CONNECTICUT
LAW REVIEW

VOLUME 39 NOVEMBER 2006 NUMBER 1

Article

The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy

GAIA BERNSTEIN

New technologies often cause social controversies by creating novel privacy threats. Academics and legal decision-makers seeking to resolve these controversies have traditionally focused on the appropriate measures to protect privacy. Yet, traditional thinking ignored the relationship between privacy pressures and a technology's diffusion process. In this Article, I examine controversies involving privacy and two recent technological innovations—genetic testing and the Internet through the privacy-diffusion prism.

First, I show that privacy-diffusion imbalances underlie important techno-privacy controversies. Specifically, I identify two models. In the first model, diffusion is inhibited despite the absence of an actual privacy threat. This model is based on the case of genetic discrimination, which shows that contrary to common belief, genetic discrimination is rare and apparently on the decline. Yet, fears of privacy violations inhibit the technology's diffusion. In the second model, diffusion accelerates despite mounting privacy threats. The second model is based on controversies involving privacy on the Internet that show that although privacy threats on the Internet are consistently on the rise, the diffusion of Internet technology continues to accelerate.

Secondly, I identify the technological characteristics that affected the diffusion process of genetic testing and Internet technologies. These characteristics include the preventive, non-triable and centralized nature of genetic testing technology and the critical mass point and decentralized qualities of Internet technology. I suggest that these diffusion characteristics made the Internet and genetic testing susceptible to their respective privacy-diffusion imbalances and could be key to their resolution. Further, I propose that since these diffusion attributes are shared by other technologies, their early identification by decision-makers would improve the social accommodation of privacy threatening technological innovations.

ARTICLE CONTENTS

I. INTRODUCTION 245

II. THE PRIVACY PROTECTION-DIFFUSION RELATIONSHIP 251

A. DIFFUSION 251
B. BALANCING DIFFUSION AND SOCIAL VALUES 253
C. PRIVACY 255

III. DISPERSING MYTHS AND FABLES IN THE TECHNO-PRIVACY ARENA 257

A. GENETIC DISCRIMINATION 257
B. COLLECTION OF PERSONAL INFORMATION BY COMMERCIAL ENTITIES ON THE INTERNET 266
C. EMPLOYER MONITORING OF INTERNET AND EMAIL 275

IV. SUSPECT PRIVACY-DIFFUSION RELATIONSHIPS 279

A. THE PRIVACY-DIFFUSION RELATIONSHIP 279
B. SUSCEPTIBLE TECHNOLOGIES 281

V. POLICY IMPLICATIONS 288

A. REGULATING PREVENTIVE, NON-TRIABLE AND CENTRALLY DIFFUSED TECHNOLOGIES 288
B. REGULATING CRITICAL MASS AND DECENTRALIZED TECHNOLOGIES 291

VI. CONCLUSION 296

The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy

GAIA BERNSTEIN*

I. INTRODUCTION

The law often acts to resolve social controversies stemming from clashes between new technologies and the value of privacy. In our age of rapid technological progress, examples are ubiquitous. Privacy advocates are concerned about the government's plans to use radio frequency identification (RFID) tags in passports.[1] Similarly, the use of large computer databases to combat terrorism in the aftermath of 9/11 prompted claims that such use of computer technology erodes individuals' privacy interests.[2]

Legal academics and decision-makers generally focus on protecting privacy interests that are compromised by new technologies. Debates revolve around the need and the appropriate measures to protect privacy.[3] Although vital, the privacy protection debates do not account for some of the more important tensions underlying new technology-privacy controversies. Moreover, resolutions achieved through these debates are frequently lacking and incomplete.

The diffusion of a new technology takes place after a technology is invented and involves the process through which society adopts the new technology.[4] Traditional thinking has so far failed to recognize that social

---

* Associate Professor of Law, Seton Hall University School of Law. Email: bernstga@shu.edu. I owe thanks to Amy Adler, Jack Balkin, Yochai Benkler, Shay David, Rochelle Dreyfuss, Erik Lillquist, Helen Nissenbaum, Frank Pasquale, Amit Solomon, Charles Sullivan, Sarah Waldeck and Tal Zarsky for comments and helpful conversations. This Article benefited from the comments of the participants of the Information Society Project Colloquium at Yale Law School, the Colloquium on Information Society and Technology at the New York University School of Law, the Law, Ethics and Life Sciences Conference at the University of Minnesota Law School, the Seton Hall University School of Law Faculty Seminar, the Society for Evolutionary Analysis in Law Conference at Vanderbilt Law School, the Fifth Annual Intellectual Property Conference at Cardozo Law School, the Genetic Information Conference at Haifa University Faculty of Law, the International Symposium on Technology and Society at Loyola Marymount University, the Health Law Teachers' Annual Conference and the Law, Culture and Humanities Annual Conference. Thanks to Joe Farano, Jill Kelly, Monica Kostrzewa and Paul Werner for valuable research assistance. The Article was made possible by the generous support of the Seton Hall University School of Law Summer Research Stipend Program.

[1] *See* Electronic Privacy Information Center, *Radio Frequency Identification (RFID) Systems*, http://www.epic.org/privacy/rfid (last visited Aug. 3, 2006).

[2] *See, e.g.*, Electronic Privacy Information Center, Secure Flight Page, http://www.epic.org/privacy/airtravel/secureflight.html (last visited Aug. 26, 2006). *See also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 165–87 (2004).

[3] *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001).

[4] *See generally* EVERETT M. ROGERS, DIFFUSION OF INNOVATIONS 5 (2003); Nicholas A. Ashford et al., *Using Regulation to Change the Market for Innovation*, 9 HARV. ENVTL. L. REV. 419,

tensions arising from technological pressures on privacy are closely intertwined with the technology's diffusion process. In this Article, I demonstrate that the relationship between privacy protection and technological diffusion is fundamental to the techno-legal debate. I proceed to explain that social controversies involving uses of new technologies often stem from an imbalance between technological diffusion and privacy protection. The relationship between diffusion and privacy protection creates social strife where a technology broadly diffuses while significantly eroding privacy interests. Similarly, tensions arise where individuals refrain from using an important new technology due to privacy concerns. Consequently, I suggest that the interaction between privacy and technological diffusion should be incorporated into the decision-making process of those charged with regulating new technologies.

This Article starts by exposing instances where the relationship between technological diffusion and privacy underlies social tensions related to uses of new technologies. I lay out the descriptive basis of the inquiry using three controversies involving pressures applied by two information technologies, which are in the midst of their diffusion process: genetic testing and the Internet on the value of privacy.[5] Specifically, I examine three case studies: (i) genetic discrimination by insurers and employers; (ii) collection of personal information on the Internet by commercial entities; and (iii) employers' monitoring of Internet and email use by employees. The debates involving these controversies focused on potential resolutions to the threats imposed by genetic testing and the Internet on privacy.[6] Some of these resolutions were even implemented.[7]

---

419 n.1 (1985) (noting that technological innovation "should be distinguished from invention, which is the development of a new technical idea, and from diffusion, which is the subsequent widespread adoption of an innovation . . . ."); Michael A. Gollin, *Using Intellectual Property to Improve Environmental Protection*, 4 HARV. J.L. & TECH. 193, 197–98 (1991) (describing the "technology cycle" as having three phases—invention, innovation, and diffusion).

[5] I chose to focus on two technologies that are traditionally treated separately, yet share important commonalities. Both are information technologies that have instigated controversies involving their use and the value of privacy. Moreover, both are currently in the midst of their diffusion process, thereby enabling me to assess the effectiveness of different intervention measures that were applied. Few scholars study medical technologies and communication technologies together. For other studies analyzing technologies within this broader framework, see generally, Dan L. Burk, *Lex Genetica: The Law and Ethics of Programming Biological Code*, 4 ETHICS & INFO. TECH. 109 (2002); Jim Chen, *Webs of Life: Biodiversity Conservation as a Species of Information Policy*, 89 IOWA L. REV. 495 (2004).

[6] *See generally* George J. Annas, *Genetic Privacy: There Ought to be a Law*, 4 TEX. REV. L. & POL. 9 (1999); Fred Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289 (2002); Pauline T. Kim, *Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace*, 96 NW. U. L. REV. 1497 (2002); Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United*

Yet, no comprehensive study has evaluated the effects of these privacy protection attempts on the diffusion of the technologies at issue. The first part of this Article, therefore, documents the relationship between interventions aimed at protecting privacy and the diffusion of each technology. In each case study I use empirical evidence to assess the extent to which privacy-threatening uses of the technology are still taking place and the effects on the diffusion of the technology.

