Volume 51 | Issue 4 Article 8

2006

When New Technologies Are Still New: Windows of Opportunity for Privacy Protection

Gaia Bernstein

WHEN NEW TECHNOLOGIES ARE STILL NEW: WINDOWS OF OPPORTUNITY FOR PRIVACY PROTECTION

GAIA BERNSTEIN*

ABSTRACT: Early intervention in the regulation of new technologies is highly controversial. In this Article, I seek to depolarize the early intervention debate and examine where timing becomes of the essence in the shaping of new technologies. At the outset, I reframe the debate in terms of social shaping in lieu of intervention.

I focus the social shaping inquiry on the development of non-privacy norms among the Internet's commercial users in order to shed light on the timing quandary. Currently, over a decade after commercial entities started collecting personal information on the Internet, the law has not restricted these collection practices. Efforts at self-regulation have failed and Internet users overall have not adopted technological measures to protect their privacy. Empirical data shows an increase in the use of privacy threatening devices, such as cookies and spyware. The data shows that commercial non-privacy norms on the Internet have become entrenched among the Internet's commercial users.

Three technological characteristics of the Internet appear to be at the crux of the fast diffusion of commercial non-privacy norms. These characteristics are: the Internet's critical mass point quality (and related network effects); its decentralized diffusion process; and the enablement of concealed monitoring.

I suggest that where a technology's characteristics are likely to cause fast entrenchment, timing may become of the essence. Insights from several fields support this conclusion. The theory of path dependence shows that where costs are sunk into one option, an alternative option even if preferable is less likely to be adopted. Further, the theory of closure demonstrates that after an initial period where a technology's design and function evolves it tends to stabilize, reaching closure—from that moment onwards change is less likely. Finally, law and social norms theory shows that laws are less effective where they contradict social norms.

I posit that the lessons learnt from the case of Internet privacy could be instrumental to the resolution of other technological controversies.

* Associate Professor of Law, Seton Hall University School of Law. I would like to thank David Barnes, Shay David, Frank Pasquale, Erik Lillquist, Helen Nissenbaum, Amit Solomon, Charles Sullivan, Peter Swire and Sarah Waldeck for their comments and for helpful conversations. I would also like to thank Michael Carroll for inviting me to participate in this symposium. Finally, I am grateful to Joseph Farano and Monica Kostrzewa for excellent research assistance and to the Seton Hall School of Law Summer Research Stipend Program for its generous support.

Specifically, I propose that where a technology's qualities show that timing may be of the essence for privacy protection, both legal and technological modes of social shaping should be adjusted to reflect sensitivity to timing. Technological shaping is more likely to be effective through proactive concerted design at the outset. For legal decision-makers the technology's sensitivity to timing points to the need to consider timing as an important factor in the decision-making process, accounting for potentially more limited options at a later stage.

I. INTRODUCTION

THE introduction of new technologies that impose privacy threats is frequently accompanied by calls for intervention to shield individual privacy.[1] Proponents of intervention often support their position by stating that the law should not lag behind technology. At the same time, concerns are sounded against the hazards of early intervention in the regulation of new technologies.[2] Apprehension is motivated by the desire to avoid action before the full potential of a technology is realized. It is feared that progress could be impeded through the obstruction of yet unrealized technological potential.

Early intervention in the regulation of new technologies is highly controversial. Its contentious status is due at least in part to intervention measures taken in highly politicized technological debates, such as the stem cell research controversy.[3] In this Article, I seek to depolarize the early intervention debate and unpack the issue of timing in the shaping of new technologies.[4] At the outset, I undertake a linguistic shift, by replacing the term "intervention" with the concept of "social shaping"—a linguistic shift that I believe helps legitimize the goal of shaping our technologies in our image.

My goal in this Article is not to advocate early social shaping across the board. Instead, I seek to commence an inquiry to examine when timing becomes of the essence in the shaping of new technologies. The question is particularly pertinent in the area of privacy—where throughout

1. *See, e.g.*, Katherine Delaney, *RFID: Privacy Yearin Review: America's Privacy Laws Fall Short with RFID Regulation*, 1 ISJLP 543 (2005).

2. *See, e.g.*, Jack E. Brown, *New Law for the Internet*, 28 ARIZ. ST. L.J. 1243 (1996); Fred H. Cate, *Law in Cyberspace*, 39 HOW. L.J. 565 (1996). For a thorough analysis of this critique, see Michael H. Shapiro, *Is Bioethics Broke? On the Idea of Ethics and Law "Catching Up" with Technology*, 33 IND. L. REV. 17 (1999).

3. *See, e.g.*, William L. Saunders, *Lethal Experimentation on Human Beings: Roe's Effect on Bioethics*, 31 FORDHAM URB. L.J. 817 (2004).

4. For an analysis of timing in the regulation of new technologies in the context of the Fourth Amendment, see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

history, new technologies have repeatedly threatened privacy—yet reaction times and the effectiveness of privacy protection have varied.[5]

In this Article, I focus on privacy norms created through the collection of personal information by commercial entities on the Internet. As the use of the Internet became widespread in the mid-1990s, commercial web sites and commercial profiling companies began collecting personal information using technological devices, such as cookies.[6] Despite public indignation, a survey of empirical data I have conducted a decade later indicates an overall increase in the use of privacy-threatening technological devices by commercial entities on the Internet. This supports the conclusion that non-privacy norms related to the collection of personal information have become entrenched among the Internet's commercial users.[7]

The entrenchment of non-privacy norms among commercial users occurred rapidly. Currently, a decade after commercial non-privacy norms first appeared on the Internet, the law has not restricted commercial personal information collection practices.[8] Efforts at self-regulation have failed, and most Internet users have not adopted technological measures to protect their privacy.[9] The benefit of hindsight provided by the evolution of commercial non-privacy norms on the Internet leads to several insights.

Three technological characteristics of the Internet appear to be at the crux of the fast diffusion of non-privacy norms. These characteristics are: (i) the Internet's critical mass point quality (and related network effects),

5. For some examples of technological privacy threats and legal reactions, see Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438 (1928); WARREN FREEDMAN, THE RIGHT OF PRIVACY IN THE COMPUTER AGE 93-112 (1987); George Annas, *Genetic Privacy: There Ought to Be a Law*, 4 TEX. REV. L. & POL. 9 (1999); Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

6. On collection practices and data mining strategies, see DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 22-26 (2004); Tal Zarsky, *"Mine Your Own Business": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1 (2002/2003).

7. *See* Gaia Bernstein, *The Paradoxes of Technological Diffusion*, CONN. L. REV. (forthcoming 2006).

8. *See In re* Toys R Us, Inc. Privacy Litigation, MDL No. M-00-1381, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001); *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

9. *See* Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment* (Mar. 4, 2005), http://www.epic.org/reports/decadedisappoint.pdf (last visited Feb. 7, 2006); MICROSOFT CORP., MICROSOFT P3P IMPLEMENTATION IN INTERNET EXPLORER 6.0 AND WINDOWS XP: FACT SHEET, http://www.microsoft.com/presspass/press/2001/mar01/PrivacyToolsIEfs.asp (last visited Feb. 7, 2006); ERNST & YOUNG, ENABLING P3P: WORKSHOP ON MACHINE READABLE PRIVACY POLICIES 4 (Jan. 2004), http://www.cdt.org/privacy/20040122enablingp3p.pdf (last visited Feb. 7, 2006); ERNST & YOUNG SECURITYSPACE, COMPACT PRIVACY POLICY REPORT (Apr. 1, 2003), http://www.securityspace.com (last visited Feb. 7, 2006).

(ii) the Internet's decentralized diffusion process and (iii) the enablement of concealed monitoring. I show that the Internet's critical mass point and decentralized diffusion process directly contributed to the fast entrenchment of non-privacy norms. Diffusion accelerated when it reached the critical mass point, inducing a rapid spread of developing norms, while decentralization enabled all users to actively re-design the technology facilitating the installation of privacy-threatening devices. Further, invisible monitoring on the Internet reduced the likelihood that Internet users will resort to self-help to protect their privacy. The absence of a perceptible threat resulted in individuals' reluctance to act to protect their privacy, contributing to the transformation of privacy from an individual right to a public value. As individual users failed to insist on their privacy preferences, the design of Internet architecture was left to the privacy preferences of commercial actors.

I then suggest that where a technology's characteristics are likely to cause fast entrenchment of non-privacy norms, decision-makers should pay particular attention to timing. This conclusion is based on insights from economic theory, science and technology studies theory, and law and social norms theory.

Commercial non-privacy norms on the Internet are characterized by path dependence, which focuses on how the path taken today is affected by the path that was selected in the past.[10] Many web sites and commercial profiling companies are dependent on the continued concerted practice of concealed collection of personal information. A shift to alternative marketing practices that do not involve concealed information collection is likely to prove inefficient and therefore likely to be resisted by these commercial actors. Furthermore, the Internet's critical mass point and decentralization qualities make it particularly susceptible to path dependence. The Internet's commercial and individual users are highly interdependent and are unlikely to shift unilaterally to an alternative path, particularly because the Internet lacks a centralized authority that could dictate such a shift.

The Social Shaping of Technology (SST) theory of closure sheds additional light on the evolution of commercial non-privacy Internet norms. Closure is the point at which controversy surrounding design and uses of a technology subsides and specific forms and norms become generally accepted. Once closure is reached, interpretive flexibility is lost and is hard to regain.[11] On the Internet, norms became rapidly entrenched and a

10. *See* Lucian Arye Bebchuk & Mark J. Roe, *A Theory of Path Dependence in Corporate Ownership and Governance*, 52 STAN. L. REV. 127, 129 (discussing structure driven path dependence).

