subject has already disclosed the information of the phone company, it is foreseeable that the information will be disclosed again, and no reasonable expectation can be claimed.

By applying the context-based privacy analysis, the data at issue are seem to be neither private nor sensitive, and the data subject lacks a reasonable expectation of privacy. On top of this, the interest in protecting such data is extremely small, and it is also unlikely that the plaintiff will suffer any real damage from others' use of the information. On the contrary, M+App allows its users to make a better and informed decision about their cell phone use. When the two competing interests are evaluated—the benefit to keeping the information private against the benefit to disclosing it, allowing Taiwan Mobile to use the information under the "facilitation of public interest" exemption in Article 20 of the PDPA seems like the more reasonable conclusion.

IV. CONCLUSIONS

Emerging technologies have made privacy invasions more difficult to detect and prevent. Businesses attempt to keep their trade secrets as long as possible to retain competitiveness, and it is unlikely to deter secret data collection and use beforehand even if revealed. As a result, an affected person has little recourse against a potential invasion of privacy. Because the harm to privacy interacts with a society's norms, and data mining activities by powerful technology firms are unstoppable and far-reaching, information privacy should not be narrowly viewed as the individual's right to protect his

or her privacy. The enormous power of giant corporations in data mining, exceeding the power of most nations, has made privacy protection no longer a matter which can be dealt with solely through individual exercise over one's own privacy. When individuals cannot detect, deter, stop or escape from privacy invasions made by giant transnational corporations whose power exceeds the control of any individual, it is imperative that the government shoulder the responsibility for protecting its citizens' information privacy.

The construction of a modified information privacy theory, as this essay has proposed, should incorporate the social value of privacy, with human dignity as the core value. As opposed to human dignity, a freedom-oriented theory emphasizes the individual's outward activities. It is true that one's control over his data relates to inner personal development, but the consequences of privacy protection mostly relate to the power to resist invasion from the outside. The value of privacy referred to here is not just an individual's subjective imagination of value. It refers to all individuals in the society. Therefore, not only subjective personal value must be noted, but, most importantly, objective standards such as democracy must also be integrated in order to improve privacy theories. Such enhanced privacy notions are not limited to passively resisting privacy infringement. They empower the government to take active measures to protect the objective social value of privacy. For instance, the government may establish regulations prohibiting anti-race activities which abuse individuals' genetic data, due to the anti-personal development effect that can be brought by such activities. Moreover, a privacy protection regime supported by government enforcement can strengthen privacy protection measures for the prevention of future privacy infringement.

Additionally, the social value concept also echoes the proposal that the value of privacy shall be reviewed under the relevant social context on a case-by-case basis. A privacy theory that incorporates social value claims that the privacy is to protect the individual privacy in the social context, not one in which the individual is isolated from society. Therefore, to determine the privacy harm, it is not only the privacy impact on the individual that has to be considered. It is also equally important to take into consideration the interest to the social value of privacy.

Identifying the social context is vital to resolving the conflicts between the interests of preserving the secrecy of personal data and its use. In determining the context of privacy, if no social precedents are available, the particular social activity's consequences, purposes, and values may first be identified, and these results then used to trace back to a starting point for consideration of how to regulate a given social activity.

REFERENCES

Allen, A. L. (2011). *Unpopular Privacy: What Must We Hide?*. Oxford: New York, N.Y.: Oxford University Press.

Ancestry.com. http://trees.ancestry.com/.

Anonymous (1999). Privacy, Technology, and the California "Anti-Paparazzi" Statute. *Harvard Law Review*, *112*, 1367-1384.

Anonymous (2013, September 3). Privacy and Big Data: Making Ends Meet, *Stanford Law Review Online*, Retrieved from http://www.stanfordlawreview.org/online/privacy-and-big-data.

Bellia, P. L., Berman, P. S., Frischmann, B. & Post, D. G. (2010). *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age* (4th ed.). St. Paul, MN: Thomson/West.

Bennett, C. J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, Mass: MIT Press.

Cate, F. H. (1999). Principles of Internet Privacy. *Connecticut Law Review.*, *32*, 877-896.

Cate, F. H. (2001). *Privacy in Perspective*. Washington, D.C.: AEI Press.

Cate, F. H. & Cate, B. E. (2012). The Supreme Court and Information Privacy. *International Data Privacy Law, 2*(4), 255-267. Retrieved from http://idpl.oxfordjournals.org/content/2/4/255.full.pdf+html.

Charter of Fundamental Rights of the European Union, arts. 7-8, 2000 O.J. (C364) 1.

Cohen, J. E. (2013). What Privacy is For. *Harvard Law Rev*iew, *126*, 1904-1933.

Convention for the Protection of Human Rights and Fundamental Freedom, art. 8, para. 1, 213 U.N.T.S. 221.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. 1995 O.J. (L 281) 31. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

Facebook. https://www.facebook.com/.

