MARKET PHILOSOPHY AND INFORMATION PRIVACY

YONG JIN PARK

Abstract

This article examines U.S. policy shaping of personal information flow in its historical trajectory. The analysis newly draws on the notion of the marketplace ideal in privacy debate and analyses a regulatory continuum that an online information protection regime is the product of active formulation of a policy principle. Proxy regulation that attributes the function of privacy protection to discrete commercial domains is analysed in analogy with the diversity principle of broadcasting. Alternative Internet policy models are discussed beyond the oversimplified dichotomy between market and government. In a critique of the Federal Trade Commission's latest proposal of "Do Not Track List," a thesis is advanced to encourage a simplified user interface with a forceful measure that can intervene in the marketplace.

Yong Jin Park is Assistant Professor in School of Communications, Howard University, Washington D.C.; e-mail: yongjinp@hotmail.com.

Introduction

Imagine, for a moment, a very young medium called the Internet. The faith of the virtual city, in which the civic, political, and commercial lives of citizens converge into digital platforms, is about to be shaped. Policymakers are concerned about how information flow should be governed; how citizens exercise their rights to privacy control; and how private organisations can access, retain, and appropriate user data. The year is 1995; the government agency is the Federal Trade Commission (FTC); and the tension is on the function of the marketplace, that is, the extent to which the government is to assume a role in determining the future of information flow in virtual environments.

The purpose of this article is to historically and critically examine the underlying information condition for marketplace institutions and individual users in the Internet. The central question is how the government policy principle helps determine the function of institutions and users in personal information control. In other words, this article aims to ask what the current state and the role of U.S. policy are in conditioning privacy control and to deconstruct the principle of marketplace rationale in its historical trajectory.

Fair Information Practices (FIPs) remain a focal point of analysis, i.e., how the FTC FIPs have evolved into the current regulatory stance in the Internet. Over the decades, the FTC has reinstated its stance in resorting to the marketplace principle online. In the proposed privacy principles for behavioural advertising, the FTC stated:

> *The [self-regulatory] principles reflect FTC staff's recognition of potential benefits provided by online behavioural advertising and the need to maintain vigorous competition in the area. At this time, Commission believes that self-regulation may be the preferable approach for this dynamic marketplace because it affords the flexibility that is needed as business models continue to evolve* (FTC 2008, 13).

Most recently, in 2010, the FTC proposed an online "Do Not Track List," however, the Commission left its implementation and enforcement to online commercial entities. What the Commission takes for grant is the validity of marketplace rationale. Perhaps more important is a consistent policy framework with no or limited shift of orientation. This study will step back to reexamine the construction of Internet privacy policy from a critical analytic perspective because it helps reformulate policy objectives in concrete terms.

Overview

This article has the following structure. First, a theoretical framework of U.S. communication policy is presented. Second, a brief U.S. privacy policy history proceeds in two stages: (1) the constitutional foundation period and (2) the computer era from the 1970s to the 1980s. Third, the FTC policy of the Internet era is dissected in concrete terms. Finally, policy recommendations will be offered for formulating concrete alternatives to the current regime that is in place online.

The organisational framework of this article is not to indicate the causal direction from new technology to policy. Rather, it is to note the reverse directionality, from policy to technology, with the critical role of policy in shaping new technology in

each of three stages. In sum, the aim is to provide a critical account of information privacy policy in historical background. Policy history, in this sense, indicates more than the aggregate of facts and events pertinent to privacy – it is a review of the root of U.S. policy and its ensuing impact before making concrete recommendations to the FTC in its formulation of online policy.

The analysis draws on the combination of historical and policy insights. For this, a comprehensive data archive was constructed. Firsthand sources came from two policy origins: (1) the government, mainly the FTC, and (2) the civic sector. The goal was to collect multifaceted resources in the reconstruction of existing policy conditions. Ultimately, this reflects how the current regime in the Internet has evolved in particular ways.

