EMPOWERING PERSONAL PRIVACY: THE CONTROL OF PERSONAL
INFORMATION IN THE DIGITAL SPHERE

by

Yong Jin Park

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Communication)
in the University of Michigan
2009

Doctoral Committee:

        Professor W. Russell Neuman, Chair
        Associate Professor Nojin Kwak
        Assistant Professor Scott Walker Campbell
        Assistant Professor Steven J. Jackson

Dedication

To My wife, Kyung Eun
My son, Roland
&
My daughter, Dainna

Acknowledgements

For me, it was a long journey – filled with pain, sorrow, and solitude. And I remember my mom working in a restaurant late at night and carrying hot noodle bowels to send me the money I needed for a long time. When my mom lost her hair, weight, and got her lymphatic system removed in a hospital bed, I knew my due share of the cause of the pain.

My Professor Neuman. … He was more than an advisor to me. As my intellectual father and mentor, he provided me with all the supports that I needed to complete this journey when others were in doubt. The support was not solely sharp and intellectual, but also warm and emotional one that carried me throughout my career at Michigan. All the best that happened to me at Michigan was due to his genuine support, care, and understanding.

I am also deeply indebted to my committee members. Professor Kwak fully understood my strengths and weaknesses in private, but always defended, supported, and praised me in public. Professor Campbell, who raised the poignant criticism, never forgot to suggest ways to solve the problems in his generous and continuous support. And Professor Jackson was more than willing to respond to my relentless request for helps in publications, job talk, and this dissertation. To be assured, to me, it was the best committee that anyone could have.

This journey took me endless nights with tears, exhaustion, and no sleep, often on the verge of failure and despair.

To those who think my journey was too quick and easy, I say the pain. To those who think my journey was too long and expensive, I say the sorrow. Then, it was a lone

journey to me and my wife. We had to endure the unbearable doubt cast on my abilities as a teacher, a researcher, and a father. The pain was the one she had to swallow just because she chose me and the agony was the one she had to endure more than she deserved. We carry on with those memories – no one but she and I could know.

Table of Contents

List of Tables

List of Figures

List of Appendices

ABSTRACT

EMPOWERING PERSONAL PRIVACY: THE CONTROL OF PERSONAL
INFORMATION IN THE DIGITAL SPHERE

by

Yong Jin Park

Chair: W. Russell Neuman

The purpose of this dissertation is to examine the institutional practices and mass

behavior that structure personal information flow in the digital sphere. The central

question is how the interplay among institutional, cultural, and political forces shapes the

definitions of public and private – specifically, how institutions and users respond to the

potential of individual empowerment in the control of personal information. The

dissertation draws upon three methodologies: (1) content analysis, (2) survey research

and (3) policy analyses.

The analysis determined that commonly used interface designs for active control

of personal information were highly ineffective. Further, differential knowledge of

privacy options has strong effects on user behavior independent of levels of concern

about privacy.   The analysis concludes that current FTC privacy policy guidelines are

less than fully successful because of these individual and institutional constraints.

Theoretically, this analysis posits that new technologies do indeed have intrinsic

properties, yet the social construction of their use and implementation does not happen in

a vacuum. Instead, it is understood to be embedded in the complex interplay of

institutional/economic, cultural/psychological, and political/policy factors. The potential

of empowerment remains highly contingent upon a forceful policy initiative to address

these structural and cultural constraints.

Chapter 1: Introduction

Empowering Personal Privacy:
The Control of Personal Information in the Digital Sphere

Introduction

The purpose of this dissertation is to examine (1) the institutional practices that structure

personal information flow and (2) the operation of individual users in cultural practices.

In the application of the notion of the digital sphere (Neuman, 1991; 2009), the central

question is how the interplay among institutional, cultural, and political forces shapes the

system of information flow/control in the Internet. The dissertation consists of two main

parts: the institutional technical structure, on one hand, and the individual user culture, on

the other. This is to ask how institutions and users shape/respond to the potential of the

empowerment in the control of personal information at the structural and cultural level.

For this, the dissertation draws upon multi-methodologies: (1) content, (2) survey, & (3)

policy analyses. In integration, the dissertation argues for the particular shaping of

structure and culture in enabling/empowering active information control.

Framework
The Digital Sphere

Habermas (1989) idealized the public sphere, e.g., the 18th century Paris

coffeehouses, in which citizens should be able to use communicative channels in order to

voice their views to the elites, to protest and to rationally engage in public discussion of

the issues that matter to them (Price & Cappella, 2002). The question is whether

Habermas' ideal can be recreated in electronic spheres. Here it is possible to theorize the

Internet as an alternative public sphere where citizens stage daily routines and engage in

their political/commercial activities (Neuman, 1991; 2009). Note the two conditions in

actualizing such ideals: (1) institutional structures that frame the reciprocal channels of information flow and (2) competent citizenry to be able to exercise assumed active roles.

In the function of such places, the shape of its information flow/control is in fact crucial because it affects every aspect of digital lives, carries one's identities and constructs 'digital personae' in the sphere in which commercial and political activities are intertwined (Agre, 1998). For Marx (1996), this is the architecture of Panopticon that sets the relationship between the theater and the audience, while every movement in theater can be tracked, monitored, and controlled in the blurred distinction between private and public. For Castells (1998), this is the bipolarity between 'the net' and 'the self' in controlling information flow in digital bits. In short, in such idealized digital spheres, the prime significance is:

(1) how information flow/control is structured

(2) how users are empowered to act within the constraints of daily uses

Here the central premise is the analogy between printing and the Internet. According to Eisenstein (1980), the invention of printing brought the birth of print shops as an early form of capitalist market enterprises. This in turn accelerated the diffusion of mass literacy that empowered individual actions against church authorities (Benkler, 2006). As Hoggart (1958) aptly stated, active reading in the 'use of literacy' is a critical component in mass empowerment in accelerating the social-democratic consensus. In short, that is to recognize the impact of printing in initiating the process of democracy, as the potential was appropriated in institution and mass culture (Pool, 1983).

```
┌─────────────────────────┐
│      Printing Press     │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│       Institutions      │
└─────────────────────────┘
             │
             ▼
┌─────────────────────────┐
│      Mass Literacy      │
└─────────────────────────┘
```
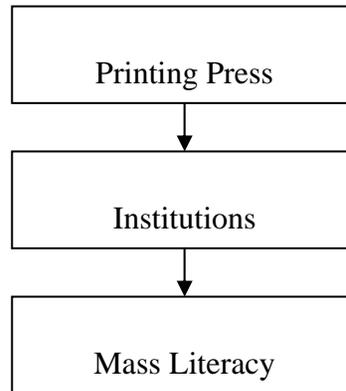
Figure1- A. Printing press & mass literacy

Note the similarities in the development of the Internet: (1) the Internet --- (2) e-commercial institutions --- (3) mass diffusion. The order is *not* necessarily linear. Rather, important is the function of the two, mass and institution, for constraining or enabling individual actions (Neuman, 1991). The central premise of this dissertation is the critical function of these two in the construction of the digital sphere, of which the viability depends upon the potential of the empowerment in information control.

Prior Debate

The concept of Internet privacy invites a polarized debate. On the one hand, there is advocacy for stronger government involvements (e.g., Litman, 2002; Rotenberg, 2000). On the other hand, there are claims for market-led solutions (e.g., Noam, 1997; Samuelson, 1998). The polarity is profound. One side clings to the faith of the self-regulating marketplace ideal, while the other emphasizes the role of the government in pursuing socially desirable goals (Napoli, 2000). In the policy circle, no middle grounds are encouraged, 'locked' in ideological commitment (Neuman et al, 1998). In academia,

pragmatic solutions are rarely sought, imbued in dogmatic convention. Rather, what
remains radical is to pursue a middle ground for pragmatic solutions.

The Orwellian Fear:
Les Vetements Noir

The heart of the debate is the unconstrained power of the commercial media
system that can monitor, collect, or engage in profiling certain segments of a population
against wills and awarenesses (Neuman, 1991). In fact, some of the Orwellian concerns
ring the truth. It was seen that Western Union discriminated the transmission of radical
political views over its telegraph lines (Wu, 2007). In 1922, AT&T invented the toll
networks in its delivery of audience to commercial clients – the practice culminated in the
implementation of a people's meter (Napoli, 2003). More recently, the acquisition of
Doubleclick by Google raised the concern of a new media giant following the digital
footprints of every citizen in digital domains. What is feared is the hyper-
commercialization of the Internet sphere that an omniscient new media system can turn
into a receptacle of passive users. History in fact shows that the 1934 Act legitimized
institutional practice of audience commodification (Sandivig, 2004; Streeter, 1996). Now
the fear is whether the Internet as closed gates of information flow will be entrenched as
legitimate forms of data practices in private Walled Gardens (Hargittai, 2004; Lessig,
2000).

The level of the public uneasiness had been well documented in line with the
Orwellian fear. For instance, a Harris Poll in 2000 showed that 86% of users wanted a
web site to provide clear consent and notification before any data collection. In a similar
vein, a 2000 study by the Pew Internet and American Life Project found that 54% of
Internet users objected to any tracking in the Internet, with the result of the USA

Weekend Poll in the same year showing that 65% of respondents believed that tracking

computer use was an invasion of privacy. Most recently, the surveys by the Truste (2008;

2009) confirmed that 64.3% of the public opposed online behavioral targeting, even when

this was directly related to their preferences of certain products. What underlies these is

the intensity of the public desire to be able to guard against the *potential* commercial

exploitation of personal data in online profiling. To put it in the policy context, the public

(64% in the 2001 Markle Foundation Survey) demanded at least certain control over the

unregulated data retention and appropriation by commercial entities.

Yet no matter how well-crafted policy design is, it is unlikely that the inception of

new privacy law keeps up with constant challenges from new technology (Brock, 1980).

On the other hand, the marketplaces alone are inept to deal with the 'public good' nature

of information flow (Kang, 1998). In addition, the politicized debate is complicated by

the false dichotomy between privacy and security (Neuman, 2004) and its zero-sum

benefit/cost analyses exaggerated in the ideological division in policy studies (Entman &

Wildman, 1992).
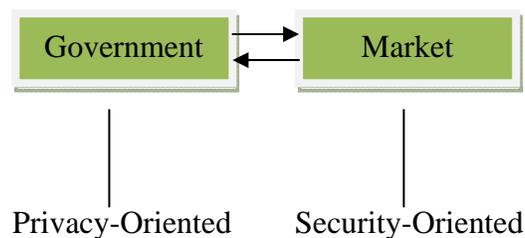
Figure 1-B. False dichotomy: privacy policy debate

It is simply impractical to resort to one over the other. Both are necessary, but *not* sufficient conditions. Put differently, neither solution is perfect. Neuman et al (1998) noted:

> We have little faith, however, in either would-be regulators or would-be
> industrialists to lead us to the information highway promised land. Put bluntly,
> given the opportunity, both would screw it up. (p. 24)

Perhaps, the right question is then *not* about the superiority of politicized abstractness. Rather, the question should be sought at the more concrete level, i.e., under what conditions, of (1) institutions and (2) citizenry, the Orwellian fear can be re-engineered or reversed. That warrants a third position in mass public and institutional practices.

The Central Position

This dissertation centers upon a 'bottom-up' user approach that is built on mass empowerment. That is, users should be able to make informed choices and assert information rights in everyday practices (Agre, 1998; Dimaggio et al., 2001; Hargittai, 2007). Architecture itself does *not* guarantee users' actions. However, it frames user behaviors and attitudes in information control. Policy concern should then be about how to enhance users' agents and to maximize architectural conditions. To restate, realistic policy solutions, beyond the dichotomy of government or market, should include the operation of users and structural constraints.

Goffman's Ideal
Technological Affordance:

Goffman (1959) in fact noted that individuals should be able to balance front and back stages in self-presentation. His central point is that the completeness of a human life requires the active management of one's self (and selves) in the realm of the public and

the private (also Arendt, 1958). In this seminal work, Goffman was concerned about face-to-face social interaction. To be more accurate, what he envisioned was in fact the rational human agent in particular social settings (Agre, 1998; see Meyrowitz, 1985). The notion is in essence similar to the earlier point by Marx (1996), in that the human life consists of the stage and the actors; the theater and the audiences; and the structure and the culture in mutual influence.

Note the enormous implication of Goffman's premise in the shaping of information flow/control in the Internet. Here the digital public sphere in its architectural nature may permit us to go back to the dynamics of the face-to-face interaction. In Neuman's term, the digital sphere is in fact inherently engaging, bi-directional, and empowering (2009; also Kwak et al, 2004). In information control, the Internet in its inherent properties may well bring back the dynamics of interpersonal interactions in managing, resisting, or rectifying one's identities to their interests (see Pool, 1983). In this vein, what is critical is to equip the structural and cultural conditions that enable the potential of the empowerment in exercising control over information – the ideal Goffman initially perceived in face-to-face interactions.
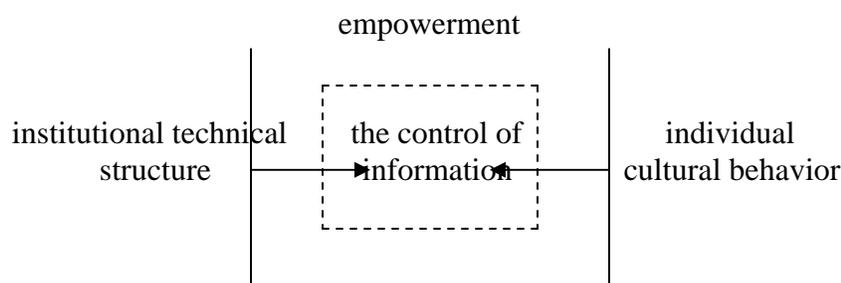
Figure 1-C. Technological potential

Neuman's Model
In Tech Appropriation:

Neuman (1991) explained the counter-force of mass psychology, on the one hand, institutional rationality, on the other hand. Television viewing, although voluntary, is embedded in inherited cultural habits of half-attentive media use. Homogeneous television content is the product of organizational market behavior that aims for 'critical mass' (see Hotelling's Centrism). The net result is the shaping of television diversity in the combined forces. In more general terms, this indicates the interplay of the multiple forces in constraining or enabling the generic 'technological push' (Neuman, 1991; 1998; 2009).
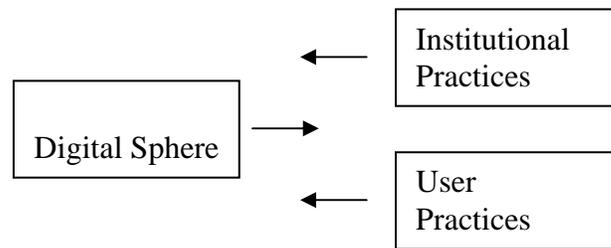
(modified from Neuman, 1991)

Figure 1-D. Technological appropriation

This point is the most crucial to understand the function of structural as well as cultural factors that constrain or enhance the viability of the media system. What this dissertation posits is that the very same rationale applies to information practices by the new media system and users. Here the question is two-fold: (1) how institutional rationalities in marketplaces hinder or promote fair data practices and (2) how a user agent is activated or curtailed in habitual behaviors. In this sense, the pivotal question addressed in this dissertation is the operation of path dependency (and its reversal) in

institutional and individual impulses embedded in economic incentive and convenient daily inattention.

Social Construction of the Digital Sphere
Theoretical Contours

> Note the premise behind the central proposition:
>
> Technology is constructed *not* in vacuum, but in interaction rooted in cultural and institutional contexts (Castells, 1998; Neuman, 1991).

This is *not* to deny the force of new technology. Rather, it is to recognize inherent properties of new technology in creating socio/democratic changes, that is, tech empowerment, according to its own logic (Pool, 1983; McQuail, 2005). However, the institutional and individual heuristics condition its social actualization in practice (Bourdieu, 1980; Fisher, 1990; See Jackson et al, 2007, for infrastructural design). Thus, the theoretical contours of this dissertation should *not* be confused with naïve assumptions of technological determinism (Campbell & Russo, 2003; Campbell & Park, 2008). The deterministic predictions lead to dystopian Panopticon fear or utopian celebration of the active user. Neither view is accurate, entailing empirical evidence. Instead, the digital spheres are contingent upon online structure and users within and through which information flows (Castells, 1998; Foot & Schneider, 2000; Lessig, 2000).

Technology

Digital
Sphere

Institutional   Culture
Structure[1]
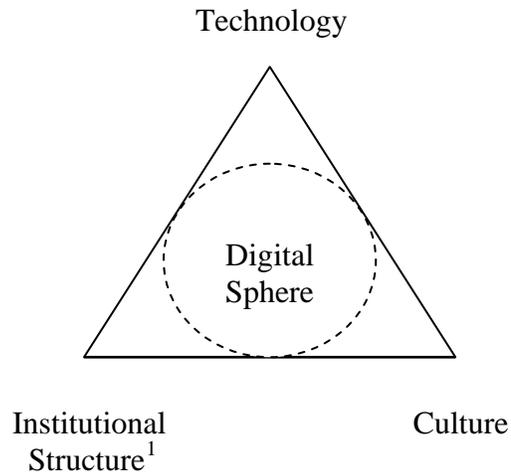
Figure 1-E. Social construction of the digital sphere

In sum, how information flow is structured and operated is a matter of social

construction, *not* inherent with technical properties. Put differently, whether or not the

electronic-sphere is constructed for the Orwellian fear depends upon such conditional

variables as institutional and cultural practices. In short, new technology stages the battle;

however, its construction is constantly being shaped and evolving (Lessig, 2000). The

following theoretical contours are then put forth:

1. Technology as an exogenous force, but constantly being shaped by institutional

and cultural practices

1.1. New media institutions pursue rational impulses in marketplaces

1.2. New media users reside in convenient digital habitats

2. However, institutional and cultural practices are dynamic, far from

deterministic

---

[1] Here institutional structure is to indicate the role of commercial institutions in responding to/shaping
the potential of new technology. The subsequent use of the term 'institutional-technical structure' in
Chapter 2 is *not* to conflate technology and institution, but to indicate the institutional appropriation of
technology in the interface level. To repeat, one of the central premises in this dissertation is that the
technology as an exogenous force is to be malleable at the two poles – with tech-institution on one
hand, tech-culture on the other.

This could be in fact understood in Giddens' terms (in his attempt to reconcile the power of structure and agent) (see Appendix A), but more clearly in Neuman's model. Here Goffman's premise serves as an ideal against which the technological potential can be shaped. In this vein, this dissertation is the attempt to advance Giddens' understanding, but in the application of Neuman's model in the shaping of the Internet and its personal information flow and control.

Structure of Dissertation
Technical-Institutions & Individuals for the Empowerment

This dissertation consists of two main parts. Part I concerns institutional practices in the commercial sector. Part II concerns cultural practices. In the first, what is at stake is the structural condition by which the design of Web architecture supports or curtails the empowerment of user control. In the second, the question is how individual agents, given such constraints, can operate in daily routines. Operating hypotheses are transparency and literacy, concerning (1) whether the empowering nature of the digital sphere can be maximized or curtailed in marketplace practices and (2) whether critical awareness of institutional data practices equips users to act to active control. In separation, each part stands on its own, speaking to different bodies of literature. In integration, however, the dissertation applies Neuman's model to understand the confluence of the multiple forces in the shaping of information control in the Internet.

```
                    ┌──── Empowerment ────┐
                    │                     │
                Part I                 Part II
              Institution             Individual
                  ┊                       ┊
                  ┊                       ┊
          Digital Transparency    Digital Literacy (i.e., Knowledge)
            ┌─────────┴─────────┐   ┌─────────┴─────────┐
            │                   │   │                   │
      1.1 Interface  1.2 Marketplace   2.1 Action  2.2 Concern/Motive
            └───────┐       ┌───────────────┘
                    │       │
                    Policy
```
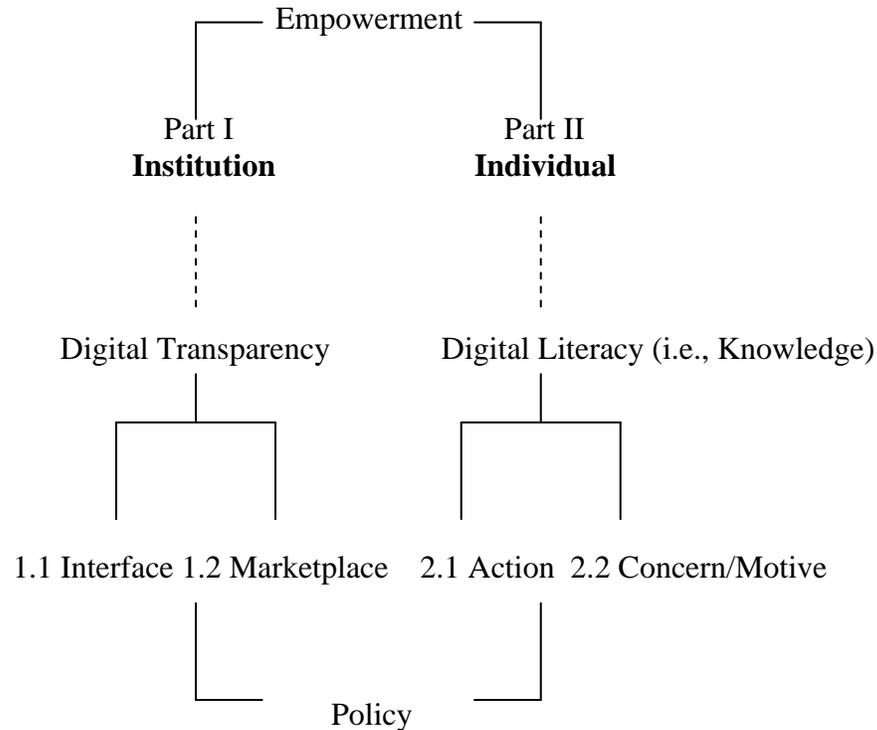
Figure 1-F. Structure of dissertation

Notes on Inspirations

The arrival of the digital revolution spurred pervasive changes in human life. This

dissertation is in essence about how we enhance (i.e., plumbing) the structure of

information-saturated Web environments and the individual action for user empowerment.

Thus, this dissertation is motivated by normative concerns of information privacy, but

strives to understand the function of marketplace and user practices. For this, this

dissertation, away from monism (Neuman, 1991), inspires to actively pursue

interdisciplinary junctures from old and new media studies.

First, methodologically, this work is built upon (1) a quantitative content analysis,

(2) a policy analysis, and (3) a survey, pulling from the mature field of political

communication (e.g., Schneider & Foot, 2004; Neuman, 1986; 1998; 2006). Second,

theoretical motivation derives from the traditional media debate on violence/sex (e.g.,

Hamilton, 1997; Napoli & Yan, 2006; Neuman, 1991). Yet rather than being disgusted, this work identifies the operation of institutional as well as cultural practices/motivations that generate violence/sex (and viewing habits), questioning passive undifferentiated audience assumptions (Lowery & DeFleur, 1983). More broadly, philosophical inspirations lie in the tension between the universal and the particular, the langue and paroles, and the signifier and the signified (Bourdieu, 1984; Castells, 1998; Giddens, 1984; Saussure, 1977) – the dialectic between online structure and user.

Warren and Brandeis' Hunch

The central question remains the same as when justices Warren and Brandeis (1890) penned the seminal piece of the Harvard Law Review because they were bothered by the intrusion of a photographer's zooming lens at their friend's wedding (Solve, 2001). Note Warren and Brandeis' concluding remark that 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 recognized 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? (p. 45, emphases added)

As this dissertation underscores individual action and empowerment, it is also to argue for redefining information privacy. Note the different context of the Warren and Brandeis' remark against 'prurient curiosity'. Herein, the motivation behind this dissertation resurrects the question by Warren and Brandeis, yet answers it in the new

context of the digital sphere – the Internet (see Appendix B). This work posits a step beyond the passive notion of 'to be let alone in an impregnable castle' into a more active dimension of information control (Margulis, 2003; Marx, 2003).

In the next, the dissertation starts with the policy history to examine the very foundation on which the institutions and individual users are to function for personal information control.

Chapter 2: Marketplace Ideal and Policy History

Empowering Personal Privacy:

Policy Section:
Institutional Technical Structure and Individual User Culture

Introduction

The purpose of this chapter is to examine the underlying policy condition for the

institution and the individual users to operate in the digital sphere. The central question is

how the government policy speaks to the two central poles of structure and culture in the

construction of the new digital sphere. The Fair Information Principle (FIP) remains the

focal point in this regard, i.e., how the Federal Trade Commission (FTC) FIP evolves into

the current form in the Internet. In other words, it asks what the current state of the policy

is in conditioning the information flow and control in the digital sphere in its historical

trajectory. This serves two purposes. First, it is to bring the discussion down to the very

concrete level and to the function of policy. Second, it is also to identify the policy

rationale behind the criteria with which to assess the validity of the technical-institutional

structure and the user culture in operation.
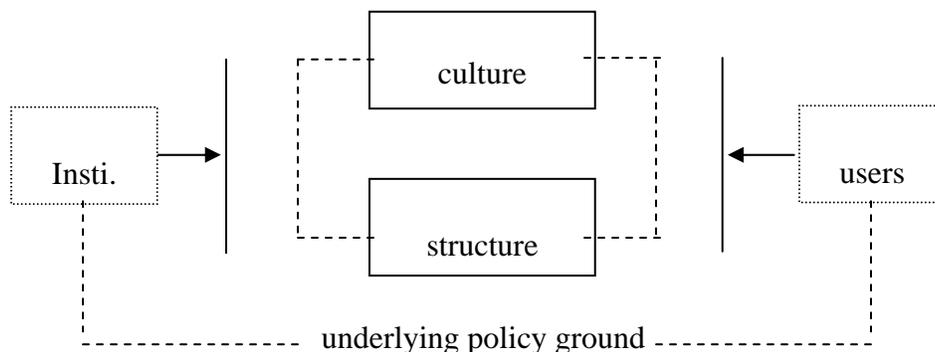
Figure2- A. Technical-institutions & individual users
in the construction of the digital sphere

This section has the following structure. First, a brief theoretical framework of the US communication policy is provided. Second, the examination of the policy history proceeds in the two stages: (1) pre-computer and (2) computer era in the 80s. Lastly, the FTC policy of the Internet era is presented in concrete terms.

1. Framework

2. Stage 1: History: the Foundation

2. Stage 2: Computer Era in the 70s to the 80s

2. Stage 3: the Internet: its advent & policy challenge in the 90s & up[2]

In sum, here the aim is to provide a factual account of the information privacy policy in the historical background. History, in this sense, indicates more than the aggregate of the facts and events pertinent to information privacy. Rather, it is to examine the philosophical root of the US policy and its ensuing impact before being able to provide concrete recommendations to the FTC.

Methodology

In this section, the approach is holistic. That is, the discussion, instead of probing one case in depth, draws upon the combination of historical and policy insights. First-hand sources came from the two: (1) the NGOs and (2) the government (mainly, the FTC). In addition, the analysis partly relied on the re-interpretation of data present in secondary academic analyses. It was to collect the multi-faceted resources in the reconstruction of the existing policy condition, i.e., how the current regime evolves in

---

[2] The organizational frame is *not* to indicate the causal direction, i.e., tech to policy. Rather, it is to note the reverse directionality, i.e., policy to tech, with the critical role of policy in shaping new technology in each of three stages.

what ways. The policy history, in this sense, is an account of the pertinent facts, but reconstructed with an analytic angle.