When viewing these controversies through the broader privacy-diffusion prism, two models of suspect privacy-diffusion relationship emerge. The genetic discrimination case study exhibits one suspect privacy-diffusion relationship model. The study reveals that despite grave public concerns regarding genetic discrimination, privacy has not been compromised.[8] Genetic discrimination is rare and apparently on the decline. Potential abusers, such as employers and insurers, do not use genetic information. Paradoxically, individuals continue to fear genetic discrimination and are, therefore, less likely to test for genetic diseases. An examination of the relevant legal arena reveals that the law had a limited function in preventing genetic discrimination. The partial and inconsistent legal protections against genetic discrimination played an expressive role, but not a coercive one. Furthermore, the partial and inconsistent legal protection appears to have induced uncertainty, thereby failing to alleviate people's fears and promote the diffusion of genetic testing technology.

The two Internet case studies exhibit a very different suspect privacy-diffusion relationship model. The data reveals that privacy threats imposed by Internet technology exist and their severity continues to rise.[9] The law has, in effect, authorized these privacy-threatening uses of the technology, pronouncing that they do not constitute illegal privacy violations. Paradoxically again, the diffusion of Internet technology has not been affected by these severe privacy threats.

This Article proceeds to identify the technological characteristics that affect the diffusion process of genetic testing and the Internet, and make

---

States and Canada, 2004 STAN. TECH. L. REV. 4 (2004); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000); Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet* Privacy, 54 HASTINGS L.J. 847 (2003); Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737 (2004).

[7] *See, e.g.*, Genetic Information Privacy Act, N.M. STAT. § 24-21-4 (2005). *See also* Simon Byers et al., *Searching for Privacy: Design and Implementation of P3P-Enabled Search Engine* (paper presented at the 2004 Workshop on Privacy Enhancing Technologies (PET), Toronto, Can., May 26–28, 2004), *available at* http://lorrie.cranor.org/pubs/pets04.html.

[8] *See infra* Section III.A.

[9] *See infra* Sections III.B–C.

them susceptible to the suspect privacy-diffusion relationships. I suggest that other technologies may share similar diffusion characteristics, and therefore be vulnerable to the same type of suspect privacy-diffusion relationships. Consequently, I propose that the consideration of diffusion characteristics could resolve, or even prevent, such suspect privacy-diffusion relationships. At the same time, since the conclusions presented in this Article are derived from the study of privacy controversies involving only two technologies, they would require further refinement through the examination of additional technologies. The following insights can, however, serve as a first step toward formulating guidelines that could be applied across technologies.[10]

First, I point out that technologies that are preventive and non-triable, like genetic testing, are susceptible to the first suspect privacy-diffusion relationship, where diffusion is inhibited despite the absence of an actual privacy threat.[11] Preventive innovations are technologies that are used to prevent unwanted consequences, while non-triable technologies are technologies that cannot be experimented with. Overall, individuals are more hesitant to adopt preventive and non-triable technologies. Consequently, where a person is already disinclined to adopt a technology and is contemplating whether to utilize it for the first time, any additional concerns—such as privacy threats—become aggravated.[12] Hence, technologies that are preventive and non-triable are more likely to become entrapped in the first suspect relationship model, exemplified by the case of genetic discrimination.

Second, I argue that where a technology's diffusion attributes increase the likelihood that a perception of a privacy threat will affect diffusion, the expressive role of the law in dispelling such misperception is of particular importance.[13] Decision-makers who choose to restrict the use of a new technology in order to protect privacy generally employ either an express

---

[10] Among the few studies developing a more general theory of law and technology are: LAWRENCE H. TRIBE, CHANNELING TECHNOLOGY THROUGH LAW (1973); Gaia Bernstein, *The Socio-Legal Acceptance of New Technologies: A Close Look at Artificial Insemination*, 77 WASH. L. REV. 1035 (2002); Arthur J. Cockfield, *Towards a Law and Technology Theory*, 30 MAN. L.J. 383 (2004); Gregory N. Mandel, *Technology Wars: The Failure of Democratic Discourse*, 11 MICH. TELECOMM. TECH. L. REV. 117 (2005); Lyria Bennett Moses, *Understanding Legal Responses to Technological Change: The Example of* In Vitro *Fertilization*, 6 MINN. J. L. SCI. & TECH. 505 (2005) [hereinafter Moses, *In Vitro Fertilization*]; Lyria Bennett Moses, *Adapting the Law to Technological Change: A Comparison of Common Law and Legislation*, 26 U. NEW S. WALES L.J. 394 (2003).

[11] *See supra* Section IV.B.

[12] ROGERS, *supra* note 4, at 232–35, 249, 991.

[13] For further discussion on the expressive function of the law, see Elizabeth S. Anderson & Richard H. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503 (2000); Robert Cooter, *Expressive Law and Economics*, 27 J. LEGAL STUD. 585 (1998); Alex Geisinger, *A Belief Change Theory of Expressive Law*, 88 IOWA L. REV. 35 (2002); Richard H. McAdams, *The Origin, Development and Regulation of Norms*, 96 MICH. L. REV. 338, 398 (1997); Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021 (1996).

clear-cut restriction or a hesitant more partial stance.[14] In the case of genetic discrimination, the law undertook a hesitant and inconsistent approach, and consequently failed to alleviate public fears regarding the use of genetic technology. I posit that individuals' risk perceptions regarding use of technologies that are preventive and non-triable are more likely to be affected by an express rule that sends a clearer message and clarifies an emerging norm consensus.[15] In the case of genetic discrimination, I suggest that a comprehensive federal law, in lieu of the current inconsistent patchwork of laws, would serve such a purpose.

Third, I argue that where a technology is centrally diffused, as is genetic testing, intervention measures would be most effective when targeting the group that diffuses the technology.[16] In the case of genetic testing, the technology is centrally diffused by the medical profession, particularly genetic counselors. Accordingly, I propose that efforts to dispel the misguided perception of a privacy threat would be most effectively targeted at the genetic counselors that are currently playing a major role in spreading fears and inhibiting diffusion.

Fourth, I point out that technologies that—like the Internet—are characterized by a critical mass point and decentralized diffusion are prone to the second suspect privacy-diffusion relationship, where diffusion accelerates despite an extensive privacy threat.[17] Interactive technologies are often characterized by a critical mass point quality (and related network effects) where the technology is of little use to the adopter unless a critical mass of people adopts it. Once the critical mass point is reached, diffusion accelerates, social norms become quickly entrenched and the technology is less likely to be abandoned.[18] This effect is amplified when the technology's diffusion is decentralized and diffusion is not controlled by an expert group, but rather emerges horizontally via peer networks. Where diffusion is decentralized, users have the ability to reinvent the technology.[19] I suggest that the Internet was vulnerable to the second suspect relationship because privacy-threatening norms emerged after the

---

[14] *See infra* notes 215–16 and accompanying text.

[15] *See* Elizabeth S. Scott, *Social Norms and the Legal Regulation of Marriage*, 86 VA. L. REV. 1901, 1925 (2000).

[16] *See* ROGERS, *supra* note 4, at 394–98 (distinguishing between centralized and decentralized diffusion systems).

[17] An additional characteristic, which contributed to this suspect privacy-diffusion relationship, is the ability to perform concealed monitoring on the Internet. Individuals are unaware that their privacy is threatened. For a thorough analysis of this characteristic, see, Gaia Bernstein, *When New Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 VILLANOVA L. REV. (forthcoming 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=927550.

[18] *See* ROGERS, *supra* note 4, at 343–44, 352; M. Lynne Markus, *Toward a "Critical Mass" Theory of Interactive Media*, *in* ORGANIZATIONS AND COMMUNICATION TECHNOLOGY 194 (Janet Fulk & Charles Steinfield eds., 1990).

[19] *See* ROGERS, *supra* note 4, at 394–98.

critical mass point had been reached, diffusion accelerated and non-privacy norms became quickly entrenched. At that point, privacy threats were less likely to affect the technology's diffusion. Moreover, decentralized diffusion facilitated the development and spread of privacy-threatening tools.

Fifth and finally, I posit that decision-makers will not necessarily view the second suspect relationship where a technology diffuses rapidly while destabilizing privacy as dysfunctional.[20] The determination will depend on their evaluation of the privacy threat. Yet, I argue that should decision-makers view this relationship as problematic, the issue of timing becomes of the essence. I explain that express legal restrictions are likely to be less effective where they contradict social norms.[21] Consequently, where a technology possesses the critical mass point and decentralized diffusion qualities and social norms involving uses of the technology become quickly entrenched, the window of opportunity for intervention narrows.

My goal here is not to advocate early intervention in the regulation of new technologies. The uncertainties accompanying the early regulation of a new technology before its effects are known suggest that such a course of action should be infrequently pursued. I suggest, however, that identification of the critical mass point and decentralized diffusion qualities could alert decision-makers charged with the regulation of new technologies to the sensitivity of the timing element in their decision-making. In the case of the Internet, efforts at self-regulation and technological measures have failed to resolve the privacy problems. Non-privacy norms are now widely entrenched and express legal prohibitions are likely to be less effective.