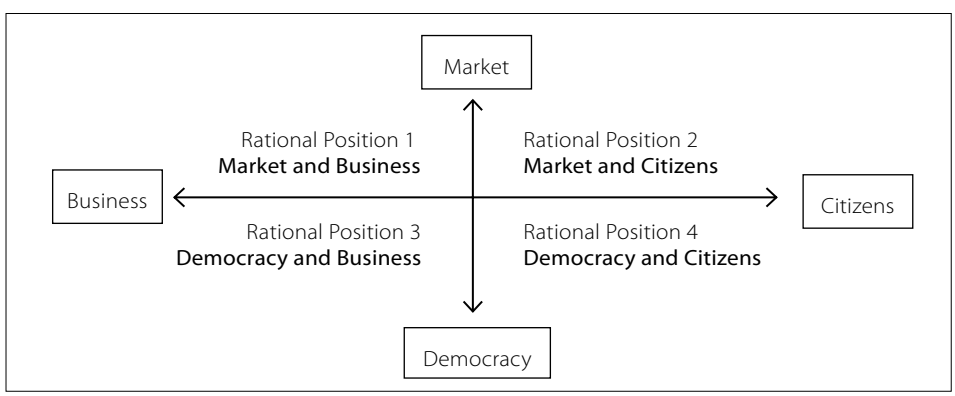
Overall, this article contributes to bringing privacy policy discussion to a concrete level in which users and institutions play out their parts under the policy assumption. Theoretically, this study aims to newly dissect the rationale that underlies Internet privacy policy from a perspective of a prominent metaphor of the marketplace of ideas.

Framework of the Marketplace Ideal

The marketplace of ideas is the most prominent metaphor in U.S. communication policy (Napoli 2000). The notion indicates more than rhetoric, but it serves as a fundamental basis for the operation of the policy principle in concrete terms. The idea goes back to John Locke[1] in the seventeenth century when he pointed out that "the attainment of the truth is best achieved through the free uninhibited exchanges of ideas/information in the marketplace" (Napoli 2000, 105). Under this viewpoint, government regulation is to be left to a minimum to keep the full functionality of the marketplace (Dalhgren 2001; Horwitz 2005). In an affirmative sense, the policy is a hindrance when the self-functioning marketplace best guarantees the sharing of diverse viewpoints, and ultimately the truth.

The two aspects of this ideal are the market and the democracy. Also we can regard the two entities in their interplay: party 1 (e.g., source, sender, or business) and party 2 (e.g., exposure, receiver, or citizens) (see Figure 1). This gives us a matrix in which each entity is positioned to practice their rational interests in four dimensions.

Figure 1: Matrix of Marketplace Ideal



One of the most important aspects of this principle is that entities involved in the free exchange of information are reduced to the relationship between two actors in perfect power symmetry. Furthermore, other political or social objectives are assumed to operate in functional equivalence to the economic rationale in the marketplace. The principle speaks to not only the faith in political liberty, but also the marketplace integrity that functions for other social goals, with no mediating force in between (Streeter 1996).

In most U.S. communication policies, policy inaction is the direct consequence of this philosophical root. Policymakers have recognised the power with which rational citizens freely choose a wide range of options, fully informed in the marketplace. Conversely, the market institutions are assumed or even theorised to perform certain standards of action fulfilling democratic responsibilities in a self-governing society.

Here the policy inaction does not mean "no action at all." Rather, it indicates the laissez-faire model (Neuman et al. 1997) in which the self-regulatory market mechanism is promoted on policy grounds. For example, marketplace ideas are often factored into binding Federal Communications Commission (FCC) policy guidelines such as "public interest, convenience, and necessity" (Napoli 2000). It is critical that the function of the marketplace is assumed to be perfectly rational in translating such policy guidelines. The metaphor, in this sense, has a tangible consequence – the assumption that the marketplace is best regulated at the hands of the parties at stake.

Drawing on the notion of the marketplace idea to privacy debate, two qualifications are in order. First, the interaction between the two entities is a simplified one. The marketplace is more complex now than in the seventeenth century and involves a wide array of groups, such as websites, credit card companies, Internet service providers (ISPs), and so forth. Second, the distinction between privacy of content and privacy-related transactional information (McManus 1990) increasingly blurs on the Internet, and it is not plausible to exclude one for the sake of the other when focusing on privacy control conditions. Subsequently, the metaphor as follows is to operationalise privacy debate in analytical parsimony.

U.S. Privacy Policy History

Constitutional Foundation of Privacy Control

The U.S. privacy policy is founded on the liberal market model in the metaphorical regulatory continuum (Solove 2001; Venturelli 2002). That is, privacy regulation in industry is self-regulated, characterised by both non-commercial obligation and no burdensome public-interest obligation. Its philosophical origin is aligned with the marketplace ideal. In fact, the U.S. Constitution per se does not explicitly state the right to privacy. While the Fourth Amendment is construed as a broad legal basis, policy intervention has always been reactionary only when the market between the involved parties fails to function.