Federal Trade Commission. (2009, February). *Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology*. Retrieved from

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

Federal Trade Commission. (2012, March). *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*. Retrieved from http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Federal Trade Commission. (2013, February). *Mobile Privacy Disclosures*: *Building Trust through Transparency*. Retrieved from http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

Ge Ren Ziliao Baohu Fa (個人資料保護法) [Personal Information Protection Act] (2010) (Taiwan). Retrieved from http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627.

Gellman, R. & Dixon, P. (2011). *Online Privacy: A Reference Handbook*. Santa Barbara, Calif: ABC-CLIO.

Gettys, T. (2013, October 15). Snack Maker Mondelēz Readying 'Smart Shelves' to Track and Influence Shopper Behavior, *Raw Story*. Retrieved from http://www.rawstory.com/rs/2013/10/15/snack-maker-mondelez-readying-smart-shelves-to-track-and-influence-shopper-behavior/.

Goldfarb, A. & Tucker, C. E. (2010, August 5). Privacy Regulation and Online Advertising. *Management Science, 57*(1), 57-71. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

Hartzog, W. & Selinger, E. (2013). Big Data in Small Hands. *Stanford Law Review Online*, *66*, 81-88.

Hartzog, W. & Stutzman, F. (2013). The Case for Online Obscurity. *California Law Review*, *101*, 1-50.

Hong Sheng-Yi (洪聖壹) (2014, October 28). M+Messenger Zao Pan Wei Fan Ge Zi Fa Tai Ge Da: Guan Nian Cuo Wu Jiang Shang Su (M+Messenger遭判違反個資　台哥大：觀念錯誤、將上訴) [M+Messenger is Ruled by the Court to Have Violated the Personal Data Protection Act; Taiwan Mobile: the Judgment is Incorrect and it will File an Appeal]. *Dong Sen Xin Wen Yun (東森新聞雲)* [*ETtoday*]. Retrieved from http://www.ettoday.net/news/20141028/418979.htm.

Katz v. United States, 389 U.S. 347 (1967).

Kobelev, O. (2004). Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance through the Use of Radio Frequency Identification Technology and the Need for Legislative Response. *North Carolina Journal of Law & Technology*, *6*, 325-342.

Leonard, A. (2013, February). How Netflix is Turning Viewers into Puppets: "House of Cards" Gives Viewers Exactly what Big Data Says We Want. This won't End Well. *Salon.com*. Retrieved from http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/.

Lin Zhi Qing [林志青] (2014, January 11). Yuan Tong Laing Ci Baojia You Ge Zi Fa Da Zhu Xing Shi Ju Chi Xu Xie Tiao (遠通2次報價憂個資法 打住　刑事局持續協調) [PDPA Concerns Halted FE-Toll Two Offers to CIB, Negotiation Continues]. *Ping Guo Ri Bao (蘋果日報)* [*Apple Daily*]. Retrieved from http://www.appledaily.com.tw/realtimenews/article/new/20140111/324266/.

LinkedIn. Your Privacy Matters: 1.4. Address Book and Other Services that Sync with LinkedIn. Retrieved from http://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv.

LinkedIn. Retrieved from https://www.linkedin.com/.

Liu Zuo-Guo v. Taiwan Mobile, No. 103-Bei-Hsiao-1360 (Taipei Dist. Ct. Oct. 20, 2014).

Liu Zuo-Guo v. Taiwan Mobile, No. 103-Bei-Hsiao-Shang-155 (Taipei Dist. Ct. Dec. 24, 2014).

Mayer-Schönberger, Viktor & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.

Mead, G. H. (1964). *On Social Psychology.* Chicago: University of Chicago Press.

Microsoft News Center (2013, February 11). The Big Bang: How the Big Data Explosion is Changing the World. Retrieved from https://www.microsoft.com/en-us/news/features/2013/feb13/02-11bigdata.aspx.

NPAC Overview. Retrieved from http://www.npac.org.tw/eng/.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif.: Stanford Law Books.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32-48.

Ohm, P. (2013). The Underwhelming Benefits of Big Data. *University of*

Pennsylvania Law Review Online, *161*, 339-346.

Olmstead v. United States, 277 U.S. 438 (1928).

People v. Riley, No. D059840, 2013 Cal. LEXIS 3714 (Cal.App. 4 Dist. May 1, 2013).

Person, A. N. (2010). Behavioral Advertisement Regulation: How the Negative Perception of Deep Packet Inspection Technology May be Limiting the Online Experience. *Federal Communications Law Journal*, *62*, 435-464.

Peterson, A. (2014, February 20). We are Drowning in a Sea of Data. And Data Insecurity, *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/20/we-are-drowning-in-a-sea-of-data-and-data-insecurity/.

Posner, R. A. (2008). Privacy, Surveillance, and Law. *University of Chicago Law Review*, *75*, 245-260.