11. *See* WIEBE E. BIJKER, OF BICYCLES, BAKELITES AND BULBS: TOWARD A THEORY OF SOCIOTECHNICAL CHANGE 85 (1995); Stewart Russell & Robin Williams, *Social Shaping of Technology: Frameworks, Findings and Implications for Policy with Glossary of Social Shaping Concepts*, *in* SHAPING TECHNOLOGY, GUIDING POLICY: CONCEPTS, SPACES AND TOOLS 37, 120 (Knut H. Sorensen & Robin Williams eds., 2002).

closure process that would normally evolve over decades was consummated at an exponential rate. In 2000, controversy regarding commercial non-privacy norms erupted.[12] Yet, individual Internet users failed to promote an alternative Internet perception. After 2000, as norms rapidly entrenched, interpretive flexibility was quickly lost and—left unchallenged—non-privacy norms prevailed among the Internet's commercial users.

Finally, law and social norms theory shows that laws are less likely to be effective where they sharply digress from existing social norms.[13] A law that diverges from existing social norms has a reduced likelihood of being effective because it faces the challenge of reforming societal structures of social stigma.[14] Consequently, any attempt at legal social shaping a decade after the appearance of non-privacy norms is likely to encounter a far greater hurdle than had a similar attempt been taken before such norms became entrenched.

Based on these insights I posit that where a new technology enables concealed monitoring, is characterized by a critical mass point quality and features decentralized diffusion, the window of opportunity for privacy protection is narrower. I do not maintain these are the only conditions that affect the timing for privacy protection. I suggest, however, that where these conditions exist they should raise a red flag for decision-makers to carefully consider the timing of social shaping.

Applying this conclusion to the case of Internet commercial privacy norms, the window of opportunity may already be partially closed, and alternatives at this point are more limited. Yet, my goal in this Article lies beyond the transformation of commercial non-privacy norms on the Internet. New technologies with the characteristics that lead to rapid entrenchment of non-privacy norms are likely to emerge. Invisible monitoring devices are increasingly embedded in technological innovations. The Internet, with its critical mass point and decentralized diffusion qualities, is likely to serve as a platform on which other non-privacy norms will materialize.

Where a technology's qualities show that timing may be of the essence, both legal and technological modes of social shaping should be adjusted to reflect sensitivity to timing. I propose that technological shaping is more likely to be effective through proactive concerted design at the outset. Privacy protection is likely to be more effective if included as a functional component in the initial design than if designed later for indi-

12. *See, e.g., Amid Protests,* DOUBLECLICK AND ABACUS Announce Plans for $1 Billion Merger, ELEC. ADVER. & MARKETPLACE REP., June 29, 1999, at 13.

13. *See* Dan Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem,* 67 U. CHI. L. REV. 607, 608 (2000); Elizabeth S. Scott, *The Legal Construction of Norms: Social Norms and the Legal Regulation of Marriage,* 86 VA. L. REV. 1901, 1926-28 (2000).

14. *See* Lawrence Lessig, *The Regulation of Social Meaning,* 62 U. CHI. L. REV. 943, 986-87, 999 (1995); Paul H. Robinson, *Why Does Criminal Law Care What the Layperson Thinks Is Just? Coercive Versus Normative Crime Control,* 86 VA. L. REV. 1839, 1861-63 (2000) .

vidual user adoption. Turning to legal shaping, I suggest that the technology's sensitivity to timing does not necessarily mandate early legal shaping. It does, however, require consideration of timing as an important factor in decision-making, accounting for potentially more limited options at a later stage.

The Article proceeds as follows. In Part II, I propose the linguistic shift from "intervention" to "social shaping." In Part III, I describe the entrenchment of commercial non-privacy norms on the Internet and identify the technological characteristics that contributed to rapid norms entrenchment. In Part IV, I examine insights from economic theory, science and technology studies, and law and social norms theory that point to the significance of timing under the identified technological conditions. Finally, in Part V, I examine ways in which timing should affect technological and legal modes of social shaping.

II. FROM INTERVENTION TO SOCIAL SHAPING

In this Part, I examine the concept of "early intervention" and urge a change in the terminology used in new technologies' regulation discourse. Specifically, I propose that the term "intervention" should be replaced with "social shaping." I start by examining objections raised to early intervention with new technologies. I then put forward two reasons for replacing intervention with social shaping. First, intervention is tied to the notion of technological determinism, which de-legitimizes the notion of proactively shaping our technologies in our image. Second, use of social shaping, in lieu of "intervention" or "design," corrects a current perceptual imbalance by placing legal measures and technological measures on equal grounds with regard to their perceived degree of intrusiveness.

A. *Opposition to Early Intervention*

A common complaint regarding the regulation of new technologies is that the law is slow to react to technological change.[15] Yet, a converse critique often sounded by policy-makers and commentators warns against the hazards of early intervention in the regulation of new technologies. Early intervention can take different forms. For instance, early intervention can take place at the invention stage, banning an innovation from being created in the first place.[16] Conversely, it can occur later at the diffusion stage, prohibiting the diffusion of a new technology that was pre-

15. *See, e.g.*, James E. Bailey, *An Analytical Framework for Resolving the Issues Raised by the Interaction Between Reproductive Technology and the Law of Inheritance*, 47 DEPAUL L. REV. 743, 814 (1998).; Shapiro, *supra* note 2.

16. *See, e.g.*, Assisted Human Reproduction Act Prohibited Activities, 2004 S.C., ch. 2, s. 5 (Can.) (Canadian law prohibiting human cloning); Human Reproductive Cloning Act 2001, ch. 23, s. 1 (Eng.) (British law prohibiting human cloning).

viously invented.[17] Early intervention, however, is not necessarily a complete ban. Restrictions on invention or use are another form of early intervention.[18] While it is usually legislative regulation that is perceived as early intervention, court rulings can have the same effect.[19]

The resistance to early intervention has several justifications. Mainly, opponents of early intervention caution against intervening before the social uses of a new technology are fully realized.[20] For instance, in the early days of the Internet, many commentators, practitioners and industry leaders advocated a wait and see approach. They cautioned against moving forward before Internet technology and its usage were fully developed and fully understood.[21]

The cautionary approach to early intervention stems from the belief that technological innovation promotes human progress and that human

17. See, for example, legal restrictions on the diffusion of nuclear weapons. 42 U.S.C. § 2014, 2131(v) & (cc) (2005); 18 U.S.C. § 831 (2005).

18. *See, e.g., President George Bush Address to the Nation on Stem Cell Research*, 37 PUB. PAPERS 32 (Aug. 9, 2001) (restricting federal funding of stem cell research to research conducted on sixty existing stem cell lines); Gaia Bernstein, *The Socio-Legal Acceptance of New Technologies: A Close Look at Artificial Insemination* 77 WASH. L. REV. 1035 (2002) (describing legal impediments to diffusion of artificial insemination).

19. The Children Online Privacy Protection Act (COPPA), which was enacted in 1999 to protect children's privacy on the Internet, is an example of an early legislative intervention. *See* Children Online Privacy Protection Act, 47 U.S.C. § 231 (2005). For examples of early judicial regulations of the Internet, see Mainstream Loudoun v. Bd. of Trs. of the Loudoun County Library, 2 F. Supp. 2d 783 (E.D. Va. 1998); Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 N.Y. Misc. Lexis 229 (N.Y. Misc. 1995). Whether intervention should be considered early intervention is also dependent on the technology's rate of diffusion. Where a technology is still used by early adopters an intervention could be considered to be early even if a court ruling takes place twenty years after a technology started diffusing. For a typology of users through a technology's diffusion process, see EVERETT M. ROGERS, DIFFUSION OF INNOVATIONS 279-86 (5th ed. 2003).

20. *See* ROGER B. DWORKIN, THE ROLE OF THE LAW IN BIOETHICAL DECISION MAKING 12-13 (1996); Lyria Bennett Moses, *Understanding Legal Responses to Technological Change: The Example of* In Vitro *Fertilization*, 6 MINN. J.L. SCI. & TECH. 505 (2005).

21. *See* Blake T. Bilstad, *Obscenity and Indecency in a Digital Age: The Legal and Political Implications of Cybersmut, Virtual Pornography, and the Communications Decency Act of 1996*, 13 SANTA CLARA COMPUTER & HIGH TECH. L.J. 321 (1997); Brown, *supra* note 2; Cate, *supra* note 2; Sally Greenberg, *Threats, Harassment and Hate On-Line: Recent Developments*, 6 B.U. PUB. INT. L.J. 673 (1997); Jane Kaufman Winn, *Open Systems, Free Markets and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177 (1998); Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1744-45 (1995); Byron F. Marchant, *On-Line on the Internet: First Amendment and Intellectual Property Uncertainties in the On-Line World*, 39 HOW. L. J. 477 (1996); Paul K. Ohm, *On Regulating the Internet: Usenet, a Case Study*, 46 UCLA L. REV. 1941, 1987 (1999). For an overview of the early approach toward privacy on the Internet, see Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847, 859-62 (2003); *see also* President Clinton, *A Framework for Global Electronic Commerce* (July 1, 1997), http://*www.technology.gov/digeconomy/framework.htm* (last visited Feb. 7, 2006).

progress promotes human welfare.[22] The corollary of this belief is the conviction that intervention with scientific and technological discoveries before their full effects and ramifications are realized could impede human progress.[23] There is often a large gap between the originally envisioned use for a technology and how the technology is eventually used.[24] Early intervention could preclude important opportunities. The telephone, for example, was promoted and used at first only as a business tool. The notion that the telephone could be used for social purposes was unimaginable, even by the phone companies marketing the invention. Private individuals—the users—transformed the early-envisioned role of the telephone and turned it into a social tool.[25] A more recent example is the Internet. The Internet started in the 1960s as a research network in universities. It is the prime example of users transforming the technology and its uses; users' choices turned it into the Internet we know today.[26]

B. *Toward Social Shaping*

The concept of "intervention" is frequently used to describe legal regulation of social behavior. "Intervention" is used in a vast array of legal fields from contracts law to cyberspace law.[27] Its use is not limited to depicting situations where legal action acts to transform society. The term "legal intervention" is used often even in contexts where the law is considered to be enforcing existing social values, norms and structures.[28] I seek

22. *See generally* Christopher Lasch, The True and Only Heaven: Progress and Its Critics 41-44 (1991). Although the belief in progress as a source of prosperity for mankind is not necessarily held by all, it remains a dominant social theme. For skeptical views of the notion of progress as promoting human welfare, see LASCH, *supra;* Leo Marx, *Does Improved Technology Mean Progress? in* TECHNOLOGY AND THE FUTURE (Albert H. Heich ed., 2006).