Framework
The Marketplace Ideal

Napoli (2000) noted that the marketplace of ideas is the most prominent metaphor in the US communication policy. By this, he meant more than rhetoric, but the operation of the policy principle in concrete terms. The idea goes back to John Locke in the 17th century when he pointed out "the attainment of the truth is best achieved through the free uninhibited exchanges of ideas/information in the marketplace" (p.105, Napoli, 2000; Dalhgren, 2001). Under this viewpoint, the government regulation is to be left to a minimum far from intervention to keep the functionality of the marketplace (Horwitz, 2005; Stein, 2004). In an affirmative sense, the policy is a hindrance when the self-functioning marketplace in the absence of government intervention best guarantees the sharing of diverse viewpoints, and ultimately the truth.

Policy

Self-Regulatory Mechanism

Marketplace
Rationale

Party 1 ◄► Party 2

Figure 2-B. Laissez faire model

Note the two aspects of this ideal: (1) the market and (2) the democracy. Also regard the two entities in interplay: (1) the source (party 1) and (2) the exposure (party 2). In other words, the principle speaks to the faith of *not* only the political liberty, but also

the economic integrity that is best achievable, with no mediating force in between

(Napoli, 2000; Streeter, 1996).

In most US communication policies, the policy inaction is the direct consequence

of this philosophical root. Here the inaction[3] does *not* mean no action at all. Rather, it

indicates the laissez faire model (Neuman, et al, 1998) in which the self-regulatory

market mechanism is promoted on policy ground. That is, the marketplace ideas factor

into the concrete policy guidelines such as 'public interest, convenience, and necessity'

(Napoli, 2001). Here the function of marketplace is to be assumed to be rationale in

operation. The metaphor, in this sense, has a tangible consequence – the assumption that

the marketplace is best regulated in the hands of the two parties at stake.

The US Privacy Policy

Stage 1:
The Foundation

The US privacy policy is summed up as the Liberal Market model (Solove, et al,

2006; Venturelli, 2002). That is, in essence, the privacy regulation is industry self-

regulatory, characterized by (1) non-commercial obligation and (2) no burdensome public

interest obligation. Note its philosophical origin in line with the marketplace ideal. In fact,

the US constitution per se does *not* explicitly state the rights to privacy. While the Fourth

Amendment[4] is construed as a broad legal basis, the policy intervention has always been

---

[3] Here Jackson et al (2007) made a clear reference to the role of political regime in infrastructural design. To repeat, the inaction does *not* mean no action: rather, it means the lack of concrete directions in the active policy role, which in fact favors certain institutional practices.

[4] To be accurate, the Fourth Amendment is about the protection against unwarranted search from the government: whether this is constituted as privacy protection remains a legal debate up to now.

reactionary only when the market between the parties involved fails to function (Agre, 1998: Farrell, 2008).

This point is significant in that communication policy, in general, had been understood primarily in the context of the First Amendment when it comes to the US Constitution. For instance, in the FCC policy, the objective of media diversity had been understood achievable at the function of commercial freedom in the marketplace as interpreted in *the Associated Press vs. US* in 1945 (Horwitz, 2005). Here, however, the policy foundation of the marketplace ideal goes to the Fourth Amendment as this is further operationalized in the consistent US privacy policy stance. The minimal privacy protection position was in fact best illustrated in the two landmark cases with the limited interpretations of constitutional privacy rights:

Case 1: Olmerstad vs. the United States

In this 1928 decision, the Supreme Court in fact ruled that the Fourth Amendment does *not* apply to telephone wiretapping. The 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'.*

Case 2: Miller vs. the United States

In 1976, the position was upheld by the Supreme Court decision[5] that citizens do *not* have a reasonable expectation to privacy when communication can be restored in third parties; thus, they can *not* be accountable. The Court stated:

---

[5] In 1970, Katz vs. the US in fact restored the protection of individual rights to a certain extent, based on the dissenting view by Brandeis in Olmerstad vs. the US. Nevertheless, this position was also weakened by the 1976 decision in Miller vs. the US.

The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose.

Note the consistent reluctance by the Court in establishing the constitutional protection. In sum, what the two cases established was the very foundation upon which the rights to privacy is left to private parties at hand. Put it differently, it is the reluctance, in line with Liberal Principle, from which the policy intervention is actively interpreted as the last resort. That is, in the broad interpretive frame, the distrust of the active administrative policy measures may well serve as a working principle for the FTC to apply in the following eras.

Stage 2:
The Computer Era:
The Inception of the FIP in the 70s to the 80s

The 1970s-1980s marked a distinctive period in the US policy stance. The inception of the OECD Guidelines was the result from the transnational effort, but its core principles were formulated by the US government in this period. The Fair Information Principles (FIP) that underlie the OECD Guidelines were in fact the concrete product of active involvement by the US government in providing a set of guidelines for the private sector[6] with the advent of the computer (Bellman et al, 2003).

---

[6] Here the discussion stays on the legislations at the federal level. For instance, there are wide variations in privacy statues (in terms of scopes & types) at the state level. Here the focus is the common thread of the regulatory environment, nevertheless.

Table 2-1.
Legislation Chronology

Legislation	Description & Scope	Sector
1970 Fair Credit Report Act	Protect credit records	Private
1974 Privacy Act	Gov. access to indiv. record	Public
1975 Privacy Act enacted		Public
1984 Cable Communications Policy Act	Protect cable subscribers	Private
1987 Computer Security Act	Federal computer	Public
1988 Video Privacy Protection Act	Records of borrowers held by video stores	Private

(modified from Flaherty, 1989)

Note the consistent legislative efforts in the 1970s to the 1980s (see Table 1). First, the formulation of the FIP was in essence that of the US Department of Health, Education, & Welfare in 1973 in response to the increasing uses of automated data records (Gellman, 2008). It was followed by the 1974 Privacy Act that highly restricts the access by federal agents to individual records. The US government also pushed for Cable Communications Policy Act, the first of this kind in network service, opening up the door for further legislations, such as the 1988 Video Privacy Protection Act that protects information regarding video rental (Flaherty, 1989). In fact, it was *not* until the 1970 Fair Credit Reporting that the US government actively stepped up to formulate the policy that protects information privacy of individual citizens in the commercial sector (Movius & Krup, 2009).

Nevertheless, in the 70s to the 80s, the active US federal policy involvement in general and the formulation of the FIP in particular needs cautionary insights. First, the legislations were introduced in the absence of a unified formal policy. Second, the policies were formulated in economic (as opposed to individual protective) terms in providing the basis for industrial or organizational conduct (Kobrin, 2004). However, this,

too, resides in the statutory level, with no binding effect. The 1974 Privacy Act, in fact, only concerns the public sector, leaving the private sector as a loophole. In addition, the privacy protection remains as sector-by-sector patchworks, where the most enforcement is up to the private entities in piecemeal solutions (Langenderfer & Cook, 2004).

Important is this very context in which the core aspects of the FIP were introduced and expected to be implemented (Rotenberg, 2000). In short, the period is marked by the active policy effort in formulating the FIP, that is, the enormous progress of principle in the strong influence to other nations' policy directions. In the 70s and the 80s, however, the path still remained clearly different from that of the European nations in that the US legislations were enacted in the context of commercial interests/guidelines, far from the public interest model in which inherent individual rights were instilled under constitutional guarantee (see Dutton, 1998; Flaherty, 1989; Venturelli, 2002; see Park, 2009). In other words, what characterizes the US policy is, *not* the absence of *any* privacy policy, but the absence of the strict governmental intervention/interpretive framework under which the administrative remedies are to be advanced. Three main factors characterize the US privacy policies that were installed in this period:

- No unified formal policy: no omnibus approach (e.g., the EU)

- State level protection

- Piecemeal solutions in sector by sector

Stage 3:
The Internet Era:
The FTC Adoption of the FIP Regime

In the 1990s, with the advent of the Internet, the FIP and its fundamental principles became the forefront of privacy policy in the US. This is to note that the

preference for self-regulatory industrial code came in place as the FTC de juror policy

standard (Leistert, 2008). The regime of the industry self-regulation should be understood

in the administrative context of the FTC, of which the main objective is to promote

commerce in business interests. Furthermore, it is important to consider the time period

of 1995 in which the FTC took over the jurisdiction of online commerce with the launch

of the first commercial search site Yahoo!. That is, the FTC (and the Clinton

administration in the mid 90s) had a clear policy incentive to promote free information

flow for the online industry (of which the growth was yet to be burgeoned) (Heckman,

1998).

In this period, the most noticeable change in fact resides in, *not* the FIP adoption,

but the continuation of the marketplace principle in its online application. In fact, the

FTC adoption of the FIP further reinforces the market friendly policy stance (Hunter,

2002). That is, the original FIP with the eight items shrank to the two: *Notice & Choice*,

while in principle adhering to the fundamental guidelines from the OECD. Also, no clear

benchmark was set for the voluntary observance of the principle itself. Most of all, in the

faith of the marketplace integrity, no enforcement mechanism was in place online. This

point was articulated in Turow and Hoofnale in 2006:

> The market-based approach to privacy adopted by the FTC was a departure from
>
> a tradition of privacy laws, such as the Fair Credit Reporting Act of 1970 and the
>
> Privacy Act of 1974, that embraced a full set of "Fair Information Practices" to
>
> protect personal information. (p.6)

The Original OECD Principle	FTC Principle	Industry Version
Collection, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, & Accountability	Notice, Choice, Security, Integrity, Enforcement	Notice & Choice

1980   1995   2000
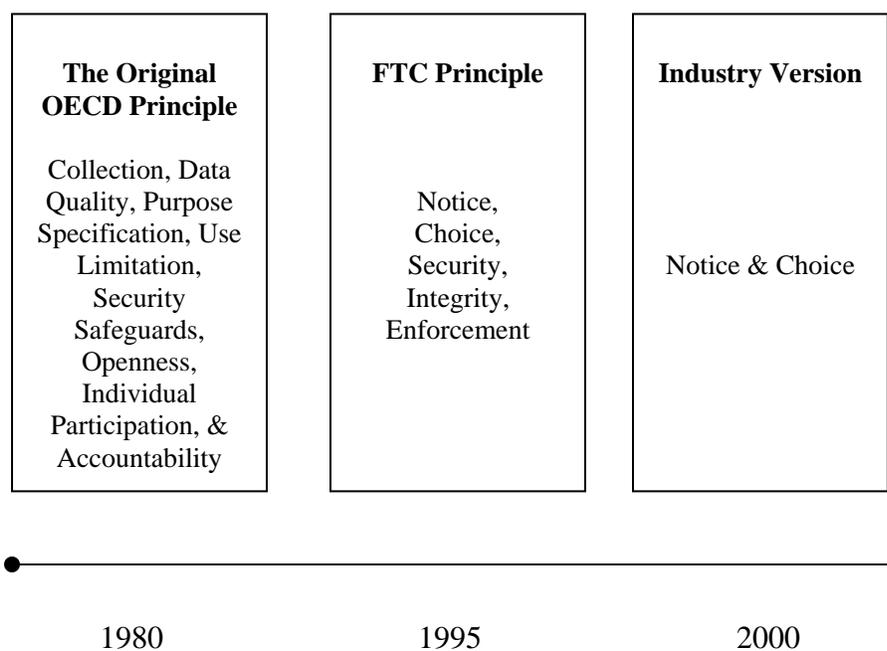
Figure2- C. The evolution of fair information principles

Here what is crucial is to recognize the shift to the much relaxation of the FIP standard in favor of online commercial entities. In fact, over the decades, the FTC, in the provision of the operating principle, made it clear that its jurisdiction was to function for commercial interests of which the potential in the new medium was yet to burgeon (e.g., also in Clinton-Gore initiative, 1997). In 1999, the FTC in its report to the House commerce subcommittee on Telecom, Trade, and Consumer Protection affirmed:

> [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

This position was embraced over and over in each of the FTC reviews in 1998, 1999, 2000, and most recently, 2007 (in its review of behavioral target advertising, EPIC,

2008; Hoofnagle, 2005). Note that in the first adoption of the FIP in 1995, the FTC refused to include a full set of the guidelines, while much of its policy position had been grounded in the encouragement of the voluntary adoption of the FIP. With no federal oversight agencies as of 2009, however, the industry version of *Notice & Choice* remains as the only working principle. Note the two types of enforcement mechanisms now in place under this principle: (1) voluntary seal certification program (e.g., Truste/BBBonline) and (2) p3p as the participation in W3C industry consortium, in which the sites are voluntarily expected to provide the elements of the FIP through the memberships.

In fact, the year 2000 was the only period in which the FTC took a serious consideration of amending the industrial self-regulatory codes (in the votes of 3 to 4 of the FTC commissioners). Nevertheless, the introduction of new legislations was overturned in 2001 in favor of existing policy guidelines under a new FTC chair at that time (Hoofnagle, 2005; Solove, 2001). 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 (Venturelli, 2002), but in a far more dramatic shift to private entities for the locus of power (Agre, 1998; Caudill & Murphy, 2000). That is, the position of the minimal 'voluntary control' regime that was introduced in 1995, reinstated in 2001 and up to 2007, remains as the operating principle in terms of online consumer protection (LaRose, 2004; FTC, 2002; Milberg, et al, 1997; Turow, 2005) (see Figure D).

FTC stance

Self Help Voluntary Control Data Commissioner Registration Licensing

Low   Medium   High

Lassiez Faire
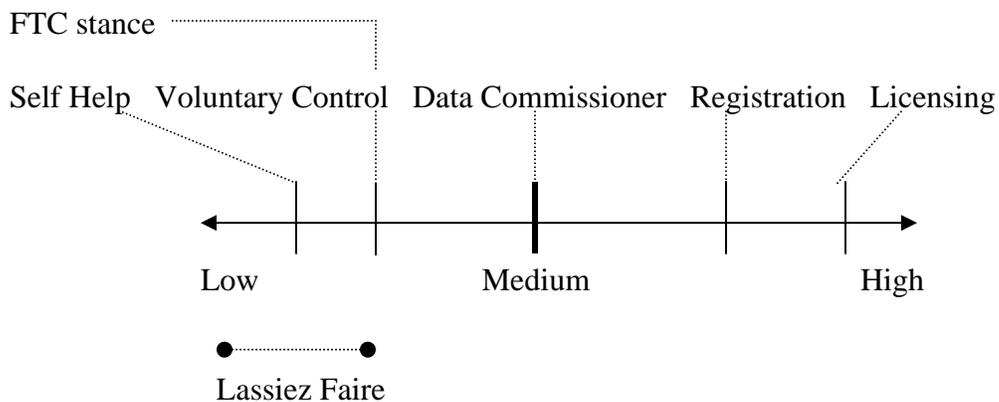
Figure 2-D. Level of policy involvement in privacy protection

(adopted from Milberg, et al, 1997)

Discussion

In sum, this policy section provided a framework of the US privacy policy in the three stages. This was to advance the understanding of how the FTC FIP regime evolved into the current state online. In line with the Liberal Market Model, the policy formulation in the earlier two stages was marked by the market-based minimalist, i.e., lassiez faire, approach to information/privacy control. With the FTC at the forefront in 1995, this became further accelerated with:

(1) the full scope of the FIP compromised

(2) no clear benchmark for adequate data protection in the voluntary FIP observance

(3) no enforcement mechanism in place

In short, the US policy inaction, built upon the industrial self-regulatory marketplace rationale, characterizes the current privacy policy regime in the commercial sphere, as this is further manifest in the FTC adoption of the FIP for online information flow in the 90s.
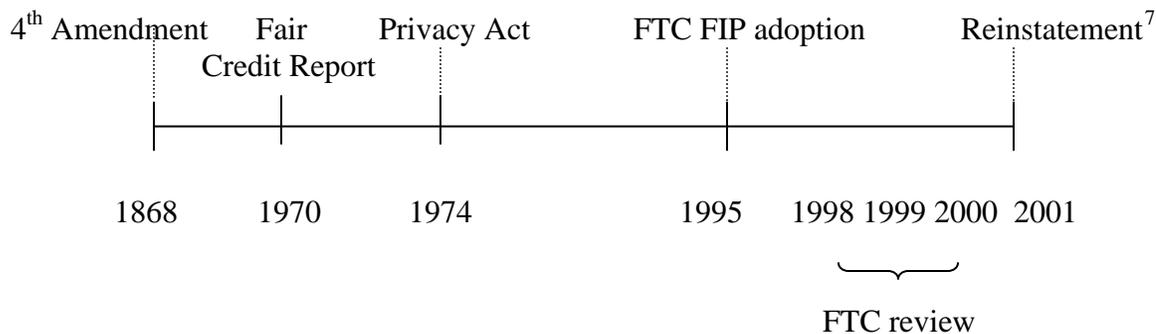
Figure 2-E. Timeline: policy regime in evolution

The Two Poles:
The Operation Under Policy Conditions

Here it is necessary to reconstruct the policy picture in terms of the two poles: (1)

structure and (2) culture as constituted by institutions and users, respectively. Under the

current FTC regime, the operational assumption is clear. First, structurally, the institution,

in its interface design, is willing to embed the core principle of the FIP in the voluntary

compliance. Second, culturally, the users, in the policy picture, are recognized as the able

agents fully capable of data control according to personal needs or concerns (LaRose,

2004; Turow, 2005; Turow & Christogle, 2007). The net result is that the faith in the

integrity of marketplace incentive – that is, the provision of information control in the

self-regulatory rationale, on one hand, with the most optimistic policy understandings of

capable users in a monolithic sense, on the other.

---

[7] The FTC 2001 reinstatement was in fact further affirmed in 2007. In the 2007 FTC review, the policy
validity of the FIP adoption was raised but with no substantial change.

Structure **x** Culture
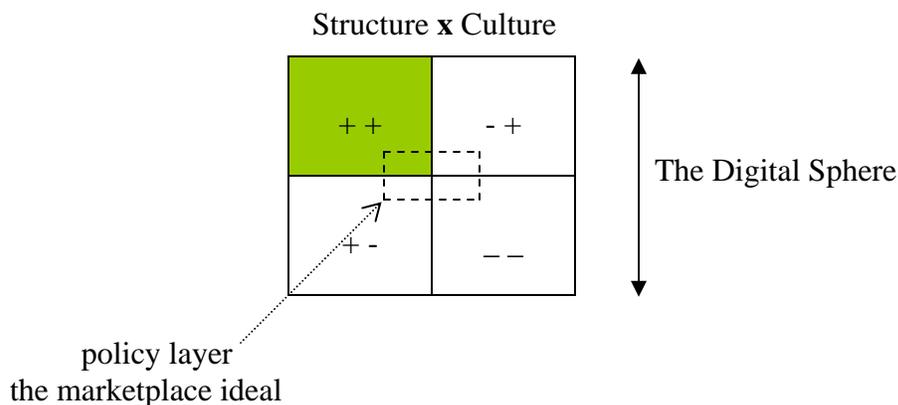
+: shaped for control
- : *not* shaped for control

+ +: the FTC rationale posited for structure/culture to operate into the green cell

Figure 2-F. FTC policy rationale

Proxy Regulation at the Structural Level

In a closer examination, it can be that if the FIP functions as a de juror standard, de facto policy in place is the proxy regulation that governs only the party of the information provision at the structural level. Note the very absence of:

(1) the enforcement mechanism in compliance

(2) the concrete details regarding users in the FTC stance

In other words, the *very* absence of users in the policy picture itself indicates the operational principle in which the adequate structural provision alone, as defined by the industry standard, suffices to the fulfillment of the marketplace ideal.

The analogy could be the policy principle of the traditional broadcasting diversity. Under the FCC principle, it is in fact assumed that the structural regulation over media consolidation/ownership on the side of production (i.e., source diversity) would guarantee the viewing diversity (i.e., exposure diversity) on the side of consumption (Napoli, 2000;

Horwitz, 2005; Neuman, 1991). In this vein, the current FTC regime too is also a form of

the proxy regulation over the structure alone. That is, under the provision of the

guidelines for the industry, if the proper organizational behavior follows, the users'

information protection is to be achieved. Put differently, in the construction of the public

sphere, the current policy layer grounds the full functionality of the marketplace ideal to

the sole function of the commercial institutions alone.

Self-Regulatory Policy:
The Validity of the FTC Regime

Here it is *not* to bluntly question the rationale of the marketplace ideal per se

(Sandvig & Bar, 2008). Instead, what is being questioned is the validity of such self-

regulatory policy measures with no due mechanism (Neuman et al, 1997). In concluding

the policy section, the skepticism by Neuman et al (1997) over the sole marketplace

mechanism is taken seriously. The next section is to empirically examine the operation of

the institutional-technical structure and individual user culture in the shape of information

flow/control, but in the absence of any valid policy measure that sustains the function of

the two (see Appendix C). The evidence serves as a guide for policymakers to fill the

policy vacuum that is currently locked in the regulatory legacy (Pool, 1983; Neuman,

1991; 1997).

Chapter 3: Institutional & Technical Structure: Content Analysis

Empowering Personal Privacy:

Interface Design

The institutional structure for the empowerment in the control of personal information

Introduction

Chapter 3 examines the empowering condition at the structural level. On the theoretical

level, this is to explore how institutions shape/respond to the potential of the

empowerment in the control of personal information at the structural level. The central

question is whether and to what extent the interface of the Web sites is constructed as an

enabler for informed choice in managing personal data. This study is a content analysis of

the 398 commercial sites. Here user control, as embedded in interface design, is indicated

through HTML text and interactive site features (e.g., Hargittai, 2001; 2002; Palmer et al,

2000; Trammell et al, 2006). On the policy level, this is to identify the institutional

arrangement of the interface design in the voluntary observance of the FIP. On the deeper

level, it challenges the validity of the self-regulatory regime in the commercial sphere. In

short, Chapter 3 is about the structural shaping of information control by the institutions

in the Internet.
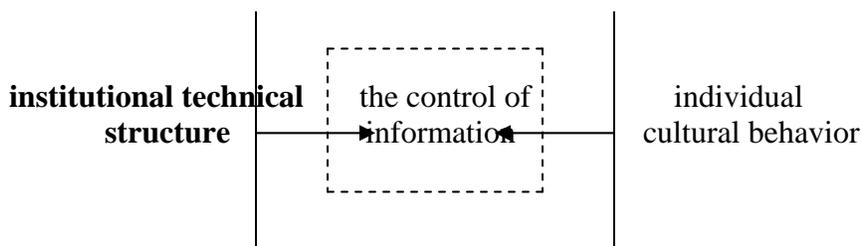
Figure3- A. Empowerment

Framework
Embedded Transparency

Note the centrality of communicative channels in providing a tool of empowerment for citizens in the electronic public sphere (Neuman, 2006; 2009). The presence of such channels is crucial because, for the viability of the segments, users should be able to freely construct political or commercial identities while being able to monitor, protest, or rectify the use of information. Foucault (1984) himself noted that the architecture itself does *not* automatically lead to the tyranny of surveillance. Rather, it is the interface channels embedded in the architecture of the Web sphere that shapes or curtails the operation of informed citizenry (Agre, 1998; Marx, 2000).

Brin (1998) in fact noted:

There any citizen may tune into bookings, arrangements, and especially the camera control room itself, making sure that agents on duty look out for violent crimes, and only crime. Above all, one thing makes life bearable: the surety that each person knows what is going on, with a say in what will happen next. And has rights equal to those of any billionaire or chief of police. …

This is to note the transparent structure in which users are permitted (1) to get informed and (2) to exercise information control. This point in fact could be understood in Goffman's terms: that is, the construction of the stage/the theater where the individuals can manage the presentation of self (and selves) in the balance of the back and the front. In short, the ideal is that the structure of the digital sphere in which the interfaces are designed to enable information control (e.g., Webster, 1998). Note the reverse of the Orwellian fear as the users are *informed* and allowed to *interact* in counter-surveillance (Marx, 2003). In this sense, the interface channels empower users with the appropriate

tools/measures of resistance against unwarranted surveillance that can be embedded or curtailed in the architecture of the Web itself.
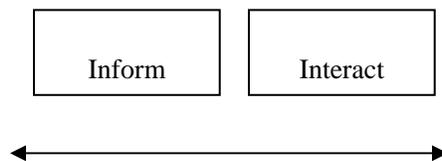
Figure 3-B. Embedded digital transparency

Prior Studies

The institutional practices by websites in structuring data flow have been under consistent scholarly and policy attention (e.g., FTC, 1998; 1999; 2000; 2007). In the next section, this study identifies the typology of prior studies and aims to fill the missing gaps in the literature.

Perspective 1
Privacy Statement

The first type of research examines the Internet privacy statement. The concern is the function of statements as a legal protection for the sites, *not* for consumers. Note that this line of research has a long history, going back to consumer research that examined the deceptive practices of fine prints in television and magazine advertising (e.g., Barlow & Wogalter, 1991; Hackbarth et al, 1995). In this vein, numerous variants (Papacharissi & Fernback, 2002; West, 2003) focused on the truthfulness of the written statements. For instance, Fernback & Papacharissi (2007) conducted a discourse analysis of highly trafficked commercial sites: Little specifics were found to protect users, with the statement serving to authorize business practices. More recently, PI (2006) investigated the rhetorical strategies of ISPs and found most statements were written 'as little as

possible' and 'as confusing as possible.' With these findings, LaRose and Rifon (2006) bluntly defined the online privacy statement as a legal 'disclaimer'.

Perspective 2
Surveillance Practices

The second type examines data surveillance practices as in privacy policies of individual websites. For example, Hong et al (2004) recorded the scope of data profiling among the news media sites. LaRose and Rifon (2006) also examined the top 200 trafficked commercial sites in terms of the 'depth' (i.e., type) and 'breadth' (i.e., amount) of data collection practices. Schwaig, Kane, and Storey (2005) analyzed the sites of Fortune 500 companies, asking whether *offline* credibility is in line with fair *online* practices (also Culnan & Milne, 1999; 2000). The most comprehensive study was conducted by PI (2006, for the Big Brother Award). The content analysis identified the extent of extraneous data retention and transfer to third parties (advertising broker) in such mega sites as Google and Yahoo – the practice rampant with no adequate information about how the data will be used.

Perspective 3
FTC Fair Information Practice

The third type concerns the observance of the FTC principles of Fair Information Practice (notice, choice, access, integrity, & redress) in commercial sites (Culnan & Milne, 2002; 2004; FTC, 1998; 1999; 2000). This is the most advanced one in that the concrete policy criteria are to put the US self-regulatory regime to an explicit test. Most studies are in fact a variant of this sort since the 1998 landmark FTC web sweep. For instance, Culnan (2000) found that more than 85% of the sites sampled collected data but with only 14% of them providing any notice regarding data collection. Also, Miyazaki

and Fernandez (2000) reported that most ecommerce sites failed to post 'integrity'

aspects of data uses. In this line, the most recent FTC inquiry (Georgetown study, 1999)

found that while 67% of the sampled sites disclosed data collection practices, only 10%

implemented all the elements of the FTC principles.