This Article progresses as follows. In Part II, I explain the importance of bringing the relationship between technological diffusion and privacy to the forefront of the techno-privacy debate. I then discuss my treatment of the value of privacy. In Part III, I examine three privacy controversies involving genetic testing and the Internet through the broader privacy-diffusion relationship prism. I provide a descriptive basis for the inquiry by evaluating the controversies on the basis of empirical data regarding privacy threats and technological diffusion. In Part IV, I discuss the two suspect privacy-diffusion relationship models emerging from the examined controversies. I then turn to identify the diffusion characteristics that entrapped genetic testing and the Internet in their respective suspect privacy-diffusion relationships. I argue that these diffusion characteristics are shared by other technologies that may also be vulnerable to the same

---

[20] *See supra* Section V.B.

[21] *See* Dan M. Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. CHI. L. REV. 607, 608 (2000); Scott, *supra* note 15, at 1901, 1925–28, 1969.

suspect relationships. In Part V, I analyze the policy implications of approaching technological controversies involving privacy through the privacy-diffusion relationship prism. Specifically, I introduce an initial framework for incorporating technological diffusion attributes into decision-making dealing with the regulation of new technologies. I argue that this approach can be useful in resolving the controversies at issue and potentially preventing other technologies from becoming entrapped in the same privacy-diffusion relationships.

II. THE PRIVACY PROTECTION-DIFFUSION RELATIONSHIP

In this Part, I focus on a question that needs be addressed at the outset—why should we be concerned with the relationship between technological diffusion and privacy? First, I explain that society's desire to promote progress warrants diffusion the same deference as technological innovation. Secondly, I discuss the contours imposed by other social values on the goal of enhancing diffusion in order to promote progress. Third, I discuss my treatment of the value of privacy.

A. *Diffusion*

A prominent social belief is that progress will inevitably improve human condition.[22] Progress has been tied to basic improvements in material comfort. It has been said that "[m]aterial comfort does not assure a good life, but a good life is impossible without it."[23] A main source of the optimistic belief in progress is rooted in the notion of progress developed during the enlightenment era.[24] Although the belief in progress as a source of flourishing for mankind is not necessarily held by all, it still serves as a dominant social theme.[25] Manifestations of this theme are ubiquitous and are incorporated into a diverse range of social and legal practices. For example, what is known as the Intellectual Property Clause of the Constitution provides Congress with the power "to promote the progress of science and useful arts."[26] Similarly, the government, through institutes such as the National Institute of Health, allocates funds for scientific research.[27] Popular culture also embodies this theme through

---

[22] CHRISTOPHER LASCH, THE TRUE AND ONLY HEAVEN: PROGRESS AND ITS CRITICS 41–44 (1991).

[23] *Id.* at 34 (quoting Barrington Moore).

[24] For a description of the enlightenment notion of progress, see Michael D. Birnhack, *The Idea of Progress in Copyright Law*, 1 BUFF. INTELL. PROP. L.J. 3, 7–15 (2001); Margaret Chon, *Postmodern "Progress": Reconsidering the Copyright and Patent Power*, 43 DEPAUL L. REV. 97, 99–100, 115–16 (1993).

[25] For critiques of the progress theme, see generally, LASCH, *supra* note 22.

[26] U.S. CONST. art. 1, § 8.

[27] *See* National Institutes of Health, Home Page, http://www.nih.gov/ (last visited Aug. 27, 2006).

different media—such as *Discover* magazine—that report on promising scientific discoveries for the layman reader.[28]

The political and legal regimes mainly endeavor to advance the goal of progress by promoting innovation.[29] Consequently, the political and scholarly debates focus on the suitability of intellectual property rights to advance innovation.[30] Yet, the effectiveness of a new technology also depends on a subsequent stage—the diffusion stage. A technology's diffusion follows the innovation stage. The innovation phase includes the technical discovery and the creation of the first successful commercial application, while the diffusion stage is the widespread adoption of a commercially successful product.[31]

Successful diffusion of a new technology is as critical to achieving progress as its successful invention. A technology that is merely invented and not used would likely be rendered to oblivion. All efforts invested in its invention would be lost together with its potential benefits. For example, the currently used computer keyboard—QWERTY—is considered inferior to an alternative design—Dvorak, which contains a different key arrangement. The original QWERTY design was initially adopted to prevent the clashing of typebars and the consequent jamming of the typewriter. This problem was resolved as early as the 19th century. Yet, users were reluctant to adopt the superior Dvorak keyboard—invented

---

[28] For the online edition of *Discover* magazine, see http://www.discover.com (last visited Aug. 27, 2006).

[29] Article I, Section 8 of the U.S. Constitution has been the main source of authority for the promotion of innovation in the arts and sciences. The provision explicitly provides that "Congress shall have the power . . . to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." U.S. CONST. art. 1, § 8.

[30] A prominent example is the political debate regarding the Digital Millenium Copyright Act. *See, e.g.*, *The Use of Copyright Programming over the Internet: Hearing Before the Subcomm. on Courts, the Internet and Intellectual Property of the H. Comm. On the Judiciary*, 106th Cong. (2000) (statement of Charles P. Moore, Vice President of Business Development Radio Active Media Partners). The general debate regarding the role of intellectual property rights in promoting innovation has produced a large body of contemporary scholarship. Some representative publications include the following: James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33 (2003); R. Polk Wagner, *Information Wants to Be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995 (2003); Yochai Benkler, *Intellectual Property: Commons-Based Strategies and the Problems of Patents*, SCIENCE, Aug. 20, 2004, at 1110; Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, SCIENCE, May 1, 1998, at 698.

[31] The main diffusion theorist—Everett Rogers—defined diffusion as the process in which an innovation is communicated through certain channels over time among members of a social system. ROGERS, *supra* note 4. Legal theorists have differentiated between three stages through which a new technology progresses. The first stage is invention, which is the technical discovery. The second stage is innovation, which is the first commercially successful application of a technology, and the third is diffusion, which is the widespread adoption of a commercially successful product. In this Article, I focus on the main dichotomy between innovation and diffusion. *See* Ashford et al., *supra* note 4; Natalie M. Derzko, *Using Intellectual Property Law and Regulatory Processes to Foster the Innovation and Diffusion of Environmental Technologies*, 20 HARV. ENVTL. L. REV. 3 (1996); Gollin, *supra* note 4.

in 1932—which enables faster and more comfortable typing. Its inventor, August Dvorak, died in 1975 after forty years of frustration from the world's stubborn rejection of his invention.[32]

The diffusion of a technology is dependent on its social acceptance—more precisely, on whether people adopt it and start using it. A technological innovation that is not diffused can be as detrimental to achieving progress as a technology that was never invented in the first place.[33] Hence, the promotion of technological diffusion is in many cases a natural corollary to the belief that innovation is crucial to social progress.

B. *Balancing Diffusion and Social Values*

History shows a correlation between the compatibility of an innovation with social values, such as privacy and its diffusion. For example, the adoption of innovations that are incompatible with cultural values can be blocked.[34] A striking instance is the tale of the diffusion process of the technology of artificial insemination in humans. The diffusion of artificial insemination was inhibited from its inception, at the end of the eighteenth-century, until the 1960s when it finally became socially accepted. The delayed diffusion of this important technology was caused by its incompatibility with the traditional conception of the family. Artificial insemination, by enabling procreation without resort to sexual intercourse, threatened the traditional concept of the genetic nuclear family. Consequently, social norms aimed at preserving the traditional notion of the family and their reflection through legal restraints deterred infertile couples from using artificial insemination in order to conceive.[35]

We have come to expect that an innovation's compatibility with social values will be positively correlated to the diffusion of the technology.[36] Consequently, the acceptance struggles of major new technologies often reflect an effort to reach equilibrium between technological diffusion and threatened social values.[37] Despite frequent fierce debates regarding the appropriate equilibrium, the end balance tends to reflect a compromise where neither diffusion nor other social values completely prevail. Society appears to reject extensive diffusion and widespread adoption of a new

---

[32] *See* Paul A. David, *Clio and the Economics of QWERTY*, 75 AM. ECON. REV. 332 (1985). *But see* S.J. Liebowitz & Stephen E. Margolis, *The Fable of the Keys*, 33 J.L. & ECON. 1 (1990) (arguing that use of the QWERTY keyboard is efficient and that the Dvorak keyboard was justifiably rejected).

[33] Of course, in the case of some technologies—such as weapons of mass destruction—technological diffusion may inhibit progress.

[34] ROGERS, *supra* note 4, at 241.

[35] *See generally* Bernstein, *supra* note 10.

[36] Louis G. Tornatzky & Katherine J. Klein, *Innovation Characteristics and Innovation Adoption-Implementation: A Meta-Analysis of Findings*, 29 IEEE TRANSACTIONS ON ENGINEERING MGMT. 28, 33 (1982).