23. *See* DAVID COLLINGRIDGE, THE SOCIAL CONTROL OF TECHNOLOGY (1980) (developing decision-making theory to address difficulty of deciding before technology's full ramifications are known).

24. Arie Rip and Johan W. Schot, *Identifying Loci for Influencing the Dynamics of Technological Development, in* SHAPING TECHNOLOGY, GUIDING POLICY: CONCEPTS, SPACES AND TOOLS 155, 156 (Knut H. Sorensen & Robin Williams eds., 2002).

25. *See* Claude Fischer, *The Telephone Industry Discovers Sociability, in* TECHNOLOGY AND CHOICE: READINGS FROM TECHNOLOGY AND CULTURE (Marcel C. Lafollette & Jeffrey K. Stine eds., 1991).

26. For a description of the early days of the Internet, see generally, TIM BERNERS-LEE, WEAVING THE WEB: THE ORIGINAL DESIGN OF THE WORLD WIDE WEB BY ITS INVENTOR (1999); JAMES GILLIES & ROBERT CAILLIAU, HOW THE WEB WAS BORN: THE STORY OF THE WORLD WIDE WEB (2000).

27. Examples of articles describing legal action as legal intervention are ubiquitous. This terminology is particularly prevalent in law and social norms literature. For some examples, see Daniel Benoliel, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology,* 92 CAL. L. REV. 1069 (2004); David Charny, *Nonlegal Sanctions in Commercial Relationships,* 104 HARV. L. REV. 375, 426-66 (1990); Sarah E. Waldeck, *Using Male Circumcision to Understand Social Norms as Multipliers,* 72 U. CIN. L. REV. 455, 499-526 (2003).

28. *See* Robert Post, *Law and Cultural Conflict,* 78 CHI.-KENT L. REV. 485 (2003).

here to replace the term "legal intervention" with the term "social shaping," because I believe that in the context of the regulation of new technologies its use is particularly detrimental.

First, the use of the term intervention in the context of the regulation of new technologies assumes a notion of technological determinism. Technological determinism is the view of technology as an autonomous entity that develops according to an internal logic and direction of its own, resulting in determinate impacts on society.[29] In other words, under the technological determinism approach, a given technology has a fixed track of evolution dictated by technological constraints and, therefore, its uses and societal effects are predestined and unchangeable. At the same time, social shaping, a term coined by the social constructivist movement in science and technology studies, embodies a different view of technological evolution.[30] Proponents of social shaping see technology as "a cause" but not "the cause" of the ensuing social effects.[31] The social ramifications of a technology are not predetermined by the technology itself, but are responsive to social reforms that seek to make the innovation compatible with social structures and values.[32] Furthermore, social shaping of a technology is conceived as an interactive process between the technology and its users and not as a top-down process.[33]

The term intervention presupposes technological determinism[34] because it refers to a change of what would otherwise be a natural course.[35] If one recognizes, as many legal scholars writing on law and technology

29. *See generally* HEBERT MARCUSE, ONE DIMENSIONAL MAN (1964); Jacques Ellul, *The Technological Order, in* PHILOSOPHY AND TECHNOLOGY: READINGS IN THE PHILOSOPHICAL PROBLEMS OF TECHNOLOGY 86 (1972). For a rejection of the technological deterministic view, see DAVID ELLIOTT & RUTH ELLIOTT, THE CONTROL OF TECHNOLOGY 5-6 (1976).

30. The term was said to be coined by Donald McKenzie and Judie Wajcman in the title of their 1985 reader "The Social Shaping of Technology: How the Refrigerator Got Its Hum." *See* DONALD MACKENZIE & J. WAJCMAN, THE SOCIAL SHAPING OF TECHNOLOGY: HOW THE REFRIGERATOR GOT ITS HUM (1985); Knut H. Sorensen, *Social Shaping on the Move? On the Policy Relevance of the Social Shaping of Technology Perspective, in* SHAPING TECHNOLOGY, GUIDING POLICY: CONCEPTS, SPACES AND TOOLS 19, 20 (Knut H. Sorensen & Robin Williams eds., 2002).

31. *See generally* WILLIAM B. THOMPSON, CONTROLLING TECHNOLOGY: CONTEMPORARY ISSUES (1991).

32. *See* Robert Heilbroner, *Do Machines Make History, in* CONTROLLING TECHNOLOGY 213, 219-20 (William B. Thompson ed., 1991); John Law & Michel Callon, *The Life and Death of an Aircraft: A Network Analysis of Technical Change, in* SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE 21 (Wiebe E. Bijker & John Law eds., 1992); Russell & Williams, *supra* note 11, at 39.

33. *See* BIJKER, *supra* note 11, at 45-50 (explaining role of "relevant social groups" in social shaping of technology).

34. Even proponents of technological determinism acknowledged that human intervention is possible. *See* Langdon Winner, *The Enduring Dilemmas of Autonomous Technique,* 15 BULL. OF SCI., TECH. AND SOC'Y 67 (1995).

35. The Oxford English Dictionary defines "intervention" as: "the action of intervening, 'stepping in' or interfering in any affair, so as to affect its course or issue" (highlight added). THE OXFORD ENGLISH DICTIONARY (2d ed. 1989).

do, that the choices we make regarding technologies matter because they can result in different social effects, then the use of the term intervention appears unsuitable.[36] Furthermore, the notion of technological innovation is also closely intertwined with the quest for progress. Following World War II, many countries adopted a technology policy framework that focused on promoting science and technology in order to drive economic growth. Technological progress became synonymous with social progress and technological change was perceived as the major driver of social change.[37] If technology is synonymous with progress, then an intervention with the natural course of events becomes an obstacle to achieving progress and human flourishing. Consequently, intervention, particularly early intervention, should be treated with great caution. Once we replace the notion of an intervention that transforms the natural course of events with the concept of social shaping that channels technology into one of several possible routes, however, the question of when should we shape technology to achieve the most effective result becomes less threatening.

A second reason to replace the term intervention with the concept of social shaping is that this would place shaping through technology and shaping through law on equal grounds with regard to our perception of the intrusiveness of the act. Legal scholars have been debating extensively the efficacy of regulation through technology (through code) versus regulation through law.[38] I do not seek to enter this debate but, instead, to emphasize one aspect in which the two modes of regulation share a similar trait. Both shape technology in the sense that they do not intervene with a predetermined route. Yet, regulating technology through technological measures is often referred to as "design," while legal regulation is con-

36. *See, e.g.*, Yochai Benkler discussing the regulation of wireless communications:

> We are in the process today of making a fundamental choice about how we will communicate with each other in the next century. . . . The decision to be made is deceptively "technical": how to regulate that part of the digitally networked environment that utilizes wireless or radio-communications technology. . . . The choice we make among these alternatives will determine the path of development of our wireless communications infrastructure. Its social, political, and cultural implications are likely to be profound.

Yochai Benkler, *Overcoming Agrophobia: Building the Commons of the Digitally Networked Environment*, 11 HARV. J.L. & TECH 287, 290 (1998); *see also*, Jay P. Kesan & Rajiv C. Shah, *Deconstructing Code*, 6 YALE J. L. & TECH. 279 (2003/2004) (adopting social shaping approach to technological design).

37. Russell & Williams, *supra* note 11, at 136.

38. *See* Julie Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); David R. Johnson, Susan P. Crawford & John G. Palfrey, *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J.L. & TECH. 9 (2004); Sonia M. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2003); Mark Lemley, *The Law & Economics of Internet Norms*, 73 CHI.-KENT. L. REV. 1257 (1998); Henry Perritt, *Towards a Hybrid Regulatory Scheme for the Internet*, 2001 U. CHI. LEGAL F. 215; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Through Technology*, 76 TEX. L. REV. 553 (1998); E. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457 (2005); Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679 (2003).

ceived as "intervention."[39] Consequently, legal action is more likely to be perceived as interference than technological action. Applying the term social shaping to both regulation through law and regulation through technology underscores that both act to channel technology towards one of several potential ways that can reflect different social values. Hence, neither is intrusive in the sense that it disrupts the natural progression of the technology.

III. UNPACKING EARLY SOCIAL SHAPING: COMMERCIAL NON-PRIVACY NORMS ON THE INTERNET

Recent technological advances have intensified the debate over the advisability of early social shaping. In this Part, I seek to depolarize the debate regarding early social shaping of new technologies by engaging in a system analysis of Internet technology with regard to the collection of personal information on the Internet by commercial entities. I believe the breadth of the data available on Internet commercial privacy norms makes the phenomenon particularly suitable as a starting point for addressing the question of when social shaping should occur. The Internet privacy threat first entered public debate in 2000. Since then different social shaping measures were tested and ample empirical data is available to evaluate their effectiveness.

I begin by discussing the polarization of the early shaping debate. I proceed to describe the rapid entrenchment of commercial non-privacy norms on the Internet. I then turn to identify three technological characteristics of the Internet: (i) its critical mass point quality (and related network effects); (ii) its decentralized diffusion process; and (iii) its enablement of concealed monitoring. I point out that all three characteristics contributed to the rapid entrenchment of commercial non-privacy norms.

A. *The Polarized Early Social Shaping Debate*

The debate regarding the desirability of early social shaping has been intensified by the implication of certain technologies, such as stem cell research in the political abortion debate.[40] The political association polarized the debate and the answer to whether early social shaping through banning or limiting research is desirable increasingly became a "yes" or "no" answer. My objective here is not to advocate for early social shaping but to take the issue out of its contentious place and to endeavor to un-

39. For writers referring to shaping technological uses through technological measures as "design, " see generally Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537 (2005); *Nimrod Kozlovski, A Paradigm Shift in Online Policing: Designing Accountable Policing (2005) (unpublished J.S.D. Dissertation, Yale Law School), http://crypto.stanford.edu/portia;* Beth Simone Noveck, *The Electronic Revolution in Rulemaking*, 53 EMORY L. J. 433 (2004).