Missing Gap
A point of further inquiry

Note that most content analysis in Internet privacy centers upon a privacy

statement per se. This is in fact a significant point of inquiry in that the FTC posits the

transparency of the statement as a consistent criterion (that is, the principle of notice &

choice) (Culnan, 1998; Lessig, 2000; Milne & Culnan, 2002) with which to measure

institutional data practices. Nevertheless, what is ignored is the technological aspect of

the Web that is inherently endowed. In fact, the scholarly inquiries paid *little* attention on

how the interactive environment can impose or curtail structural constraints for the user.

In other words, how a website is framed, channeled, and deployed to be accessible for

informed choice (notice & choice) is *rarely* examined.

Here the difference is about *How* vs. *What* (see Cranor & Acquisti, 2007). That is,

rather than probing what's in the statement, this study examines how a site is structured

to inform and to direct users' attention and action (Cockburn et al, 2003; Foot &

Scheinder, 2002; Hargittai, 2002). The architectural condition alone does *not* determine

cultural usages; however, it frames user behaviors and attentions in information control.

In short, the primary concern is the particularities of the site features embedded in

interface design, as this is a manifestation of the deliberate choice from the part of the

institution (Castells, 2006; Shneiderman, 2000).

Research Question

RQ1.1: Whether and to what extent is the interface designed for users to get informed of data practices?

RQ1.2: Whether and to what extent is the interface designed for users to exercise/control information flow?

Method
Sampling Logic:

Modeling after the 1998 FTC landmark 'web sweep' content analysis (e.g., the studies in this vein: FTC, 1998; 1999; Culnan, 2001; Milne & Culnan, 2002; GIPPS, 1999), this study proposed to combine the several methods from prior studies. The sample selection was based on the combination of the two:

- Group (1) *Most Popular*: the top 500 sites (from Alexa.com) with the highest traffic

- Group (2) *Random Sample*: the list of AOL search log from 500,000 users

(modified from Milne & Culnan, 2002)

Note that this combination was to complement the shortcoming of each method alone. That is, the use of the AOL log was to ensure the variance of the sampled sites, with the inclusion of the top sites incorporating the most routinely visited venues as operated in daily context. Despite the large target pool size (N = 1,000), the final sample size (n) significantly decreased as (1) foreign sites, (2) B-to-B sites, (3) adult-sites (see GIPPS, 1999, for the exclusion), and any replicates between the two were eliminated from the sample.

Step 1: Sampling Pool

The sample pool proceeded in two steps. In the case of Group (1), the top US sites were identified from the top ranked site (Group (1): n = 153/500). In the case of Group (2), 500 commercial websites was randomly selected from the first 10,000 AOL search queries (http://www.gregsadetsky.com/aol-data/). This resulted in the creation of the sample pool of 1,000 websites, the top and random samples (500 + 500) combined.

Step 2: Sample Selection

2.1 Top Sample:

In the sample, there was one government-operated site (www.usps.com)[8]. This makes up the total of 152 full domain sites. From this, the three sites with the same policy (e.g., MS) sites were excluded from the sample. Also, the site, with the US IP address, but operating under foreign ownership was eliminated (for this reference: www.domain.com). As a result, a total of 148 sites were created for analysis.

2.2 Random Sample:

Here the multi-stage sampling was employed (Babbie, 2001). First, the 500 clusters of individual search queries were identified from the random start in the 10,000 user AOL batches. Second, an individual URL within each cluster was randomly selected. Each cluster was mutually exclusive, consisting of about 20-70 unique URLs. With a total of 500 clusters, this includes 10,000-35,000 sites from which to select the final samples. Note the advantage of this technique in increasing the chance of equal selection when it is impossible to locate all the elements within the sample frame (Malhotz, 1998; Webster, 1996, for marketing research).

- Stage 1: random start within the 10,000 user batches

---

[8] The official site URL is www.USPS.gov; however, its operation leads to www.usps.com

- Stage 1.1: 500 clusters randomly selected

- Stage 2: from each cluster: random selection

For the meaningful construction of the Internet universe, the sites lower than 1000,000 in traffic/share (www.alexa.com) were filtered. Furthermore, the three broken URLs were identified and eliminated during the coding process. Overall, in Group (2), the sampling rate = (0.25)*(0.01), with the confidence level of 95%: SE + - 4.9.

Intercoder Reliability

Two coders were hired to code the individual websites. The coders underwent at least three training sessions at the beginning of November 2008. The coding proceeded during the 2008 Fall academic term. Intercoder reliability, based on a (40 randomly selected) pilot sample (that is, 10% of the full sample, see Lacy & Riffe, 1999), was calculated for both (1) percent agreement and (2) Cohen's kappa (Neuendorf, 2002). Despite its simplicity, however, the percent agreement raised the criticism for being too liberal, especially with nominal observations (Neuendorf, 2002) (for this study, 91% agreement in the total items). Cohen's kappa was calculated to accommodate the shortcoming (kappa = .84 in the total items: Inform + Interact in the pilot sample)[9].

Coding Instrument

Based on the extant literature (e.g., Culnan, 2000; 2001; FTC, 1998; 1999; Hong, 2004; LaRose & Rifon, 2006, Turow, 2001), the study modified the previous instruments to incorporate the primary goal of this research. The aim was to use the consistent items (i.e., criterion validity), while advancing prior measures. The key here is the easiness of accessibility and use/choice in managing information flow (that is, interface design that

---

[9] Also, note the high level of Cronbach alpha (.77) for the total items in all sampled sites combined. In other words, the reliability was further ensured across the individual measures as well as across the coders (Neuendorf, 2002).

supports informed choice) and how these two functionalities are embedded in the architecture of interface design (see Hargittai, 2002; Lessig, 2000; Trammell et al, 2006; Palmer et al, 2000).

Interface design for informed action/choice is indicated through HTML site features and links (e.g., Hargittai, 2001; 2002; Palmer et al, 2000; Trammell et al, 2006). Note that HTML text and its interactive characteristics are the most fundamental architectural codes of the Internet (Castells, 2006; Foot & Schneider, 2002; Hargittai, 2002; Stromer-Galley & Foot, 2002). In adopting these key natures of the Internet for privacy, this study operationalized the site attributes in terms of the two functionalities: (1) Inform and (2) Interact.

Inform

Five items were adopted from prior studies (as well as FTC FIP Guidelines) to operationalize the function of Inform. The items are to capture the interface design that informs users, i.e., how users are structured to get informed of data practices by websites. The following items were modified (or directly borrowed) from

- Turow (2001; 2003, Annenberg Policy Center)
- LaRose & Rifon (2006)
- Culnan (1998; 1999)
- FTC (1998; 1999; 2000; 2001)
- Hong et al (2004)
- West (2003)

(1) Presence of link to privacy statement in the front/home page
(1) 1. Presence of one clear policy statement in the policy page
(1) 2. Readability (i.e., accessibility of the statement)
(2) Placement: Link placed in a clear prominent place
(3) Font size & color: of privacy statement & link
(3) 1. Font style is different from adjacent words
(3) 2. Font size is larger than adjacent words
(4) Clearly labeled as 'Privacy Policy'
(5) The link has other features (italics; highlighted; underlined) that make it stand out

Interact

Five items were complied from prior studies (as well as the FTC FIP Guidelines) to operationalize the function of the Interact. The items are to capture the interface design that structures users in controlling data, i.e., how users are structured to exercise/control information flow. The following items were modified (or directly borrowed) from

- Palmer et al (2000)
- Culnan (1998; 1999)
- FTC (1998; 1999; 2000; 2001)
- Cai et al (2003)
- Kaaya (2005)
- Helling (1998)

(1) Privacy policy is linked from each page
(1) 1. Number of clicks to the privacy policy page
(2) Presence of out-links to any of third party sites
(2) 1. Privacy seal or Safe Harbor visible with a tagged link
(3) Active email link to review or request no data transfer
(3) 1. Link to file a complaint to the site manager
(4) Availability of downloadable document/form to request, correct, or confirm data use
(5) Link to privacy policies in third party sites associated

Here units of analysis are (1) links and (2) site features. The links function at the macro level to structure the traffic in/out of the site, while the individual features reside at the micro level organized within a page (e.g., Cockburn et al, 2003; Hong & Cody, 2002; Elmer, 2004; Lazar, et al, 2003; Trammell et al, 2006). The logic is that to include (or exclude) links and associate features, internally or externally, is to channel and direct users' attention/action (Hargittai, 2002; Stromer-Galley & Foot, 2002). For information privacy, this is to ask whether or not users are structurally conditioned to be able to rectify, protest, or monitor to control data flow, while easily informed of institutional practices (see Palmer, et al, 2000; Ribak & Turow, 2003).

	Function	
Indicators	Inform	Interact
Links		
Features		

(Each item developed from the FTC FIP principle of notice & choice)

Policy Ground
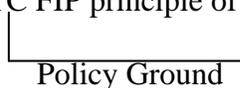
Figure 3-C. Summary

Note that this typology does *not* mean the function of each dimension in a linear manner. Neither is it to suggest the operation of user attention and behavior in dichotomous pattern. Here the logic of 'thin and thick' democracy may provide an analogy. That is, the interface embedded in architecture should be designed to encourage informed, interactive, and voluntary action by users. The key criterion is the transparent interface design against which to measure personal information control as experienced by typical users.

Analysis

For analysis, the comparison was made in the provision of data practices among the sites with different domain and site characteristics. The first line of comparison is between Group 1: The most popular sites vs. Group 2: The randomly selected sites (see FTC, 1998; 1999). Then, the second line of comparison proceeded, taking into account domain/site characteristics (see this analytic suggestion for Milne & Culnan, 2002; Palmer et al, 2000) in terms of Inform, Interact, and Combined.

For the first line of analysis, the analytical scheme is as follows:

	Top sites	Random sites	Combined
Inform			
Interact			

This constructed a series of 2 x 2 tables that were suitable for mean comparison. The nominal nature of content items entailed the Chi-square test. However, with the creation of the Index score on a continuous scale, multivariate regression (on site characteristics, such as seal membership; length of operation; traffic ranking; etc) was run for the second line of comparison (e.g., Palmer et al, 2000; also Miyazaki, & Krishnamurthy, 2002, for the precedent; Napoli & Yan, 2006, for television stations).

For this, the *digital transparency* Index was created. Second, the characteristics of individual sites were included to explain the function of commercial media institutions in Internet data practices. In the Index, the presence or absence of each content criterion, as indicated by links and features, was scored (0 = absence; 1 = presence) for addition in each dimension (Inform & Interact):

- The *digital transparency* Index =
    - Dimension 1: Inform Score = Item 1 + Item 2 + ….
    - Dimension 2: Interact Score = Item 1 + Item 2 + ….

Market & Site Factors

Table 3-1
Key Measures

Dependent variable	Independent variables
1. Digital Transparency Index	1. Type of domain (Milne & Culnan, 2002)
1.1 Inform Score	2. Traffic ranking (Hargittai, 1999)
1.2 Interact Score	3. Number of years in site operation (Palmer et al, 2002)
	4. Seal membership (LaRose & Rifon, 2006)
	5. Financial performance (Kane and Storey, 2005)

The IV measures (see Table above) are in line with prior literature. In specific, it is modeled upon the analytical models of broadcasting diversity (Napoli & Yan, 2007;

Yan & Park, forthcoming). In large, it is grounded upon the marketplace premise that

underpins the function of commercial media (Hamilton, 1997; Neuman, 1991). The aim

was to apply the understandings from the traditional media debates into the new media in

the provision of information control. Note the two levels in the IVs: (1) the market and (2)

the site factors. Here the market factors serve to measure whether the sites in a specific

domain, e.g., sensitive vs. non-sensitive, are in fact more inclined to provide protection in

information. The site factors were included to measure the influences of individual site

attributes, such as financial resources, in providing the incentives for further provision.

Milne and Culnan (2002) in fact urged for the inclusion of the market domain

factors in the assessment of the voluntary provision of the FIP, warranting the

investigation in this regard. Note the consistent reviews of commercial sites by the FTC

(1998; 1999; 2000) in determining the necessity of any policy intervention. For instance,

the poor provision of personal data control in the sites that operate in sensitive domains

(such as medical or financial) raises the normative policy concern, given the extent of

public concern (Ohm, 2009). On the other hand, the sites, with more resources as

indicated in revenues and traffic ranking (Kane and Storey, 2005; Hargittai, 1999; Napoli

& Yan, 2007; Napoli, 2004), may be more responsive to the demand from the public in

the marketplace. The number of years in site operation, in particular, may indicate the

successful brand establishment (Palmer et al, 2002). Here the logic follows that the

economic efficiency in the viable marketplace may or may *not* translate into the provision

of socially desirable objectives as in diversity (Napoli, 2000; 2004; Yan & Park,

forthcoming). A similar logic applies to the sites with the seal of which the membership

is certified according to the certain extent of the voluntary provision of the FIP (LaRose & Rifon, 2006).

Contribution

In sum, Part I 1 examined whether and to what extent users are (1) to be informed of data practices and (2) to exercise their rights to data control. Few studies (e.g., LaRose & Rifon, 2006) attempted to examine the association between websites and data practices in the commercial sector. This study contributes to update the previous findings with (1) focus on interface design, (2) a bigger sample size (with a different sampling logic), and (3) further analyses with the inclusion of site/domain characteristics.

Results
Description: the overall picture

Result 1:

Chi-Square Test

Table 2 and 3 present the extent to which commercial sites are designed for users in terms of discrete items in each dimension: (1) to get informed and (2) to be able to control. In Inform items, the mean comparison (2 x 2) showed no significant difference between the top and the random sites. The only item with the significant difference was IF3.2 (other features for clarity), with the more random sites in such provision. In text length, it was found that the texts in the top sites tended to be longer than that of the random sites. Furthermore, among the sealed sites, the random sampled sites were more likely to display seals in the front page than the top sites (8.9% vs. 3.4%). Note there were in fact the three items (colored in green) that more than 50% of both top and random sites voluntarily provided. When compared, however, the differences between random and top sites did *not* reach the significance level.

In the Interact items, the results were in sharp contrast (See Table 3). In most items, significant differences between the top and the random sites were found. Moreover, the differences were in favor of the top sites: that is, more top sites tended to score well in the provision of Interact items. The biggest difference (24.9%) was found in item IT9 (link to third parties associated), with 35.8% of the top sites in contrast to only 10.9% of the random sites. Nevertheless, it is most critical to note that the provision of most Interact items remained very low in the absolute sense despite the differences between the top and random sites. In fact, there were only the three items (colored in green), where more than 50% of both top and random sites voluntarily provided. In other words, while the top sites performed better in this dimension, the voluntary provision of most Interact items remained extremely low as indicated in the Table 3.

Table 3-2
Descriptive Statistics: Inform

	top	random	comb.
Inform	%	%	%
IF (1) presence of link to privacy statement in front page	89.9	86.7	87.9
IF (1) 1. presence of one clear policy statement	88.4	81.5	84.1
IF (1) 2. readability (accessibility of the statement)	18		12.27
IF (1) 2.1 text length	8614		1786.44
IF (1) 2.2 text font size	12		8.97
IF (2) placement: link placed in a clear prominent place	4.7	4.4	4.5
IF (2) 1. link placed in main menu	2.0	2.0	2.0
IF (3) font size & color of the link to privacy statement			
IF (3) 1.1 font size is different from adjacent words	7.1	2.9	4.5
IF (3) 1.2 font size is different from the main text	4.3	8.8	7.1
IF (3) 2.1 font color is different from adjacent words	6.4	8.8	7.9
IF (3) 2.2 font color is different from the main text	34.3	36.3	35.5
IF (4) clearly labeled as 'privacy policy'	77.9	70.8	73.4

	top	random	comb.
IF (4) 1. other clarity in labeling	5.0	3.8	4.2
IF (5) the link has other features (italics; highlighted; underlined) that make it stand out	31.4	45.4*	40.3

Table 3-3

Descriptive Statistics: Interact

	top	random	comb.
Interact	%	%	%
IT (1) privacy policy is linked from each page	87.2	82.7	84.4
IT (1) 1. number of clicks to the privacy policy page	2.12*	1.93	2
IT (1) 2. others: privacy blog, discussion lists, etc	14.9**	4.5	8.4
IT (2) safe harbor or privacy seal visible with a tagged link[10]	23.0*	12.6	16.5
IT (3) active email link to make inquiries	62.2	54.3	57.2
IT (3) 1. out-links to complain or make inquires (e.g., FTC)	19.6**	7.7	12.2
IT (4) availability of downloadable form to request, correct, or confirm data uses	16.9	17.8	17.5
IT (4) 1. edit function, e.g., preferences or profile	39.2**	17.8	25.8
IT (4) 2. p3p embedded	83.1*	74.5	77.7
IT (4) 3. click to opt out from the site	26.0**	10.0	16.0
IT (5) link to privacy policies in third party sites associated (e.g., opt out from NIA)[11]	35.8**	10.9	20.3
IT (5) 1. number of clicks away	2.21**	1.41	1.71

Note: * Significant at .05 level; ** Significant at .01 level.

IF = Inform items
IT = Interact items

In both dimensions, the sub-items were included to further measure the subtlety of

each dimension. These are the variants of the main items presented in Coding Instrument

---

[10] Note the distinction between IF and IT is arbitrary to a certain extent. For instance, IT (2) could be categorized as IF given its function. Nevertheless, the main distinction, again, could be established because IT (2) is in essence to measure how the channel for interacting with external sites is embedded within the site.

[11] A similar note can be made for IT (5) in that it not only carries users to the policies of other sites, but also provides users with the function to interact, e.g., opt out, with associated sites.

(see p. 26). The added items could be understood as discrete units within each main

factor. In the IF (Inform) items (see Table 2), these are IF (1) 2.1: IF (1) 2.2 in the factor

of the policy presentation; IF (2) 1. in the factor of the link prominence; IF (4) 1. in the

factor of the link labeling. In the IT (Interact) items (see Table 3), these are IT (1) 2 in the

factor of the interaction within the site; IT (4) 1: IT (4) 2: IT (4) 3 in the factor of the data

management to the site.

Result 2:

Regression Test

      The OLS multivariate regression was run in the combined samples. This served

two purposes. First, it allowed the incorporation of diverse IVs in explaining institutional

practices beyond the simple contrast between top and random sites, i.e., how the

marketplace determinants in a commercial sector influence the provision of information

control. Second, the large variance of the DV Index (SD = 4.54), with each dimension

(Inform + Interact Index), enabled the observation of the depth and the breadth of such

provision that the single item can *not* capture. Table 3 presents Index scores (Cronbach

alpha = .77 for the IF; .58 for the IT) among the sample of 398 commercial sites (240

random + 148 top sites).

Table 3-4
Transparency Index

Variables	Range	Mean	SD
IF index	0-14	6.51	3.09
IT index	0-10	3.53	1.83
Transparency Index	0-24	11.59	4.54

Table 6 presents the results from OLS regression analyses. In terms of the IF, the regression coefficients indicated no significant impact of market factors. Further, none of the site factors (see Table 4, for the IVs) had any effect on the IF index. In terms of the IT, there was a positive significant impact of MIV 2.1. Also, SIV2, SIV3, & SIV5 were found positive on the IT with the biggest contribution from SIV4. When combined, however, the significance was *not* found except with respect to SIV4. Here, however, note that the impact of SIV4 should *not* be over-interpreted. In fact, the function of the IT is to be understood in the continuum of the IF. In other words, it seems less meaningful to have the full IT when its elements were deeply embedded (i.e., hard to locate) within the site – to begin with[12]. The full model, as a whole, only contributed to .10 (SE = 2.81). This result remained robust as the truncated model, with no high provision item, providing almost the identical results (F = 2.53*). That is, even when taking into account the most common items in either dimension, both market and site factors had limited contributions.

---

[12] Note the similar results of SIV 3 with its significant impact in the IT dimension disappearing in the Full Model. That is, very few indicated the operation of marketplace incentive in the provision of socially desirable objective such as the FIP.

Table 3-5
Independent Variables

Variables	Definitions	Mean	SD
Market Factors	type of domain		
MIV 1: online alone	whether the site operation is confined online	.63	.48
MIV 2: ecommerce	ecommerce sites	.30	.46
MIV 3: new media	search engine or directory sites	.10	.29
MIV 4: sensitive	whether a site deals with sensitive data such as health or financial information	.08	.26
MIV 5: family/teen	whether a site is targeted toward children, teenagers, or younger users (such as game sites)	.08	.27
Site Factors	characteristics of an individual site		
SIV 1: revenue	annual site revenues in 2008	9.30E+09	32496766
SIV 1.1: public	the site (or its parent company) in public stock market	.30	.46
SIV 2: ranking	traffic ranking in September 2008	56978.3	302953.7
SIV 3: years	number of years of operation	1997.7	3.50
SIV 4: seal member	whether a site is a member of Truste, BBBonline, or Safe Harbor		
SIV 5: US percent	percent of US users	62.38	26.38

Table 3-6

Results: OLS Regression Analysis

	Full Model	Each Dimension	
	IF + IT	IF	IT
Market Factors			
MIV 1: online alone	.05 (.61)	.04 (.56)	.03 (.44)
MIV 2: ecommerce	-.01 (-.19)	.03 (.44)	-.10 (-1.74)
MIV 3: new media	.06 (.77)	.00 (.01)	.12* (2.32)
MIV 4: sensitive	.06 (.89)	.08 (1.19)	.00 (.01)
MIV 5: family/teen	.07 (1.08)	.07 (1.10)	.02 (.41)
Site Factors			
SIV 1: revenue	-.01 (-.13)	-.06 (-.91)	.07 (1.32)
SIV 2: ranking	-.02 (-.31)	.04 (.63)	-.12* (-2.14)
SIV 3: years	-.13# (-1.70)	-.06 (-.79)	-.17** (-2.77)
SIV 4: seal member	.23** (3.43)	-.00 (-.07)	.49** (8.95)
SIV 5: US percent[13]	-.01 (-.13)	.06 (.81)	-.13* (-2.15)

Note: # Significant at .10 level; * Significant at .05 level; ** Significant at .01 level.

IF = Inform Index
IT = Interact Index

Note that in none of the models the level of tolerance for multi-collinearity was above .5 in the measure of VIF. Also, the correlations among the IVs were *never* found prohibitively high. Furthermore, it was important to point out that the variances of the DVs (Indexes) were relatively large, with the large sample size (n = 398). Given the limits of the secondary data, alternative IV, whenever available, were employed in a

---

[13] The inclusion of this variable was to measure (1) whether the site mainly targets the US user market and (2) if the site operation is under the purview of the FTC.

separate model. For instance, the variable of 'public vs. private' (parent companies in public listing or not) was used instead of revenues (of which the data reliability is questionable, given its extremely wide SD). Yet the OLS results remained more or less the same. These all indicate that the non-effect of both market and site factors on the voluntary provision of information control (in the core aspects of the FIP) were the result of robust statistical tests.

Discussion

Summary: Inform + Interact

The main findings are two fold. First, the limited extent to which the channel for information control (inform + interact) was embedded in the interface of commercial sites was found. Second, the chi-square tests showed that while for the IT dimension the top sites performed better, there was no critical difference between the top and the random in most IF items. The regression analyses reinforce these results in the combined samples, with the market and site factors taken into account. This result is in particular significant in that it provides the empirical evidence that assesses the operation of the marketplace incentive in providing the data control for users. The full utilization of the architectural potential is far from being practiced. Put differently, most users in a majority of the commercial sites are situated to exercise personal information control only in limited contexts, i.e., usability, while being unable to get informed, i.e., accessibility, of the data practices.

Overall, what the findings indicate is:

(1) the potential of informed action, as through HTML site features/links, is

curtailed in interface design with its distortion far manifested in IF dimension

(2) commercial incentives in marketplace alone are *not* sufficient in the provision

of personal information control

Comparison: Zone by Zone

In this light, the particular concern is the poor design in the sites that are

family/teen oriented and sensitive data driven, e.g., medical or financial sites. Note that

there were no significant differences in those sites in regard to the voluntary provision of

personal information control. As LaRose (2003) pointed out, this carries significant

weight in terms of the safety of the commercial net in its blood stream. An analogy to city

zone may work here. For example, it may be that school zone, where the certain speed

limits are expected, is by de facto inoperative online. This is to point out the problem in

specific sectors of which the potential misuse of data may have tangible consequences: (1)

for the younger users in their heavy online time spending and (2) for the users who may

well expect privacy, given the sensitive nature of the personal data identified (Ohm,

2009). In addition, the greater potential of data mining in these sectors (in interconnection

with offline industries, see Dana & Gandy, 2002) is alarming with the institutional

interface design far from being transparent in each and the combined dimension.

Comparison: the Past vs. the Present

In fact, the regression results came into further light, when temporally compared

to those in prior studies (see Appendix D, for the item comparison). Few equivalent

measures among the studies based on different samples make it hard to compare the

findings in a direct sense. However, whether and to what extent the core aspects of the

FIP had been implemented can be inferred within the broad parameters. Here what

remains clear is that no clear improvement was made in the commercial spheres since

1998 when the first web sweep by the FTC was undertaken. In 1998, for instance, the main spirit of *Notice*, as indicated in the prominent placement, remained more or less the same in 2008 with only 4.7% of the top sites in such provision. Also, no apparent improvement of readability had been found in the policy statement since 1999 (e.g., Culnan & Milan, 2000).

There were some improvements in the Interact dimension. For instance, the provision of active email link increased from 53% in 2003 to 57.2% in 2008. However, it should be noted that today the commercial data collection has become far more overarching. Also it should be in the overall context in which users are structured to get poorly informed. Besides, it is premature to conclude dramatic changes in commercial sites with no equivalent base that captures precise longitudinal site trends. Perhaps, the analogy is powerful in the traditional diversity debate in which Low Common Denominator (LCD) is entrenched in the commercial broadcasting sector (Hamilton, 2003; Neuman, 1991). The model may well apply here to explain 'the apparent race to the bottom' (PI, 2007) – Low Common Denominator in the provision of information control for users in the curtailment of the technological potential.

the commercial Yahoo IP launched: 1995

the first FTC web sweep:1998   **sensitive** domain

2000

non sensitive domain   2003

Michigan Study by Park: 2008
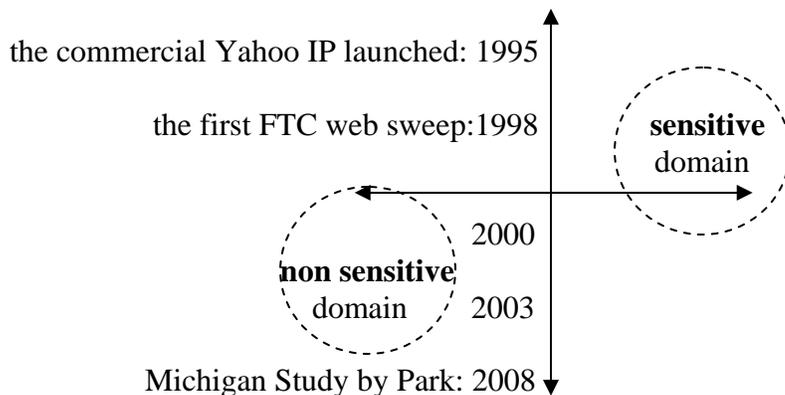
x = domain type
y = year

Figure 3-D. Comparison: time & zone

Policy Implications
Inform + Interact:

The policy implications of the findings are as follows. First, on the surface, what

was found is the low voluntary observance of the FIP (in its core aspects) in terms of

'*how*', that is, the actual implementation in the interface. Second, on the deeper level, this

indicates the invalidity of the current FTC regime under which the institutional practices

are being embedded. It is important that in this study the very emphasis was placed on the

design of the actual interface for informed action. The central logic was to measure how

it is implemented as opposed to what is written in the policy statement. In this sense, the

contribution of this study is far more direct than those in most previous endeavors[14]. The

most problematic assumption in prior studies (that served as evidence for the FTC

decision making) was that personal privacy control was enabled in architectural interface

as written in the policy statement. In sum, in institutional practices, this study found that

the potential of the empowerment as indicated in interface design is being curtailed in

---

[14] This may be one of the reasons the rates of the voluntary provision in the previous studies are higher
than the ones in this content analysis.

marketplace incentive alone. This is *not* to bluntly criticize the marketplace ideal; rather,

to point out the function of commercial entities that may well be at odds with the very

policy rationale.