This point is significant because most communication policy has been understood primarily in the context of the First Amendment. For example, in FCC policy, the objective of media diversity has been understood to be achievable as a function of commercial freedom in the marketplace as interpreted in the *Associated Press v.*

United States in 1945. Here the foundation goes to the Fourth Amendment as this is further operationalised in the consistent U.S. privacy policy stance imbued in the marketplace ideal.

The minimal privacy protection position is best illustrated in three landmark cases. The case of *Olmstead v. United States* (which involved the telephone – the new technology of the day) shows limited interpretation by the Court of constitutional privacy rights. In this 1928 decision, the Supreme Court ruled that the Fourth Amendment does not apply to telephone wiretapping. Chief Justice Taft, in the majority opinion, noted:

> *The Fourth Amendment should be construed liberally; but it is submitted that by no liberality of construction can be a conversation passing over a telephone wire become a "house," no more can it become a "person," "paper," or an "effect"* (Taft 1928, 451).

In 1970, *Katz v. United States* restored the protection of individual rights to a certain extent. The Court ruled that wiretapping constituted a search under the Fourth Amendment. However, the majority opinion also made it clear that the Fourth Amendment protects only against certain kinds of governmental intrusion in highly limited contexts, refusing to establish its constitutional ground for general rights to privacy. Even this limited position was weakened by the 1976 decision in *Miller v. United States*, in which the Supreme Court upheld that citizens do not have a reasonable expectation to privacy when communication can be restored in third parties; thus, they cannot be held accountable.

The Miller decision came just before the computer era of the 1980s. The date remains critical because this set the reassuring regulatory tone for commercial telephone operators in ensuing digital networks. The significance is that personal information condition, with the absence of explicit regulatory principle, was reduced to the matter of individual discretion in the uses of commercial networks – subsequently, in a minimised role for the state to play in free information exchange.

It is important to recognise that the Fourth Amendment principle reflects an enriched respectful tradition of citizens' rights that set the United States apart from the rest of the world (Rotenberg 2001). Yet a critical point is that the de facto protection, from the very early forms of communication technology, has been compromised through case and statuary laws. Further, the consistent reluctance by the Court in establishing constitutional protection became a broad interpretive frame. The early cases established the foundation on which the rights to privacy are left to private parties at hand. To rephrase, it is the reluctance, in line with liberal principle, from which policy intervention is interpreted as the last resort.

The Era of Computerisation from the 1970s to the 1980s

The absence of an explicit regulatory framework governing the protection of personal information flow continued from the 1970s to the 1980s. The advent of information technology opened up opportunities in which to reshape policy initiatives. However, a patchwork of policy was constructed within the existing regulatory legacy instead of a new cohesive policy framework that could better address increased infringement on personal privacy.

Three main factors characterise the formulation of U.S. privacy policies in this period. First, there was no unified formal policy created at the federal level. Second,

such absence was filled with a multitude of state-level protections in complex variations of scope and implementation. Third, this complicated policy configuration exacerbated the problem as sector-by-sector piecemeal solutions were introduced, which further varied depending on the technological platforms (Park 2009).

This is not to say that there was a complete regulatory ignorance of privacy rights. Most notably, the 1974 Privacy Act was enacted to restrict the access by federal agents to records of individual citizens. The U.S. government also pushed for the Cable Communications Policy Act, the first of this kind in network service, opening up the door for further legislation, such as the 1988 Video Privacy Protection Act that protects information regarding video rental (Flaherty 1989). Furthermore, through the 1970 Fair Credit Reporting Act, the U.S. government formulated the policies that protect the privacy of citizens in commercial transactions. In this period, the inception of fair information practice (FIP) principles is particularly noteworthy. The originator of the FIP principles was the U.S. Department of Health, Education, and Welfare in 1973 in response to the increased use of automated data records. It was this earlier version of the FIP principles that provided the rationale behind the 1980 Organization for Economic Cooperation and Development (OECD) guidelines. Thus it is accurate to say that active U.S. policy formulation created a core set of guidelines for private-sector privacy protection earlier than the rest of the world (Bellman et al. 2004).