40. *See* Janet Dolgin, *Embryonic Discourse: Abortion, Stem Cells and Cloning*, 19 ISSUES L. & MED. 203 (2004); Saunders, *supra* note 3.

pack the question of timing. I would like to pose the question, when does timing become of the essence for the social shaping of new technologies? The question is particularly pertinent in the context of privacy. Throughout history, new technologies have destabilized the value of privacy. These privacy controversies involved diverse technologies, such as the camera, computer databases and genetics testing. Yet, these controversies varied not only with regard to their technological subject matter but also with regard to the reaction times to the privacy threat.[41]

B. *Commercial Non-Privacy Norms on the Internet*

As the Internet became increasingly popular, web sites and commercial profiling companies began collecting personal information. Their goal was to target advertising to Internet users and sometimes to transform sites to match users' interests and socio-economic status. Web sites and commercial profiling companies collected personal information, such as names, email addresses, web searches conducted and sites visited through a variety of technological devices, primarily cookies, spyware and web bugs.[42]

The Internet privacy threat came into public awareness in 1999-2000.[43] Since then efforts at social shaping were based mainly on self-regulation through privacy notices, privacy seals and through technological measures.[44] Yet, a survey I conducted of empirical studies of the current state of collection practices on the Internet demonstrated an overall increase of privacy-threatening technological devices. We currently have

41. *See* FREEDMAN, *supra* note 5, at 93-112; RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 178-301 (1989); Brandeis & Warren, *supra* note 5.

42. *See* WEB STREET STUDIOS, COOKIE BASICS, http://www.webstreetstudios.com/school/cookies.htm (last visited Mar. 17, 2006); MICROSOFT CORP, UNDERSTANDING COOKIES, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx (last visited Mar. 17, 2006); CENTER FOR DEMOCRACY & TECHNOLOGY, GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM (Nov. 2003), http://www.cdt.org/privacy/03110spyware.pdf (last visited Mar. 17, 2006); David Martin & Hailin Wu, *Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use* 46(12); COMMUNICATIONS OF THE ACM 259, 260 (2003); CYVEILLANCE WHITE PAPER, WEB BUGS: A STUDY OF THE PRESENCE AND GROWTH RATE OF WEB BUGS ON THE INTERNET 2-3 (2001), http://www.cyveillance.com/web/corporate/white_papers.htm (last visited Mar. 17, 2006) [hereinafter *Cyveillance White Paper*]. For a description of the formation of non-privacy norms on the Internet, see STEVEN A. HETCHER, NORMS IN A WIRED WORLD 245, 250, 274 (2004).

43. *See, e.g.*, *Amid Protests*, *supra* note 12, at 13 (reporting on commercial profiling company Doubleclick's intention to incorporate online information with offline database).

44. For a discussion of privacy policies, see THE PROGRESS AND FREEDOM FOUNDATION, PRIVACY ONLINE: A REPORT ON THE INFORMATION PRACTICES AND POLICIES OF COMMERCIAL WEB-SITES (2002). For a discussion of privacy seal organizations, see ELECTRONIC PRIVACY INFORMATION CENTER, ONLINE PROFILING PROJECT, COMMENT, P994809/DOCKET 990811219-9219-01 (1999), http://www.epic.org/privacy/internet/profiling_reply_comment.PDF (last visited Mar. 17, 2006) [hereinafter Epic, *Online Profiling Project*].

more cookies, spyware and web bugs than before.[45] The empirical studies reveal that use of privacy threatening technological devices has become routine among websites and commercial profiling companies on the Internet.

While commercial practices are generally motivated by the desire to achieve financial gain, they can be simultaneously motivated by social norms.[46] Social norms include behavioral patterns relying on conformity that is not necessarily derived from a sense of obligation or normative meaning.[47] At this point, websites and commercial profiling companies have an incentive to conform to each other's behavior.[48] A website unilaterally selecting to cease collecting personal information will be significantly disadvantaged with respect to its competitors who continue to rely on the information for purposes of targeted marketing. In addition, websites have an incentive to assure that other websites maintain their information collection practices. Commercial profiling becomes effective as information is collected across web-sites. Commercial profiling companies converge information collected from different websites and provide their website clientele with profiles based on this combined information. A significant reduction in the number of participants would be detrimental to the usefulness of the practice. Finally, websites have an incentive to assure that other commercial users maintain the stealthy nature of the collection in order to prevent public outrage and potential lawsuits. Consequently, not only do websites have no incentive to change their behavior, they also have an incentive to encourage others not to change the nature of their information collection practices. It appears that the use of privacy threatening tools, such as cookies, web bugs or spyware has become an entrenched social norm among the Internet's commercial users.

C. *Internet Technology — A System Analysis*

The question becomes, what caused the rapid entrenchment of non-privacy norms? Three technological characteristics of the Internet appear to be at the crux of the fast diffusion of non-privacy norms. These characteristics are: (i) the Internet's critical mass point quality (and related net-

45. *See* Bernstein, *supra* note 7.

46. *See* Melvin A. Eisenberg, *Corporate Law and Social Norms*, COLUM. L. REV., 1253, 1253, 1283-87 (1999) (discussing institutional investors' participation norms); *see also* Jody S. Kraus, *Legal Design and the Evolution of Commercial Norms*, 26 J. LEGAL STUD. 377 (1997) (stating that commercial norms will only develop if they provide merchants with on average more cost-effective method of adopting commercial practices). For an example of commercial practices described as social norms, see Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation Through Rules, Norms and Institutions*, 99 MICH. L. REV. 1724 (2001).

47. *See* HETCHER, *supra* note 42, at 1, 18, 30; Eisenberg, *supra* note 46, at 1256-57; Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV J. L. & TECH. 149, 153-56 (2001) (distinguishing between traditional rule conception of norms and pattern conception of norms).

48. *See* HETCHER, *supra* note 42, at 247-50.

work effects); (ii) the Internet's decentralized diffusion process; and (iii) the concealed nature of the privacy threat imposed by the Internet.

1. *Critical Mass Point*

Interactive technologies are often characterized by "network effects." Network effects exist in markets where the value an individual places on a good increases as others use the good. For example, the telephone became more useful and desirable as more people had it and an individual who owned a telephone had more people to call.[49] Network effects become significant once a critical mass of individuals has adopted a technology to make its use worthwhile.

Network effects particularly influence diffusion once critical mass is reached.[50] First, once a technology reaches the critical mass point, its rate of diffusion accelerates.[51] Consequently, where critical mass is attained, technological structures and related norms are rapidly diffused. Second, when critical mass is reached, the dependence on the technology reduces the likelihood of abandonment because the costs of abandonment are increased to unacceptable levels.[52] For example, in 2006, it is more costly for an individual to stop using email unilaterally than it was for her counterpart ten years earlier. Hence, where an interactive technology reaches the critical mass point, existing technological structures and related norms are less likely to be abandoned.

The Internet is considered a network effects technology. The value of the Internet is a function of the number of people who are connected to it.[53] The Internet reached its critical mass point in 1990 with four million

49. *See* Michael Katz & Carl Shapiro, *Technology Adoption in the Presence of Network Externalities*, 94 J. POL. ECON. 822, 822-23 (1986); Mark Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 481, 483 (1998).

50. Another important characteristic of network effect technologies that becomes significant once critical mass is reached is the nature of the demand curve. Goods that do not have network effects have demand curves that slope downwards, that is, as price decreases more of the good is demanded. Goods that have network effects, however, feature a different demand curve. The willingness of individuals to pay for the good increases as the number of goods expected to be sold grows, therefore, price may increase instead of decreasing. *See* Nicholas Economidas & Charles Himmelberg, *Critical Mass and Network Size with Application to the US Fax Market, Discussion Paper No. EC-95-11*, Stern School of Business, N.Y.U., http://raven.stern.nyu.edu/networks/95-11.pdf (last visited May 12, 2006). It should be noted, however, that the presumed increasing returns might not be the only effects at work, because other preferences may eventually also affect choices. *See* Lemley & McGowan, *supra* note 49, at 497.

51. *See* ROGERS, *supra* note 19, at 343-45; M. Lynne Markus, *Toward a "Critical Mass" Theory of Interactive Media*, *in* ORGANIZATIONS AND COMMUNICATION TECHNOLOGY 194 (Janet Fulk & Charles Steinfield eds., 1990); Nicholas Economides, *The Economics of Networks*, INT'L J. OF INDUS. ORG. 27 (Oct. 1996), *available at* http://www.stern.nyu.edu/networks/site.html (last visited May 27, 2006).

52. *See* ROGERS, *supra* note 19, at 343-45; M. Lynne Markus, *supra* note 51.

53. *See* Lemley, *supra* note 38, at 1281.

users worldwide. Commercialization and the growth in the number of commercial users closely followed rapid popular diffusion.[54] Privacy threatening technologies appeared at a period of rapid diffusion and the accompanying non-privacy commercial norms were quickly entrenched.[55] Furthermore, by 2000, the Internet became an integral part of our lives.[56] Consequently a change in non-privacy norms imposed through the threat of abandonment became less likely as abandonment became less plausible.

2. *Decentralization*

A second major characteristic of the Internet—its decentralized nature—also contributed to the rapid entrenchment of non-privacy norms. Decentralized innovations are not controlled by a group of experts. Instead, they are spread horizontally among users. Furthermore, decentralization is not limited to the technology's diffusion. The ability to re-invent or re-design the technology is also decentralized and available to users.[57] The Internet is, in fact, the archetype of a decentralized innovation—its development has historically relied on its users.[58] When the rapidly increasing number of commercial Internet entities discovered the potential for collecting personal information, they were easily able to develop Internet technology to conform to these needs. The ability of individual commercial actors to incorporate privacy-threatening tools, such as cookies, within the developing Internet architecture exacerbated the quick entrenchment of non-privacy norms.