[37] *See id.* at 34.

technology that significantly erodes a central social value. At the same time, it also appears to disfavor the inhibition of the diffusion of important technologies due to value threats—such as privacy concerns—that prevent individuals from adopting a technology.

The balancing of diffusion and the value of privacy is prevalent in technological regulatory schemes. The history of wiretapping technology and the threat it imposed on the value of privacy reflects the rejection of extremes and the struggle toward an appropriate balance. Phone wiretapping was first introduced at the end of the 19th century.[38] The social controversy that ensued included state statutes that prohibited wiretapping and a famous Supreme Court opinion, *Olmstead v. United States*, which held that wiretapping does not constitute a search that is protected under the Fourth Amendment.[39] However, thirty years later, another Supreme Court opinion, *Katz v. United States*, held that wiretapping does constitute a violation of the Fourth Amendment.[40] Subsequently, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act, which provides specific limitations on the circumstances under which wiretapping can be used.[41] The struggle to maintain a balance between use of wiretapping technology and privacy protection continues to this day. It is reflected in the continued deliberations regarding the powers granted to the government under the Patriot Act to use new wiretapping technology to fight terrorism.[42]

Although the history of technologies—such as wiretapping—manifests a social aspiration toward balancing technological diffusion and privacy protection, these resolutions are not always achieved. In some cases, an equilibrium may occur only decades later.

My first goal in this Article is to identify these suspect privacy-diffusion relationships. The suspect relationships involve cases where either extensive technological diffusion significantly erodes privacy or where a privacy threat prevents people from adopting a technology. I define these relationships as suspect and not necessarily dysfunctional since an imbalanced equilibrium may indeed be a result of a conscious

---

[38] Orin S. Kerr, *The Fourth Amendment and the New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 840–41 (2004).

[39] Olmstead v. United States, 277 U.S. 438, 466 (1928); PRISCILLA M. REGAN, LEGISLATING PRIVACY 111–12 (1995); Kerr, *supra* note 38, at 839

[40] Katz v. United States, 389 U.S. 347, 358–59 (1967).

[41] REGAN, *supra* note 39, at 123.

[42] *See, e.g.*, *Protecting Constitutional Freedoms from Infringement by Counterterrorism Efforts: Hearing Before the Subcomm. on the Constitution, Federalism and Property Rights of the S. Judiciary Comm.*, 107th Cong. (2001) (statement of Jerry Berman, Executive Director of the Center of Democracy and Technology on Civil Rights and Anti-Terrorism Efforts); *Crime, Terrorism and the Age of Technology: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the H. Judiciary Comm.*, 108th Cong. (2005) (statement of Peter Swire, Professor, on Patriot Act Reauthorization: Sections 209, 217 and 220).

social choice. I argue, however, that these suspect relationships warrant increased scrutiny and signal a cause for concern and deliberation among decision-makers.

C. *Privacy*

Privacy has often taken central stage in the acceptance struggles of new technologies. New technologies have repeatedly threatened and destabilized personal privacy. As early as 1890, Warren and Brandeis pronounced the threat imposed on privacy by the advent of a new technology—the camera.[43] Through the years, privacy protection dominated many controversies involving the acceptance of technologies. These controversies concerned technologies as diverse as computer databases and the birth control pill.[44] In this Article, I focus on two contemporary acceptance struggles involving the technologies of genetic testing and the Internet.

Much academic discussion has been dedicated to the conceptualization of the value of privacy. Privacy is considered a vague and protean concept.[45] Commentators' writings reveal that privacy serves as an umbrella concept for many different conceptions.[46] Privacy was conceived, for example, as enabling control over information, as protecting autonomy, or as promoting democracy.[47] I endeavor in this Article to look beyond the specific privacy debates to the privacy-diffusion relationships that underlie social tensions related to a broad range of techno-privacy controversies. Accordingly, I do not adopt a substantive conceptualization

---

[43] Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[44] *See* Whalen v. Roe, 429 U.S. 589 (1977) (databases); Griswold v. Connecticut, 381 U.S. 479 (1965) (birth control pill). *See also* WARREN FREEDMAN, THE RIGHT OF PRIVACY IN THE COMPUTER AGE 93–112 (1987); RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 178–301 (1989).

[45] *See* ARTHUR MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977) (stating that privacy has "a protean capacity to be all things to all lawyers," yet is lacking limitations of its own); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) ("Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."); Daniel J. Solove, *The Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–78 (2006) (opining that nobody can articulate what privacy means, and that it "is far too vague a concept to guide adjudication and lawmaking").

[46] Many theorists have contributed to the robust debate to refine the understanding of the value of privacy. For a representative sample of these writings, see JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION (1992); REGAN, *supra* note 39; JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY (2000); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861 (2000); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

[47] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482–83 (1968); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

of privacy in order to determine whether a privacy violation that warrants protection has occurred. My approach is in a sense "procedural." It relies on the notion of social change without inquiring into the value-laden effects of the transformation. In other words, I do not inquire whether a technology threatens privacy because personal autonomy is circumscribed or because individuals' ability to control their personal information is now limited.

Instead, I identify a privacy threat where the relevant social structures are transformed. Individuals' sentiments that a new technology changed the status quo and eroded their previously held sense of privacy are key to my analysis. The sense of threat matters most where diffusion is considered. A sense of change and pursuant perception of threat can affect diffusion. Consequently, I posit that a change in social structures that affects privacy warrants concern regardless of the specific value-laden implications of the dispute.

My focus on social change as an indicator of a privacy problem relies heavily on the contextual integrity approach developed by Helen Nissenbaum.[48] Nissenbaum suggests that a privacy problem is manifested where either of two types of relevant social structures undergoes transformation.[49] First, a privacy problem can occur where the norms of appropriateness are violated. Norms of appropriateness dictate what information about persons is appropriate to reveal in a particular context.[50] Consequently, a violation could occur, for example, where a third party uses a new technology to obtain personal information that was not previously obtained in this context. Second, Nissenbaum suggests that a privacy problem can materialize where norms of flow are violated. Norms of flow are violated where information flows in a way that is not traditionally expected in a specific context. For example, a friend divulging an important secret to a third party would violate the expected norms of flow.[51]

Nissenbaum's contextual integrity approach highlights the type of social structural transformations that often indicate a privacy problem. In the following Part, I examine three controversies where the underlying tensions originate from the type of social transformations described by Nissenbaum. In all cases, norms of appropriateness, norms of flow or both were transformed, causing concern among individuals.

---

[48] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).
[49] *Id*, at 136–40.
[50] *See id.* at 138–40.
[51] *See id.* at 140–43.

III. DISPERSING MYTHS AND FABLES IN THE TECHNO-PRIVACY ARENA

Regulators and academics have proposed different resolutions for privacy problems created by genetic testing and the Internet.[52] Although some of these proposals were implemented,[53] no comprehensive study was conducted to evaluate the efficacy of these interventions—that is, whether the privacy threat was in fact eliminated. Furthermore, the proposals focused on the resolution of the privacy issue alone—the reciprocal relationship between privacy and diffusion was not considered.

In this Part, I seek to provide a descriptive basis for the examination of the privacy-diffusion relationship. I examine empirical data that measures technological diffusion and privacy threats imposed by genetic testing and the Internet. The technological applications described in this Part are entrapped in privacy-diffusion relationships that merit concern and increased scrutiny. The controversies examined in this Part are: (A) genetic discrimination by insurers and employers; (B) collection of personal information by commercial entities on the Internet; and (C) employers' monitoring of email and Internet use by employees.[54]

A. *Genetic Discrimination*

For over a decade, the media has been focusing on the threats of genetic discrimination.[55] Common wisdom points out that as the number of available genetic tests increases, so will genetic discrimination. Consequently, for many individuals, concerns about genetic discrimination became an inseparable part of genetic testing. As one genetic counselor reported:

> People will call up and they won't give you their address. I can't even mail them any information because they think I am going to keep their address somewhere and distribute it to somebody. So I can't even mail them a brochure or they won't give me their phone number. They will call and leave a message saying: "I'm calling about Huntington's. I'll call

---

[52] *See supra* note 6.

[53] *See, e.g.*, Genetic Information Privacy Act, N.M. STAT. § 24-21-4 (2005); Byers et al., *supra* note 7.

[54] This Article focuses on diffusion to the individual end-user. The adoption of genetic testing, unlike many other medical technologies, is dependent significantly on adoption by the patient and not on adoption by physicians. Individuals seeking genetic testing are rarely referred by physicians. *See* Katrina Armstrong et al., *Early Adoption of BRCA 1/2 Testing: Who and Why*, 5 GENETICS MED. 92, 96–97 (2003). My selection of controversies was guided by my focus on diffusion to individual end-users.

[55] *See, e.g.*, Gina Kolata, *Advent of Testing for Breast Cancer Genes Leads to Fears of Disclosure and Discrimination*, N.Y. TIMES, Feb. 4, 1997, at C1, *available at* LEXIS, News Library, NYT File.