Nevertheless, the two contexts qualify the active policy formulation in this era. First, the 1974 Privacy Act concerned government data collection in the public sector. That is, the 1974 Privacy Act created a significant and vast legal loophole in which the private sector was insulated from burdensome public obligations for the use, collection, and retention of information regarding citizens in public spheres. This hailed a completely different regulatory model from which the function of the mass media industry at its minimum presupposes the fulfilment of certain standards of public-interest obligations in use of spectrum and access to the general public (see Streeter 1996).

Second, the construction of sector-by-sector patchworks indicates the creation of the environment in which much of the scope and implementation of data protection is up to the discretion of separate industry norms, under varied government sanctions. Citizens are assumed to exercise discretion and control in direct negotiation with individual sectors and scattered regulatory protections. This is a critical point because the notion of the marketplace ideal, in which the private sectors and individual citizens are under one-to-one symmetrical contacts, is now sealed in a myriad of statuary grounds for personal information protection.

It is not difficult to document a clear orientation entrenched in this era leading up to the Internet age. In discrete sectors, the patchwork of policy, instead of a rigid strict government standard, was intended to function as a flexible open frame in which information would flow more freely (Langenderfer and Cook 2004). Conversely, the multitude of policies and the segmented marketplace formed a complex environment for citizens to function in. The key to understanding privacy policy and regulation in the United States is to understand the fundamentally fragmented nature of its making, in light of the Constitutional provisions regarding federal and state powers on one hand and the division of power and checks and balances on

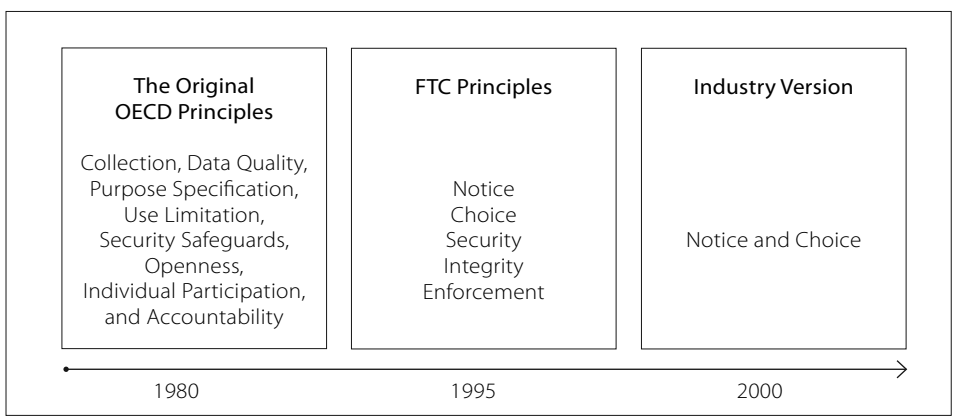
the other. In sum, the 1970s and 1980s marked the translation of market-oriented regulatory legacy into tangible policy forms, providing offline statutory grounds for the online regime to function.

The Internet Era

In the 1990s, with the advent of the Internet, the fundamental principles of the FIPs came to the forefront of privacy policy in the United States. The pattern of industry self-regulation should be understood in the administrative context of the FTC, of which the main objective was to promote commerce in business interests. Furthermore, it is important to consider the time period of 1990s in which the FTC took over the jurisdiction of online commerce with the launch of the first commercial search site – Yahoo! The FTC (and the Clinton administration in the mid-1990s) had a clear policy incentive to promote free information flow for the online industry, which was in its infancy.

The most noticeable change resides in, not the adoption of FIP principles, but the acceleration of the marketplace principle in its online application. In fact, the FTC adoption of the FIP principles further reinforced the market-friendly policy stance. The original FIP principles with eight items were reduced to two items (Notice and Choice) (see Figure 2), and technically, they adhered to the fundamental guidelines from the OECD. Also, no clear benchmark was set for the voluntary observance of Notice and Choice. Most of all, in the faith in the marketplace integrity, no enforcement mechanism was in place online. The relatively active policy formulation of the 1970s and 1980s, even within such limited statutory contexts, ground to a halt and succumbed to the entire discretion of industry sectors in the online marketplace.