---

54. *See* ROGERS, *supra* note 19, at 343-44, 346.

55. Mark Lemley cautioned as early as 1998 that norms built around technological structures in a network market are likely to prove quite durable. *See* Lemley, *supra* note 38, at 1283-84.

56. A study conducted in 2000 demonstrated the extent to which the Internet had become integral to everyday life. The study surveyed Internet users and showed that 91% used email, 47% purchased products online, 36% made travel reservations online, 60% read news online, 54% searched health information online, 38% looked for a job online, 36% made travel reservations online, 17% engaged in online banking, 36% listened or downloaded music, 35% played online games and 28% participated in chat rooms. *See* PEW INTERNET AND AMERICAN LIFE PROJECT, NEW INTERNET USERS: WHAT THEY DO ONLINE, WHAT THEY DON'T, AND IMPLICATIONS FOR THE NET'S FUTURE (2000), http://www.pewinternet.org (last Visited Mar. 17, 2006).

57. *See* ROGERS, *supra* note 19, at 180, 394-98; DUNCAN J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE 50-55 (2003); Brian S. Butler & Deborah E. Gibbons, *Power Distribution as a Catalyst and Consequence of Decentralized Technology Diffusion, in* INFORMATION SYSTEM AND TECHNOLOGY INNOVATION AND DIFFUSION (McGuire & T. Larsen eds., 1997).

58. *See* Steven R. Salbu, *Who Should Govern the Internet? Monitoring and Supporting a New Frontier,* 11 HARV J.L. & TECH. 429, 435 (1998); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law,* 79 NOTRE DAME L. REV. 815, 832 (2004).

3. *Concealed Monitoring*

The Internet possesses a third characteristic that particularly affects individuals' perception of the privacy threat. Individuals are unaware of the privacy threat because cookies, spyware and web bugs are invisible. Even when Internet users are knowledgeable about Internet information collection practices, the concealed nature of the monitoring dilutes the perception of a threat.[59] Consequently, Internet users have been reluctant to adopt technological measures, such as the Platform for Privacy Preferences (P3P), that can protect their privacy on the Internet.[60] The invisibility of the privacy threat made individuals less likely to undertake measures to protect their privacy.[61]

Although privacy has been traditionally protected as an individual right, a number of writers have pointed out that it also possesses the qualities of a public value. In other words, privacy is important not only to the individual but also to society as a whole. In particular, privacy contributes to a well-functioning democracy.[62] Recently, Paul Schwartz has taken the point further by describing privacy as a public good that benefits society as a whole and cannot be created through an unregulated market. He refers to the privacy public good as "the privacy commons," which requires maintenance through social and legal controls.[63]

The invisibility of the privacy threat underscores the growing need for concerted, instead of individual action, to protect privacy. Devices that

59. For studies examining Internet users' awareness of the privacy threat, see Alan F. Westin, *Social and Political Dimensions of Privacy*, 59(2) J. SOC. ISSUES, 445, 445-46 (2003); Epic, *Online Profiling Project*, *supra* note 44; PEW INTERNET & AMERICAN LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 7 (2000), http://www.pewinternet.org (last visited Mar. 17, 2006).

60. S. REP. NO. 2201, at 11-12 (2002); MICROSOFT CORP., MICROSOFT P3P IMPLEMENTATION SHEET, *supra* note 9; ERNST & YOUNG, ENABLING P3P, *supra* note 9; ERNST & YOUNG, SECURITYSPACE, *supra* note 9. A potential exception is the adoption of anti-spyware software protection. Yet, spyware not only collects personal information, it also disrupts the computer's normal function and its online communications. Hence, user willingness to adopt anti-spyware technology does not, in fact, reflect a reaction to the privacy threat. *See* CENTER FOR DEMOCRACY & TECHNOLOGY, *supra* note 42, at 3; *see also* Bob Tedeschi, *Spyware Heats Up the Debate over Cookies*, N.Y. TIMES, Aug. 15, 2005, at C3. An additional factor that contributed to the failure of the P3P was the inability of Internet users who selected high privacy preferences to use many websites. Websites obstruct entry of users who reject cookies. The limitations and cumbersome interaction likely inhibited even the few users who initially elected to use P3P.

61. *See* James P Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH L. REV. 1, 62 (2003); Malla Pollack, *Opt-In Government: Using the Internet to Empower Choice – Privacy Application*, 50 CATH. U. L. REV. 653, 669-71 (2001).

62. For discussion of privacy as a public value, see PRISCILLA M. REGAN, LEGISLATING PRIVACY 225-27 (1995); Nehf, *supra* note 61, at 1; Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999).

63. *See* Paul M. Schwartz, *Property, Privacy and Personal Data*, HARV. L. REV. 2055, 2079, 2087-89 (2004).

monitor individuals and threaten their privacy have become increasingly concealed. One example is the shift from cameras to cell-phone cameras that can be clandestinely used.[64] Other devices are even more invisible, such as Global Positioning Systems that are being installed in cars and cell phones.[65] Yet, the effect of the increasingly invisible nature of the privacy threat on individuals' willingness to assert their privacy rights can be seen most starkly in the context of the Internet. The effect is more discernible because on the Internet, individuals have an array of technological options to protect their privacy that do not exist in other contexts.[66] Yet, Internet users overall do not adopt these options.[67] It appears that the absence of a perceptible threat makes individuals less likely to act to protect their privacy, contributing to the shift of privacy from a private right to a public value.

The transformation of privacy into a public value sheds additional light on the fast entrenchment of non-privacy norms. As individual users lacked the incentives to act to protect their privacy online, the design of Internet architecture was left to the privacy preferences of commercial actors. These actors embedded the Internet's architecture with privacy threatening technologies that lead to the prevalence of commercial non-privacy norms.

IV. WHY DOES TIME BECOME OF THE ESSENCE?

The previous Part examined the technological characteristics of the Internet that led to the rapid entrenchment of non-privacy norms. In this Part, I suggest that where a technology's characteristics are likely to cause a fast entrenchment of non-privacy norms, decision-makers should pay particular heed to the issue of timing. My conclusion is supported by insights from several fields: (i) the economic theory of Path Dependence; (ii) the science and technology studies theory of Closure; and (iii) law and social norms theory.

---

64. *See Phone Spies Sneak Peeks; Cell Phone Cameras Pose Threat to Privacy*, BOSTON HERALD, July 10, 2003, at 1; Susan Kuczka, *Photo Phones Dial Up Concerns on Privacy; More Towns, Businesses Make Camera Gadgets Off-Limits in Sensitive Locations*, CHI. TRIBUNE, Feb. 25, 2004, at C1.

65. *See* PRIVACY RIGHTS CLEARINGHOUSE, WHEN A CELL PHONE IS MORE THAN A PHONE: PROTECTING YOUR PRIVACY IN THE AGE OF THE SUPER-PHONE (2005), http://www.privacyrights.org/fs/fs2b-cellprivacy.htm (last visited May 27, 2006); Davis D. Janowski, SiRF GPS Chipsets *Your Son's Out Late, Not Answering His Phone*, PC MAGAZINE, Dec. 21, 2005; Joni Morse, *GPS the Newest Tool for Fighting Crime*, RCR WIRELESS NEWS, Oct. 24, 2005; *Wireless Management to Triple*, FLEET OWNER, Dec. 1, 2005, at 73.

66. *See generally* ELECTRONIC PRIVACY INFORMATION CENTER, EPIC ONLINE GUIDE TO PRACTICAL PRIVACY TOOLS (2006), http://www.epic.org/privacy/tools.html (listing privacy enhancing technologies that include: anonymous remailers; anonymous surfing tools; cookie busters; encryption devices; and firewalls).

67. For an extensive discussion of the empirical evidence pointing to the failure to adopt privacy-enhancing technologies on the Internet, see Bernstein, *supra* note 7.

More specifically, in the case of commercial privacy norms on the Internet, the law has proclaimed that commercial profiling on the Internet does not amount to a privacy violation.[68] Similarly, efforts at self-regulation and reactive technological shaping that focused on the individual user have proven ineffective. The theoretical insights derived from the concepts of path dependence, closure and law and social norms studies shed light on the increased difficulties of changing Internet commercial privacy norms at the point when norms have already become entrenched. Thus, these insights underscore the need to consider early shaping to protect privacy where technologies have a critical mass point quality, are decentralized and enable concealed monitoring.

A. *Path Dependence*

Path dependence, broadly defined, refers to the ways in which the path or the way things are done today is affected by the path or choices that were initially selected in the past.[69] For example, we drive a car down a curving road and wonder why it winds around when it is obvious from the landscape topography that a straight road could have been built and would have been much easier to drive. Yet, the road was built decades ago and the authorities are unlikely to raze the houses and commercial establishments built around it to build a straight road even if it should have been done that way in the first place.[70]

Several explanations are offered to account for our dependency on existing paths. First, efficiency and sunk adaptive costs are used to explain path dependence. Where the investments of building the path and creat-

68. *See In re* Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003); *In re* Toys R Us, Inc. Privacy Litigation, No. 00-CV-2746, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001); *In re* DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001). Nevertheless, some restrictions relating mainly to collection of personally identifiable information were imposed by FTC and state settlement agreements. *See* Agreement Between the Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick, Inc. (Aug. 26, 2002), http://www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf (last visited Mar. 17, 2006); Official Ct. Notice of Settlement In re DoubleClick, Inc. Privacy Litig., Master File No. 00-CIV-0641 (NRB) (Mar. 29, 2002), http://www.epic.org/privacy/internet/cookies/dblclkproposedsettlement.pdf (last visited Feb. 7, 2006). In addition, use of spyware has prompted some restrictive legislation and case law. Yet, these protections are not primarily focused on privacy interests but on other spyware harms, such as computer malfunction. *See* CAL BUS. & PROF CODE § 22947 (2005); UTAH CODE ANN. § 13-40-102 (2005); Washington Post et al. v. The Gator Corporation, 2002 U.S. Dist. LEXIS 20879 (E.D. Va. 2002); *Hearings on The Spy Act H.R. 29, Before the House Committee on Energy and Commerce on Combating Spyware*, 108th Cong. (2004).