Chapter 4: Individuals: Privacy & Literacy Online: The Survey of Public Awareness

Empowering Personal Privacy:

Individual Users
The individual user culture for the empowerment in the control of personal information

Chapter 4 examines the empowering condition at the cultural level. On the theoretical level, this is to explore how users shape/respond to the potential of the empowerment in information control at the cultural level. The central question is: whether and to what extent does user knowledge function as an enabler for information control within the structure of the commercial web-sphere? Chapter 4 proceeds in the two studies in interconnection: (1) the relationship between knowledge and action in managing information flow and (2) the function of knowledge in fixing the 'mass paradox' in the Internet, i.e., the incongruence between the privacy concern and users' inaction in managing their privacy rights (e.g., Acquisti & Grosslags, 2005). On the policy level, this is to identify the presence of digital divide that may be prevalent among the public with the growing level of privacy concern (see Orwellian fear over the potential abuse of personal data, p.4 in the Intro Chapter). On the deeper level, it is to challenge the validity of the FTC self-regulatory regime that is grounded upon the monolithic user assumption. In short, Chapter 4 is about the cultural shaping of information control by the users in the Internet.
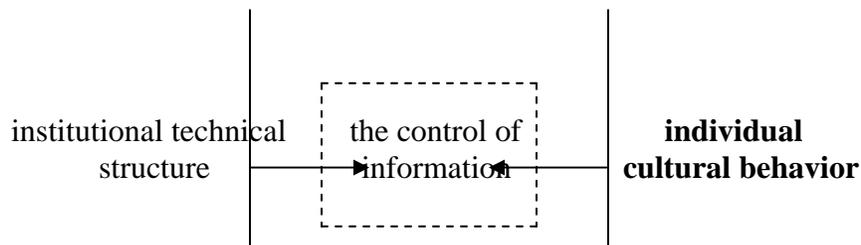
Figure 4-A. Empowerment

Framework
Digital Literacy

Literacy is one of the most fundamental human conditions in diffusing democratic

potentials (Inglehart & Welzel, 2005; Pool, 1983). Neuman (1991) also noted the

centrality of literacy in promoting participatory orientation for the development of a

viable civic culture. Note the effect of the printing press. It was *not* until after the

diffusion of mass literacy that democracy became actualized in Western Europe

(Huntington, 1996). Here the notion of 'digital literacy' takes the democratizing power of

literacy to the digital age. The term describes individuals' actual knowledge regarding

computer-related functions (Bunz, 2004; Dutton & Anderson, 1989). According to

Hargittai (2003; 2006), the divide in digital literacy impairs democratic potentials as most

political and civic activities move toward online. In this sense, it is crucial to identify

digital divides at the user levels, i.e., what distinguishes differentiated uses. That is,

individual differences in cognitive ability may explain different types of digital media use

(Hargittai, 2002).

Note the two types of media behavior: (1) habitual and (2) systematic (MacKuen,

et al., 2007; Neuman, 1991; see Petty & Cacioppo, 1996). In fact, there are the two basic

behavioral strategies to which ordinary users may resort. While careful considerations

and efforts mark systematic uses, habitual behaviors take quick/heuristic routes of

comfort, entrenched in daily routines (see Bourdieu, 1984; Neuman et al., 2007). The

logic is similar to the counter-force of mass psychology embedded in inherited cultural

habits of passive half-attentive media use. Here, then, digital literacy may open up mass

psychology by enabling individuals to control media channels to citizens' interests. This

is to identify the conditions in which inattentive human habits can turn into the practices

of active citizenry. In short, if the Internet has the empowering potential, individual

capabilities of using it may well diffuse democratic possibilities.

Digital Literacy (i.e., knowledge)

| Habitual | vs. | Systematic |
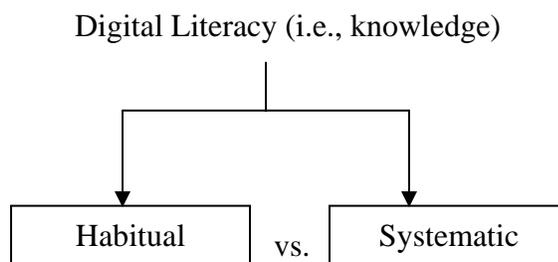
Figure 4-B. The function of knowledge

Chapter 4 proposes the notion of digital *privacy* literacy. Goffman's premise

provides a point of departure. Goffman (1959) noted that individuals should be able to

manage or control private/public boundaries by selectively revealing one's identity (also

Agre, 1998; Bellotti & Samarajiva, 1998). Note the critical role of understanding

tacit/implicit codes in operation. That is, awarenesses of institutional practices and

systems may equip individuals before being able to take appropriate actions. The idea

encompasses critical understandings of data flow and its implicit rules, for users to be

able to act upon it. Here it can be argued the operation of different user habitats within

the premise of Goffman. Literacy may well serve as a principle that is likely to support,

encourage, and empower users for informed choice and action. In short, in order to
exercise appropriate measures of resistance against the potential abuse of personal data,
users should be able to understand data flow in cyberspace and its acceptable limits of
exposure (Ball & Webster, 2003).

Active vs. Passive

Here the systematic behavior indicates careful information control in the Internet.
The habitual uses, on the other hand, mean reckless user behavior in the release of
personal information in the Internet[15]. In more general terms, the distinction between the
active and passive audiences/users may work (e.g., Williams, 2004). That is, while the
passive users reside in the convenient daily habitats of inaction, the active users control
information in the full engagement with the potential of the empowerment in the Internet.
Note these are *not* mutually exclusive categories; rather, the constitutive ones while
residing in the continuum of information control behavior in daily Internet uses.
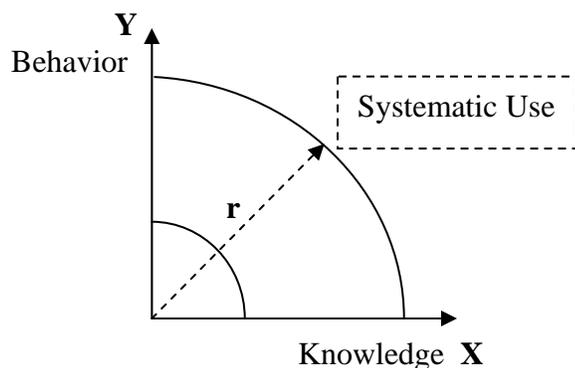
Figure 4-C. Correlation between knowledge and behavior

---

[15] In actuality, it could be that some users are habitually engaged in systematic information control.
However, the distinction between the two, i.e., habitual and systematic, is conceptually defined. Also,
the use of the term 'habitual' is to indicate the general tendency that most users rarely exercise control
in daily routines.

Prior Studies
The Centrality of Knowledge

A consistent research agenda puts forth the relationship between cognitive skills and use in the context of Internet privacy. First, on the policy ground, the FTC posited the individual understandings as a primary operational principle. Second, on the research ground, user knowledge is suggested as fundamental to the ability of individuals to assert the control of their personal information (Hoffman et al, 1999; Turow, 2003; 2005). In sum, the premise is this: the interactive nature of the Internet migrates the control to the end users in managing information flow, with its potential further empowered with the increased level of knowledge (see Barnes, 2006; Freese et al, 2006).

Nevertheless, little evidence was gathered in the context of Internet privacy, while most studies had focused on the identification of the trend of the public concern (e.g., Westin, 2002; 2003). Plus, the paucity of empirical studies makes it hard to draw any conclusive linkage between knowledge and uses. Besides, most studies paid less attention to the interactive nature of the Internet and the potential empowerment in its purposive uses. Enhancing the accounts of (1) knowledge and (2) information control and the investigation into (3) its posited association between the two will be warranted.

Earlier Efforts

In this vein, few studies attempted to identify the extent of public knowledge. Earlier works include: (1) Nowak and Phelps (1997); (2) Culnan (1995); and (3) Milne and Rohm (2000). Later works, in explicit discussions of the Internet privacy, are: (1) Graeff and Harmon (2002) and (2) Dommeyer and Gross (2006). Central in these efforts is the posited function of knowledge in exercising information control. For example, Culnan (1995) observed the low level of awareness among US consumers regarding the

removal from mailing lists. Milne and Rome (2000) also found the lack of procedural knowledge of name removal despite the fact that most respondents indicated their intention to 'opt out' with the appropriate knowledge. Even earlier, the finding by Nowak and Phelps (1997) indicated the wide uncertainties and misinformation prevalent among consumers about the practices of direct mail marketers.

In the Internet/digital era, the practices by database marketers came to the forefront of the scholarly and policy concern. In fact, the research efforts were sharpened to observe the consequences of knowledge with an updated account. Dommyer and Gross (2003), for instance, found the association between the level of awareness of privacy protection strategies and 'opt out' status from the telephone directory. Patterson et al (1997) also suggested the explicit connection between demographic variables and the level of knowledge. The Pew Survey (2000; 2005) also attempted to measure Internet users' knowledge in different segments of the online population – with its general finding (the low level of public knowledge) confirmed in the Berkeley research (EPIC, 2006). The main empirical finding that emerged includes:

1. Finding: the low level of public awareness of 'cookies' (Fox, 2000)

2. Finding: the lack of procedural knowledge in 'opting out' (Culnan, 1995)

Nevertheless, the empirical studies that explicitly examined the relationship between measured cognitive ability and variations of uses remain rare, if *not* anecdotal. Milnan and Culnan (2002) in fact found that the user awareness of fair procedural practices in the websites alleviated the level of privacy concern. A study by Hoffman et al (1999) also indicated that users, when explicitly aware of malpractices by sites, tend *not* to disclose information. These findings are significant in that they illustrate the presence

of the dichotomy between the stated concern and behaviors (e.g., Park, 2008; Sheehan &

Hoy, 1998) as potentially moderated through the function of knowledge. Note, however,

the findings are limited in effect size and statistical significance. Furthermore, the single

item measure based on the familiarity with the term cookies was used as a proxy variable

that assessed user knowledge (e.g., Pew, 2000). Different measurement scales based on

convenience samples (e.g., Hargittai, 2007) further makes it hard to generalize the

findings in a specific causal directionality.

Advanced Research

In a series of carefully designed surveys, Turow et al (2003; 2005) advanced this

line of research. What Turow contributed is the sophistication of the measures that

observed users' understandings of data practices by websites. In 2003, the first national

sample survey found two alarming facts: (1) the wide ignorance among users regarding

the fundamental aspects of data flow and (2) the lack of protective steps taken on the part

of users. According to Turow (2001; 2003), this is particularly startling in that the

cognitive power of the user remains limited in contrast with advanced institutional

surveillance techniques. In the second survey in 2005, these findings were generally

confirmed. Knowledge items further included (1) policy and (2) technical aspects of the

online/offline data flow. The survey proceeded in the construction of a true-false scale.

Some respondents reported the falsification of information when they were explicitly

aware of data surveillance. However, most consumers misunderstood the mere presence

of policy as data protection, vulnerable to commercial exploitations (also Harris

Interactive, 1996; 1998). The study was advanced to identify the significant association

between demographic characteristics, such as education and race, and the lack of

knowledge, attesting to the presence of a 'knowledge gap' among users of different

populations.

Acquisti (2004) further advanced the discussion into the general population as

well as Internet users. His survey assessed the level of factual knowledge, as indicated by

privacy risks and modes of information protection. The findings are similar to those of

Turow et al (2003; 2005): Most consumers are unaware of institutional data practices and

associated risks. Furthermore, among the respondents, the levels of protective skills were

found limited, despite the fact that most consumers *did* adopt one or two strategizing

behaviors (also LaRose et al, 2004; Metzger, 2004). Acquisti et al (2005) expanded this

line of research into a combined but interactive environment of a social networking site.

In the Facebook study, he found that most FB members were hardly aware of inside data

collection rules, regardless of different levels of concern. Some were found to manage

their privacy. Yet again, this happened with limited (or misinformed) awareness of the

visibility of their personal data. The finding is important in that it casts a possible linkage

between the low level of knowledge and the low level of data management even in a

highly interactive setting.

Premise 1: Knowledge & Action

A Line of Further Research
Missing Gaps

Note that the studies by Turow (2003; 2005) posited users' knowledge and uses in

a broad context of social differentiation, while Acquisti (2004; 2005) attempted to

analyze this as information processing at the individual level. Combined, both works

contributed to understand the mechanism of the decision-making process in terms of

Internet privacy strategizing behaviors. In short, the lack of knowledge over the extent of

data flow is either explicitly or implicitly posited as a hindrance in the complex decision making process. To put it differently, the engagement itself is assumed to be the function of knowledge to an extent. In essence, the fundamental question remains the same: While unaware of the data flow behind the screens, users are unable to engage in active control/participation (see Westin, 2002, for this explicit assumption).

Nevertheless, the prior studies failed to identify the consistent role of knowledge on empirical ground. First, methodologically, the knowledge items in most studies were limited in one-dimensional measure, if *not* single items (e.g., Culnan, 1995; Acquisti & Grosslags, 2005; Hargittai, 2007). Second, analytically, the relationship between knowledge and differentiated uses and control were *never* explicitly tested as in multivariate regression, despite the posited function of knowledge in the decision-making process (e.g., Acquisti & Grosslags, 2005; Acquisti et al, 2006; Turow, 2003; 2005). Third, drawing from the strategic marketing literature, any consistent theoretical basis that explains the linkage between knowledge and behavior was *rarely* developed (e.g., Culnan, 1998; Culnan & Milnan, 2001; Hoffman et al, 1999; Turow, 2003; 2005). This is *not* to disregard the significant contribution from the prior research. Rather, it is to identify the missing gaps that the proposed research aims to fill in an updated account.
Proposition

This study sets forth to test the explicit premise of digital literacy as applied to the case of Internet privacy. This is to identify the function of knowledge in strategizing behaviors. In general, it is posited that critical understanding is required of citizens to participate in digital activities (Hargittai, 2002; 2003; Jenkins, 2006; Van Dijk, 2005). In specific, it follows that the more users are knowledgeable about data flow, the more

equipped they are to act to manage to their control (see Barnes, 2006; Hargittai, 2007, Turow, 2005, for this suggestion). Conversely, the less aware users are, the more they are susceptible to manipulation, unable to act and control information flow to their interest.

Premise 2.1: Privacy Paradox

Public Concern
The Interaction Between Concern & Knowledge

However, the posited relationship between knowledge and behavior is a simplified picture, *not* taking into account the motivation behind personal information control. This is the question about the fundamental impulse behind user behavior. That is, if the users are *not* concerned about online privacy, why are they expected to actively act at all even with certain levels of knowledge?

Knowledge

Premise 1. Action

Premise 2. Concern/Motive
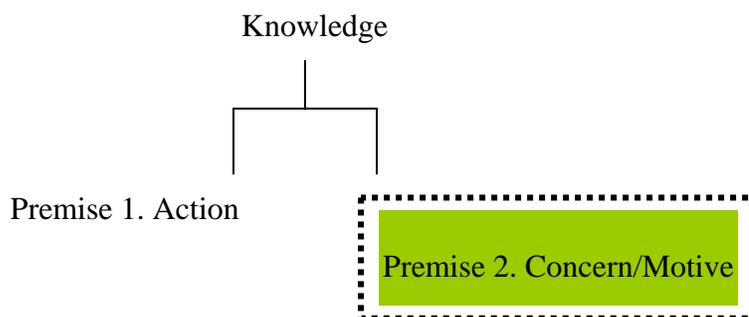
Figure4- D. Concern & knowledge

Proposition

In fact, there are consistent research findings (e.g., Acquisti, 2004; Acquisti & Gross, 2005; LaRose & Rifon, 2007; Park, 2008; Turow et al, 2003; Ribak & Turow, 2003) that indicated the incongruence between the stated privacy concern and behavior. Here this study proposes the function of knowledge in filling in the apparent dichotomy between the privacy concern and the actual behavior. That is, if the knowledge has any

explanatory power at all, it follows that the level of concern motivates informed users to

control data. To state it differently, it is posited that the knowledge may open up mass

behavior from those who remain perplexed, confused, or at a loss despite certain levels of

privacy concern in daily routines. In short, what is proposed here is the rival hypothesis

that it is the knowledge, rather than the concern alone that functions as an impediment to

active control in the full engagement with the potential of the empowerment in the

Internet.

X 2 Knowledge

X 1 Motive ⟶ **Y** Action

Concern   Information Control
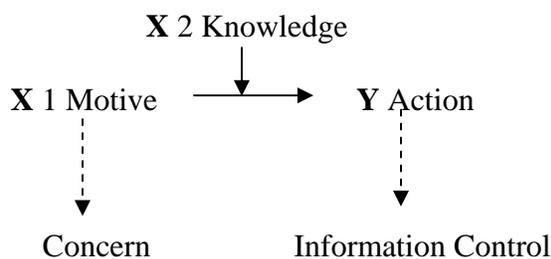
Figure 4-E. The moderating role of knowledge

Note the foundation based on which this strategic logic is formulated. First, it is

the public policy (FTC) premise that knowledge is in accordance with the level of privacy

concern to empower the public to engage in protective behavior (Danna & Gandy, 2004).

Second, in the tradition of human rationality, the general literature on cognitive ability

consistently suggested the role of knowledge in fixing the incongruence between attitudes

and behavior (e.g., Ajzen, 1991; Dietrichson, 2001; Fishbein & Ajzen, 1975; Lazonder et

al, 2000; Thomas et al, 2007). Then, it should hold true that among those who are

concerned, any systematic difference is further present between those who are literate and

non-literate in particular uses of the Internet (see Hargittai, 2007). That is, the informed

users are equipped to manage data flow to their interest – with this posited relationship

particularly manifest among those who are concerned.
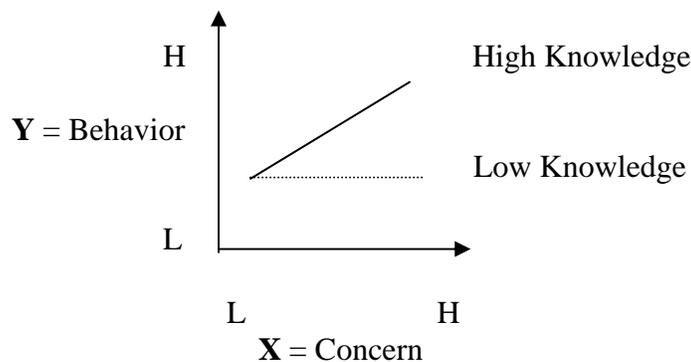
Figure 4-F. Hypothesized Interaction

Premise 2.2: Privacy Paradox

Convenience
The Three-Way Interaction between Concern, Convenience, & Knowledge

In explaining the operation of the privacy paradox, however, willingness to trade

off personal information for convenience (e.g., financial gains such as free access or

coupon) should be further specified (Acquisti, 2004; Craincross, 2000; Sheehan, 1999;

Westin, 2001). The cost-benefit analysis by individual users is in fact a plausible

explanation for the dichotomy between concern and behavior, i.e., while many Internet

users express privacy concern, most are willing to trade off their concern for immediate

benefits or gratifications (Acquisti & Grossklags, 2005; Acquisti, 2004; Sheehan & Hoy,

1998). This is to note the alternative model in which the possible role of convenience in

curtailing highly attentive new media uses and information control.

Empirical Findings

Nevertheless, caution is needed as empirical findings are mixed. On the one hand, the school of 'economics of behavior' posits the operation of 'bounded rationality'. That is, human behavior is *not* constantly optimal, but only in limited conditions. The school reasons that perfect rational decisions are often infeasible with the cost of gathering and processing information in complex situations (see Simon, 1984). However, an experiment by Metzger (2007) found that most subjects *do* strategize to protect their identities despite their willingness to trade basic demographic data for short-term benefits (also Acquisti & Grossklags, 2005; Sheehan, 1999). Turow (2005) also reported that only 16% of the respondents said they are willing to give up personal data for instant satisfaction. In a Georgia Tech University survey (2002), a majority of respondents (72%) indicated that they in fact prefer privacy protection to short term economic benefits, while expressing the policy preference for stronger government regulations (also Acquisti, 2006)[16].

Here it is critical to note that the willingness to provide information to a website is situation-specific. Most disclosure is often limited in generic demographic information (e.g., gender or age). Metzger (2006) in fact found that most users tended to withhold sensitive information, such as medical or shopping history, when asked upon registration (Ackerman et al, 1999; also Phelps et al, 2000). Also, Internet users, when explicitly informed of the likely transfer for purposes other than the original collection, refused to register or provided fictitious information (see Culnan, 1998; Metzger, 2007; Ribak & Turow, 2003). In other words, it remains still uncertain/an empirical question to ask

---

[16] Here for the inflated responses, the self-report nature of the survey should be considered. However, Metzger's finding was based on an experiment. Also, the finding of this Michigan survey validates the high percentage of the public who at least in rational assessment favors privacy over short term benefit (see the result in premise 2.2a).

whether and to what extent most Internet users tend to strategize the release of sensitive types of information in a trajectory of daily routines.

Concern, Convenience, & Knowledge
Further Integration

This study proposes the integrated model of the three-way interactions (see Kwak, 1999; Kwak & Campbell, 2009). Here the convenience (i.e., cost/benefit calculation from the release of data) is moderated through the level of knowledge, while this too may differ according to the level of concern. What is central in this complex relationship is the critical role of knowledge, that is, while information control may be the function of perceived cost/benefit from the part of the user, the operation of this calculation further depends upon knowledge, i.e., how much users are aware of contextual information/associated risks.

Bounded Rationality, Reconsidered

Note the assumption behind 'bounded rationality'. That is, human action is only partly rational or perhaps mostly habitual; yet in the remaining part of their actions rationality may well still function. Simply put, it is *not* necessary to reject or accept the entire premise of rational choice tradition. Rather, to be incorporated is the process of the interplay between habitual and systematic variables because user action is situated somewhere in between being 'active and passive' (e.g., Neuman, 1991) – that is, an alternative to the full rationality model. Acquisti (2006) himself noted:

> Constraints on the information-processing capacities of the individuals or entities can be incorporated in various ways: (i) by introducing risk and uncertainty into demand and/or cost functions. (p. 9)

In sum, a user's action, i.e., the posited engagement with the interactive potential of the Internet in controlling one's identities, may result from the complex mix of:

1. <u>Knowledge</u>: how much a user knows about institutional data practices

2. <u>Convenience</u>: whether a user perceives cost or benefit from revealing sensitive or non-sensitive data for financial compensation

3. <u>Concern</u>: how much a user is concerned about Internet privacy

Here it is possible to conceive different causal directionalities (see Appendix F, for discussion). However, the critical point is that passive and half-attentive uses, i.e., succumbed to *convenient* habitats, constrain the interactive potential of the Internet. Subsequently, more knowledge, when further activated/sensitized, is likely to produce more engaged or active uses of the Internet in information control (despite the use of heuristics to make decisions under most circumstances). That is, when equipped with knowledge, the users should be able to evaluate the situation more systematically, e.g., when to act to control or not.

Research Question

RQ 1: To what extent are the users concerned about institutional data practices?

RQ 2: To what extent are the users aware of institutional data practices?

RQ 3: To what extent are the users inclined to trust/distrust the institutional use of data?

RQ 4: To what extent do the users value convenience over privacy online?

RQ 5: To what extent do the users exercise data control regarding one's identities?

RQ 6: To what extent are the users motivated to decouple privacy concern from privacy behavior? [17]

---

[17] This is to investigate the rival hypothesis that the level of knowledge explains public inaction in information control. Put differently, the investigation is culminated to solve the privacy paradox.

Hypotheses

Premise 1

H 1:   There will be a positive association between knowledge and information control behavior.

H 1.1:   The level of knowledge will be positively associated with the level of information control.

Premise 2.1

H 2.1:   There will be an interaction between the levels of privacy concern and knowledge.

H 2.1.1:   Among those who are concerned, the users with a high level of knowledge are more likely to exercise information control than those with a low level of knowledge.

Premise 2.2

H 2.2:   There will be three-way interactions between concern, convenience, and knowledge.

H 2.2.1:   The positive interaction between convenience and knowledge will be stronger among those who are concerned than those who are *not*.

Method

The Study Population

Description:
Sample Characteristics

The sample is a national probability sample of adult Internet users (18 and up).

The Knowledge Networks recruited the panel respondents, using random digit dialing

(RDD). The panel participants were asked to complete an online survey, which took

about 13 minutes for completion. In order to improve response, an email reminder was

sent to non-respondents after three days. The data were collected between October 31 and November 12, 2008. The cross sectional data included only adult Internet users who had Internet access at home, eliminating the Web-TV based KN panel participants.

The demographic characteristics of the KN panel are *not* far different from those of the general population. However, the exclusive Internet user panel included the subjects who are younger, more ethnically homogeneous, and more educated than the profile of the general population (see US Census ASC). For instance, the level of education was higher, with 72.2% of the respondents having some college education. There were more white respondents (81%) in the sample than in the general population. The total sample size was 456 with the completion rate of 69% (456 interviews completed among 663 contacted). Although the 456 interviews were completed, the final dataset was limited to 425 after the item check[18].

---

[18] Following Hargittai (2008), a bogus knowledge item was included to check the validity of the response. A total of 31 people reported a high level of familiarity with this item. Furthermore, these respondents reported extremely inflated scores in other key variables (knowledge, behavior, & attitudes), challenging the validity of the responses by this particular group (see Hargittai, 2008).

Table 4-1
Sample Characteristics

Gender	
Female = 0	48.7%
Race/Ethnicity	
White = 1	81.2%
Education	
Less than high school	5.2%
High school	22.6%
Some college	33.6%
Bachelor's degree or higher	38.6%
Age	
Group 1: 18-29	18.7%
Group 2: 30-44	37.2%
Group 3: 45-59	37.6%
Group 4: 60+	4.5%
Income	
Less than $5,000 – Up to $175,000	12.7
(19 categories)	(3.59)
Parental Status	
Children under 18 = 1	30.1%
Employment	
Job = 1	62.8%

Internet Experiences

Table 2 displays that the Internet is much of the panel's daily lives. On average,

the respondents reported that they spend 4.84 hours surfing per day. Also, the medium

number of the Internet experience was 10 years, indicating the early adoption of the

Internet among the participants. Yet the relatively big SD (4.43) also showed the wide

variance of Internet experience in this regard. More than half of the participants reported

that they have at least 2 or more Internet access locations. Furthermore, only 8.5% said

they rely on the dial up connection, while most have broadband Internet access.