Figure 2: The Evolution of Fair Information Principles



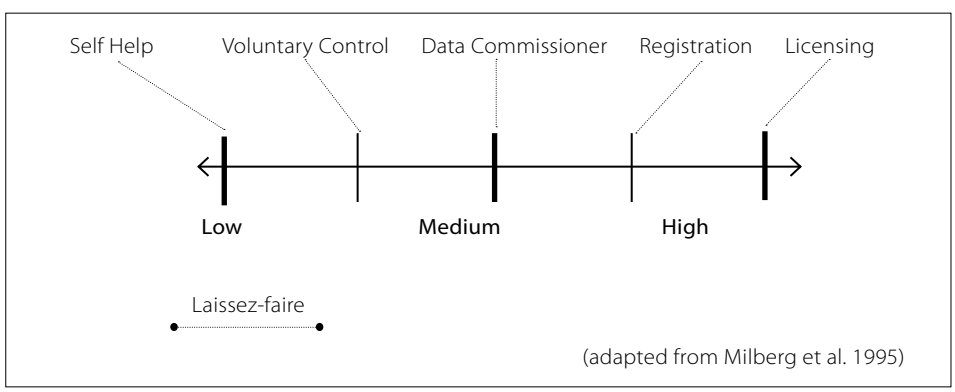
It is crucial to recognise the shift to the much-relaxed FIP standard in favour of online commercial entities. Over the decades, the FTC, in the provision of the operating principle, made it clear that its jurisdiction was to function for commercial interests in the new medium (e.g., in the 1997 Clinton-Gore initiative). In 1999, the FTC in its report to the House commerce subcommittee on Telecom, Trade, and Consumer Protection affirmed that

> *[self-regulation is] the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology. … The Commission believes that legislation to address online privacy is not appropriate at this time* (FTC 1999, section II).

This position was embraced again and again in each of the FTC reviews in 1998, 1999, 2000, and most recently, 2007 (in its review of behavioural target advertising; EPIC 2007). In the first adoption of the FIP principles in 1995, the FTC refused to include a full set of the guidelines, while much of its policy position was grounded in the encouragement of voluntary adoption of the FIP principles. With no federal oversight agencies as of 2010, however, the industry version of Notice and Choice remains as the only working principles. Two types of enforcement mechanisms are in place under this principle: (1) the voluntary seal certification program (e.g., TRUSTe, BBBonline) and (2) the Platform for Privacy Preferences Project (P3P) of the World Wide Web Consortium (W3C), in which websites are voluntarily expected to provide the elements of the FIP principles through their memberships.

Prior to the proposal of "Do Not Track List" in 2010, the only period in which the FTC seriously considered amending the industrial self-regulatory codes (in a vote of 3 to 4 of the FTC commissioners) was 2000. Nevertheless, the introduction of new legislations was overturned in 2001 in favour of existing policy guidelines under a new FTC chair. It should be understood that this consistent emphasis on the privileges of parties at hand is the continuation of a hands-off position in liberal market principle, in a more dramatic shift of power to private entities (cf. Agre and Rotenberg 1997). The position of the minimal "voluntary control" regime introduced in 1995, reinstated in 2001, and in place up to 2007, remains as the operating principle in online consumer protection (FTC 2002) (Figure 3).

Figure 3: Level of Policy Involvement in Privacy Protection



The Inertia of Market Philosophy

A critical point to debunk is the somewhat naïve notion that the self-regulatory regime is a product of policy inaction. Rather, the online information regime is a regulatory construct that did not evolve in vacuum. It is a product of active formulation within the marketplace policy ecology that is best oriented toward the minimalist approach of non-public obligations. Note that aligned with the liberal

market model, the policy formulation in the earlier two stages was characterised by the market-based minimalist approach, that is, a laissez-faire approach to information and privacy control. With the FTC at the forefront in 1995, this accelerated with the following:

(1) The full scope of the FIP principles was compromised.
(2) There was no clear benchmark for adequate data protection in the voluntary FIPs observance.
(3) No enforcement mechanism was in place.

In short, the hyperactive policy continuum of the regulatory construct of marketplace rationale characterises the current privacy policy regime in online spheres, as manifested in the FTC adoption of the FIP principles in the 1990s.

In this policy continuum, then, questions naturally arise: What is the viable future for the users to exercise control? How are we to understand the function of the underlying regulatory condition of privacy control? And for shaping the information flow in digital spheres, how should the FTC proceed from the marketplace legacy, and with what imperatives?

To answer, it is important to cautiously dissect the posited function of institutions and users in interplay. The operational assumption of information privacy protection is linear. First, online market institutions are willing to embed the FIP core principle in voluntary compliance. Second, the users are recognised as able agents fully capable of data control according to personal needs or concerns (Marx 2007). The net result is complete faith in the integrity of marketplace incentive – the provision of privacy control, on one hand, with the most optimistic view of capable users, on the other.