69. The literature differentiates between two types of path dependence: structure driven path dependence and rule driven path dependence. I refer to structure driven path dependence. *See* Bebchuk & Roe, *supra* note 10, at 129.

70. *See* Mark J. Roe, *Chaos and Evolution in Law and Economics*, 109 HARV. L. REV. 641, 643 (1996).

ing the related resources along the path have already been expended, it may be more efficient to keep the existing path than to build a new one.[71] The inefficiency of the existing path is insufficient to justify creating a new one after comparing the expenses for improving the old structure versus creating a new one. Second, the actors who are motivated to induce change may be ineffective in influencing public choice. This is often the case where existing structures strengthened the influence of the actors who are benefiting from them.[72] Third, information may be unavailable regarding the alternative primarily because imagining the alternative path clashes with the path induced perception that consists of the normal state of affairs.[73]

The concept of path dependence has been primarily used in corporate law literature.[74] Yet, technologies are also, at times, captured by path dependence. Particularly compelling is the story of path dependence evidenced in current computer keyboard design. The computer keyboard design used by most computer users is called QWERTY. QWERTY is, in fact, believed by many to be a sub-optimal keyboard design.[75] Its arrangement of keys was selected to deal with an ancient technological problem—the clashing of type bars on the typewriter—a problem solved by the nineteenth-century. DVORAK, a keyboard design that enables more effective typing, was invented in 1932. Were we to choose between the two keyboards today, without past adaptive sunken costs, we would most likely select the DVORAK keyboard. Yet, users reluctant to adjust to a new typing method declined to adopt the DVORAK path. The preferences of existing users repeatedly outweighed those of new users for whom it would have been more efficient to adopt the DVORAK design.[76]

Similarly, a proposed change of the commercial non-privacy norms, currently dominating the Internet, would be challenged by the forces of path dependence. A large number of commercial actors on the Internet are dependent on the concerted and concealed collection of personal information. A potential switch to an alternative path with different privacy

71. *See* Bebchuk & Roe, *supra* note 10, at 137.

72. *See* Roe, *supra* note 70, at 650.

73. *Id.*

74. *See, e.g.*, Marcel Kahan & Michael Klausner, *Path Dependence in Corporate Contracting: Increasing Returns, Herd Behavior and Cognitive Biases*, 74 WASH. U.L.Q. 347 (1996); Frederick W. Lambert, *Path Dependent Inefficiency in the Corporate Contract: The Uncertain Case with Less Certain Implications*, 23 DEL. J. CORP. L. 1077 (1998); Ronald J. Mann & Curtis J. Milhaupt, *Path Dependence and Comparative Corporate Governance: Forward*, 74 WASH. U.L.Q 317 (1996).

75. For an explanation and history of the DVORAK keyboard, see The DVORAK Keyboard, http://www.mit.edu/~jcb/Dvorak/.

76. *See* Paul A. David, *Clio and the Economics of QWERTY*, 75:2 AM. ECON. REV. 332 (1985); Clayton P. Gillette, *Lock-In Effects in Law and Norms*, 78 B.U. L. REV. 813, 817 (1998). *But see* S.J. Liebowitz & Stephen E. Margolis, *The Fable of the Keys*, XXXIII J.L. & ECON. Apr. 1990, *available at* http://wwwpub.utdallas.edu/~liebowit/keys1.html (last visited May 13, 2006) (arguing that use of QWERTY keyboard is efficient and that Dvorak keyboard was justifiably rejected).

norms that restrict the collection of personal information is likely to be inefficient for the Internet's commercial users.

In addition, the Internet's commercial users, websites and commercial profiling companies that engage in non-privacy norms are significantly more motivated and powerful than individual users in influencing public choice regarding information collection. The individual users, who would benefit from a change in the commercial non-privacy norms, remain relatively passive with regard to the collection of their personal information. Surveys show that, when asked, Internet users vehemently oppose the collection of personal information by commercial actors on the Internet.[77] Yet, the surveys also reveal that Internet users are only partially aware of the scope of these practices.[78] Furthermore, as discussed, the invisibility of the monitoring reduces the likelihood that individuals will react to the privacy threat because they are not aware of it on a daily basis. The invisible nature of Internet monitoring also affects the existing universe of information. The concealed privacy threat affects individual users' ability to appreciate the extent to which a change in privacy norms is needed and to imagine a potential new privacy path. Consequently, individual users are less likely to take the necessary steps to influence public choice and transform existing Internet architecture toward a more privacy enhancing one.

Moreover, Internet technology's vulnerability to path dependence is not solely an indirect result of the technological characteristics that produced the rapid entrenchment of norms. The Internet's susceptibility to path dependence is also a direct consequence of its critical mass point and decentralized qualities. Where a technology is standardized, a shift to an improved standard is less likely because a single user is unlikely to shift to a new system without assurances that a critical mass of potential users will follow suit. If a centralized authority that governs the technology exists, it may enforce such a shift and thereby allay fears that other users will not move to the alternative system.[79]

Internet users, whether individual or commercial, are highly dependent on each other and are unlikely to shift unilaterally to an alternative path. The Internet's commercial users are dependent on concealed technological devices that are effective through sharing information across websites. Even a major commercial website is likely to abandon existing practices without assurances that a significant number of other commercial users would follow. Individual users face a similar quandary. Users who try independently to maintain their privacy, for example, by rejecting cookies find themselves unable to access websites that utilize cookies. The

77. *See* Federal Trade Commission, *Online Profiling: A Report to Congress*, 15-16 (2000) [hereinafter, FTC, *Report to Congress*]; Mary Madden, *Americans' Online Pursuits*, at *5 (2003), http://www.pewinternet.org [hereinafter Pew, *Online Pursuits*].

78. *See* THE PRIVACYPLACE.ORG, 2002 INTERNET PRIVACY USER VALUES SURVEY (2002), http://william.stufflebeam.cc/privacySurvey/results/resultsPage.php; FTC, *Report to Congress, supra* note 77, at 11-12.

79. Gillette, *supra* note 76, at 817.

standardized use of privacy-threatening technological device prevents them from unilaterally protecting their privacy. Further, the Internet lacks a centralized authority that could dictate a shift by commercial or individual users to alternative paths. For instance, a centralized authority's assurance that a significant number of users will concertedly reject cookies could influence websites privacy norms. Websites are unlikely to turn away a large number of customers because their browsers reject cookies. Yet, in the absence of such an authority, individual efforts to combat standardization are less likely to succeed. Hence, the critical mass point quality and decentralization make the Internet particularly vulnerable to the effects of path dependence.

B. *Closure*

Closure is a concept that was coined by the Social Shaping of Technology (SST) movement. Closure is the point by which controversy, surrounding competing designs, uses and norms that are advocated by different groups, subsides. At this point, specific designs, uses or norms become generally accepted. One interpretation of how a technology should be designed or used becomes the norm.[80] Up to the point of closure there is an interpretive flexibility regarding potential designs and uses. But, closure has far-reaching consequences. In a sense, closure restructures the techno-social world related to the technology. Once closure is reached, interpretive flexibility is essentially lost, and although its recapture is possible, it becomes much more difficult to re-open the controversy and regain the status of interpretive flexibility.[81]

The history of the bicycle has been used to portray the concept of closure. The bicycle as we know it today generally has two wheels of equal size. We no longer doubt the effectiveness of this design of the bicycle for what we conceive to be its primary function: transportation. Yet, neither the use nor the design was settled during the early days of the bicycle. The bicycle underwent many design alternatives until it reached its current form.[82] Furthermore, the evolution of the bicycle's design, that many today view as a result of functional solutions, was in fact laden with social value choices.[83]

---

80. *See* Russell & Williams, *supra* note 11, at 120. For further discussion of closure, see Shay David, *On the Uncertainty Principle and Social Constructivism: The Case of Free and Open-Source Software*, http://www.shaydavid.info/papers/shaydavid_scot_of_foss_121803.pdf (last visited May 14, 2006).

81. *See* BIJKER, *supra* note 11, at 85.

82. *Id.* at 19-100.

83. One striking illustration involves the effect of Victorian values on the design of the bicycle. A new design of the bicycle with the two pedals on one side was created to enable women to side-ride the bicycle without engaging in a revealing posture. *Id.* at 43.

The history of the bicycle is not a linear history of evolution progressing toward the safest and most convenient transportation vehicle.[84] Many bicycle designs emerged through the years, including tricycles (three wheel bicycles) and different wheel sized bicycles. Nevertheless, two main conceptions of the bicycle dominated its history: the bicycle as a macho athletic vehicle and the bicycle as a mode of transportation.[85]

The macho bicycle that emerged around 1870 included two wheels of unequal size. The front wheel was about ten times larger than the back wheel. This bicycle was extremely difficult to ride and its main function was not viewed as transportation. It was perceived as a macho sport vehicle and was mainly ridden by young men. The conception of the bicycle as a macho sports vehicle gave rise to different designs all emphasizing the size of the front-wheel.[86] At the same time, the alternative view of the bicycle as a transportation vehicle instigated the creation of a series of designs to improve safety.

Eventually the view of the bicycle as a transportation vehicle prevailed and the safest design was selected. At that point, the bicycle has reached closure. Interpretive flexibility regarding the design and uses of the bicycle was essentially lost; the bicycle debate is unlikely to be re-opened.[87] Closure does not mean, however, that the selected design was necessarily the overall best or most efficient design because this determination would depend on the use of the bicycle. It was the best design for the prevailing use conception—transportation.[88]

Closure can be a major obstacle to change as it forecloses options and curtails flexibility.[89] The debate remains open as to the degree to which closure is necessarily final. In particular, critics have questioned whether the concept of closure is equally applicable to all technologies or to all aspects of complex dynamic technologies.[90] Yet, even allowing that closure is merely a matter of degree—that stabilization may be incomplete and that controversy could potentially be re-opened—it is apparent that closure has an impact. Once controversy subsides and individuals cease to hold conflicting interpretations regarding social uses and designs of the technology, our ability to transform design and uses is substantially decreased.