Table 4-2
Internet Use Experiences

	Mean	SD	
Number of Internet Use: Year	11.09	4.43	
Number of Internet Use: Daily (Minutes)	290.96	297.27	
Number of Internet Access	2.28	1.30	
Type of Internet Connection	8.5%	37.7%	35.3%
	(dial up)	(cable)	(DSL)

Measures

Behavior
Systematic Information Control

One of the main purposes in this study is to identify information control behavior as currently operated in daily routine. Information control was operationalized as user behavior in strategizing information release – that is, to opt out or not. Here, central is to capture how users systematically manage/control personal data and its flow (that can be associated with one's identity) (Culnan, 2000). Note that personal information control is 'multifaceted' in nature (Acquisti, 2005), requiring the combination of social and technical skills as intertwined in Internet uses (see Putnam, 2004; Hargittai, 2007; Resnick, 2007, for 'socio-technical' capital). This study elaborated pre-existing survey items into (1) socio and (2) technical dimensions (Marx, 2003; Metzger, 2007; Rifon et al, 2005).

Each survey item was modified from the extant literature (e.g., Aquisti, 2005; 2006; Culnan, 1993; LaRose, 2005; Marx, 2003; Metzger, 2007; Pew Internet, 2005; Turow, 2003; 2005; Turow & Hennesy, 2007). Informed by the pre-established items, the survey aimed to establish the criterion validity of each item. Most questions were presented as questions that ask: (1) the types of information strategies adopted and (2) the

intensity, as indicated in frequency, of such strategies (see Bryant & Zillmann, 2002).

The composite Index (summation of items) was created to construct a continuous scale in

each dimension (Cronbach alpha = .72 for socio dimension; .74 for tech dimension) (see

page 81 for the Index scores).
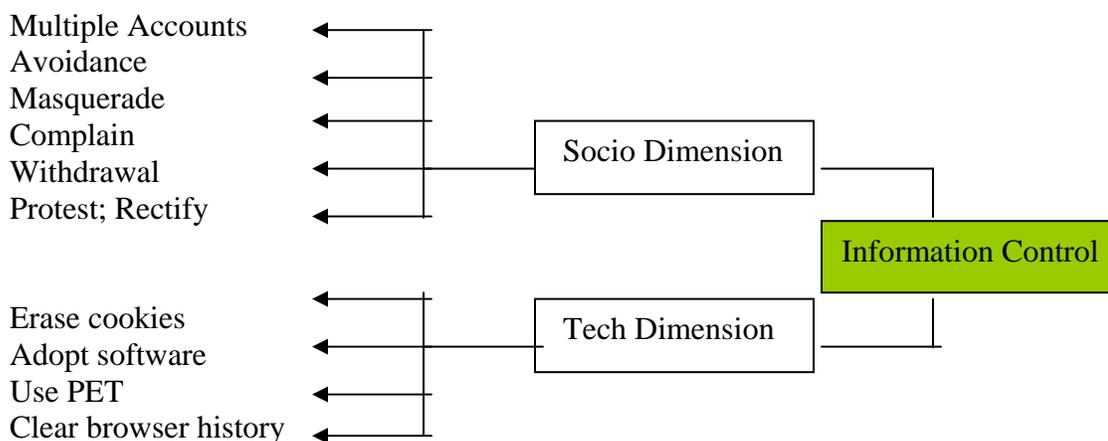
Figure 4-G. Dimension of systematic information control[19]

This general scheme is adopted from Marx (2003) & Rifon et al (2005)

Advancement in Measurement:

Note the limitations in the prior studies. Most behavioral measures were confined

in either single dimension (e.g., Turow for tech adoption) or dichotomous scale (e.g.,

Yes/No; Acquisti, 2005; Metzger, 2007) that observed the presence or absence of user

skills/strategies. This survey advanced the prior measures in order to encompass (1)

breadth/scope (i.e., different types of social and technical dimensions) as well as (2)

depth (i.e., intensity) of user strategies in daily routines. Within Dimension 1, further

specifications were made between active and passive control to capture the subtlety of

user behavior.

---

[19] The correlation between the two dimensions was .52, p < .01.

Information Control =

Scope: diversity of opt out strategies		+	Intensity: frequency of each activity

Figure4- H. Michigan behavioral measure

Knowledge

Digital *Privacy* Literacy

Digital *Privacy* Literacy is the users' cognitive abilities to critically read or understand institutional practices of data flow. That is to measure whether and the extent to which users are aware of information practices by websites (Hargittai, 2007). Note the notion of literacy that encompasses the contextual awareness of data flow. Media literacy encompasses more than understanding Internet privacy in a technical sense. Rather, it is about being able to assess the production of institutional practices as intertwined with policy and technical conditions.

Here digital literacy was operationalized as user awareness in the following three dimensions: (1) technology, (2) institutional practices, & (3) policy landscape. Each dimension of user knowledge was combined to create an Index, adopting from prior studies (e.g., Ackerman et al., 2001; Cranor et al., 1999; Culnan & Armstrong, 1998; Hargittai, 2007; Pew Internet, 2002; Shah & Sandivig, 2005; Turow, 2003; 2005). This was to capture a whole dimension of data flow in the context of institutional practice (Cronbach alpha = .80 for tech knowledge; KR 20 = .79 for institutional awareness; KR 20 = .73 for policy knowledge) (see page 81 for the Index scores).

Advancement in Measurement:

In fact, the notion of knowledge in most studies is confounded. The previous studies in privacy (e.g., Turow, 2005) did *not* make explicit distinctions between technical and policy aspects. Furthermore, new media studies (e.g., Hargittai, 2002; 2004; 2007) did *not* distinguish self-assessed and factual knowledge – that is, the difference between subjective and objective measures. This study further included both aspects of knowledge in multiple dimensions in order to capture more valid measures of user knowledge that may operate in daily routines.

Dimension	Factual	Self assessment
Policy	X	
Institution	X	
Technology		X

Figure4- I. Michigan knowledge measure

Internet Privacy Concern
Concern vs. Distrust

Internet privacy concern was measured using a 6-point Likert scale. The items required the respondents to rate the intensity of Internet privacy concern in terms of the entities, from "Strongly Disagree" (1) to "Strongly Agree" (6). Westin (2001; 2002) originally developed a set of measures on a 5-point scale. This survey specified Westin's items and scale into the subsequent two items: (1) concern 1: business (mean = 3.35, SD = 1.23) & (2) concern 2: government (mean = 3.04, SD = 1.20).

Advancement in Measurement:

Note, however, these measures were limited to observe the user concern in terms of generic institutional entities (i.e., Business vs. Government), *not* capturing the level of

concern in terms of specific information aspects (i.e., data collection vs. appropriation).

Moreover, what Westin's items observed was the perceived level of the risk, instead of

the trust/distrust over information flow online (LaRose, 2005). Here the main logic is the

distinction between net risk and net confidence. While net risk observes how much the

users are worried about the loss of privacy, net confidence indicates the extent to which

the users are confident about the online institution and its personal data practices (Dutton,

et al, 2004). In this vein, the two trust/distrust items are *not* only situated on the opposite

end in the continuum of the user concern, but also in the different levels of the domain

(see page 81 for the item scores).
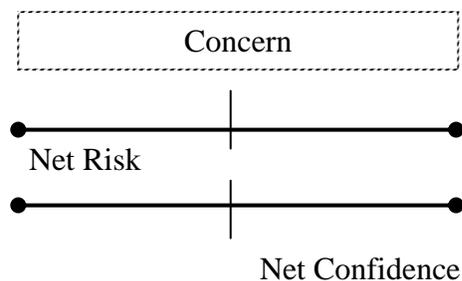
Figure 4-J. Measure of concern

Convenience

Convenience was defined as the rational cost/benefit calculation as indicated by

the level of the likelihood to tradeoff personal data, i.e., the cost, for financial gain or

access to favorite content, i.e., the benefit. The question was modified from Turow and

Hennesy (2007), but with more emphasis on individuals' rational calculation in specific

scenarios (see Appendix C for wording). The data type was from Ackerman, Cranor, and

Reagle (1999), Culnan (1998), Ribak & Turow (2003), and Acquisti (2005). In large,

these items was described in two types: (1) sensitive and (2) non-sensitive (see Sheehan

& Hoy, 1998). Convenience Index (Cronbach alpha = .86) was created to capture the extent to which the individual users value privacy over convenience/benefit at hand (see page 86 for the individual item scores).

Covariates [20]

Experience

The two items measured general online experiences in daily routines as these were related to differentiated uses of the Internet (Hargittai, 2004; 2005; 2007). First, the number of hours on the Web per week was asked. Second, the number of years in terms of Internet use was measured (Kwak et al, 2003; 2004).

- Number of hours browsing the Web per week
- Number of years since the first use of the Internet

Socio Economic Status

Four items measured the demographic characteristics of users. Prior studies (e.g., Kim & Ball-Rokeach, 2006; CDT, 2007) consistently pointed out the role of SES in maintaining different levels of digital divide.

- Income
- Gender
- Education
- Age: Younger users were found better skilled in general (Hargittai, 2007)

Autonomy of Use

According to Hargittai (2003; 2004; 2007), the freedom to be able to use the Internet anytime, anywhere, and with any purposes is one of the most significant single

---

[20] See the descriptions of individual variables in page 71.

predictors for different levels of online skills. In other words, those who have more access to use the Internet (i.e., easier access to Internet) are likely to be more sophisticated in Web uses. A single item was adopted from Hargittai (2007; also Turow, 2003).

Internet Connection

One item asked the quality of online access as the different types of Internet connection were found to relate to differentiated social and political uses (e.g., Hargittai, 2003; Kwak et al, 2004; Skoric & Park, 2005).

- Broadband: (cable vs. DSL) vs. Dial up connection

Analytical Strategies

The analyses proceeded in the following two stages: (1) premise 1 & (2) premise 2.1 & premise 2.2. This was to investigate the centrality of knowledge in the logical culmination – the two premises in interconnection from the simple regression to the two- and three-way interactions. Each premise has the two results in large. First, in order to answer the research questions, the descriptive data were included, identifying the overall trends in the main variables. Second, under each premise, the separate hierarchical regressions were run to test the hypotheses. To reduce the multi-collinearity problem, all the independent variables were standardized prior to the construction of the interaction terms (see Kwak, 1999; Kwak et al, 2005; Kwak & Campbell, 2009).

Results

Premise 1:
Knowledge & Action

Descriptive Statistics:
The Extent of Public Knowledge

The descriptive statistics shows the two results. First, the study found the highly limited extent of public knowledge about data flow online. Second, it was found that the extent of the knowledge was divided along with age, gender, and race/ethnicity. The limited knowledge was found in all the three dimensions of knowledge: (1) Tech: K1 (2) Institution: K2.1 (3) Policy: K2.2 (see Table 3). Indeed, the public *does* possess the basic understandings of the websites' acquisition and use of personal information (mean = 12.70, SD = 2.42). Yet, what the result indicated was that more than 40% of the respondents misunderstood the most basic aspects of institutional data practices. Only 8 respondents (1.9%) scored correctly on all of the policy-related knowledge questions. Furthermore, a majority of the respondents reported a low level of familiarity with the very basic technical terms (mean = 9.67, SD = 4.59) (see the knowledge items in the Appendix G).

SES & Divide

The extent of the public misunderstandings was magnified among the older users (see Appendix H). Those who are older than 50 scored consistently low in the technology knowledge dimension (K 1: $r = -.17$, $p < .01$; K 2.1: $r = -.13$, $p < .01$). The gender gap was found even more widespread: Male respondents scored significantly higher on all of the knowledge items (K 2.1: $r = .18$, $p < .01$; K 2.2: $r = .26$, $p < .01$). Among the females, only 29% scored correctly in some of the items. The population of the non-white scored significantly lower than the white in the policy-related knowledge items ($r = .13$, $p < .01$). Education was the consistent predictor; however, the magnitude of the difference was comparable to or even smaller than that of the gender or age gap. No difference in the level of public knowledge was found in terms of income/economic status.

Table 4-3
Descriptive Statistics of Main Variables

	Min	Max	Mean	Std. Deviation
Knowledge Index				
Knowledge 1: technology	2	18	9.67	4.59
Knowledge 2.1: institution	7	16	12.70	2.42
Knowledge 2.2: policy	1	14	8.88	1.99
Behavior Index				
Socio Dimension [21]	2	36	17.81	7.20
Passive	1	18	10.95	4.34
Active	1	18	6.86	3.91
Tech Dimension	1	24	11	4.42

The Extent of Public Behavior

The descriptive data provided multi-faceted pictures. Overall, the sample

respondents adopted one or more types of information control strategies[22]. Nevertheless,

the levels of the behavioral involvement in information control were found consistently

low. Table 3 shows that the public inaction in terms of (1) the type and (2) the intensity in

each and sub-dimension of the three knowledge dimensions.

In the tech dimension, the mean score was 11, indicating the most rarely adopted

or used technology through either web browser or PET. In the socio dimension, the

public involvement remained moderately high in terms of the passive control. But most

respondents, in the active dimension, did *not* take actions (mean = 6.86, SD = 3.91). The

---

[21] The socio dimension is the combined score of the passive + the active information control items.

[22] Here one prime attention should be given to the public behavior of reading the policy statement. This survey in fact found that 57.6% of the respondents said they do pay attention to the statement. The result is in line with prior studies (Culnan, 2001; 53% of the respondents indicated they usually read the website in their first visits). Nevertheless, note the difference between reading and other control (i.e., opt out) behaviors. That is, the measure of reading alone does *not* capture whether and to what extent users exercise data control strategies. With the strong correlation between reading and other control behavior (.25, p < .05), however, it seems more accurate to say that paying attention to the statement may function as a preceding behavior in the prime significance, but *not* as active control behavior as conceptualized in this study.

public inaction was further magnified in the three of the most active control behaviors. For instance, only 9% said that they ever complained to websites for data malpractices. A majority of males (40%) reported that they tended to exercise technology-related behaviors. However, this was mixed as the females adopted considerable strategies in the non-technical/socio dimension. Minorities displayed the lack of action in the socio dimension (r = -.08, p <.05). The most consistent impact was in age, displaying the presence of the age gap in information control behavior in the Internet more than any other SES factors.

Hierarchical Regression:

In premise 1, H 1 posited that user knowledge is positively associated with information control behavior in the Internet. Note that this was investigated in each of the three separate dimensions: (1) K 1: technical knowledge (2) K 2.1: institutional data practices and (3) K 2.2: policy understandings. Here, further specification was made in the dimension of technology knowledge: (1) Internet in general and (2) privacy in specific: risk and protection. This was to capture the operation of subtle knowledge structures that may be present in the two types of user behavior: (1) tech and (2) socio dimensions.

H 1.1: tech familiarities

The findings in Table 4 show that hypothesis 1.1 was supported in both tech and socio dimensions (ß = .31, p <.01; ß = .26, p <.01). However, in a separate hierarchical regression that only accounts for the active items of socio dimension, the support for H 1.1 disappeared for the knowledge of risk. Further, the level of protection knowledge

(that is, the familiarity with p3p) alone provided no support for H 1.1 in the combined socio index measure.

H 1.2: institutional knowledge

Hypothesis 1.2 posited the positive association between knowledge 2.1 (that is, the factual knowledge about institutional data practices) and the levels of information control. The support for H 1.2 was robust across all dimensions of information control (ß = .15, p <.01; ß = .26, p <.01). As a block, the knowledge alone accounted for 7% and 8% of the variance in behavior after the prior two blocks were taken into consideration. The control block accounted for 20% of the variance.

H 1.3: policy understandings

Hypothesis 1.3 posited the significant association between policy knowledge 2.2 (that is, the factual knowledge about Internet privacy policy & regulations) and information control in a positive direction. The hierarchical regression results provided a mixed support for H 1.3. The support for the tech dimension was consistent as in the prior hypotheses. For the socio dimension, strong support was also found for the combined socio dimension (ß = .26, p <.01). However, when only accounting for the most active dimension, the regression coefficients did *not* reach the significant level.

Table 4-4
Association between Knowledge & Information Control

	Tech		Socio[23]	
	Beta	t value	Beta	t value
SES:				
Income	-.01	-.31	-.14	.16
Education	.00	.18	.04	.91
Age	-.14**	-2.97	-.22**	-4.58
Gender	.20**	4.17	.08*	1.78
Internet Experience				
Year	.16**	3.33	.18**	3.75
Daily Use	.07	1.55	.19**	4.11
Autonomy	.19**	3.86	.16**	3.36
Literacy:				
Knowledge 1	.31**	6.29	.26**	5.24
K1.1: Risk: phishing	.23**	4.71	.12*	2.49
K1.2: Protection: p3p	.15**	3.17	.06	1.26
Knowledge 2.1	.14*	2.81	.26**	5.59
Knowledge 2.2	.13*	2.85	.22**	4.76

Note: * Significant at .05 level; ** Significant at .01 level.

The hierarchical regression proceeded from Block 1: SES to Block 2: Experience to Block 3: Knowledge. Note that separate hierarchical regressions were run for each of the three knowledge dimensions, with knowledge 1 further specified for K1.1 & K 1.2. The coefficients in Block 3 were the results of separate hierarchical regression models while the variables in prior Blocks remained constant.

Premise 2.1:
Knowledge & Concern

Descriptive Statistics:
The Extent of Public Concern

Figure 5 shows the extent to which the public expressed some concern about the

business and the government handling/protecting personal data, respectively (56% for

business; 71.8% for government). Note the contrast between the levels of concern and

---

[23] Coefficients were on the combined score for the socio dimension.

public action[24]. The incongruence was *not* as dramatic as in prior studies (e.g., Acquisti, 2004; Acquisti & Gross, 2005; LaRose & Rifon, 2007; Park, 2008; Turow et al, 2003; Ribak & Turow, 2003). Nevertheless, the presence of the privacy paradox was evident in line with prior literature. Here the privacy paradox was indicated by the following two: (1) the disjuncture between concern and behavior in an absolute sense and (2) no apparent effect of concern on user behavior[25].

Hierarchical Regression:

In premise 2.1, the primary purpose was to identify the function of the user knowledge in moderating the relationship between concern and behavior. For this, H 2 posited the positive interaction effect between the level of privacy concern and knowledge.

Hypothesis 2

The support for H 2 was in fact highly limited (see Table 5). As predicted, the interaction term between knowledge 1 and concern B was significant in both (1) tech use and (2) the socio dimension: that is, among those who are more concerned, users with a higher level of knowledge 1: technical familiarities exercised a higher level of information control. However, the support was limited only among those with concern for business practices. Furthermore, the levels of knowledge 2.1 and 2.2. did *not* interact with the levels of business and government concerns in either tech or socio dimension.

---

[24] Here, in Figure I, the public action was indicated by the tech dimension.

[25] This was the result from a separate OLS regression model. In the subsequent hierarchical regression models, the concern was included as the main variable.
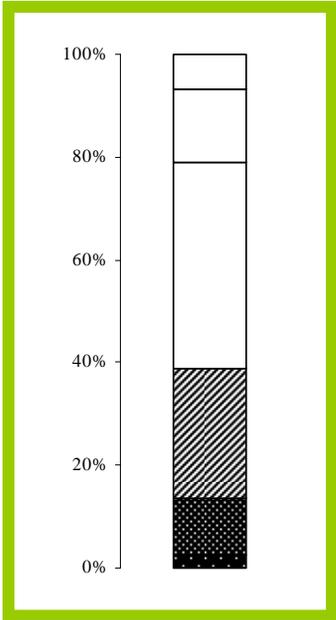
Figure 4-K. Public Inaction
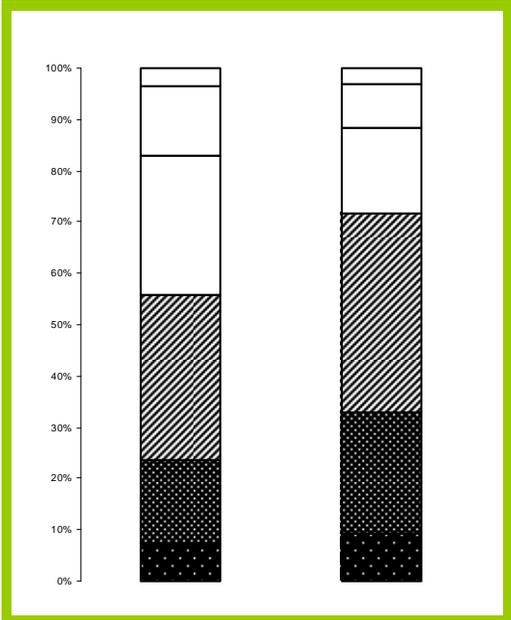
Figure 4-L. Public Concern

Table 5
Interactive Relationship Between Literacy and Concern

	Tech Use		Socio	
	Beta	t value	Beta	t value
Prior Block (R2)	22%		23%	
Interaction Terms				
Knowledge 1 x Concern B	-.13**	-3.07	-.09*	-2.09
Knowledge 1 x Concern G	-.05	-1.18	-.05	-1.18
Knowledge 2.1 x Concern B	-.03	-.81	.00	.03
Knowledge 2.1 x Concern G	.02	.49	-.02	-.45
Knowledge 2.2 x Concern B	-.06	-1.38	-.00	-.04
Knowledge 2.2 x Concern G	-.02	-.55	-.02	-.44

Note. * Significant at .05 level; ** Significant at .01 level.

Concern B: concern over business practices
Concern G: concern over government practices/protection

A total of six interaction terms were created: (concern B:G) x (K 1: tech: K 2.1: institution: K 2.2: policy). Each interaction term was run in separate hierarchical regressions. In each model, the prior block included the same variables as in Table 4.

Premise 2.2a:
Knowledge, Concern, & Convenience

Descriptive Statistics:
The Extent of Convenience

Table 6 shows the extent of the public rationality, as measured in the likelihood in which individuals are to tradeoff privacy for convenience. More than half of the respondents (52.3%) said it is unlikely that they would trade personally identifiable data for such benefits as favorite contents or monetary rewards. In terms of sensitive items, the figure went up to 65.9%, while 35.4% indicated such unlikelihood in non-sensitive item/scenarios. Rank order revealed the consistent pattern: it was most unlikely that the public trades off personal data associated with financial history (-2.40, SD = .7), whereas

the likelihood for foregoing the mundane items such as email, name, computer, &

favorite food increased in their rational assessments.

Table 4-6
Rational choice: Benefit over privacy cost

	No	Never	Likelihood	Rank
Non Sensitive ID				
Food	58.1	35.2	-1.49	8
Computer	69.1	36.2	-1.67	7
Name	72.5	39.3	-1.73	6
Email	56	30.9	-1.44	9
Sensitive ID				
Sexual	80.4	60.1	-1.95	4
Health	96.2	80.4	-2.33	2
Financial	98.6	86.7	-2.40	1
Purchase habit	83.6	53.2	-1.97	3
Political	80.4	49.2	-1.88	5

Note. No is the percentage of the respondents who scored the response options 1, 2, & 3, while *Never* indicates the percentage of the respondents who indicated no likelihood at all. The likelihood was calculated to identify the rank order.

Hierarchical Regression:

In premise 2.2, H 3 was proposed for the three-way interaction[26] in order to

incorporate the rational cost/benefit calculation in the relationship between concern and

behavior. For this, the three-way interactions were run, taking into consideration the two-

way interaction between knowledge and convenience[27].

Hypothesis 3

---

[26] Following the suggestion by Kwak (1999), the basic model = constant + control variables + x1 + x2 + x3 + x1*x2 + x2*x3 + x3*x1 + x1*x2*x3 + error

[27] The interaction between knowledge and convenience was significant. Knowledge 1, in particular, showed the strongest support in this regard ($\beta = .13$, $p < .01$ for the tech; $.18$, $\beta = p < .01$ for the socio dimension). Further, the support was robust in K 2.1 ($\beta = .07$, $p < .05$ for the tech).

The results did *not* confirm H 3. The three-way interactions were run separately, for concern: business, concern: government, and for K 1: tech, K 2.1: institution, and K 2.2: policy. While the prior block explained 25% and 27% of the variance for the tech and socio dimension, respectively, the impact of the rational cost/benefit calculation was *not* significant even when taking into account the significant interaction between K 1: tech familiarity and concern: business (see Table 5 for the two way interaction).

Table 4-7
Literacy, Concern, and Convenience

	Tech Use		Socio	
	Beta	t value	Beta	t value
Interaction Terms				
Knowledge 1 x Concern B x Convenience	.04	.92	-.04	-1.10
Knowledge 1 x Concern G x Convenience	.02	.48	-.00	-.07

Premise 2.2b:
Knowledge, Distrust, & Convenience

Note that in premise 2.2a, however, the public concern was measured in terms of information entities: (1) business and (2) government. Here the proposed three-way interaction was investigated in terms of information aspects: (1) collection and (2) appropriation. Here another important distinction was the observation of the public concern in the continuum of net confidence, instead of net risk. The extent of public distrust was in fact widespread. In terms of data collection, 71.4% of the respondents indicated some level of distrust toward institutional practices (mean = 2.76, SD = 1.42). In terms of information appropriation, 53.6% expressed the distrust (mean = 3.48, SD = 1.66). It was also found that the privacy paradox existed with no apparent effect of the levels of distrust on user behavior.

Table 9 displays the results from the three-way interaction among knowledge, distrust, and convenience. The three way interaction term among K 1, T 1, and C was found significant for tech use (ß = .10, p <.05) (see Appendix I). Also, the interaction K 1, T 2, and C was supported in both tech and socio dimensions. The support was the strongest with K 2.2 and K 1: the three way interaction was significant with the levels of T 2 in both dimensions (K 1: ß = .11, p <.05; ß = .21, p <.05; K 2.2: ß = .15, p <.01; ß = .20, p <.05). Nevertheless, it is important to note that the overall results also should be accepted with some reservation. No support was found in: (1) K 2.1, T 2, and C for the tech dimension and (2) K 2.2, T 1, and C for the socio dimension. Further, no support for K 2.1, T 1, C was found in either tech or socio dimension.

Table 4-8
Literacy, Distrust, and Convenience

	Tech Use		Socio	
	Beta	t value	Beta	t value
Interaction Terms				
Knowledge 1 x Trust 1 x Convenience	.10*	2.02	.03	.69
Knowledge 2.1 x Trust 1 x Convenience	-.04	-.85	.03	.77
Knowledge 2.2 x Trust 1 x Convenience	.16*	1.78	.11	1.19
Knowledge 1 x Trust 2 x Convenience	.11*	1.81	.21*	2.51
Knowledge 2.1 x Trust 2 x Convenience	.06	1.04	.19**	4.22
Knowledge 2.2 x Trust 2 x Convenience	.15**	3.29	.20*	1.69

Note: * Significant at .05 level; ** Significant at .01 level.