> you back." Or they won't let me call them at work. They won't talk at work.[56]

It is not only the public, but also the medical professionals administering the tests that are preoccupied with the potential of genetic discrimination. Thus, once a person decides to test and enters the genetic counselor's office, she will be asked to sign an informed consent form along the following lines:

> If you learn that you have a genetic disposition to breast and/or ovarian cancer, you will have knowledge that you may be forced to disclose to third parties. For example, as insurance companies learn more about hereditary risk for cancer, they may ask about the results of genetic tests of those who have to apply for coverage. In most states, life and disability insurers may ask such questions and use the answers in underwriting decisions. . . . Knowledge that you have a genetic predisposition to breast and/or ovarian cancer may compromise your ability to obtain or maintain insurance coverage.[57]

Given this warning, some will proceed to test, while others may not. Some will never cross the threshold and enter the genetic counselor's office.

On its face, this is a case of a legal failure to eliminate a privacy threat that is impeding the diffusion of an important medical technology. Yet, an examination of empirical evidence related to genetic discrimination uncovers a different picture. The findings reveal that despite our fears, in practice, genetic discrimination is rare and, if anything, is on the decline. Yet, misperceptions of the privacy threat by both the general public and the medical profession in charge of diffusing the technology are inhibiting the use of genetic testing technology. The legal failure is, hence, different from that perceived at first blush—in fact, it is a failure to alleviate fears of a privacy threat in order to promote the use of genetic testing technology.

Let us first identify the potential discriminators. Genetic discrimination can take many forms. It can take a personal form of a fiancé canceling her engagement once she learns that her future husband carries the genetic mutation for the currently untreatable, devastating Huntington disease.[58] Yet, most concerns have focused on potential

---

[56] Mark A. Hall & Stephen S. Rich, *Genetic Privacy Laws and Patients' Fear of Discrimination by Health Insurers: The View from Genetic Counselors*, 28 J.L. MED. & ETHICS 245, 246 (2000).

[57] *Id.* at 247–48.

[58] A carrier of the Huntington disease genetic mutation has a 100% probability of incurring the disease. It usually strikes people between the ages of thirty-five to forty-five, and entails a long process of neurological deterioration culminating in death. *See* Huntington Disease Society of America, Frequently Asked Questions about HDSA and HD, http://www.hdsa.org (follow "Get Help/Info/Learn" hyperlink; then follow "FAQs" hyperlink) (last visited Aug. 27, 2006).

discrimination by insurers and employers. Employers and insurers appear to have strong incentives to use genetic information. Health insurers and self-insured employers could be subject to higher medical costs once an employee becomes sick.[59] Life insurers would prefer to screen out those likely to die an untimely death.[60]

Employers may be subject to liability should working conditions exacerbate an existing genetic predisposition. Employers may also incur other costs, such as missed workdays or may be liable for accidents arising from a medical condition for which the employee was genetically predisposed; for example, a pilot incurring a heart attack during flight.[61]

Concerns about such uses of genetic testing have not escaped the public eye. The media has played a major role in spreading such fears.[62] Through movies—such as the 1997 film *Gattaca*—and threatening newspaper titles—such as "Flunk the Gene Test and Lose Your Insurance"—the concerns voiced by legal commentators have reached the general public.[63] These concerns were publicly expressed by public interest organizations and governmental entities.[64]

For many individuals, genetic testing has become synonymous with genetic discrimination. Genetic counselors described their patients' knowledge about genetic testing as often limited to one topic—genetic discrimination.[65] Reports of genetic discrimination by employers and insurers particularly concern those closest to the issue. Family members of those afflicted by genetic disease are hounded by these reports.[66]

---

[59] *See* Eric Mills Holmes, *Solving the Insurance/Genetic Fair/Unfair Discrimination Dilemma in Light of the Human Genome Project,* 85 KY. L.J. 503, 556–57 (1996–1997); Council for Responsible Genetics, *Genetic Discrimination: Position Paper* (2001), *available at* http://www.gene-watch.org/educational/genetic_discrimination.pdf.

[60] *See* Roberta B. Meyer, *Justification for Permitting Life Insurers to Continue to Underwrite on the Basis of Genetic Information and Genetic Test Results*, 27 SUFFOLK U. L. REV. 1271, 1272, 1279 (1993); Mark A. Rothstein, *Genetic Privacy and Confidentiality: Why They Are So Hard to Protect*, 26 J.L. MED. & ETHICS 198, 200 (1998). *See also* MAXWELL J. MEHLMAN & JEFFREY R. BOTKIN, ACCESS TO THE GENOME: THE CHALLENGE TO EQUALITY 42–49 (1998) (describing different forms of potential genetic discrimination).

[61] *See* Henry T. Greely, *Genotype Discrimination*: *The Complex Case for Some Legislative Protection*, 149 U. PA. L. REV. 1483, 1490–91 (2001); Paul A. Lombardo, *Genetic Confidentiality: What's the Big Secret?*, 3 U. CHI. L. SCH. ROUNDTABLE 589, 596 (1996).

[62] Hall & Rich, *supra* note 56, at 246–47.

[63] Geoffrey Cowley et al., *Flunk the Gene Test and Lose Your Insurance*, NEWSWEEK, Dec. 23, 1996, at 48, *available at* LEXIS, News File, NWEEK File; GATTACA (Sony Pictures 1997). For a description of genetic discrimination concerns, see LORI ANDREWS & DOROTHY NELKIN, BODY BAZAAR: THE MARKT FOR HUMAN TISSUE IN THE BIOTECHNOLOGY AGE 82–101 (2001).

[64] *See* Council for Responsible Genetics, *supra* note 59; National Human Genome Research Institute, *Health Insurance in the Age of Genetics* (1997), *available at* http://www.genome.gov/10000879.

[65] *See* Hall & Rich, *supra* note 56, at 247.

[66] *See* E. Virginia Lapham et al., *Genetic Discrimination: Perspectives of Consumers*, SCIENCE, Oct. 25, 1996, at 621.

Media reports and the statements made by government entities and public interest organizations are supported by a number of studies that warned of genetic discrimination becoming a widespread phenomenon.[67] However, these studies have been extensively criticized for methodological failures. The main point of critique was a limitation also acknowledged by many of the authors of these studies, namely that the studies were based on isolated anecdotes and not on survey methodology.[68]

In contrast, the bulk of methodologically sound empirical research on discrimination by employers and insurers points otherwise. It overwhelmingly demonstrates that genetic discrimination by employers and insurers is rare and is generally on the decline. I will discuss the evidence related to employers and insurers separately, although the conclusion drawn from the studies of both groups are uniform. Despite the growth in the number of available genetic tests, genetic discrimination has not become an extensive or even a limited societal phenomenon.

Studies utilizing survey methodology to examine employment discrimination have demonstrated that not only is genetic discrimination rare, but also that it is on the decline since the 1980s, when the first studies were conducted. The first comprehensive survey conducted at the beginning of the 1980s revealed that few (1.66%) of major U.S. companies utilize genetic testing.[69] Furthermore, even companies that used genetic testing rarely proceeded to use the information to discriminate against employees who were identified as disease gene carriers.[70] A subsequent

---

[67] Paul R. Billings et al., *Discrimination as a Consequence of Genetic Testing*, 50 AM. J. HUM. GENETICS 476 (1992); Lisa N. Geller & Joseph S. Alper, *Individual, Family and Societal Dimensions of Genetic Discrimination: A Case Study Analysis*, 2 SCIENCE & ENGINEERING ETHICS 71 (1996). *See also* Kathy L. Hudson et al., *Genetic Discrimination and Health Insurance: An Urgent Need for Reform*, SCIENCE, Oct. 20, 1995, at 391 (surveying the earlier studies).

[68] *See* Billings et al., *supra* note 67, at 477–78, 481 ("The pilot study identifies multiple facets of genetic discrimination. It . . . does not establish the prevalence of these attitudes or discriminatory practices. A comprehensive study of the significance and varieties of genetic discrimination is critical to design strategies to ensure the ethical and appropriate use of genetic testing in the future."). *See also* Geller & Alper, *supra* note 67, at 83; Larry Gostin, *Genetic Discrimination: The Use of Genetically Based Diagnostic and Prognostic Tests by Employers and Insurers*, 17 AM. J.L. & MED. 109, 117–18 (1991). These studies were also criticized for other methodological defects, including leading questions, non-representative samples, and confounding individuals manifesting disease symptoms with pre-symptomatic gene carriers. Philip R. Reilly, *Genetic Discrimination*, *in* GENETIC TESTING AND THE USE OF INFORMATION 106, 112–15 (Clarisa Long ed., 1999); Mark A. Hall & Stephen S. Rich, *Laws Restricting Health Insurers' Use of Genetic Information: Impact on Genetic Discrimination*, 66 AM. J. HUM. GENETICS. 293, 302 (2000).