Let us return to the case of the Internet and privacy norms. Despite their awareness of the use of privacy violating tools, individual users failed to challenge the commercial actors' information collection practices. They did not initiate and compel a competing perception of commercial privacy—consequently, the non-privacy norm prevailed among commer-

84. *Id.* at 50-51.
85. *Id.* at 19-100.
86. *Id.* at 37-41.
87. *See id.* at 19-100.
88. *Id.* at 75.
89. *See* Russell & Williams, *supra* note 11, at 58.
90. *See id.* at 57.

cial users. The Internet's critical mass point and decentralized diffusion induced a rapid evolution of technological artifacts, such as cookies, and of non-privacy norms. Determinations regarding designs and modes of use, that for some technologies evolve over decades, were made rapidly, reaching closure at an exponential rate and with it the loss of interpretive flexibility. While the bicycle reached closure after decades of shifting between the athletic macho and transportation conception, commercial non-privacy norms reached closure within several years. Once interpretive flexibility was lost, the reversal of existing privacy practices is likely to encounter increased difficulties.

C. *Law & Social Norms Theory*

Additional support for the significance of timing can be drawn from law and social norms literature. Law and social norms literature does not address the issue of timing directly; instead it focuses on the reduced effectiveness of legal measures where they stand in stark contradiction to existing social norms.

The literature shows that laws are less likely to be effective where they sharply digress from existing social norms.[91] Imagine a law aimed at reducing instances of drug and alcohol use among youngsters by requiring that individuals under twenty-one years of age live with their parents, an adult guardian or a government institution. Such a law would contradict deeply engrained liberal convictions expecting the young American to leave home in a quest for self-fulfillment, whether through studies or work.[92] Consequently, it is unlikely to be effective in changing relationships between young adults and parents.

Conversely, the literature shows that laws are generally more effective where a new rule does not digress from a community's expectations and social meanings of certain acts.[93] For example, a law requiring that children under five reside with an adult, a guardian or an appropriate institution does not deviate from existing social norms that accept that very young children are unable to care for themselves. Such a law is, therefore, more likely to accomplish effective compliance.[94]

---

91. *See* Kahan, *supra* note 13, at 608; Scott, *supra* note 13, at 1926-28.

92. *See* ROBERTY NEALY BELLAH ET AL., HABITS OF THE HEART: INDIVIDUALISM AND COMMITMENT IN AMERICAN LIFE 62 (rev. ed. 1996).

93. *See* Robert Cooter, *Do Good Laws Make Good Citizens? An Economic Analysis of Internalized Norms,* 86 VA. L. REV. 1577, 1597 (2000) (stating "[t]he primary way to prompt people to instill civic virtue in each other is by aligning law with morality"); Robinson, *supra* note 14, at 1858 (explaining that deference to layman intuitions is useful because it enhances criminal laws' normative control power).

94. Lawrence Lessig differentiates between offensive and defensive uses of social meanings construction. Some laws seek offensively to transform social meaning construction while others seek to defensively maintain an existing social meaning and prevent it from changing. Lessig concludes that defensive social meaning construction is more likely to be effective than offensive social meaning construction. *See* Lessig, *supra* note 14, at 986-87, 999. The law requiring individu-

Looking back to laws that diverge substantially from existing social norms, it appears that such laws may not only be less effective in transforming social norms, but may actually backfire by enhancing the very norms they seek to change.[95] It was suggested, for instance, in the context of criminal law, that some crimes may be self-defeating. In other words, criminalizing the behavior may, in fact, result in bolstering the social norm that the crime was designed to dilute.[96]

Specifically, the insights described above shed light on instances of non-compliance involving laws that are structured to regulate conduct related to uses of new technologies. Laws criminalizing uses of technologies that amount to a copyright violation have been particularly ineffective. A prominent example involves peer-to-peer file sharing. Despite numerous lawsuits by the Recording Industry Association of America (RIAA) against file-sharers, file sharing remains a prevalent phenomenon.[97] Dominant social norms do not conceive of file sharing as immoral conduct and it appears that copyright violations are not embedded with social stigma.[98] Hence, peer-to-peer file sharing remains an extensive practice despite legal action. The inefficacy of prohibitory laws designed to reinforce contra-

---

als to reside with adults until age twenty-one would be an example of a law seeking offensive meaning construction. The law requiring children under five to reside with adults could be viewed as defensive meaning construction if it was enacted to deal with, say, a concern regarding an evolving trend of use of private boarding schools for children of tender years.

95. *See generally* Francesco Parisi & George Von Wagenheim, *Legislation and Countervailing Effects from Social Norms, in* THE EVOLUTION AND DESIGN OF INSTITUTIONS (C. Shubert and G. Von Wagenheim eds., 2006), http://www.papers.ssrn.com/sol3/papers.cfm?abstract_id=569383.

96. *See* William J. Stuntz, *Self-Defeating Crimes,* 86 VA. L. REV. 1871, 1872 (2000).

97. *See* Ben Depoorter, Sven Vanneste et al., *Gentle Nudges v. Hard Shoves in Copyright Law: An Empirical Study on the Conflict Between Norms and Enforcement,* (Ghent Ctr. for Advanced Studies in Law & Econ., Working Paper No. 6, 2005 at 3), http://www.law.ugent.be/grond/casle; David W. Opderbeck, *Peer to Peer Networks, Technological Evolution and Intellectual Property Reverse Private Attorney General Litigation,* 20 BERKELEY TECH. L.J. 1685 (2005); ELECTRONIC FRONTIER FOUNDATION, RIAA V. THE PEOPLE: TWO YEARS LATER, http://www.eff.org/IP/P2P/RIAAatTWO_FINAL.pdf (last visited Apr. 8. 2006); Jefferson Graham, *File-Sharing Beat Goes On,* USA TODAY, June 29, 2005, at 3B. *But cf.* Lee Rainie & Mary Madden, *Pew Internet Project and Comscore Mediametrix Data Memo: The State of Music Downloading and File-Sharing Online* (Apr. 2004), http://www.pewinternet.org/pdfs/pip_filesharing_April_04.pdf (last visited May 14, 2006). For a general discussion of the effect of law on file-sharing social norms, see Yuval Feldman & Janice Nadler, *Expressive Law and File Sharing Norms,* Northwestern University School of Law Public Law and Legal Theory Research Paper Series, Research Paper No. 12-05, http://www.ssrn.com (last visited May 14, 2006).

98. *See* Steven A. Hechter, *The Music Industry's Failed Attempt to Influence File Sharing Norms,* 7 VAND. J. ENT. L. & PRAC. 10, 10-13 (2004); Chris Collins, *Downloading Lowdown: File-Sharing Is the Moral Equivalent of Stealing a Car,* SEATTLE TIMES, Oct. 25, 2003 (quoting Gallop poll showing that only 18% of 13- to 17-year olds considered cheating on test morally acceptable, while 83% considered downloading music through file-sharing to be morally acceptable).

dictory social norms is not restricted to the file sharing phenomenon. Similar trends have been identified with regard to unauthorized copying of software, music CDs and videotapes.[99] In all these instances of social norms related to unauthorized copying individuals do not perceive the conduct as immoral. Consequently, unauthorized copying remains prevalent despite prohibitory copyright protection rules.

Law and social norms scholars have offered two main theories to explain this counter-intuitive phenomenon. One theory focuses on the nature of the task that the law is charged with. Under this explanation, the law has an easier task when implementing a rule that does not contradict existing social norms because the prohibited conduct is already embedded with social stigma.[100] People obey the law because they fear the disapproval of their social group. They follow the social norms of their group because they would be rewarded for following them and sanctioned for failing to do so. Hence, the law is not required to re-structure social stigma. Its role is limited to reinforcing existing stigma structures and disciplining violators who do not abide by social expectations. Conversely, where a norm does not carry social stigma, instead of fearing social sanctions violators often receive sympathy when breaking the law prohibiting this conduct. The law is faced by a much more arduous mission that requires transforming structures of social stigma in order to accomplish compliance.[101]

An alternative theory concerns legitimacy. Two main factors contribute to legal compliance. One is deterrence–the effect of potential legal sanctions and benefits. The second is legitimacy—the belief that the law-making authority and the substantive content of the law are entitled to deference.[102] Studies show that legitimacy is undermined when the content of the law diverges from social norms.[103] Consequently, where a law departs from accepted social norms a crucial ingredient of compliance is lost and the law is less likely to be effective.

Law and social norms theory suggests that an attempt at social shaping, after norms related to a technology are entrenched is likely to encounter a significant hurdle. The history of privacy on the Internet illustrates this point. Non-privacy norms are currently prevalent among the Internet's commercial users. They have existed and been reinforced since the mid-1990s. Although only the Internet's commercial actors exercise the non-privacy norms, studies show that law encounters enforcement

99. *See* Stuart P. Green, *Plagiarism, Norms, and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights*, 54 HASTINGS L.J. 167, 173, 236-37 (2002).

100. *See* Parisi and Von Wagenheim, *supra* note 95, at 3.

101. *See* Lessig, *supra* note 14, at 999; Robinson, *supra* note 14, at 1861-63; Lior Jacob Strahilevitz, *How Changes in Property Regimes Influence Social Norms: Commodifying California's Carpool Lanes*, 75 IND. L.J. 1231, 1266-67 (2000).

102. *See* TOM R. TYLER, WHY PEOPLE OBEY THE LAW 19-57 (1990).