Each interaction term was run in separate hierarchical regressions.
T 1: distrust over institutional collection; T 2: distrust over institutional appropriation
C: convenience index

In sum, in investigating the centrality of the knowledge, the results from the

hierarchical regression analyses in the two stages: (1) premise 1 & (2) premise 2.1 &

premise 2.2. were as follows:

	Hypothesis	**Result**
Premise 1	+ three knowledge dimensions	Mixed
Premise 2.1	+ + the interaction: concern x knowledge	Limited support
Premise 2.2a	+ + + three-way interaction with concern: information entities	Not supported
Premise 2.2b	+ + + three-way interaction with concern: information aspects	Mixed; but generally supported

In short, what was supported: (1) the positive co-variation between knowledge and

behavior and (2) the critical role of knowledge in fixing the incongruence between

concern, as measured in distrust, and information control behavior.

Discussion

Premise 1:
Knowledge, Action, & SES

The findings of premise 1 are twofold. First, in general, the positive impact of

knowledge on information control behavior was strongly supported. Second, however, it

was found that the extent of the public knowledge remains limited, further divided in SES.

The impact of age and gender was significant and consistent in explaining information

control behavior (Turow, 2003; see Hargittai, 2003). Keeping those factors constant, the

primary concern was to observe the explanatory power of cognitive skills/particular

knowledge in differential uses/information control behavior in the Internet. In sum, the

main thesis is robust in that knowledge serves as a principle that is likely to support, encourage, and empower the users for informed choice and action.

Knowledge Structure & Action

The function of knowledge in behavior was in fact subtle in diverse dimensions (e.g., Freese, et al, 2006). This is to note the operation of the particularities of knowledge. The tech knowledge of risk and protection (Acquisti, 2004), the most direct items that concerned about Internet privacy per se, provided no support or only modest support in both socio and tech dimensions. On the other hand, the impact of the general Internet knowledge was significant to a greater extent. Further, while the knowledge of institution practices provided the strong support in both dimensions, the policy knowledge was modest in that no support was found in the three most active behaviors (mean = 6.86, SD = 3.91; see Appendix G for question wording)[28]. This all indicates that all of the three dimensions are highly correlated, but operating in the subtle different contexts/actions. In other words, the subcomponents are related yet may well reside independently in separate domains, far from producing the monolithic effects of knowledge (see Freese & Rivas, 2005).

General Tech Familiarities

Institution Knowledge

Policy Knowledge

Route 1: Tech adoption/use

Route 2: Socio dimension

---
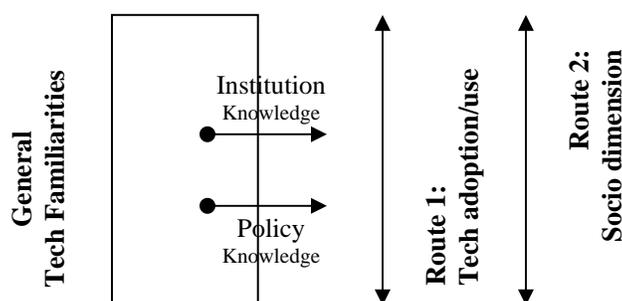
[28] Passive behaviors are (1) withdrawal, (2) avoidance, & (3) masquerading, while active behaviors are (1) complaining, (2) rectifying, & (3) using multiple accounts (see Marx, 2003 for the typology of surveillance neutralization moves). Note the distinction between active and passive behaviors in both conceptual and empirical levels (see page 55 for the difference in score between active and passive dimensions).

Figure 4-M. Knowledge activation
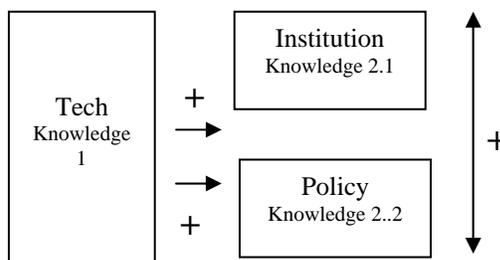
Figure 4-N. Subcomponents of knowledge

Table 4-9
Literacy Correlation Matrix

	Knowledge 1	Knowledge 2.1	Knowledge 2.2
Knowledge 1	-		
Knowledge 2.1	0.36**	-	
Knowledge 2.2	0.32**	0.46**	-

Knowledge Activation

In sum, the finding in premise 1 confirmed that critical understanding is essential of citizens in participating in digital activities (Hargittai, 2002; Jenkins, 2006; Van Dijk, 2005). In specific, the empowering power of the knowledge, as measured in both factual and subjective instruments, was found critical in exercising appropriate measures of the resistance against the potential misuse of personal data. Put differently, the knowledge may well activate users to exercise control and open up mass psychology of habitual routes of lack of control or inaction. This is *not* to suggest knowledge alone is sufficient. In fact, this power was embedded within the gender and age divide[29] (de Haans, 2004;

---

[29] See Table 4, page 84.

Hargittai, 2003). Further, Internet experience, as indicated in years, had positive influence in behavior, with the impact of the particular knowledge highly contextualized along with age and gender. On the flip side, it attests the presence of the knowledge divide that may function as an impediment to systematic information control, further reinforcing the social SES divide within digital information realms (Dimaggio, et al, 2001; Hargittai, 2004; 2005; Turow, 2005).

Premise 2.1 & 2.2
Knowledge & Privacy Paradox

The findings in premise 2.1 & 2.2 are as follows. First, the limited support for the interaction between the knowledge and the concern was found. Second, in this line, the support for the proposed three way interaction was *not* found. However, the public concern, as measured in distrust/trust over the different aspects of information privacy, provided support for the interactions. That is, when the incongruence was understood in terms of net confidence, the three-way interaction among knowledge, distrust, & convenience was found. Among those who weighted privacy cost over benefit in rational assessment, the positive interaction effect between the knowledge and the distrust remained true. In this regard, the most support came from Knowledge 2.2 (policy understanding) x Distrust 2 (appropriation) x Convenience – with the critical function of the policy knowledge in solving the paradox in both socio and tech dimensions.

Concern
Net Risk vs. Net Confidence:

Note the measure of the concern in the two levels: (1) risk and (2) confidence. In general, the concern, in terms of net risk, was *not* supported in solving the paradox, but the trust alternative, in terms of net confidence, provided the support. Here one more

dimensionality should be in account. That is, it may be that the generic risk assessment in terms of entities (i.e., government vs. business) had less explanatory power (e.g., Cranor et al, 2008). What is important is that the distrust measured one's concern in terms of specific aspects of personal information flow (i.e., collection vs. appropriation). In other words, one's specific assessment of information flow, when aided by knowledge, is to function while the general assessment of risk associated with government or business (as in Westin, 1998) did *not* necessarily translate into the systematic action. The interaction was further supported in relation with the convenience, i.e., rational calculation[30]. This provided the evidence that in daily Internet uses the function of knowledge was embedded in the interplay with the particular components in net confidence.

Knowledge:
Its Centrality in User Sophistication

In sum, premise 2.1 & 2.2 identified the function of knowledge in moderating the relationship between the concern, as measured in net confidence, and the behavior. That is, knowledge plays a significant role in resolving the privacy paradox, i.e., the incongruence between the concern and the behavior. To put it differently, the lack of knowledge may well function as an impediment among those who are concerned/distrusted in translating the concern into concrete actions. Thus, the empowering power of knowledge in fixing the incongruence was shown, but only in highly particular contexts. In short, knowledge was found to reside in the central locus of empowerment, mediating between other social-individual factors, in the full engagement with the potential of the active information control.

---

[30] Put differently, the interaction should be understood as the meaningful translation of the cost/benefit analysis into concrete actions, only when informed.

It remains unclear why the concern, in terms of net risk, provided less explanatory power than that of distrust/trust. It may be the case of a poor measurement in the concern items (Acquisti, 2004, Cranor et al, 2008, LaRose, 2008). Or in the regression model it is possible that the affective dimension in Internet uses (e.g., Neuman, et al, 2007, for political affection) may *not* have been fully specified. The self-report in the nature of the survey should be taken into account as well[31]. That is, when asked about the generic concern, the respondents may well be under the pressure of social desirability of indicating a certain level of concern. Yet even this has a limited explanatory power because the skewedness of the concern (towards the business and the government practices) was *not* in fact more dramatic than expected: (1) concern 1: business (mean = 3.35, SD = 1.23) & (2) concern 2: government (mean = 3.04, SD = 1.20).

What remains clear, however, is the critical role of cognitive power in resolving the paradox when the concern is specified in terms of information privacy aspects. In this vein, it should be understood that those with less likelihood of trading off privacy in rational cost/benefit assessment too remain ill equipped with incomplete knowledge hindering their abilities to exercise control[32]. In sum, the knowledge, in combination with other social factors, may *not* be sufficient, but a necessary enabler in empowering the users for systematic action/control (Neuman, 1988, for political sophistication).

---

[31] In this regard, these findings should be accepted with some reservation. The inflated responses were obvious in the respondents' self-reports of the number of hours they spend per day, Convenience Index, etc.

[32] Reminded is the significant interaction between knowledge 1 and convenience (β = .13, p <.01 for the tech; .18, β = p < .01 for the socio dimension).
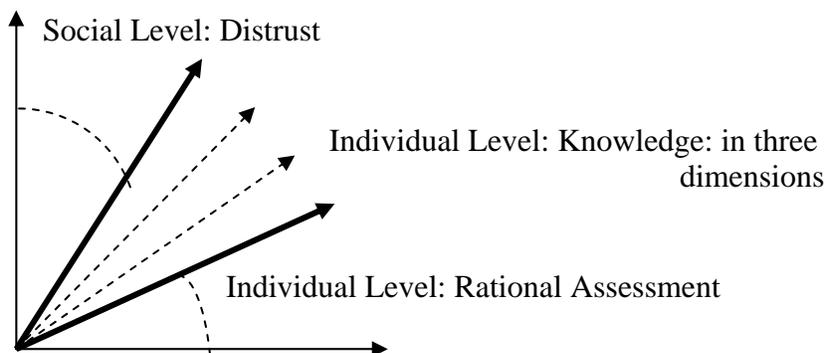
Figure4- O. The centrality of knowledge in the interplay

Policy Implications
Synthesis: Premise 1 & Premise 2.1:2.2

      The policy implications are twofold: (1) the presence of digital *privacy* divide &

(2) the questionable validity of the FTC self-regulatory regime. First, while knowledge

plays a critical role in user empowerment, the level of understandings among the majority

of the public remains limited. Second, the function of knowledge in resolving the privacy

paradox (as indicated by both (1) no apparent effect of distrust on user behavior and (2)

the disjuncture between distrust and behavior in an absolute sense) indicates the limited

extent of knowledge as the impediment in public action. In sum, the findings in premise 1

demonstrated the public is far from monolithic and omni-competent, which is different

from the policy premise in the operation of the Internet information culture. The findings

in premise 2.1 & 2.2 indicated the function of knowledge in the interplay, while the

public is fundamentally divided with the knowledge in the central locus of the divide[33].

Second Level Divide:
Users in the Policy Picture

---

[33] Note the policy version of the public fully equipped with understandings and capable of actions to their interests in rational assessment. In other words, this is to show the limited policy understanding of the public, detached from how users actually exercise control in daily contexts.

It is critical to note that the sample surveyed is the exclusive group of Internet users. In other words, the subjects were those who had high Internet experiences, a high education level at relatively young ages, while most were connected in broadband Internet. Given such technology-rich experiences, it is surprising to observe the extent of the lack of understanding and action, with the two significantly connected. In sum, when it comes to information privacy, the presence of the digital divide is evident in the following three regards:

(1) in exercising control in the full dimensions: socio + tech uses

(2) in leveling the action to the level of concern: i.e., resolving the paradox

(3) in making informed cost/benefit analysis: i.e., turning rational assessment into tangible actions

Note the centrality of the knowledge divide in curtailing the potential (i.e., in all of the above three actions) on the massive scale. In short, the variation of the public action was in fact found *not* randomly distributed (Hargittai, 2008). Some users are better positioned to exercise control, while others remain *systematically* excluded in the active role. That is to note the fundamental locus of knowledge as the source of inequality being entrenched on the second level of the digital infrastructure (e.g., Freese, et al, 2004).

Chapter 5: Revisiting the Integrated Model & Policy Recommendations

Empowering Personal Privacy:

The Final Equation
Institutional-Technical Structure & Individual User Culture for the Empowerment

The purpose of this dissertation was to examine the process in which the potential of the new technology is being shaped, constrained, and enabled by institutions and users. In Part I as spelled out in Chapter 3, the focus was the appropriation of information control on the structural level, i.e., how institutions in the commercial sector shape the potential of the empowerment in what ways. In Part II as in Chapter 4, the focus was information control on the cultural level, i.e., how users shape/respond to the potential of the empowerment on the other side of the equation. The two poles of institutional structure and user culture, as linked to the FTC policy principle, were the two constitutive components in the digital sphere. In sum, this dissertation was the attempt, in its empirical vigor and a tangible policy focus, to understand the construction of the digital sphere and its shaping of personal information control as conditioned by the current policy principle.

$$\textit{Equation}: x = p * q * z$$

- *part I: institutional force = p*

- *part II: cultural force = q*

- *policy = z*

- *the empowerment in controlling personal information = x*

In integration, the main findings of this dissertation are as follows. In the technical-institutional level, the interface design for active control was found curtailed to a large extent, with the Inform dimension manifest in particular. In the cultural level, the function of knowledge, as embedded in the interplay with net confidence, was found central in user action. These two poles, under the FTC policy principle, are in fact situated to function only in limited contexts. That is, while the commercial sphere is constrained for active information control, the users, with certain types of knowledge, were found able to resist to act to their interests – at least, to certain extents. Here the two forces in the shaping of control should *not* be understood as contradictory, but rather co-existent (Fisher, 2001). In other words, it may be that the two forces in actualizing the empowerment of the active control enable or curtail each other in mutual shaping (Neuman, 2007a; 2007b, for digital interactivity) (see Figure A).

institutional technical structure | the control of information | individual cultural behavior

the underlying policy ground
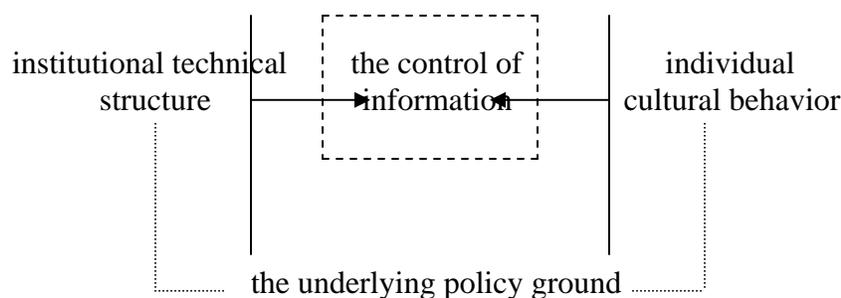
Figure 5-A. Conceptual mapping: the control of personal Information

In sum, the key in understanding the contour of this dissertation is this:

The confluence from both institutional and cultural forces in mutual influence, with the shaping of structure and culture explained/understood by the lack of

marketplace incentives and the knowledge in actualizing the potential of active

information control

Theoretically, this could be understood in terms of the empirical attempt to

reconcile the power of structure and agents in the constitution of a social system (Giddens,

1994; 1998), but more clearly in Neuman's poignant expositions (1991, for diversity;

2007, for interactivity). According to Neuman (1991; 2009), new technology *does* indeed

have intrinsic properties, yet its construction does *not* happen in a vacuum, embedded in

the complex interplay of institutional/economic, cultural/psychological, and

political/policy factors intertwined (see the model, p. 8 in Intro). What this dissertation

illustrates is that this broad *multivariate* understanding, in the appropriation of new

technology, precisely applies into the shaping of information control, too. That is, the

potential of the empowerment remains highly contingent upon the particular structural

and cultural conditions as the two are being constrained and enabled by institutions and

users in their limits and agencies.
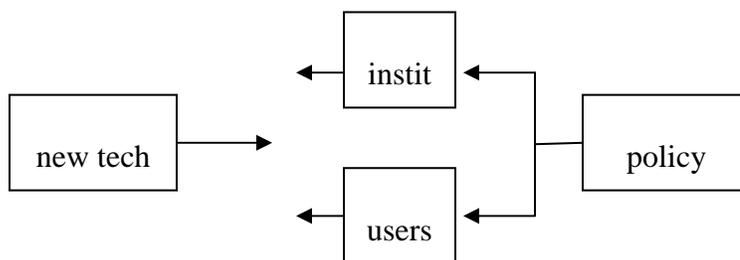
Figure 5-B. Revisiting the Integrated Model

(modified from Neuman, 1991)

To the Future of the Empowerment

Policy in Transition:
In recommendations to the FTC

Note the findings of this dissertation in the FTC policy context. First, structurally, it was found that the low voluntary provision of the FIP (at least its core aspects) remains entrenched in most commercial sites. Second, culturally, the digital *privacy* divide is present in which the public understandings remain limited, with a large portion of the user population in inaction. The two poles, in this light, indicate the invalidity of the current self-regulatory regime that is grounded upon the two operational assumptions:

(1) the monolithic understanding of *able* users

(2) the voluntary organizational behavior in the provision of privacy

control/protection in the commercial sector

Quasi-Public Infrastructure Model:
The QPI model

Based on these findings, a recommendation for Quasi Public Infrastructure (QPI) Model is proposed for the FTC to achieve the potential of the empowerment in controlling personal information. Note the two components in this model: (1) quasi-public and (2) infrastructure. Here the model is *public* in nature because of the imposition of basic requirements for certain sub-sectors in interface design. However, it is also *quasi* because the model posits that its viability is grounded upon sophisticated users who can exercise their control to their interests and concerns. The QPI is modeled after the spirit of the Open Communication Infrastructure (OCI) in that it attempts to spur the marketplace function, but in certain restraints[34] (Neuman et al, 1993; 1997). The overall

---

[34] To be more accurate, the OCI model aims to 'cut' the regulatory legacies that base the arbitrary division among telecommunication industries. Note that in the QPI model the core principle of *Notice*

purpose remains the same in its effort to harness the *unregulated* commercial forces, but the ultimate control and action reside in the individual users whose knowledge can stimulate them to evaluate the situation more systematically, e.g., when to act to control or not.

Technical-Institutional Structure
Micro Level Implementation:

In terms of the Inform dimension, in particular, the policy imperative is greater, given both top and random sites were unable to fully implement in this aspect. In terms of the Interact dimension, the betterment in the top sites should still be advanced, while improvement of the random sites (Internet universe) is urgent. In synthesis, the most important benchmark items are proposed in the observance of the FIP in its core aspects (of notice/choice):

- Item 1: in terms of Inform

    o Factor 1: *prominence*

    o Link to privacy statement in the main menu

    o Factor 2: *label*

    o Labeling privacy policy as 'the site uses of your personal information'

    o Factor 3: *easiness*

    o Readability set to the level of the eighth grader (i.e., the average)

- Item 2: in terms of Interact

    o Factor 1: *confirmation*

    o One click, in the policy page, to confirm the personal data collected

---

& Choice remains intact, without further burdensome impositions of other items in commercial sites. In other words, what the QPI model aims is the full realization of the current policy stance – with moderate stimuli in the interface/architecture of certain sub sectors.

- o Factor 2: *withdrawal*

- o One click, in the policy page, to opt out

- o Factor 3: *complaint*

- o One click to the FTC complaint page

Macro Level Implementation:

One of the main findings in Part I: Chapter 3 was that the marketplace incentive

alone did *not* lead to the full provision of information control in the Internet. This

necessitates the two enforcement mechanisms:

(1) the provision of incentive: *incentitize as a provision requirement*

(2) the establishment of a clear benchmark (e.g., in a scale of full vs. half of the

original OECD guidelines)

Table 5-1
Zoning the Internet

Zoning	Standardization: FIP scope	Enforcement
	Zone 1: sensitive	Required
	Zone 2: non sensitive	Non required

Here the standardization is to be operationalized in the introduction of *zoning*

(Neuman, 2007). Zoning, with different (1) standardization and (2) requirements, is to be

enforced according to the site domain type. The idea is similar to the one proposed for

'red light street zones' in identifying adult-only sites by the ICANN in 2007. Under the

current FTC regime, no difference is recognized, for instance, among the online estates of

financial districts or family safety zones and regular ecommerce sites. This is to enforce the principle of the FIP but to differentiate its scope for the sites that deal with sensitive information such as financial or health related data [35].

Here the QPI model draws upon the FCC regulation of 'seven dirty words' as the fundamental policy analogy. The history of the broadcast regulation tells that the government in fact actively engaged in the restriction of the broadcast of patently offensive language. The notion is that some indecent language could be broadcast in certain hours because fewer children are in the audience from midnight to 6 am. Two important policy considerations follow: (1) the time of day that offensive language is broadcast and (2) the type of language that could be restricted. This is to narrowly define the scope of regulation on the behaviors of broadcasters. A similar principle presented in the QPI model applies to the commercial sites through the establishment of (1) the venues, such as sensitive or non-sensitive sites, and the variations of (2) certain mandatory provision.

Nevertheless, it is important to ask whether these types of requirements in the commercial sites would be feasible at all. Note that this proposal concerns the commercial entities that are currently under no mandatory regulation. Yet the marketplace ideal does *not* necessarily mean the freedom from *any* regulation per se. Even in the tradition of the First Amendment protection of freedom of press, for instance, there are such exceptions as obscenity and fighting words. In privacy regulations, too, the strict policies, such as the 1984 Cable Act and the 1988 Video Act, apply to organizational behaviors in *offline* commercial sectors (see legislation chronology, p.14).

---

[35] Here one more layer of the requirement could be placed on the top + sensitive sites.

In this vein, what is proposed is zoning with moderate and flexible design standards (i.e., the standardized benchmark) (Edwards et al, 2007) to ensure the function of the limited segments in online commercial sectors.

Individual Users

On the other side of the QPI model, the inclusion of the public must be advanced in a delicate manner. In specific, this means that the *notice-choice* based proxy regulation is no longer effective when the public remains digitally divided at the second level. Here an urgent change to the proxy regulation is proposed. The policy vacuum in the lack of user understanding only serves as 'one size fits all'. That is, with the presence of a knowledge gap, only a set of elite *knowledgeable* users are situated to exercise information control. This should be understood with the increasing level of privacy concern among the public segments. In fact, the Pew in 2000 found 54% of the public expressed certain levels of privacy concern, with the result further confirmed in the latest surveys by the Truste (2008; 2009). Granted the centrality of knowledge in user action, the limited extent of the public understanding poses a significant challenge to policymakers in responding to the public concern.

Public education is perhaps the most direct way to change this. However, this, too, should be done in combination with other measures. Key is the specific targeting according to different user segments. For instance, for young children, the inclusion of accessible education materials in the k-12 curriculum should be made (Turow, 2005, for a similar proposal). For older and female users, this should take the form of targeting in a long term, rather than a piecemeal approach. In fact, the media habit is only subject to gradual change (Neuman, 1991). For this, the FTC must design a long-term program for

incremental change, such as the distribution of the FTC literacy manual to local

community organizations and the design of a specific FTC site for circulating consumer

information.

- Public Education k-12 Initiative

- General Public: Distribution: Digital *Privacy* Literacy Manual

- Specific Segments: Targeting the older vs. the younger users

Quasi Public Infrastructure (QPI) Model
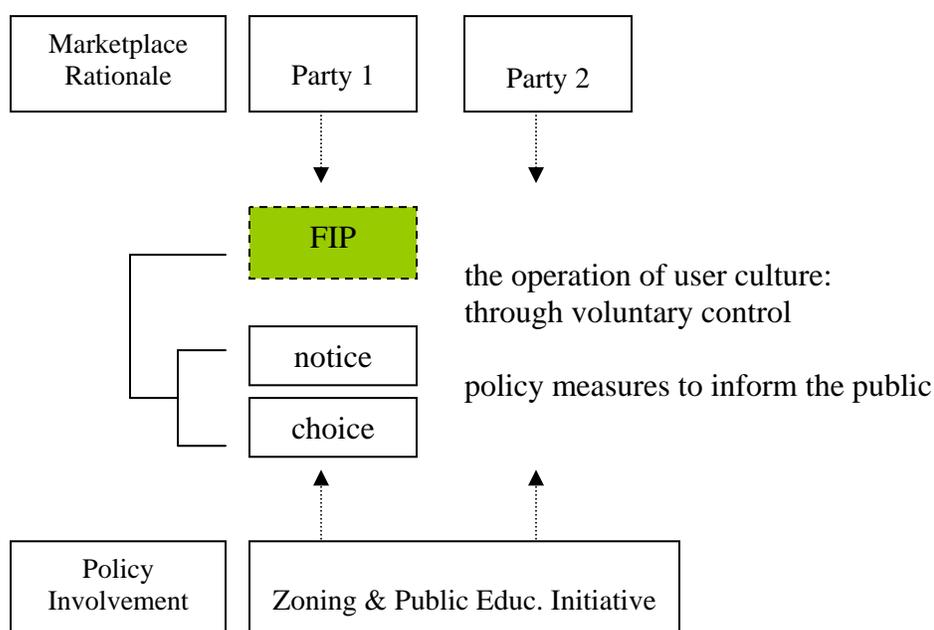
Figure 5-C. New Policy Model[36]

---

[36] To clarify the contour of the QPI model, it is important to note that the full scope of the original FIP (as in the OECD guidelines) is *not* advanced as mandatory requirements. Rather, what is proposed is the mandatory provision of Notice & Choice in different zones. In other words, the central concern is to establish the robust baseline of Notice & Choice, that is, the most fundamental aspect of the FIP. To further clarify, the proposed zoning differentiates the implementation of the diverse elements within each component of Notice & Choice.

In complementation, the most powerful tool is the utilization of the new media channel (Lessig, 2001). One prime method is the provision of the reference links in the commercial sites. The reference links should include the generic Internet terminology, data practices and policy knowledge that are *not* necessarily pertinent to the site operation, but in more general terms of knowledge. This is to make the knowledge available beyond the scope of a specific site of which the policy statement only functions as a legal disclaimer constrained within the site business. In this vein, a separate one-click link to the disclaimer, as perhaps it is now, could be installed independently of a page that is allocated for Inform + Interact. In this sense, the zoning, proposed above, should serve to mandate the provision of internal and external reference links according to zone (that is, domain) type.

Concluding Remarks

In synthesis, the bigger picture is the provision of the infrastructural interface bases with the informed users who are equipped to act in the construction of the digital sphere of which information flow/control is critical to its viability (also see Figure 1.F, p.6 in Intro). In line with this goal, what's proposed is, *not* the abandonment of the marketplace ideal in its entirety, but the active role of the policy in stimulating the function of the marketplace rationale. At the interface level, this means the application of the zoning in the provision of the FIP. At the individual user level, this can lead to the initiative that equips the users (and diverse segments) so that they can (1) systematically assess the level of information protection before being able to act and (2) control personal

information flow in line with their interest and concern. In short, the administrative measure proposed in the QPI model is:

- the FIP in its core aspects but required according to zone types

- in complementation with user education initiative to support its cultural ground

Note that the scope of the current studies in the dissertation precludes the effectiveness of such new policy measures. In this vein, further studies are proposed as follows. First, in terms of the interface design, longitudinal studies must be conducted on the panel of the top and random commercial sites that are in different zones. Second, in terms of the users, a series of experiments, with different design interfaces, should measure (1) its main impact on user behavior and (2) the interactive effect with knowledge in order to establish a direct causal mechanism. Finally, in-depth interview (with different segments of the user population) will facilitate understandings of how users in actual settings perceive different interface designs in commercial sites. It is important to note that what this dissertation establishes is a tentative springboard not only to challenge the current policy regime, but also to establish concrete future directions.