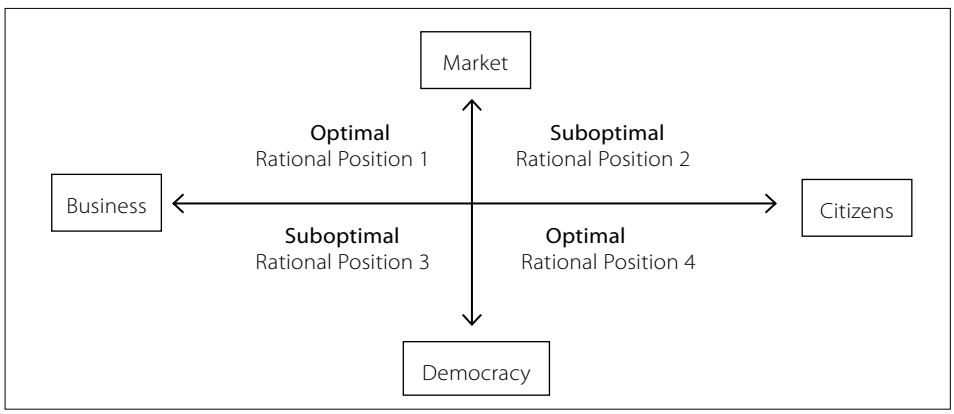
An analogy would be the policy principle of traditional broadcasting diversity. Under the FCC principle, it is in fact assumed that structural regulation over media consolidation and/or ownership on the side of production (i.e., source diversity) would guarantee viewing diversity (i.e., exposure diversity) on the side of consumption (Horwitz 2005, Napoli 2000). In this vein, the current FTC regime is also a form of proxy regulation over the structure alone. That is, under the provision of the guidelines for the industry, if the proper organisational behaviour follows, users' information protection will be achieved. In other words, the current policy attributes the full function of the marketplace ideal to the functional power of commercial institutions alone.

In a practical sense, if the FIP principles function as a de juror standard, a de facto policy is the proxy regulation that governs only the party of the information provision. The absence of users in the policy picture indicates the operational principle in which the adequate structural provision alone, as defined by the industry standard, satisfies the fulfilment of the marketplace ideal. This is not to bluntly question the rationale of marketplace ideal per se. What is being questioned is the validity of self-regulatory measures with no due mechanism. Under the current FTC regime, the rationale is to set up the condition, as operationalised in the proxy (FIP principles) regulation, in which entities are to function. The irony is that the FTC stance is grounded on the absence of a valid policy measure that sustains the very function of the entities.

In 2001, the Patriot Act vastly expanded the government power of data surveillance, and is pending extension as of 2011. The debate over the scope of ad-

ministrative snooping power (and its due process) is to be distinguished from the concern on the regulatory model of privacy control and protection in commercial transactions. However, critics worry about the encroachment of government data tracking in the domain of business. This broader post September 11, 2001, context offers even more serious vulnerability to the posited self-regulatory conditions for information protection on the Internet. The problem of the idealised marketplace is that the market functions to the optimal interest of business (dimension 1), whereas democracy, when it best positions, functions to maintain interests of citizens' rights (dimension 4). The policy imperative is to correct this potential imbalance between market and democracy in rational positioning.

Figure 4: Functional Dimensions of Marketplace Ideal



Possible Remedies

Possible alternatives can be varied. Yet the dramatic shift of FTC policy orientation toward concrete grounds is paramount to move beyond the oversimplified dichotomy between market and government. In other words, the marketplace metaphor embedded in privacy policies needs to be substantiated with policy instruments that help sustain the function of users and online institutions.

The alternative policy model should be equipped with effective standards covering two strata. The first stratum covers online market-institutions, with a focus on the interface design of each site that enables the actual function of the FIP principles so that users can rely on a site interface to make conscious decisions to reject or accept information collection and use. The second stratum covers users. Here policymakers should concentrate on how to build competent citizenry in which users are ably equipped to exercise control of their interests. Each stratum could restore functional power symmetry between entities (Dana and Gandy 2002) by empowering users through interface and competency.