[69] The survey included 366 major U.S. industrial, utilities companies and unions. The survey also showed that use of genetic tests declined in the twelve years that preceded the survey. OFFICE OF TECHNOLOGY ASSESSMENT, THE ROLE OF GENETIC TESTING IN THE PREVENTION OF OCCUPATIONAL DISEASES 34–39 (1983).

[70] *Id.* at 37. "Of the 18 companies that reported taking some action, eight reported that they had informed an employee of a potential problem. Five respondents reported transferring the at risk employee. Two suggested that the employee seek another job as a result of testing. One discontinued or changed a product." *Id.*

survey conducted in 1989 showed that although the number of genetic tests was constantly growing, there was no significant change in the use of the technology by employers.[71] Furthermore, instances of negative personnel decisions stemming from genetic testing were still rare, and no increase since 1982 had been noticed.

A more recent study conducted in 1997 demonstrated that discrimination related to a genetic pre-symptomatic carrier status was a rarity.[72] Finally, a series of studies conducted annually between 1998 and 2000 showed that after clarifying what constitutes genetic testing, it became evident that genetic testing by major U.S. firms is extremely rare.[73]

Empirical data has yielded similar results concerning use of genetic information by health insurers.[74] A study conducted in 1992 demonstrated that health insurers do not require individuals to undergo genetic testing.[75] Health insurers could still obtain genetic information through questions inquiring about genetic predispositions known to the individual. Yet, the study revealed that most insurers did not inquire about genetic predispositions.[76] Overall, the study showed that insurers viewed genetic information no differently than other forms of medical information.[77] A 1997 study also showed that health insurers rarely discriminate on the basis of a pre-symptomatic genetic carrier status.[78] Finally, a study conducted in 2000 concluded that little or no genetic discrimination by health insurers is taking place.[79] The study found that genetic test results played no role in the evaluation of insurance agents. Specifically, the study revealed that

---

[71] OFFICE OF TECHNOLOGY ASSESSMENT, GENETIC MONITORING AND SCREENING IN THE WORKPLACE 197–98 (1990), *available at* http://www.wws.princeton.edu/ota/disk2/1990/9020/9020.PDF. This survey included the five hundred of the largest U.S. industries, utilities and major unions and a representative sample of all other companies with one thousand employees or more. The authors of the survey attribute a small increase in the number of companies reporting genetic testing to a change in the questioning format. *Id*.

[72] *See* Dorothy Wertz, *Society and the Not-So-New Genetics: What Are We Afraid of? Some Future Predictions from a Social Scientist*, 13 J. CONTEMP. HEALTH L. & POL'Y 299, 308–10 (1997).

[73] *See* AM. MGMT. ASS'N, 2001 AMA SURVEY ON WORKPLACE TESTING: MEDICAL TESTING SUMMARY OF KEY FINDINGS 2 (2001), *available at* http://www.amanet.org/research/pdfs/mt_2001.pdf; AM. MGMT. ASS'N, 1999 AMA SURVEY ON WORKPLACE TESTING: MEDICAL TESTING (1999); AM. MGMT. ASS'N, 1998 AMA SURVEY: WORKPLACE TESTING AND MONITORING 5 (1998).

[74] There is not, at this point, sufficient empirical data regarding life insurance. A 2003 study concluded that there was no evidence of life insurance discrimination of individuals who underwent genetic testing for a breast cancer genetic mutation. *See* Armstrong et al., *supra* note 54. A study conducted in 1991 concluded that genetic information is used in underwriting decisions, however, it was based on hypothetical questions and did not indicate that life insurers required genetic testing. *See* Jean E. McEwen et al., *A Survey of Medical Directors of Life Insurance Companies Concerning Use of Genetic Discrimination*, 53 AM. J. HUM. GENETICS 33 (1993).

[75] OFFICE OF TECHNOLOGY ASSESSMENT, GENETIC TESTS AND HEALTH INSURANCE: RESULTS OF A SURVEY, 33–34 (1992).

[76] *Id.* at 12.

[77] *Id.*

[78] *See* Wertz, *supra* note 72.

[79] *See* Hall & Rich, *supra* note 68.

insurers do not inquire about genetic tests, do not use the information if they come across it in a medical record and do not include this type of information in their underwriting guidelines.[80]

The empirical data examining the phenomenon of discrimination by both employers and insurers demonstrates that genetic discrimination has always been very rare. Moreover, the findings show that despite increased availability of genetic tests, discrimination has been on the decline. Commentators are increasingly acknowledging this phenomenon.[81] Recently, Henry Greely, who earlier predicted that health care costs would provide a strong incentive for employers to avoid hiring or retaining people with genetically predictable high costs, conceded that current data does not support this prediction.[82]

Despite overwhelming evidence pointing to the absence of genetic discrimination, anecdotal stories amplified by the press continue to dictate the public's mind-set toward genetic testing. Stories of genetic discrimination appear to dominate public opinion. An overwhelming majority of the public believes that positive genetic testing results, i.e., being diagnosed as a carrier of a disease gene, will lead to discrimination by health insurance companies and employers.[83] Of particular concern is the fact that even genetic counselors believe that significant discrimination is taking place. Although virtually no genetic counselor has ever encountered cases of genetic discrimination personally, they base their opinions on accounts heard in professional meetings and read in professional journals.[84] The endorsement of such misguided beliefs by genetic counselors is of particular significance because of their role as gatekeepers and authority figures for the public regarding the uses of the technology. Since genetic counselors hold erroneous beliefs regarding the scope of genetic discrimination, they play a major role in spreading fears of such discrimination. In their counseling sessions, genetic counselors

---

[80] *Id.* at 297. Health underwriters' lack of interest in a genetic carrier status was also evidenced from their use of family history information. Although some insurers use family history information for important disease categories, they use it only to evaluate signs of an existing disease. They do not use the information to predict future health problems. *Id.* at 298. The study was based on interviews with health insurers, genetic counselors and insurance agents. It was also based on a marketing test of a fictitious small employer who had to get insurance for a disease gene carrier. *Id.* at 294.

[81] *See* Philip R. Reilly, *Genetic Discrimination*, *in* GENETIC TESTING AND THE USE OF INFORMATION, *supra* note 68, at 106, 106–107; Gostin, *supra* note 68, at 115–16; Mark A. Rothstein & Sharona Hoffman, *Genetic Testing, Genetic Medicine, and Managed Care,* 34 WAKE FOREST L. REV. 849, 866 (1999).

[82] Henry T. Greely, *Banning Genetic Discrimination*, 353 NEW ENG. J. MED. 865 (2005); Greely, *supra* note 61, at 1490.

[83] Eighty-four percent believe that health insurance companies will deny coverage, and 69% believe that employers will deny people jobs because of genetic test results. *Americans Welcome Scientific Advancements with Caution: VCU Life Sciences Survey Released*, VCU NEWS, Oct. 4, 2001, *available at* http://www.vcu.edu/uns/Releases/2001/oct/100401.htm.

[84] *See* Hall & Rich, *supra* note 68, at 295–96.

routinely advise patients that genetic discrimination is a risk that accompanies genetic testing.[85] Furthermore, the risk of genetic testing is included in the majority of informed consent forms submitted by genetic counselors or other medical professionals administering the tests.[86]

The prevalence of fears of discrimination despite the absence of supporting evidence is disconcerting because of its effect on individuals' decisions to undergo genetic testing for adult onset diseases.[87] Although the decision of whether or not to undergo genetic testing is motivated by additional factors, research has shown that fear of genetic discrimination by insurers and employers is the primary barrier against testing.[88] While some individuals would be undeterred by the risk of genetic discrimination, others may avoid availing themselves of an important medical technology. The impact of discrimination concerns on the decision to test varies according to the immediacy of the medical benefits. Those least likely to be affected are individuals already incurring symptoms and couples undergoing prenatal screening. The ability to improve medical treatment by providing a clearer diagnosis of the disease or to prevent the birth of a child with a genetic disease tends to outweigh discrimination concerns. But, those individuals at the focus of this inquiry—adults who are currently pre-symptomatic—are most likely to be deterred.[89]

Concerns about genetic discrimination inhibited decisions to test for adult onset diseases even among individuals who have a higher incentive to test than the general population, because they have one or more family members with a genetic disease.[90] Those who do not have a relative sick with a genetic disease are even more affected by concerns of genetic discrimination. In surveys, these individuals repeatedly affirmed their disinclination to test if insurers and employers could gain access to the results.[91]

---

[85] According to the study, 84% of genetic counselors conduct this discussion. Hall & Rich, *supra* note 56, at 247.

[86] *Id.* at 249.

[87] Adult onset diseases are genetic diseases that may develop later in life, such as breast cancer, Altzheimer or Huntington.