Taken together, the shift from the self-regulatory regime is justified, *not* because of the failure of the marketplace, but because of the failure of the policy action that supports it on tangible grounds. Here, this dissertation concludes with the urge to the dramatic shift, in institutional behavior, cultural/mass psychology, and policy, with all combined forces in actualizing the potential of the empowerment in controlling personal information.

Appendices

Appendix A: Theoretical Genealogy

The Table below sums up the highest level of the discussion that underlies this dissertation in theoretical genealogy. The direct theoretical contour is culminated in Neuman's model (1991; 2009) as this dissertation attempts to apply the model in the context of Internet information privacy.

	Terms & Concepts	Research	Source
Giddens	Structuration	Social System	1994
Bourdieu	Habitats	Social Stratification, tastes	1989
Castells	Self Net	Network Society	1999
Fisher	Social Constructivism	Telephone	1998
DeSanctis/Poole	AST: Adaptive Structuration	Organization	1994
Dimaggio et al	Social Implications	Internet	2001
Neuman	Soft Technological Determinism	Diversity/Digital Media	1991; 2009

Appendix B: **Private/Public vs. Political/Commercial**

Note the blurred distinction between the public and the private in the digital sphere (in green). In fact, in the Internet, personal information flows across the political and commercial sectors/sites. But more importantly, the Internet is increasingly the commercialized media. In this regard, how the commercial sector is operated carries significant political and commercial implications.

		Digital Information Flow	
Boundaries		Political	Commercial
	Public		
	Private		

To return to the central premise of this dissertation, important is the function of the institutional-technical structure and individual user culture in the construction of the digital sphere, of which the viability depends upon the potential of the empowerment in information control.

Appendix C: Policy Connection to Structure & Culture

The connection between the FTC current policy regime and the two central poles (i.e., structure & culture) is further clarified. Note the entities – institutions and users – in the two levels. This is to say that users constitute tech-culture on the one hand, whereas commercial institutions shape tech-structure, on the other. Here the FTC policy in its current contour speaks to institutions alone for ideal practices (the FIP). In this sense, Chapters 3 and 4 are: (1) to inform the FTC of the current statuses of institutional and user practices and (2) to guide the future policy directions.

	Chapter 3	Chapter 4
Object of Regulation	Institutional Structure	User Culture
Operating Principle	Proxy Regulation	Competent Users
Policy Assumption	Voluntary Provision: FIP	Mass Knowledge
Underlying FTC Principle	Self-Regulation	Self-Regulation

Appendix D: Comparison: Timeline

Here included are the items (in respective studies) that may be comparable in identifying a longitudinal trend. The numbers in parenthesis indicate *what*. In other words, they are the percentage of the websites of which the privacy policy 'says about', for instance, the procedure of 'opt out'. Note that the 2008 Michigan study measured the presence/absence of the actual channel for 'opt out' embedded in interface design. Put differently, the question was whether and to what extent users can actually opt out (that is, the assessment in terms of usability). The inflated figures in prior studies may well come from this difference.

Inform	Michigan 2008 %	FTC 98,2000 %	Culnan 2001, 2 %	LaRose 2003 %	Turow 2001 %
IF (1) presence of link to privacy statement in front page	87.9	76			
IF (1) 2. readability (accessibility of the statement)	12.27		11.43		
IF (1) 2.1 text length	1786.44		1408.18		
IF (2) placement: link placed in a clear prominent place	4.5				23
IF (2) 1. link placed in main menu	2.0			10.6	
IF (3) 1.1 font size is different from adjacent words	4.5				6
IF (3) 2.2 font color is different from the main text	35.5				39
IF (4) clearly labeled as 'privacy policy'	73.4	68.6		83.5	
IF (5) the link has other features (italics; highlighted; underlined) that make it stand out	40.3				21

	Michigan	FTC	Culnan	LaRose	Others
	2008	98,2000	2001,2	2003	2001
Interact	%	%	%	%	%
IT (1) privacy policy is linked from each page	84.4		83		
IT (3) active email link to make inquiries	57.2			53	
IT (4) availability of downloadable form to request, correct, or confirm data uses	17.5			(41.2)	
IT (4) 1. edit function, e.g., preferences or profile	25.8	(14.7)		(32.9)	
IT (4) 2. p3p embedded	77.7				57.6
IT (4) 3. click to opt out from the site	16.0			(20.0)	
IT (5) link to privacy policies in third party sites associated (e.g., opt out from NIA)	20.3				22

Appendix E: Sampled Sites

Top Sites

www.yahoo.com
www.google.com
www.youtube.com
www.facebook.com
www.msn.com
www.myspace.com
www.blogger.com
www.rapidshare.com
www.hi5.com
www.ebay.com
www.aol.com
www.photobucket.com
www.wordpress.com
www.flickr.com
www.amazon.com
www.imdb.com
www.imageshack.us
www.orkut.com
www.cnn.com
www.fastclick.com
www.fotolog.net
www.livejournal.com
www.adobe.com
www.espn.go.com
www.ask.com
www.apple.com
www.about.com
www.zshare.net
www.nytimes.com
www.mediafire.com
www.4shared.com
www.mozilla.com
www.deviantart.com
www.comcast.net
www.geocities.com
www.weather.com
www.download.com
www.partypoker.com
www.metacafe.com
www.doubleclick.com
www.gamespot.com
www.tagged.com
www.sourceforge.net
www.imeem.com
www.cnet.com

www.ign.com
www.dell.com

www.mapquest.com
www.tinypic.com
www.aim.com
www.gamefaqs.com
www.icq.com
www.alibaba.com
www.smileycentral.com
www.files.wordpress.com
www.hp.com
www.nbcolympics.com
www.watch-movies.net
www.answers.com
www.reference.com
www.pogo.com
www.sendspace.com
www.mlb.com
www.digg.com
www.typepad.com
www.target.com
www.walmart.com
www.linkedin.com
www.freewebs.com
www.slide.com
www.netflix.com
www.foxsports.com
www.wwe.com
www.ning.com
www.bestbuy.com
www.invisionfree.com
www.mywebsearch.com
www.reuters.com
www.wikia.com
www.symantec.com
www.worldofwarcraft.com
www.match.com
www.fanfiction.net
www.people.com
www.information.com
www.att.net
www.tripod.com
www.att.com
www.ezinearticles.com
www.foxnews.com
www.break.com

www.cartoonnetwork.com
www.filefront.com
www.msplinks.com
www.careerbuilder.com
www.rr.com

www.sweetim.com
www.chase.com
www.monster.com
www.brothersoft.com
www.myway.com
www.fimserve.com
www.ikea.com
www.nba.com
www.washingtonpost.com
www.scribd.com
www.quizrocket.com
www.freelotto.com
www.gametrailers.com
www.playlist.com
www.bankofamerica.com
www.gaiaonline.com
www.mtv.com
www.technorati.com
www.wamu.com
www.verizon.net
www.webshots.com
www.wowhead.com
www.neopets.com
www.wowarmory.com
www.addictinggames.com
www.truveo.com
www.tripadvisor.com
www.ups.com
www.expedia.com
www.feedburner.com
www.latimes.com
www.newgrounds.com
www.tv.com
www.real.com
www.thottbot.com
www.forbes.com
www.y8.com
www.univision.com
www.crunchyroll.com
www.justin.tv
www.wachovia.com
www.ibm.com
www.verizonwireless.com
www.yimg.com
www.circuitcity.com
www.thefreedictionary.com
www.newegg.com
www.playstation.com
www.winamp.com
www.wordreference.com
www.wsj.com

www.plentyoffish.com

Random Sites

http://www.ameriprise.com
http://www.alltel.com
http://barbie.everythinggirl.com
http://www.bizrate.com
http://www.imagestation.com
http://www.rentclicks.com
http://www.victoriassecret.com
http://www.troybilt.com
http://www.wxyt.com
http://www.animationfactory.com
http://www.cooks.com
http://www.shoplet.com
http://www.sandals.com
http://www.nike.com
http://www.webmd.com
http://www.emedicinehealth.com
http://www.biblio.com
http://houston.backpage.com
http://www.letssingit.com
http://www.saroyanzils.com
http://www.mondotimes.com
http://www.morfurniture.com
http://www.aaasouth.com
http://www.sublet.com
http://www.mercola.com
http://www.babyhomepages.net
http://www.eteamz.com
http://www.musicarts.com
http://www.drugstore.com
http://www.printfree.com
http://www.backpage.com
http://www.ajc.com
http://www.skinstore.com
http://www.koolprint.com
http://www.bandlu.com
http://www.frysfood.com
http://www.kleinfeldbridal.com
http://www.borders.com

http://www.orientaltrading.com
http://www.treehugger.com
http://parenting.ivillage.com
http://www.bluemountain.com
http://romance.virtualpune.com
http://www.honda.com
http://www.aftercollege.com
http://www.mostchoice.com
http://news.tradingcharts.com
http://www.radisson.com
http://www.nscorp.com
http://www.active.com
http://www.bradpaisley.com
http://www.allonlinecoupons.com
http://www.partypop.com
http://clayonline.sparkart.com
http://www.floridasmart.com
http://www.commerceonline.com
http://www.rottentomatoes.com
http://classifieds.timesdispatch.com
http://www.discovercard.com
http://www.celebritywonder.com
http://www.newgrounds.com
http://www.theholidayspot.com
http://www.popularmechanics.com
http://www.unexplained-mysteries.com
http://www.yellow.com
http://www.go-cartsrus.com
http://www.wchstv.com
http://www.primeoutlets.com

http://www.securityarms.com
http://www.travelpost.com
http://www.nothnagle.com
http://www.fandango.com
http://www.canon.com
http://www.legacy.com
http://www.abercrombie.com
http://www.pinkmonkey.com
http://www.coasttocoasttickets.com
http://www.topix.net
http://www.suncoast.com
http://www.womencelebs.com
http://www.whowhere.com
http://www.city-data.com
http://www.mrfreefree.com
http://www.tenant.net
http://www.alamo.com
http://www.driverzone.com
https://www.jetnet.aa.com/
http://www.guitarnoise.com
http://www.fastaccess.com
http://www.longhornsteakhouse.com
http://www.urbandictionary.com
http://www.mercurymarine.com
https://www.ibsnetaccess.com/
http://www.freewillastrology.com
http://www.unique-vintage.com
http://www.automart.com
http://www.mathplayground.com
http://www.mtbr.com
http://www.americanbridal.com
http://find.yuku.com
http://www.collegehoopsnet.com
http://www.beau-coup.com

http://www.goodysonline.com

http://www.cruisecheap.com

http://www.classiccloseouts.com

http://www.mothernature.com

http://www.homeenvy.com

http://www.zap2it.com

http://www.godlikeproductions.com

http://www.nintendo.com

http://chicagosports.chicagotribune.com

http://www.pregnancyguideonline.com

http://www.extrasformovies.com

http://www.paypal.com

http://www.audiovox.com

http://www.arbonne.com

http://www.homeexpo.com

http://www.nick.com

http://www.naturalhealers.com

http://www.modernpostcard.com

http://www.kltv.com

https://www.achievacu.com/

http://www.topsecretrecipes.com

http://www.coolmath4kids.com

http://www.pimall.com

http://www.sdcitybeat.com

http://www.southwest.com

http://hockeysfuture.com

http://www.majorgeeks.com

http://www.twcol.com

http://homeharvest.com

http://static.reunion.com

http://nc.essortment.com

http://www.owners.com

http://www.snopes.com

http://www.azcentral.com

http://www.abctoy4me.com

http://reference.allrefer.com

http://www.fool.com

http://www.continental.com

http://www.planetware.com

http://www.hollywoodvideo.com

http://www.libertymutual.com

http://seattletimes.nwsource.com

http://www.curves.com

http://www.healthsquare.com

http://www.harrisburgpahotels.worldweb.com

http://www.familyfirst.com

http://www.arcadepod.com

http://www.123helpme.com

http://entertainment.howstuffworks.com

http://www.answerbag.com

http://www.rapidswaterpark.com

http://www.fetchbook.info

http://www.lyricsdepot.com

http://www.linspire.com

http://www.vandykes.com

http://www.freewebs.com

http://www.americanmusical.com

http://www.inboxdollars.com

http://www.shopzilla.com

http://www.ediets.com

http://www.teagames.com

http://www.hilton.com

http://myspace.nuclearcentury.com

http://www.selfhealingexpressions.com

http://www.playonline.com

http://www.mizuno.com

http://www.rxlist.com

http://www.suite101.com

http://www.realestate.com

http://www.harmonhomes.com

http://www.crwflags.com

http://www.heraldextra.com

http://www.edmunds.com

http://www.bareminerals.com

http://www.babiesrus.com

http://www.thinkbabynames.com

http://www.era.com

http://www.avis.com

http://www.partycity.com

http://www.thepartsbin.com

http://www.homedepot.com

http://www.sears.com

http://www.uhaul.com

http://atlantahappenings.creativeloafing.com

http://boardgamecentral.com

http://www.medscape.com

http://www.targetwoman.com

http://www.bankatlantic.com

http://dsc.discovery.com

http://www.superseventies.com/

http://en.thinkexist.com

http://www.online-literature.com

http://www.classicreader.com

http://www.songmeanings.net

http://www.popmatters.com

http://allfreethings.com

http://www.the.hojo.com

http://www.hamptoninn.com

http://www.edressme.com

http://www.tropicana.net

http://www.joggingstroller.com

http://www.statefarm.com

http://www.homesdatabase.com

http://www.halfthedeck.com

http://www.consumersearch.com

http://www.visitflorida.com

http://www.roadsideamerica.com

http://www.buy.com

http://www.thecarconnection.com

http://www.cureresearch.com

http://www.nycroads.com

http://www.babyuniverse.com

http://www.costumecraze.com

http://www.naturessunshine.com
http://www.ebgames.com
http://www.graffitigen.com
http://www.wunderground.com
http://hotel-guides.us
http://www.rent.com
http://www.rir.com
http://www.apartments.com
http://www.beneficial.com
http://ths.gardenweb.com
http://www.livedaily.com
http://fooddownunder.com

http://www.buyonlinenow.com
http://www.brandsonsale.com
http://www.xequte.com
http://www.ifriends.net
http://www.tuscaloosanews.com
http://www.joblo.com
http://www.cduniverse.com
http://education-portal.com
http://www.angelfire.com
http://health.allrefer.com
http://www.converse.com
http://www.usbank.com

http://www.capitalone.com
http://www.seventhavenue.com
http://www.answerbag.com
http://www.igourmet.com
http://www.fotosearch.com
http://www.apparelsearch.com
http://www.sierratradingpost.com
http://www.pcmall.com
http://runehq.com
http://www.valleynationalbank.com
http://www.linear.com

Appendix F: Moderator vs. Mediator

It is plausible to posit knowledge as a mediator, rather than a moderator. This is to
suggest different causal mechanisms among knowledge, concern, and behavior. In other
words, knowledge may well be the function of concern. The alternative causal models, in
each of the premises 1, 2.1 & 2.2, may be as follows:

(1) alternative analysis: in premise 1

```
┌──────────┐        ┌──────────┐        ┌──────────┐
│ Concern  │  ───▶  │ Knowledge│  ───▶  │ Behavior │
└──────────┘        └──────────┘        └──────────┘
```

(2) alternative analysis: in premise 2.1 & 2.2

```
                    ┌──────────┐
                    │Convenience│
                    └──────────┘
                         │
                         ▼
┌──────────┐        ┌──────────┐        ┌──────────┐
│ Concern  │  ───▶  │ Knowledge│  ───▶  │ Behavior │
└──────────┘        └──────────┘        └──────────┘
```
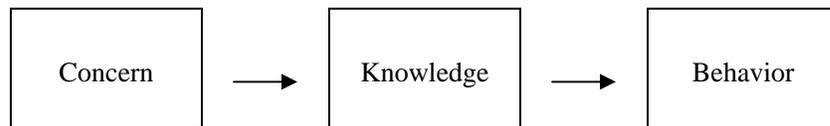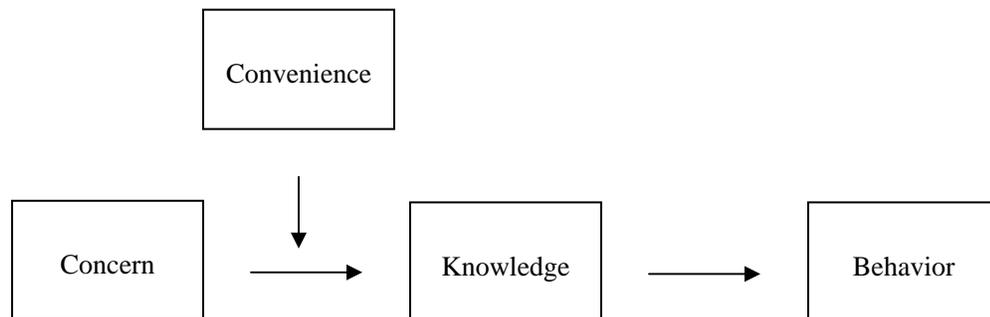
However, a caution is needed in these alternative models because of the strong causal
assumptions among variables. To address this concern, the next step is to establish
antecedents and consequences of knowledge through (1) laboratory experiments (internal
validity) and (2) longitudinal survey data (external validity).

Appendix G: Survey Items

1. Attitudinal Measures

Concern 1:	Most businesses handle the personal information they collect about consumers in a proper and confidential way.	Westin 1998; 2003
Concern 2:	Government provides a reasonable level of protection for consumer privacy today.	Westin 1998; 2003

Convenience scenario	
Imagine you come across a site and it asks you to provide personal information about yourself in exchange for a free gift or access to its content you find interesting. How likely is it that you provide each of the following types of personal information for a free gift or access to the content?	Turow 2003

Trust 1:	When websites, such as Google or Amazon, collect information about me, they do so to provide me with benefits.	Turow 2005
Trust 2:	I trust websites <u>not</u> to share information about me with other sites when they say they won't.	Ribaek & Turow 2003

2. Knowledge Measures

Knowledge Index 1:	Technology Familiarities	Original Source
1. Generic Internet	HTML	Hargittai 2003
2. Generic Internet	Preference setting	Hargittai 2003
3. Generic Internet	ISP	Hargittai 2003
4. Privacy Risk	Phishing	Hargittai 2003
5. Privacy Protection	p3p	Hargittai 2003
6. Bogus	Proxypod	Hargittai 2008

Knowledge Index 2.1: Institutional Data Practices

1. Companies today have the ability to place an online advertisement that targets you based on information collected on your web-browsing behavior.	Turow 2005
2. A company can tell you that you have opened an email even if you don't respond.	Turow 2005
3. When you go to a web site, it can collect information about you even if you don't register.	LaRose 2005
4. Popular search engine sites, such as Google, track the sites you come from and go to.	LaRose 2005
5. E-commerce sites, such as Amazon or Netflix, may exchange your personal information with law enforcement and credit bureau.	Turow 2005
6. What a computer user clicks while online surfing can be recorded as a trail.	LaRose 2005
7. Most online merchants monitor and record your browsing in their sites.	LaRose 2005
8. When a web site has a privacy policy, it means the site will not share your information with other websites or companies.	Turow 2005

Knowledge Index 2.1: Policy Understandings

1. Government policy restricts how long websites can keep the information they gather about you.	
2. It is legal for an online store to charge different people different prices at the same time of day.	Turow 2005
3. A website is legally allowed to share information about you with affiliates without telling you the names of the affiliates.	Turow 2003
4. By law e-commerce sites, such as Amazon, are required to give you the opportunity to see the information they gather about you.	Turow 2005

5. Privacy laws require website policies to have easy to understand rules and the same format.	Turow 2005	
6. US government agencies can collect information about you online without your knowledge and consent.	Turow 2005	
7. When I give personal information to an online banking site such as citibank.com, privacy laws say the site has no right to share that information, even with companies it owns.	Turow 2005	

3. Behavioral Measures

Index 1: Socio Dimension	Items	Original Sources
1. Avoidance	stopped visiting particular web sites because you fear they might deposit unwanted program on your computers	Culnan 1993; 2000
2. Masquerade	given false or inaccurate email address or fake name to websites because of the privacy concern	Culnan 2000; Metzger 2007
3. Withdrawal	decided not to make an online purchase because you were unsure of how information would be used	Culnan 2000; Metzger 2007
4. Complain	complained to a consumer or government agency about marketing practices of particular websites	Culnan 2000; Marx 2003
5. Rectify	asked a website to remove your name and address from any lists used for marketing purpose	Culnan 2000; Marx 2003
6. Multiple accounts	used an email address that is not your main address, in order to avoid giving a website real information about yourself	Pew Internet 2005

Index 2: Tech Dimension	Items	Original Sources
1. Clearing history	cleared your web browser history	Turow 2003
2. Filtering emails	used filters to block or manage unwanted email	Acquisti 2005
3. Erasing cookies	erased some or all of the cookies on your computer	Turow 2003
4. Using PET Software	used software that hides your computer's identity from websites you visit	Acquisti 2005

Appendix H: Digital Divide & SES

In particular, age was the most consistent factor among socio-economic statuses. The following two graphs show the dramatic decrease in the level of knowledge (2.1: institution; 2.2: policy) with the increase of age. Further studies are necessary to identify and to alleviate the presence of digital divide among different socio-economic groups.
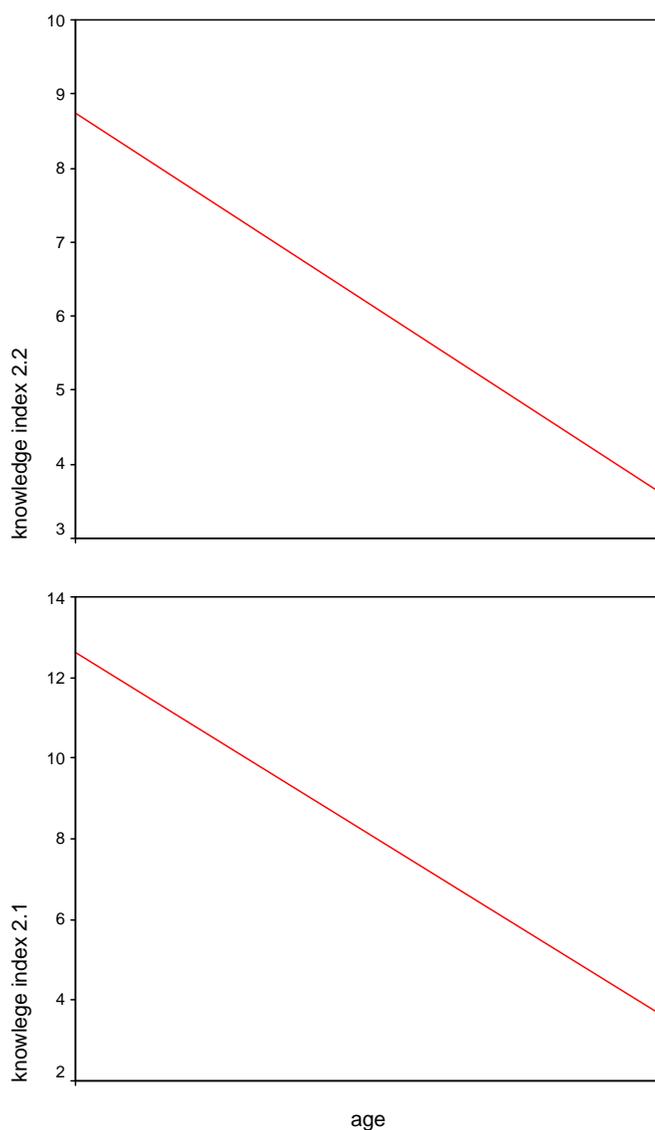
Appendix I: Three Way Interaction

The graphs below demonstrate the three way interaction among knowledge (K1: tech familiarity), distrust, and convenience. The first shows the presence of the significant interaction between K1 and distrust among those who value privacy over convenience. This is in contrast with the second that shows no such interaction among those who are more likely to trade off privacy for convenience[37].

---
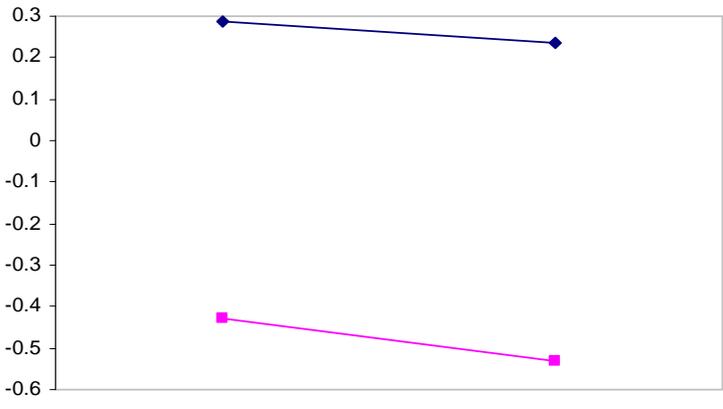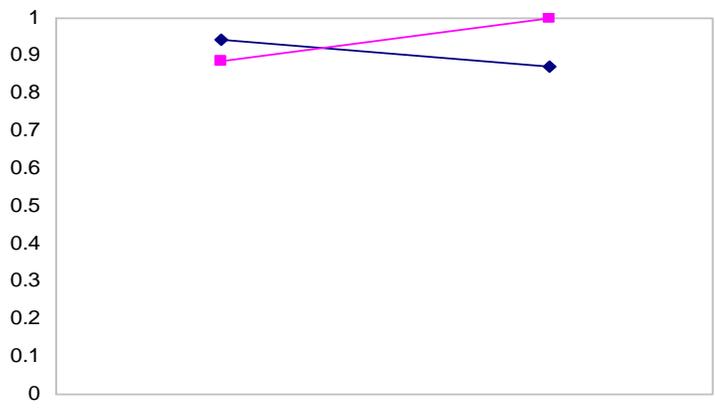
[37] For the purpose of demonstration, the medium value was assigned to separate the two groups: the high and low convenience groups. The line with the square markers indicates the high level of knowledge. Here x = distrust, while y = information control.

References

References

Abbate, J. (1997). *Inventing the Internet.* The MIT Press.

Ackerman, M., Cranor, L., & Reagle, J. (1999). Beyond concern: Understanding net users' attitudes about online privacy. *AT&T Labs-Research Technical Report*.

Acquisti, A. (2006). Information revelation and privacy in the Facebook. *PET.* Available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf

Acquisti, A. & Grosslags, J. (2005). Privacy and rationality in decision making. *IEEE Security and Privacy.*

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the ACM Electronic Commerce Conference* (EC 04). New York, NY: ACM Press, 21-29.

Agre, P. (1997). *Technology and privacy: The new landscape.* The MIT Press.