Another ingredient in effective standards for market-institutions is privacy zoning. The FTC must achieve regulatory standardisation through benchmark interface-design requirements that vary according to website zones or types. The current FTC recognises no difference among websites, for example, financial, family oriented, or regular e-commerce sites. Privacy zoning should *mandate* the

FIP principles for all websites but differentiate their scope for the sites that deal with sensitive financial or health-related data. For the users, public education is the most direct intervention. Yet this should be executed in combination with other powerful government initiatives. Specific targeting is key. For example, for children, the inclusion of accessible educational materials in the K–12 curriculum should be made. For other demographic groups, such as older or ethnic minority users, the FTC must design a long-term program for incremental change, such as the distribution of a FTC privacy protection manual to local communities and a specific FTC interactive site channel for circulating consumer information.

This privacy zoning proposal concerns the commercial entities that are currently under no mandatory regulation. One may question whether these types of requirements in commercial sites would be feasible at all. Yet the marketplace ideal does not necessarily mean the freedom from *any* regulation. Even in the tradition of the First Amendment protection of freedom of press, for example, there are such regulatory exceptions such as obscenity and fighting words.

Do Not Track List

In a similar vein, the latest FCC proposal of the "Do Not Track List" would bring no meaningful change to the Notice and Choice approach without mandatory interface requirements. The proposed framework will let consumers decide if they want websites and advertisers to track them. However, there is no mechanism of enforcement for websites to ensure the transparency of the step to "Opt in the Do Not Track List." This is a fundamentally similar proposal to the pre-existing industry standard of P3P or TRUSTe in which commercial sites offer a voluntary choice option to wilful users amid long incomprehensible website policies. Even this voluntary provision does not presuppose the implementation of the full scope of the FIP principles.

The solution is, not the option of opting out of being tracked, but the option of opting in for specific sites and allowing them to track and tailor the particular needs of users. If the current premise of the FTC proposal holds any promise, the creation of a "Do Track List" as opposed to a "Do *Not* Track List" of trusted sites must be implemented with specific interface design requirements that vary according to privacy zones. To mandate a simplified step that allows users to select the scope of tracking is paramount in creating a condition that will incentivise the marketplace.

Conclusions

A critical analysis of U.S. policy formulation in the past, present, and future is critical in advancing the understanding of how the FTC FIP principles regime evolved into the current state online. The historical trajectory in the deconstruction of the principle of marketplace ideas showed the foundation on which the online privacy protection regime was built. Further, as this foundation was reinforced in the 1970s and 1980s, offline statutory grounds with which the online protection regime functioned were analysed. One of the main theses was the entrenchment of marketplace logic for information flow. In other words, market utility, instead of protection, for which one-to-one entities are situated in discrete domains, contextualises privacy control.

The central task remained the same as when Justices Warren and Brandeis (1890) penned a seminal piece in the Harvard Law Review because they were bothered by the intrusion of a photographer's zooming lens at their friend's wedding. Warren and Brandeis' concluding remark has lingered with privacy scholars for more than 100 years:

> *If he condones what he reprobates, with a weapon at hand equal to his defence, he is responsible for the results. …. 'Has he then such a weapon?' ….. The common law has always recognised a man's house as his castle, impregnable, often, even to his own officers engaged in the execution of its command. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?* (Warren and Brandeis 1890, 45, emphasis added).

Yet no matter how well-crafted policy design is, it is unlikely that the inception of new privacy law by itself keeps up with constant challenges from new technology. Conversely, the marketplace alone is inept to deal with the "public good" nature of information flow. In addition, the politicised debate is complicated by the dichotomy between government and market and its zero-sum cost-benefit analyses exaggerated in the ideological division in policy studies (Entman and Wildman 1992).

Answers may be found in a story of post-World War II Eastern Europe where government leaders had to decide on how to redesign devastated cities. While they had an opportunity to build entirely new efficient roadways, most cities resorted to the same flawed construction of narrow, winding city blocks – they were locked in history making the same mistakes. Lessons can be learned from the 1995 FTC regulatory construction of personal information flow over the Internet. The shift from the self-regulatory regime is warranted, not because of the failure of the marketplace metaphor, but because of the failure of the policy action that supports it on tangible grounds. The dramatic shift of policy orientation is urgent in visioning beyond regulatory legacy.

Acknowledgements:

This research was supported by Rackham Research Fund, the University of Michigan. The author wishes to express the gratitude to Dr. W. Russell Neuman at the University of Michigan for his guidance and support. The author also fully acknowledges the kind supports from Dr. Malek, Dean Dates, Dr. Ford, Dr. Merritt, and the faculty members of Howard Media Group, from School of Communications, Howard University.