[88] *See* Katherine P. Geer et al., *Factors Influencing Patients' Decisions to Decline Cancer Genetic Counseling Services*, 10 J. GENETIC COUNSELING 25, 30–31 (2001).

[89] Hall & Rich, supra note 56, at 249–52. Hall and Rich's study, which focused on individuals visiting counselors for the purpose of testing, found disparity in the reports. While 38% of genetic counselors reported that discrimination concerns are a major barrier to testing, and that large numbers of clients decline testing primarily for this reason, the other respondents reported a lesser effect. *Id.* at 249.

[90] Nine percent of respondents who had one or more family members inflicted by a genetic disorder and belonged to genetic support groups reported that they, or a family member, refused to test due to their fear of discrimination. Lapham et al., *supra* note 66, at 621–23.

[91] A 1997 national telephone survey reported that 63% of the participants would not take genetic tests for diseases if health insurers or employers could get access to them. *See* U.S. DEP'T OF LABOR ET AL., GENETIC INFORMATION AND THE WORKPLACE (1997), *available at* http://www.genome.gov

Discrimination fears affect the diffusion and utilization of genetic testing technology in additional ways. First, discrimination concerns create a cost barrier because individuals prefer to pay for genetic tests out of pocket in order to avoid revealing the results to their insurers. Consequently, those who cannot afford to pay out of pocket are less likely to test.[92] Secondly, the desire to keep genetic testing results secret from insurers prevents individuals diagnosed with a genetic pre-disposition from undergoing potentially beneficial treatments.[93] For example, a woman diagnosed with the breast cancer genetic mutation may benefit from undergoing a preventative mastectomy. Since many cannot afford to pay for such medical costs out-of-pocket, this results in an under-utilization of the technology.

Hence, a close look at the state of genetic discrimination portrays a surprising and disconcerting picture. The widespread phenomenon of genetic discrimination was shown to be a myth. At the same time, though, the myth prevails in the eyes of the public and, consequently, the diffusion of genetic testing technology is held back. The factor that remains to be analyzed in this equation of technology and social attitudes is the role played by the law.

The law provides only partial and inconsistent protection from genetic discrimination. On the federal level, three statutes provide limited protection. First, the Health Insurance Portability and Accountability Act of 1996 prohibits group insurers from denying coverage or charging higher rates on the basis of genetic information.[94] Yet, these restrictions do not apply to all forms of health insurance insurers and to employers. Second, the Americans with Disabilities Act prohibits employers from discriminating on the basis of disability. However, it does not contain provisions that specifically prohibit genetic discrimination where no disease has yet developed but the individual is diagnosed as a carrier of the

---

/10001732.

[92] Prices for genetic tests range from $100 to over $2000. *See* GeneTests.com, Ordering Genetic Testing, http://www.genetests.org (follow "Educational Materials" hyperlink; then follow "What is Genetic Testing?" hyperlink; then follow "Ordering Genetic Testing" hyperlink) (last visited Aug. 27, 2006). However, this effect may be mitigated by the fact that the less affluent tend to be covered by government insurance plans—such as Medicaid—where the likelihood of discrimination is lower. *See* Geer et al., *supra* note 88, at 31; Hall & Rich, *supra* note 56, at 249–52.

[93] *See* Caryn Lerman et al., *BRCA1 Testing in Families with Hereditary Breast-Ovarian Cancer: A Prospective Study of Patient Decision Making and Outcome*s, 275 J. AM. MED. ASS'N 1885, 1890 (1996).

[94] *See* Health Insurance and Portability Act, 29 U.S.C. § 1182 (2000). For a survey of genetic discrimination laws, see, John V. Jacobi, *Genetic Discrimination in a Time of False Hopes*, 30 FLA. ST. U. L. REV. 363, 368–75 (2003). *See also* Ellen Wright Clayton, *Comments on Philip R. Reilly's "Genetic Discrimination"*, *in* GENETIC TESTING AND THE USE OF INFORMATION 134, 134–136 (Clarisa Long ed., 1999) (arguing that HIPAA affords only partial protection).

disease gene.[95] In 1995, the Equal Employment Opportunity Commission issued a policy guide, stating that protection against discrimination based on disability applies to pre-symptomatic individuals.[96] However, this statement has no binding force and has not yet been tested.

Genetic discrimination protection under state law fares somewhat better, although not considerably so. Protection is comprised of a confusing patchwork of laws offering only limited protection. Currently, forty-one states have statutes governing genetic discrimination in health insurance, and thirty-one states have laws regarding genetic discrimination in the workplace.[97] These statutes generally do not offer comprehensive protection. Some target certain genetic diseases, some focus on prohibiting discrimination by employers, and others focus on prohibiting discrimination by insurers.[98]

Thus, legal protection against genetic discrimination is partial and inconsistent. This raises two questions: To what extent has the current inconsistent legal patchwork contributed to inhibiting genetic discrimination, and what is the effect of the state of the law on individuals' concerns about genetic discrimination?

The current legal regime regarding genetic discrimination does not appear to be directly responsible for the absence of genetic discrimination, although it appears to have had some effect. Studies show that insurers were as disinclined to use genetic information in states that had laws restricting genetic discrimination as in states that did not have such laws.[99] Yet, the law appears to have had some indirect impact in deterring health insurers from using genetic information. Some insurers believe that use of this information is morally unacceptable. To that effect, the laws have had some impact in influencing the industry's conformation to social norms.[100] Health insurers appear to avoid the use of genetic information not because

---

[95] *See* American With Disabilities Act, 42 U.S.C. §§ 12101–12213 (2000); Edward J. Larson, *The Meaning of Human Gene Testing for Disability Rights*, 70 U. CIN. L. REV. 913, 927–28 (2002).

[96] *See* 3 EEOC COMPLIANCE MANUAL 902–45 (1995); Rothstein & Hoffman, *supra* note 81, at 870.

[97] National Human Genome Research Institute, Genetic Discrimination in Health Insurance, http://www.genome.gov/10002328 (last visited, Aug. 27, 2006).

[98] *See, e.g.*, Larson, *supra* note 95, at 929; Paul Steven Miller, *Is There a Pink Slip in My Genes? Genetic Discrimination in the Workplace*, J. HEALTH CARE L. & POL'Y 225, 259–63 (2000).

[99] Hall & Rich, *supra* note 68, at 297, 300. The study showed that insurers have only spotty knowledge of the law. Only 42% of the agents had any awareness of the existence of a genetic specific law, either state or federal. Almost none had a basic accurate understanding of what these laws say. Of those who had some awareness, their perception of the restrictions tended to be over-broad. For example, they would assume that federal law contained a general prohibition or that state law prohibits the use of family history when in fact it does not. None believed that genetic discrimination laws have changed underwriting practices for health insurance. *Id.* at 197, 300. *See also* Geer et al., *supra* note 88, at 35.

[100] Hall & Rich, *supra* note 68, at 301, 304.

of a specific legal threat, but because the law reinforces the instinct that doing otherwise would be socially wrong.

The current legal patchwork has not alleviated the genetic discrimination concerns of either genetic counselors or those contemplating the use of the technology. Studies have shown no reduction in patients' fears following the enactment of genetic discrimination laws. Concerns appear to have increased due to the publicity accompanying the enactment of these laws. Further, the enactment of genetic discrimination law has not altered genetic counselors' perception of the danger of genetic discrimination.[101]

Genetic counselors have demonstrated a good awareness of existing law. However, the accuracy of their knowledge was low, in particular with regard to state law, which provides the bulk of current protection.[102] Genetic counselors are in the position to educate the public with regard to genetic discrimination. Yet, although the genetic counselors that have some knowledge of state law do mention the laws to their patients, few give the legal protections much emphasis or provide reassurance.[103]

Hence, the empirical data examined points to a privacy-diffusion relationship that gives cause for concern. Genetic discrimination is rare and apparently on the decline. Yet, misperception of the practice of genetic discrimination inhibits the diffusion of genetic testing technology. Genetic discrimination laws provide partial protection at best and contribute to the uncertainty as to the status of privacy protection. Consequently, the law has not been a major factor in inhibiting genetic discrimination. Furthermore, and more significantly, it has been unsuccessful in alleviating individuals' genetic discrimination concerns, thus impeding broader adoption of the technology.

B. *Collection of Personal Information by Commercial Entities on the Internet*

In 1990, an MIT computer science graduate student sat at his department's computer lab late at night using the search program "Gopher" to search certain libraries for materials for his dissertation. Once he finished working, he visited a newsgroup whose members were animated players of the computer adventure game "Moria." It was getting late and he was alone in the lab. Before turning to go home, he entered a chat room

---

[101] *Id.* at 253.

[102] Sixty percent of genetic counselors had accurate knowledge of federal law, and 35% of genetic counselors had accurate knowledge of state law. *Id.* at 252.