Agre, P. (1999). The architecture of identity: Embedding privacy in market institutions. *Information, Communication and Society* 2(1), 1-25.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* 50, 179-211.

Arendt, H. (1958). *The human condition*. University of Chicago Press.

Babbie, E. (2001). *The practice of social research.* Wadsworth Publishing

Ball, K. & Webster, F. (2003). *The intensification of surveillance.* Pluto Press. London.

Barber, B. (1998). Three scenarios for the future of technology and democracy. *Political Science Quarterly,* 113 (4), 573-589.

Barlow, T. & Wogalter, M.S. (1991). Alcohol beverage warnings in print advertisements. In: Proceedings of the Human Factors Society 35th Annual Meeting. Human Factors and Ergonomics Society, Santa Monica, pp. 51–55.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday.* 11 (9).

Benkler, Y. (2006). *The wealth of networks.* Yale University Press.

Bellotti, V. & Samarajiva, R. (1998). Interactivity as though privacy matters. In (eds.) Agre, P. 1997. *Technology and Privacy: The New Landscape*. The MIT Press.

Bellman , S., Johnson , E., Stephen , K., & Gerald , L. (2004). International Differences In Information Privacy. *The Information Society* , *20*, 313-324.

Brin, D. (1998). *The transparent society: will technology force us to choose between privacy and freedom?* Perseus Press.

Brock, G. (1980). *The telecommunications industry: the dynamics of market structure*. Harvard University Press.

Brown, J.A. (1998). Media literacy perspectives. *Journal of Communication, 48*(1), 44 57.

Bunz, U. (2004). Growing from computer literacy towards computer-mediated communication competence: Evolution of a field and evaluation of a new measurement instrument. *Information Technology, Education, and Society*. 4 (2), 53-84.

Bourdieu, P. (1984). Distinction: A Social Critique of the Judgment of Taste. London: Routledge.

Cai, S. & Jun, M. (2003). Internet users' perceptions of online service quality: a

comparison of online buyers and information searchers." *Managing Service Quality*, 13 (6), 504-519.

Campbell, S. & Park, Y.J. (2008). Social implications of mobile telephony: The rise of personal communication society. *Sociology Compass.*

Campbell, S. & Kwak, N.J. (2007). Mobile communication and social capital in localized, glocalized, and scattered networks. Paper presented at the Depart. of Comm. Studies Colloquium, University of Michigan.

Campbell, S. and Russo. T. (2003). The social construction of mobile telephony: An application of the social influence model to perceptions and uses of mobile phones within personal communication networks. *Communication Monographs*, *70*(4), 317-334.

Castells, M. (1998). *The Power of Identity, The Information Age: Economy, Society and Culture,* Vol. II. Cambridge, MA; Oxford, UK: Blackwell

Castells, M. (2006). "The Network Society: From Knowledge to Policy," Washington D.C: The Johns Hopkins University Press.

Castells, M. (2007). Communication, Power and Counterpower in the Network Society. *International Journal of Communication*. 1, 238-266.

Castells, M. (2006). "Informationalism, Networks, and the Network Society: A Theoretical Blueprint."

Caudill, E. & Murphy, P. (2000). Consumer online privacy: legal and ethical issues. *Journal of Public Policy & Marketing* 19(1), 7-19.

Cockburn, A. Greenberg, S., Jones, S., McKenzie, B., Moyle, M. (2003). improving Web page revisitation: analysis, design and evaluation. Pages 159-183 *IT & Society*.

Cranor, L, Acquisti, A., Tsai, J., & Elegman, S. (2006). Studying the impact of privacy information on online purchase decisions. Paper available at: http://cups.cs.cmu.edu/pubs/chi06.pdf

Cranor, M. Ackerman, M., & Reagle. J. (1999). Privacy in E-Commerce: examining user scenarios and privacy preferences. *Proceedings of the ACM Conference on Electronic Commerce (EC'99)*, 3-5 November 1999, Denver, Colorado

Culnan, M. (1995). Consumer awareness of name removal procedures: implications for direct marketing. *Journal of direct marketing* 9(spring), 10-19.

Culnan, M. J. & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organization Science*, *10*, 104–115.

Culnan, M.J. (2000). Protecting privacy online: is self--regulation working? *Journal of public Policy and Marketing*, 19(1), 20--26.

Culnan, M. & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10(1), 104-115.

Culnan, M. & Milne, G. (2001). The Culnan-Milne survey on consumers and online privacy notices: summary of responses," December 2001. Available at: http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf

Culnan, M. J. (1999). The Georgetown Internet privacy policy survey: Report to the Federal Trade Commission. Washington DC: Georgetown University.

Craincross, F. (2000). *The death of distance.* Harvard business school press.

Danna, A. & Gandy, O. (2002). All that glitters is not gold: digging beneath the surface

of data mining. *Journal of Business Ethics*, 40, 373-386.

DeSanctis , G., & Poole , M. (1994). Capturing the Complexity in Advanced Technology Use. *Organizational Science* , *5*(2), 121-147.

Dietrichson, A. (2001). Digital literacy: how to measure browsing behavior. Ph d dissertation Columbia University.

Dimaggio, D., Hargittai, Neuman, R., Robinson, J. (2001). Social implication of the Internet. *The Annual Review of Sociology*.

Dommeyer, C. J., & Gross, B. (2003). Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. *Journal of Interactive Marketing*, *17*(2), 34–51

Dutton, W. & Anderson, R. (1989). Computers and literacy: Differing perspectives in the social sciences. *Social Science Computer Review*, 7, (1), 1-5.

Dutton, W., & Shepherd , A. (2006). Trust in the Internet as An Experience Technology . *Information, Communication & Society* , *9*(4), 433-451.

Edwards, P., Jackson, S., Bowker, G., & Knobel, C. (2007). *Understanding Infrastructure: Dynamics, Tensions, and Designs*. Final report of the workshop, "History and The Design of Infrastructure".

Eisenstein, E. (1980). *The Printing Press as an Agent of Change*. Cambridge University Press.

Entman, R. & Wildman, S. (1992). Reconciling economic and non-economic perspectives on media policy: Transcending the "Marketplace of Ideas" *Journal of Communication* 42 (1) , 5–19

Electronic Privacy Information Center. (EPIC). (1998). Notice is not enough: Surfer beware. EPIC Report. Available at: http://epic.org/reports/surfer-beware2.html

Electronic Privacy Information Center. (EPIC). (1999). Privacy polices without privacy protection. EPIC Report. Availabe at: http://epic.org/reports/surfer-beware3.html

Electronic Privacy Information Center. (EPIC). (2008). Google, online advertising, and privacy. EPIC Press Report.

Farrell, K. (2008). Global privacy in flux: Illuminating privacy across cultures in China and the U.S. *International Journal of Communication* 2, 993-1030.

Fernback, J., & Papacharissi, Z. (2007). Online privacy as legal safeguard: The relationship among consumer, online portal, and privacy policies. *New Media & Society, 9*(5), 715-734.

Federal Trade Commission. (FTC). 1998; 1999; 2000 (Culnan). Privacy online: Fair information practices in the electronic marketplaces. A Federal Trade Commission Report to Congress.

Federal Trade Commission. (FTC). (1998). Online profiling: A report to Congress Part 2 recommendations, Jul. 2000, available at http://www.ftc.gov/os/2000/07/onlineprofiling.htm

Federal Trade Commission. (FTC). (1999). Self regulation and privacy online, Before The House Commerce Subcomm. on Telecom., Trade, and Consumer Protection, 106th Cong., Jul. 13, 1999, available at http://www.ftc.gov/os/1999/07/pt071399.htm

Fisher, C. (1992). *America Calling: A social history of the telephone to 1940*. University of California Press.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Flaherty, D. H. (1989). *Protecting Privacy in Surveillance Societies.* University of North Carolina Press.

Foot, K. & Schneider, S. (2002). Online action in campaign (2000). An exploratory analysis of the U.S. political web sphere, *Journal of Broadcast and Electronic Media*, June 2002, 46 (2), 222-244.

Foucault, M. (1984). *Discipline and Punish: The Birth of the Prison.* Vintage.

Fountain, J. (2001). *Building the Virtual State: Information Technology and Institutional Change.* (Washington, D.C.: Brookings Institution Press, 2001).

Fox. S. (Pew Internet). (2000). Trust and privacy online: why Americans want to rewrite the rules. The Pew Internet & American Life Project.

Freese, J. Rivas, S. & Hargittai, E. (2006). Cognitive Ability and Internet Use Among Older Adults. *Poetics,* 34(4), 236-249. August-October.

Giddens, A. (1984). *The constitution of society: outline of the theory of structuration.* Cambridge: Polity.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*, University of Edinburgh Social Sciences Research Centre.

Graeff and Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns, *Journal of Consumer Marketing,* 19(4), pp. 302–318.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society.* Polity, Cambridge

Diana P. Hackbarth, D., Silvestri, B. and Cosper, W. (1995) Tobacco and alcohol billboards in 50 Chicago neighborhoods: Market segmentation to sell dangerous products to the poor. *Journal of Public Health Policy*, 16 (2), 213-230

Hamilton, J. (1997). *Channeling violence: The economic market for violent television programming.* Princeton University Press.

Hargittai, E. (2000). Open portals or closed gates: Channeling content on the World Wide Web. *Poetics*, 27(4), 233-254.

Hargittai, E. (2002). Second level digital divide: Differences in people's online skills. *First Monday*, 7 (4).

Hargittai, E. (2004). Internet access and use in context *New Media and Society*. 6(1), 137-143.

 Hargittai, E. (2005). Survey measures of Web-oriented digital literacy *Social Science Computer Review*, 23(3), 371-379.

Hargittai, E. **(**2007). A framework for studying differences in people's digital media uses. In *Cyberworld Unlimited.* Edited by Nadia Kutscher and Hans-Uwe Otto VS Verlag für Sozialwissenschaften/GWV Fachverlage GmbH. Pp. 121-137.

Hargittai , E. & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social Science Quarterly*, 87 (2), 432–448.

Hargittai, E. (2008). An update on survey measures of Web-oriented digital literacy. *Social Science Computer Review,* 27(1), 130-137.

Heckman, J. (1998). *Legislation.* Marketing News (December 7), 1, 16.

Hoffman, D. Novak, T., & Peralta, M. (1999). Information privacy in the marketplace: implications for the commercial uses of anonymity on the Web. Information Society, 15 (2), 129-139.

Hoofnale, C. (2005). Privacy self regulation: A decade of disappointment. March 4, 2005 EPIC report.

Hoggart, R. (1958). *The uses of literacy: Aspects of working class life*. Chatto and Windus.

Hong, T., McLaughlin, M.L., Pryor, L., Beaudoin, C.E., & Grabowicz, P. (2005). Internet privacy practices of news media and implications for online journalism. *Journalism Studies*, 6(1), 15-28.

Hong, T. & Cody, M. (2003). Presence of pro-tobacco messages on the Web. *Journal of Health Communication*, 11, 273-307.

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

Hunter, C. (2002). Political privacy and online politics: How E-campaigning threatens voter privacy. *First Monday*, *7*(2).

Huntington, S. (1996). *The Clash of Civilizations and the Remaking of World Order*.

Inglehart, R. & Welzel, C. (2005). *Modernization, Cultural Change and Democracy*. New York and Cambridge: Cambridge University Press.

Jackson, S., Edwards, P., Bowker, G., & Knobel, C. (2007). Understanding Infrastructure: History, Heuristics, and Cyberinfrastructure Policy. Volume 12, Number 6 — 4 June 2007.

Jenkins, H. (2004). Media literacy goes to school, Technology Review. Available at: http://www.technologyreview.com/Biotech/13429/

Jenkins, H. (2006). Game On! The Future of Literacy Education in a Participatory Media Culture," *Threshold*, Winter 2006.

Jennings, B. & Zillmann, D. (2002). *Media Effects: Advances in Theory and Research*. Elbaum Associates.

Kaaya, J. (2005)**.** Implementing e-government services in East Africa: assessing status through content analysis of government websites. *Electronic Journal of e government,* 2(1), 39-54.

Kang, J. (1998). Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193 1294.

Kim, Y. C., & Ball-Rokeach, S. J. (2006). Civic engagement from a communication infrastructure perspective. *Communication Theory*, 16 (2), 173-197

Kobrin, S. (2004). Safe Harbors are hard to find: transatlantic data privacy dispute, territorial jurisdiction and global governance. *Review of International Studies*, 20, 111-131.

Kumaraguu, P. & Cranor, L. (2005). Privacy Indexes: A survey of Westin's studies Available at: http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05 138.pdf

Kwak, N. (1999). Revisiting the knowledge gap hypothesis. *Communication Research*, 26(4), 385-413.

Kwak, N., Williams, A. Wang, X., & Lee, H. (2005). Talking politics and engaging politics: an examination of interactive relationships between structural features of political talk and discussion engagement. *Communication Research*, 32, 87-111.

Kwak, N., Skoric, M.M., Williams, A.E., & Poor, N.D. (2004). To broadband or not to broadband: The relationship between high-speed Internet and knowledge and participation. *Journal of Broadcasting and Electronic Media*, 48(3), 420-445.

LaRose, R. & Rifon, N. (1999). *Analyzing media messages: Using quantitative content analysis in research.* Lawrence Erlbaum Associates.

LaRose, R. & Rifon, N. (2006). Your privacy is assured - of being disturbed: websites with and without privacy seals. *New Media & Society*, 8 (6), 1009-1029.

LaRose, R. & Rifon, N. (2007). Promoting i-Safety: Effects of privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs*, 41(1), 127-149.

Lazar, J., Bessiere, K., Ceaparu, I., Robinson, J., & Shneiderman, B. (2003). Help! I am lost: User frustration in Web navigation. IT & Society, Pages 18-26. Available at: http://www.stanford.edu/group/siqss/itandsociety/v01i03/v01i03a02.pdf

Lessig, L. (2000). *Code and Other Laws of Cyberspace.* Basic Books; New Ed edition.

Lessig, L. (2001). *The Future of Ideas* Vintage.

Lindlof, T. (1995). *Qualitative communication research methods*. Thousand Oaks, Calif.

Litman, J. (2002). "Information privacy/Information property". Stanford Law Review.

Livingstone, S. (2003). The changing nature and uses of media literacy. Available at: http://www.lse.ac.uk/collections/media@lse/pdf/Media@lseEWP4_july03.pdf

Lowery, S. & DeFleur, M. (1983). *Milestones in mass communication research: Media effects.* Longman :New York.

Luo, X. (2002). Trust production and privacy concern on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management,* 31(2), 111-118.

Malhotra, N. (1999). *Marketing Research: An Applied Orientation*. Prentice Hall.

MacKuen, et al., (2007). The Third Way: The Theory of Affective Intelligence and American Democracy. In (eds.) Marcus, George E., W. Russell Neuman, Michael MacKuen, and Ann N. Crigler, The Affect Effect: *Dynamics of Emotion in Political Thinking and Behavior*.

Markle Foundation. (2001). *Toward a framework for Internet accountability*. Markle Foundation Press Release, July 10, 2001.

Margulis, S. (2003). On the status and contribution of westin's and altman's theories of privacy. *Journal of Social Issues*, 59 (2) 411-429.

Marx, G. (1996)*. Privacy and Technology.* Telektronik January 1996. Available at: http://web.mit.edu/gtmarx/www/privantt.html

Marx, G. (2000). *Murky Conceptual Waters: the Public and the Private Ethics and Information Technology*, 3 (3), 157-169). Available at: http://web.mit.edu/gtmarx/www/murkypublicandprivate.html

Marx, G. (2003). A tack in the shoe: neutralizing and resisting the new surveillance. *Journal of Social Issues*, 59(2), 369-90.

McQuail, D. (2005). *Mass Communication Theory*. Sage Publications.

Metzger, M. J. (2004). Exploring the barriers to electronic commerce: Privacy, trust, and disclosure online. *Journal of Computer-Mediated Communication, 9(4)*.

Metzger, M. (2007). Effects of site, vendor, and consumer characteristics on Web site trust and disclosure. *Communication Research*, 33(3), 155-179.

Meyrowitz, J. (1985). No Sense of Place. Oxford University Press.

Milberg, S., Burk, S., Smith, J., & Kallman, E. A. (1997). Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38(12).

Milne, G., & Rome, A. (2000). Consumer privacy and name removal across direct marketing channels: exploring opt-in an opt-out alternatives. *Journal of public*

policy and marketing, 19(2), 238-249.

Milne, G. R & Culnan, M. (2002). A longitudinal analysis of the privacy Web sweep data: Using marketing research to inform public policy. *The Information Society,* 18 (5), 345-359.

Miyazaki, A. & Krishnamurthy. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs* 36 (1), 28-49.

Miyazaki, A & Fernandz, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, 35 (1), 27-44.

Miyazaki, A.D., and Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing,* 19(1), 54--61.

Moy, P., McCluskey, M. R., McCoy, K., & Spratt, M. (2004). Political correlates of local news media use. *Journal of Communication*, 54, 532-546.

Napoli, P. (2000). *Foundations of communications policy: Principles and process in the regulation of electronic media*. Cresskill, NJ: Hampton Press.

Napoli, P. (2003). *Audience economics: Media institutions and the audience marketplace*. New York: Columbia University Press.

Napoli, P. (2004). Television station ownership characteristics and local news and public affairs programming: an expanded analysis of FCC data. Info, 6(2), 112-121.

Napoli, P. & Yan, M. (2006). Media ownership regulations and local news programming on broadcast television: An empirical analysis. *Journal of Broadcasting & Electronic Media*, 51 (1), 2007

Neuendorf, K. A. (2002). *The content analysis guidebook.* Thousand Oaks, CA: Sage.

Neuman, R. (1986). The Paradox of Mass Politics: Knowledge and Opinion in the American Electorate. Harvard University Press.

Neuman, R. (1991). The Future of the Mass Audience. Cambridge University Press.

Neuman, R. (1996). Political Communications Infrastructure? The Annals of the American Academy of Political and Social Science. July 1996.

Neuman, R. (1997). The Gordian Knot: Political Gridlock on the Information Highway. (with Lee McKnight and Richard Jay Solomon), MIT Press.

Neuman, R. (2000). The Impact of the New Media in W. Lance Bennett and Robert M. Entman (Eds.) Mediated Politics : Communication in the Future of Democracy. New York: Cambridge University Press.

Neuman, R. (2004). Invited Talk at Depart. of Political Science. University of Rochester.

Neuman, R. (2006). Media Technology and Society: Lessons from the Past and Opportunities for the Future Conference at University of Michigan, Ann Arbor.

Neuman, R. (2007a). The Concept of Interactivity. International Encyclopedia of Communication, Blackwell Publishers and the International Communication Association.

Neuman, R. (2007b). Interaction. International Encyclopedia of Communication, Blackwell Publishers and the International Communication Association.

Neuman, R. (2009). *Media technology and society: The challenge of digital convergence.* University of Michigan Press.

Noam, E. (1997). Privacy and self-regulation: Markets for electronic privacy. Available at: http://www.citi.columbia.edu/elinoam/articles/priv_self.htm

Nowak, G. & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: determining how and when privacy matters. *Journal of Interactive Marketing*, 11(4), 94-108.

Ohm, P. (2009). The Rise and Fall of Invasive ISP Surveillance. *University of Illinois Law Review* .

Palmer J. W., Bailey, J. P., & Faraj. S. (2000). The role of intermediaries in the development of trust on the WWW: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication, 5*(3).

Park, Y.J. (2008). Privacy regime, culture, and user practices in cyber-marketplaces. Info – Journal of policy, regulation, and strategy in telecommunications.

Park, Y.J. (2009). Regime Formation and Consequence: The Case of the Internet Security of the East Asian Four Tigers. *Government Information Quarterly*, 26(2), 398-406.

Papacharissi, Z., Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media, 49*(3), 259-281.

Petty, R. E., & Cacioppo, J. T. (1996). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag.

Pew Internet. (2005). Spyware: The threat of unwanted software programs is changing the way people use the Internet.

Pew Internet (Princeton Survey Research Associates). May-June 2000. Daily Internet Tracking Survey.

Pew Internet. (Lenhart & Madden). (2007). How teens manage their online identities and personal information in the age of MySpace.

Phelps, J. Nowak, G. & Ferrell. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing* 19(1): 27-41.

PI. (2006). A Race to the Bottom: Privacy Ranking of Internet Service Companies A Consultation report. Available at: http://www.privacyinternational.org/issues/internet/interimrankings.pdf

Pool, I. D. (1983). *Technologies of freedom*. Belknap Press.

Putnam, R. & Feldstein, L. (2003). Better Together: restoring the American community. Simon & Schuster.

Resnick, R. (2007). Beyond bowling together: SocioTechnical capital In (eds). Carroll & Wesley, HCI in new Millennium.

Rifon, N., Quilliam, E.T., & LaRose, R. (2005). *Consumer Perceptions of Online Safety.* Paper presented at the 55th Annual Conference of the International Communications Association.

Price, V., & Cappella, J. N. (2002). Online deliberation and its influence: The Electronic dialogue project in campaign 2000. *IT and Society*, 1, 303-328.

Ribak, R. & Turow, J. (2003). Internet power and social context: A globalization approach to Web privacy concerns. *Journal of Broadcasting and Electronic Media*, Fall 2003.

Reidenberg, J. (1998). "Resolving Conflicting International Privacy Rules in Cyberspace,"52 *Stanford L. Rev.*

Rotenberg, M. (2000). What Larry doesn't get: fair information practices and the architecture of privacy. *Stanford Technology Law Review*.

Samuelson, P. (1998). Privacy as Intellectual Property? *Stanford Law Review 1125*.

Sandvig, C. (2004). May. Welcome to 1927: The Creation of Property Rights and Internet Domain Name Policy in Historical Perspective. IN: P. Day & D. Schuler (eds.), *Community Practice in the Network Society: Local Action/Global Interaction*. New York: Routledge.

Sandvig, C. & Shah, R. (2005). Defaults as De Facto Regulation: The Case of Wireless Access Points. Paper presented at the 33rd Telecommunications Policy Research Conference (TPRC) on Communication, Information, and Internet Policy, Arlington,Virginia, USA.

Sandvig, C. & Bar, F. (2008). US communication policy after convergence. *Media Culture Society.* 30, 531-550.

Saussure, F. (1977). Course in General Linguistics, Glasgow: Fontana/Collins.

Sheehan, K.B. (1999). An investigation of gender differences in online privacy concerns and resultant behaviors. Journal of Interactive Marketing, 13(4), 24-38.

Sheehan, K.B. & Hoy, M.G. (1998). Flaming, complaining, abstaining: how online users respond to privacy concerns. Journal of Advertising, 28(3), 37-51.

Stein, L. (2004). Understanding speech rights: Defensive and empowering approaches to the First Amendment. *Media, Culture & Society* 2(1), 103-120.

Strommer-Galley, j. & Foot, K. (2002). 'Citizens, campaigns, and online interactivity', *Journal of Computer-Mediated Communication*, 8 (1).

Schneider, S. & Foot, K. (2004). The Web as an object of study. *New Media and Society* , 6 (1), 114-122.

Schneider, S. & Foot, K. (2002). Online structure for political action. *Javnost* (The Public), 9, (2), 43-60.

Schwaig, K., Kane, G., and Storey, V.C. (2005). Compliance to the fair information practices: How are the Fortune 500 handling on-line privacy disclosures?" ACM (36) , 1 (Winter), 49 - 63

Skoric, M. & Park, Y. J. (2005). Cultures matter: Vertical media don't. Paper presented at the annual meeting of the AEJMC.

Simon, H.(1984). Models of Bounded Rationality, Volume 1: Economic Analysis and Public Policy (Models of Bounded Rationality)**.** The MIT Press; New Ed edition.

Solve, D. (2001). Privacy and Power: Computer Databases and Metaphors for Information Privacy *Stanford Law Review, Vol. 53, p. 1393, July 2001*

Solove, D., Marc , R., & Paul , S. (2006). *Information Privacy Law* . New York : Aspen.

Stein, L. (2004). Understanding Speech Rights: Defensive and Empowering Approaches to the First Amendment. *Media, Culture & Society* 26, 102-120.

Streeter, T. (1996). *Selling the air: A critique of the policy of commercial broadcasting in the United States.,* University of Chicago Press.

Stromer-Galley, J. (2004). Interactivity as process and interactivity as product. *The Information Society*, 20(5), 391-394.

Truste (2008; 2009). Consumer attitudes about behavioral targeting. Research conducted by TNS Global. March 2008.

Tsai, J., Cranor, L., Acquisti, A., & Christina M. (2006). What's it to you? A survey of online privacy concerns and risks (October 2006). NET Institute Working Paper No. 06-29.

Turow, J. (2001). Public policies on children's Websites: Do they play by the rules? Report No. 38 of the Annenberg Public Policy Center, March 2001, 22 pages.

Turow, J. (2003). Americans and online privacy: The system is broken. Report of the Annenberg Public Policy Center, June 2003.

Turow, J. & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media & Society,* 9(2), 300-318.

Turow, J. (2005). Open to exploitation: American shoppers online and offline, Report of the Annenberg Public Policy Center, June 2005.

Turow, J., Christopher Hoofnagle, Deirdre Mulligan, Nathaniel Good, and Jens Grossklags (U.C. Berkeley Boalt Hall School of Law), "The FTC and Consumer Privacy in the Coming Decade," Presented at the Federal Trade Commission meeting, "Protecting Consumers in the Next Tech-ade," November 8, 2006.

Trammell, K.; Williams, A, Postelnicu, M; Landreville, K. (2006). Evolution of online campaigning: Increasing interactivity in candidate Web sites and Blogs through text and technical features. *Mass Communication and Society*, 9 (1), 21 – 44.

USA Weekend Magazine. (2000). USA Weekend poll, July 2, 2000.

Van Dijk, J. (2005). *The deepening divide: Inequality in the information society*. London: Sage.

Venturelli, S. (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 and Brandeis. (1890). Vol. IV "The Right to Privacy" December 15, 1890 No. 5

Webster, J. & Lin, S. (2002). The internet audience: Web use as mass behavior. *Journal of Broadcasting & Electronic Media, 46(1),* 1-12.

West, D. (2005). *Digital government: Technology and public sector performance*. Princeton University Press.

West, D. (2006). Digital divide in public e-health sites: barriers to accessibility and privacy in health department websites. *Journal of Health Care for the Poor and Underserved,* 17(3), 652-666.

Westin, A. (1967). *Privacy and freedom*. New York, Atheneum.

Westin, A. (2003). Social and political dimensions of privacy. *Journal of social issues*, 59(2), 193-220.

Westin, A. & Louis Harris and Associates (1996). 1996 Equifax-Harris Consumer privacy survey. Atlanta, Georgia: Equifax Inc.

Westin, A. & Louis Harris and Associates (1998). Ecommerce & privacy: What Net users want. Hackensack, NJ: Privacy & American business.

Wu, T. (2007). A brief history of American telecommunications regulation. Oxford Encyclopedia of Legal History.

Yan, M. & Park, Y. J. (Forthcoming). Duopoly ownership and local informational programming on broadcast stations: Before-after comparisons. *Journal of Broadcasting & Electronic Media.*