103. *See id.*; Parisi & Von Wagenheim, *supra* note 95, at 26-28.

hurdles even where the norm that the law seeks to enforce is held only by part of the population. The failure of national prohibition provides a prime example of the law's inefficacy in accomplishing compliance and transforming social norms, even where a significant portion of the public supports the change.[104] Commercial users of the Internet are a dominant group both online and offline. Consequently, non-privacy norms, actively used by this group will likely be hard to change. Existing personal information collection and privacy norms are currently not enshrouded with social stigma. Hence, a legal effort to transform these norms would face the hurdle of transforming stigma structures in cyberspace. The hurdles faced by such a delayed legal reaction highlight the significance of deferring to timing when evaluating reactions to technologies that are characterized by a critical mass point quality, decentralized diffusion and concealed monitoring.

V. MODES OF EARLY SOCIAL SHAPING

The theoretical insights discussed in the previous Part point to the relatively narrow window of opportunity for privacy protection that is available where a new technology has a critical mass point quality, decentralized diffusion and imposes a concealed threat. In such instances, both legal and technological privacy protection measures are likely to be less effective beyond the initial period of change and fluidity. In these cases, timing is of the essence. I seek in this Part to explore the ways in which both legal and technological decision-makers can sensitize their decisions to account for the importance of timing when dealing with new technologies that share the aforementioned characteristics.

I do not suggest that early shaping could be warranted only where these characteristics exist. Nor do I maintain that early social shaping is always the best resolution in these cases. I propose, however, that the existence of these conditions should raise a flag of urgency. Decision-makers faced with such instances should give the option of early social shaping particularly careful consideration. Although social shaping at a later point could still be possible, and could take place through user interaction, early social shaping should be carefully evaluated because options and modes of shaping may be considerably more limited at a later point.[105]

In the case of the Internet, a decade after the development of commercial non-privacy norms—and in the absence of a significant legal or technological reaction—the window of opportunity may already be partly closed. This is not to say that options are unavailable to influence non-privacy norms. The task faced by legal decision-makers and technological

104. *See generally* RICHARD F. HAMM, SHAPING THE EIGHTEENTH AMENDMENT (1995); DAVID E. KYVING, REPEALING NATIONAL PROHIBITION (1979).

105. Options may still be available for changing entrenched social norms although they may be more limited. *See generally* Parisi & Von Wagenheim, *supra* note 95 (noting descriptions and proposals demonstrating possibilities of transforming entrenched social norms); Strahilevitz, *supra* note 101 (same).

designers at this point, however, is significantly more difficult than the one encountered ten or even five years ago.

At the same time, the examination of Internet commercial non-privacy norms carries significance beyond offering a potential resolution for transforming the specific non-privacy norms at issue. Technologies sharing the characteristics that lead to rapid entrenchment of non-privacy norms are likely to emerge. The current trend in monitoring devices points to a development of increasingly invisible tracking mechanisms, such as Radio Frequency Identification (RFID) tags that can be invisibly implanted in objects such as passports or even currency.[106] Furthermore, the Internet's critical mass point and decentralized diffusion qualities that led to the entrenchment of commercial non-privacy norms on the Internet could serve as a platform for the emergence of other non-privacy norms.[107]

Both legal and technological modes of social shaping are influenced where the technological characteristics of a technology point to the significance of timing. The passage of time reduces the effectiveness of both modes of shaping. Yet, both modes can be sensitized to timing.

Technological design to protect privacy can take place during the period of initial design where the technology is constructed to meet functional requirements.[108] For example, a medical database that is designed for effective collection and retrieval of medical information can also be programmed to ensure that unauthorized personnel will be denied access to the information. Alternatively, technological design for privacy can be executed at a later stage, once individuals are using the technology and the privacy threat becomes apparent. The P3P project was an example of subsequent technological design. It consisted of privacy protecting design that was added to Internet browsers at a later stage.

Initial and subsequent designs are not necessarily alternative options. In many cases, a technology would be designed initially and then subse-

106. *See generally* ELECTRONIC PRIVACY INFORMATION CENTER, RADIO FREQUENCY IDENTIFICATION (RFID) SYSTEMS, http://www.epic.org/privacy/rfid (last visited Apr. 8, 2006).

107. For other examples of non privacy norms, see generally Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH L. REV. 335 (2005) (discussing ISPs and non-privacy norms); Frank Pasquale, *Theorizing the Law of Search: Toward Authoritative and Responsible Metadata Providers* (unpublished manuscript on file with author) (discussing search engines and non-privacy norms).

108. An example of a proactive project of early social shaping through design is UrbanSim. *See* Batya Friedman, Peter H. Kahn & Alan Borning, *Value Sensitive Design and Information Systems*, *in* HUMAN-COMPUTER INTERACTION IN MANAGEMENT INFORMATION SYSTEMS 9-12, 14 (P. Zhang & D. Galletta, eds. forthcoming 2006), http://epl.scu.edu:16080/~stsvalues/readings.html. For a description of the challenges of early social shaping through design, see, Mary Flanagan, Daniel Howe & Helen Nissenbaum, *Embodying Values in Technology: Theory and Practice*, 21-26, http://www.nyu.edu/projects/nissenbaum/papers/Nissenbaum-VID.4-25.pdf (last visited, Apr., 8, 2006).

quently redesigned through user participation.[109] Yet, the problems encountered in the P3P experiment point to the significance of making a concerted effort to design for privacy at the outset. Decentralized technologies require user action to transform privacy preference design. Where the technology is broadly diffused, non-privacy norms are likely to be widespread. Consequently, extensive user cooperation is needed to implement privacy enhancing design. The P3P case shows that where the technology enables concealed privacy monitoring, user adoption of privacy protecting tools is less likely. This is particularly the case where the privacy harm is not accompanied with a more tangible or salient harm, such as identity theft or computer malfunction.[110] Consequently, a proactive and concerted approach to design privacy protection at the outset is likely to be most important for interactive technologies that have a critical mass point quality, are decentralized and are likely to enable concealed monitoring.[111]

Legal decision-makers considering potential privacy protection of technologies that are prone to rapid norm entrenchment and enable concealed monitoring should account for the issue of timing in their decision-making process. This is not to say that early shaping should always be preferred. Additional considerations may outweigh the timing factor. My argument is constrained to emphasizing the need for decision-making to be particularly sensitive to timing in the above-specified circumstances.

Furthermore, I do not endeavor to give exact estimates of the breadth of the window of opportunity for early legal social shaping.[112] The breadth of such a window may vary between technologies. Looking back to the case study of commercial norms on the Internet, one example stands out. Unlike collection of adult personal information by commercial entities, the collection of children's personal information received early attention by the legislature. The Child Online Privacy Protection Act (COPPA), which applied to the collection of personal information from children under thirteen, was enacted in 1998.[113] By April, 2000, a Federal Trade Commission rule pursuant to COPPA was in effect.[114] COPPA included requirements that directly limited collection of personal informa-

109. *See* Friedman, Kahn & Borning, *supra* note 108, at 13-14.

110. Individuals are more likely to install software and firewalls to prevent computer harm by viruses or spyware than to protect themselves against collection of information harms. They are also more likely to take precautionary measures to avoid identity theft, mainly by being more cautious about giving their personally identifiable information online.

111. Proactive designing for privacy is already taking place through the PORTIA Project. For a description of the project, see Dan Boneh, Joan Feigenbaum & Avi Silberschatz, *PORTIA, Privacy, Obligations, and Rights in Technologies of Information Assessment*, http://crypto.stanford.edu/portia (last visited Apr., 8, 2006).

112. Views differ as to the appropriate timing of early legal social shaping. *See, e.g.*, Swire, *supra* note 21, at 863-71.

113. COPPA, 15 U.S.C. § 6502(b) (2000).

114. *See* 16 C.F.R. § 312.1 (1999).

tion about children.[115] Website operators are prohibited from collecting personal information about children unless they obtain verifiable parental consent.[116] In addition, website operators are prohibited from conditioning a child's participation in a game, the offering of a prize or other activities on a child's disclosure of more personal information than is reasonably necessary for participation.[117]

The main bulk of empirical data regarding compliance was collected a year after the COPPA restrictions came into effect. Yet, even this early data shows significant reductions in the personal information collected about children and a growing compliance with parental notification requirements.[118] Furthermore, the Electronic Privacy Information Center, a privacy watchdog, recently issued a letter to the Federal Trade Commission, in which it urged additional compliance research, but stated that: "There is a sense of increasing compliance, that COPPA has curtailed the development of a large data collection culture targeting children online."[119] Although additional research needs to be conducted regarding COPPA compliance, early legal social shaping appears to have created different privacy social norms on the Internet regarding personal information of children from those applying to adult personal information. The creation of two different sets of privacy norms in a relatively similar situation support the significance of timing in this context.

VI. CONCLUSION

This Article sought to commence an inquiry into the relationship between time, technology and privacy. My goal was not to advocate early social shaping as an ultimate resolution for protection of privacy against new technological threats. Instead, I aspired, through careful examination of the case of Internet commercial privacy norms, to provide initial guidelines as to when timing becomes an important factor in structuring social reactions to privacy threats.

This Article identified three conditions that lead to rapid entrenchment of non-privacy norms: critical mass point quality; decentralized diffusion; and concealed monitoring. It showed that where these conditions exist timing becomes of the essence and both technological and legal modes of social shaping are affected. The Article proposed that under these conditions, social shaping through technological design would be

115. *See* COPPA, 15 U.S.C. § 6502(b) (2000).

116. *See id.* § 6502(b)(1)(A)(ii).

117. *See id.* § 6502(b)(1)(C).

118. *See* CENTER FOR MEDIA EDUCATION, COPPA: THE FIRST YEAR: A SURVEY OF SITES– A REPORT ON WEB SITE COMPLIANCE, 7 (2001) (reporting early success of COPPA); FTC, *Protecting Children's Privacy Under COPPA: A Survey on Compliance,* 3-6, 13-14 (Apr. 2002) (same).

119. Letter from Electronic Privacy Information Center to FTC (June 27, 2005), http://www.epic.org/privacy/kids/ftc_coppa_62705.html (last visited Apr., 8, 2006).

more effective through concerted proactive design for privacy protection at the outset. As for legal social shaping, it suggested that although early social shaping may not always be the appropriate response under these conditions, timing needs to be considered as an important factor in legal decision-making.