Post, R. C. (1989). The Social Foundations of Privacy: Community and Self in the Common Law Tort. *California Law Review*, *77*, 957-1010.

Post, R. C. (2000). Three Concepts of Privacy. *Georgetown Law Journal*, *89*, 2087-2098.

President's Council of Advisors on Science and Technology. (2014, May). *Big Data and Privacy: A Technological Perspective*. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Rachels, J. (1975). Why Privacy is Important. *Philosophy & Public Affairs*, *4*(4), 323-333. Retrieved from http://www2.warwick.ac.uk/fac/soc/philosophy/undergraduate/modules/ph212/2014-15/rachels_james_-_why_privacy_is_important.pdf.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press.

Richards, N. M. (2008). Intellectual Privacy. *Texas Law Review*, *87*, 387-445.

Riley v. California, 134 S. Ct. 2473 (2014).

Rosen, J. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.

Schwartz, P. M. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review*, *52*, 1607-1702.

Secretary's Advisory Committee on Automated Personal Data Systems. (1973). *Records, Computers and the Rights of Citizens*. Retrieved from http://www.justice.gov/opcl/docs/rec-com-rights.pdf.

Sifa Yuan Dafaguan Jieshi No. 603 (司法院大法官解釋No. 603) [Judicial Yuan Grand Justice Interpretation No. 603] (Taiwan), (2005, September 28). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603.

Sifa Yuan Dafaguan Jieshi No. 689 (司法院大法官解釋No. 689) [Judicial Yuan Grand Justice Interpretation No. 689] (Taiwan), (2011, July 29). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=689.

Simitis, S. (2010). Privacy: An Endless Debate. *California Law Review*, *98*, 1989-2006.

Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, Mass.: Harvard University Press.

Solove, D. J. (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven [Conn.]: Yale University Press.

Solove, D. J. & Schwartz, P. M. (2011). *Information Privacy Law* (4th ed.). New York: Wolters Kluwer Law & Business.

Solove, D. J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*, 1880-1903.

Sullivan, G. (2014, June 30). Facebook Responds to Criticism of its Experiment on Users. *The Washington Post*. Retrieved from http://www.washingtonpost.com/news/morning-mix/wp/2014/06/30/facebook-responds-to-criticism-of-study-that-manipulated-users-news-feeds/.

Telecom Technology Center. Retrieved from http://www.ttc.org.tw/index.php?apps=pgarticle&action=index&cat_id=8.

Tsukayama, H. (2014, April 15). Google Explains Itself after E-mail Scanning Backlash. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/15/google-explains-itself-after-e-mail-scanning-backlash/.

United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).

Veasman, L. (2008). Piggy Backing on the Web 2.0 Internet: Copyright Liability and Web 2.0 Mashups. *Hastings Communications & Entertainment Law Journal*, *30*, 311-338.

Vogel, P. S. (2013, November 8). Is LinkedIn Being Sued for Doing Just

What It Says It Will Do?. *E-Commerce Times*. Retrieved from http://www.ecommercetimes.com/story/79383.html.

Warren, S. D. & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220.

White House (2012). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promotion Innovation in the Global Digital Economy*. Retrieved from http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Whitman, J. Q. (2003). The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*, *113*, 1151-1221.

Xu, H. (2012). Reframing Privacy 2.0 in Online Social Network. *University of Pennsylvania Journal of Constitutional Law*, *14*, 1077-1102.

新興科技下之資訊隱私：社會價值取向之資訊隱私理論

張 陳 弘

摘 要

新興資訊科技的發展所形成個資蒐集、使用的難以察覺性與難以預測性，嚴重地衝擊著現行資訊隱私保護制度設計的基本想法：透過賦予個資主體自主決定權以保護資訊隱私。蓋個資主體難以察覺個資的被使用，因而無從主張資訊隱私保障，使得強調個人控制權的資訊隱私保護制度，愈加顯得力有未逮。然而，一味貫徹個資主體的自主決定權，亦將妨礙資訊自由流通所可能帶來之公共利益。再加上因資訊科技的不斷革新，使得仰賴個資自由流通所能獲取的公共利益愈趨多樣化，在質、量上皆不斷增加，公共利益追求的評價逐漸凌駕於個人資訊隱私權保護利益之上。因此，過度偏重個資主體自主決定的個人利益之主張，將使得資訊隱私權在面對公共利益追求的壓迫下，處於弱勢地位。此外，過度強調個人價值的隱私主張，亦將使得國家甚難取得著力點介入私人間事務。資訊隱私理論及保護制度的修正方向，應朝向改善上述缺失處著手。其中最重要的關鍵之處乃在於導入資訊隱私的社會價值面向，以提供政府出面承擔起個資主體無法靠一己之力保護隱私部分的理論基礎，並提供資訊隱私與公共利益抗衡的力量。

關鍵詞： 資訊隱私、隱私權、巨量資料、大數據、告知後同意、公平資訊實踐原則