Note:

1. Also see *Areopagitica* (Milton 1644) for a marketplace principle for regulating speech.

References:

Agre, Philip and Mark Rotenberg. 1997. *Technology and Privacy: The New Landscape*. Cambridge, MA: The MIT Press.

Bellman, Steven, Eric Johnson, Stephen Kobrin and Gerald Lohse. 2004. International Differences in Information Privacy. *The Information Society 20, 5*, 313-324.

Dalhgren, Peter. 2001. The Public Sphere and the Net: Structure, Space, and Communication. In W. L. Bennett and R. Entman (eds.), *Mediated Politics: Communications in the Future of Democracy*, 33-55. Cambridge: Cambridge University Press.

Danna, Anthony and Oscar Gandy. 2002. All that Glitters is Not Gold: Digging Beneath the Surface of Data Mining. *Journal of Business Ethics* 40, 373-386.

Electronic Privacy Information Center (EPIC). 2007. Regarding the Majority Opinion of the Federal Trade Commission in Proposed Acquisition of Doubleclick. <http://epic.org/privacy/ftc/google/EPIC_statement122007.pdf>

Entman, Robert and Steve Wildman. 1992. Reconciling Economic and Non-Economic Perspectives on Media Policy: Transcending the "Marketplace of Ideas." *Journal of Communication* 42, 1, 5-19.

Federal Trade Commission (FTC). 1998. Online Profiling: A Report to Congress Part 2 Recommendations. <http://www.steptoe.com/assets/attachments/934.pdf>

Federal Trade Commission (FTC). 1999. Prepared Statement of the Federal Trade Commission on Self Regulation and Privacy Online Before the House Commerce Subcomm. on Telecom., Trade, and Consumer Protection. <http://www.ftc.gov/os/1999/07/fcrahr10.htm>

Federal Trade Commission (FTC). 2008. Prepared Statement of the Federal Trade Commission on Behavioral Advertising Before the Senate Committee, Science, and Transportation. <http://www.ftc.gov/os/2008/07/P085400behavioralad.pdf>

Federal Trade Commission (FTC). 2010. FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers. <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>

Flaherty, David. 1989. *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.

Horwitz, Robert. 2005. On Media Concentration and the Diversity Question. *The Information Society* 21, 181-204.

Hunter, Chris. 2002. Political Privacy and Online Politics: How E-campaigning Threatens Voter Privacy. *First Monday 7,* 2. <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/930/852>

Langenderfer, Jeff and Don Lloyd Cook. 2004. Oh, What a Tangled Web We Weave: The State of Privacy Protection in the Information Economy and Recommendations for Governance. *Journal of Business Research* 57, 7, 734-747.

Marx, Gary. 2007. Desperately Seeking Surveillance Studies: Players in Search of a Field. *Contemporary Sociology* 35, 2, 125-130.

McManus, Thomas. 1990. Telephone Transaction Generated Information: Rights and Restrictions. <http://www.pirp.harvard.edu/pubs_pdf/mcmanus/mcmanus-p90-5.pdf>

Milberg, Sandra, Sandra Burk, Jeff H. Smith and Ernest Kallman. 1995. Values, Personal Information Privacy, and Regulatory Approaches. *Communications of the ACM* 38, 12, 65-74.

Milton, John. 1644. Areopagitica. <http://www.pinkmonkey.com/dl/library1/milt16.pdf>

Napoli, Philip. 2000. *Foundations of Communications Policy: Principles and Process in the Regulation of Electronic Media*. Cresskill, NJ: Hampton Press.

Neuman, W. Russell, Lee McKnight and Richard Solomon. 1997. *The Gordian Knot: Political Gridlock on the Information Highway.* Cambridge: The MIT Press.

Park, Yong Jin. 2009. Regime Formation and Consequence: The Case of Internet Security of the East Asia 'Four Tigers.' *Government Information Quarterly* 26, 2, 398-406.

Rotenberg, Mark. 2001. What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy. *Stanford Technology Law Review* 1, 44.

Solove, David. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review* 53, 1393-1462.

Streeter, Thomas. 1996. *Selling the Air: A Critique of the Policy of Commercial Broadcasting in the United States*. Illinois: University of Chicago Press.

Venturelli, Shalleni. 2002. Inventing E-regulation in the US, EU and East Asia: Conflicting Social Visions of the Information Society. *Telematics and Informatics* 19, 2, 69-90.

Warren, Samuel and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review* Vol.IV.