[103] *Id.* at 253.

occupied by Canadian students studying in the United States.[104] Through these nocturnal journeys, although sitting in a school computer lab, he was completely alone—he was unobserved—no trail followed him from one site to another.

In the early days of the Internet, every time a person clicked on a link, their computer's browser entered the new site as a clean slate. No references were left of previous surfing activities.[105] This changed in 1994, however, when Netscape created cookies to facilitate web surfing.[106] Cookies operate by identifying the individual and highlighting trails already taken; for example, by storing passwords or coloring links.[107] Yet, by creating individual trails, cookies eliminated the newly-discovered anonymity enabled by the Internet. Furthermore, as time went by, cookies became a tool in the hands of commercial profiling companies who used them to collect personal information about Internet users in order to target advertisements.[108] Cookies became one of many new tools that enabled private companies to collect information on the Internet.

Let us look at a typical 2006 Internet user. Imagine, a fifty-six year-old woman who lives in Washington D.C., works in marketing and uses the Internet extensively.[109] Although surfing the Internet while sitting by herself in her study, unlike the 1990 MIT student, she is never alone. Her personal information and Internet moves are constantly collected, filed and categorized. Her email account is a Gmail account, which she likes because it is free and provides her with extensive storage space. Yet, she is unaware that in return for this free offer, Gmail tailors the advertisements she receives to her emails according to their content. For example, an email from a friend suggesting a joint vacation in Hawaii was recently accompanied by advertisements for flights and hotels in Hawaii.[110] In

---

[104] 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).

[105] *See* BERNERS-LEE, *supra* note104, at 145.

[106] PEW INTERNET & AMERICAN LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 7 (2000), *available at* http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf [hereinafter TRUST AND PRIVACY ONLINE].

[107] *See* WebstreetStudios.com, Internet Cookies and Internet Privacy, http://www.webstreet studios.com/school/cookies.htm (last visited, Aug. 27, 2006) [hereinafter Cookie Basics].

[108] *Id.*

[109] Originally males dominated the Internet. In 1995, 18% of adult men were online, while only 10% of adult women were online. PEW INTERNET & AMERICAN LIFE PROJECT, AMERICAS' ONLINE PURSUITS: THE CHANGING PICTURE OF WHO'S ONLINE AND WHAT THEY DO 5 (2003), *available at* http://www.pewinternet.org/pdfs/PIP_Online_Pursuits_Final.pdf [hereinafter AMERICAS' ONLINE PURSUITS]. By 2003, 65% of men and 61% of women were online. *Id.* at ii. Since there are more women in the general population, women became the majority of the online population (51%) in 2003. *Id.* at 5.

[110] Katie Hafner, *In Google We Trust? When the Subject is E-Mail, Maybe Not*, N.Y. TIMES, Apr. 8, 2004, at G1, *available at* LEXIS, News Library, NYT File; Gmail Home Page, http://www.gmail.com (last visited Aug. 27, 2006).

addition, she has recently downloaded a free software application that unbeknownst to her was accompanied by GAIN software. GAIN software is one of many spyware software companies. The software now installed in her computer traces her geographical location, previous searches, and web-visits on the Internet.[111] Based on this information it delivers targeted advertising of Washington D.C. area dating services. Finally, she usually reads the Washington Post online. Yet, she can no longer read the newspaper without identifying herself. She is now required to register her personal information, including her job status.[112]

How did this shift take place? With the advent of the Internet to popular use, web sites and commercial profiling companies started collecting personal information. Their goal was to target advertising at Internet users and sometimes, more generally, to transform their site to match a visitor's interests and financial ability. Cookies were the main collection tool used. A cookie is a small text file that is saved in the user's computer. It contains code that identifies the user and stores certain information about her. This information can include a name, address, web searches and sites visited.[113] Some sites implanted their own cookies, while others implanted third-party cookies that usually originated from commercial profiling companies. These third-party cookies enabled the collection of personal information across web sites. Now, Site A could adjust its content based on searches that the user performed in Site B.[114]

Cookies were soon followed by other tools that enabled the collection of personal information. Among these tools are spyware and the less well-known web bugs. One form of spyware includes "Adware" and similar applications that install themselves covertly, sometimes by piggybacking on other applications that are downloaded by the user.[115] For example, many of the popular file sharing applications come bundled with spyware.[116] Web bugs are inserted in a web page for the purpose of

---

[111] *See* Rob Cheng & Dave Methvin, *Lack of Consent: A Survey of GAIN Users*, (2004), *available at* http://www.ftc.gov/os/comments/spyware/040315pcpitstop.pdf (describing GAIN software).

[112] Anitha Reddy, *Post's Web Site Will Seek More Information on Visitors*, WASH. POST, Feb. 4, 2004, at E5, *available at* LEXIS, News Library, WPOST File.

[113] *See* Cookie Basics, *supra* note 107; Microsoft.com, Understanding Cookies, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx (last visited Aug. 27, 2006) [hereinafter Understanding Cookies].

[114] Understanding Cookies, *supra* note 113..

[115] *See* CTR. FOR DEMOCRACY & TECH., GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM 2 (2003), *available at* http://www.cdt.org/privacy/03110 spyware.pdf. There are two additional types of spyware, although these are somewhat less related to general Internet use. First, keystroke loggers and screen capture utilities that are installed by a third party to monitor work habits, observe online behavior or capture passwords and other information. In such cases, a person usually installs the software intentionally into a computer used by others. Secondly, legitimate applications that have faulty privacy protections. *Id at 2.*

[116] *See id*. at 10.

collecting information about visitors without being detected.[117] Both are able to collect information similar to the information collected by cookies.[118] Spyware is also able to hijack a user's Internet connection for the software's own use, for example, as part of a distributed computing network or as a spam remailer.[119]

Public objections to the collection of personal information through use of cookies appeared as early as 1996.[120] Yet, it was 1999–2000 when the issue can be said to have reached public awareness. The mass media reported more frequently about the ways in which the use of cookies affects personal privacy on the Internet.[121] Public pressure resulting from such reports prevented, for instance, DoubleClick—a major commercial profiling company—from merging its online information with that of Abacus—a marketing database containing real space personal information.[122] Privacy watchdog organizations filed a complaint with the Federal Trade Commission (FTC), and several class actions were filed against commercial profiling companies[123]

Yet, despite mounting public pressure, the resulting case law did not find that commercial profiling through use of cookies compromises individuals' privacy.[124] The courts determined the cases by applying traditional communications statutes, such as the Electronic Communications Privacy Act (ECPA), the Wiretap Act, and the Computer Fraud and Abuse Act, and found that these statutes were not violated.[125] The settlements reached between the Federal Trade Commission and

---

[117] *See* David Martin et al., *Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use*, 46 COMM. OF THE ACM 258, 259 (2003), *available at* http://portal.acm.org/citation.cfm?id=953509; CYVEILLANCE, WEB BUGS: A STUDY OF THE PRESENCE AND GROWTH RATE OF WEB BUGS ON THE INTERNET 2 (2001), *available at* http://www.cyveillance.com/web/corporate/white_papers.htm.

[118] *See* Martin et al., *supra* note 117; CYVEILLANCE, *supra* note 117. *See also* CTR. FOR DEMOCRACY & TECH., *supra* note 115, at 4.

[119] *See* CTR. FOR DEMOCRACY & TECH., *supra* note 115, at 4.

[120] For an early report, see Marc Slayton, *The Risks of Cookies*, HOTWIRED, Jan. 3. 1996 (on file with Connecticut Law Review).

[121] *See, e.g.*, *Amid Protests, DoubleClick and Abacus Announce Plans for $1 Billion Merger*, ELECTRONIC ADVERTISING & MARKETPLACE REP., Jun. 29, 1999, at 13; Joseph Gallivan, *Privacy Group Calls for DoubleClick Nix*, N.Y. POST, Jun. 22, 1999, at 39, *available at* LEXIS, News Library, NYPOST File. Descriptions of the cookies' privacy threat also began appearing in legal scholarship. *See e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1486–90 (2000).

[122] Bob Tedeschi, *In a Shift, Doubleclick Puts Off Its Plan for Wider Use of the Personal Data of Internet Consumers*, N.Y. TIMES, Mar. 3, 2000, at C5, *available at* LEXIS, News Library, NYT File.

[123] *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003); *In re* Toys R Us Privacy Litig., MDL No. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Complaint and Request for Injunction, Request for Investigation and for Other Relief by the Electronic Privacy Information Center, *In re* DoubleClick Inc. (FTC Feb, 10, 2000), *available at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[124] *See In re Toys R Us*, 2001 LEXIS 16947, at *18, *27; *Chance*, 165 F. Supp. 2d at 1162; *In re DoubleClick*, 154 F. Supp. 2d at 526.

[125] *See id.*; *Chance*, 165 F. Supp. 2d at 1158–63; *In re DoubleClick*, 154 F. Supp. 2d at 507–19, 525–26.

collectors of personal information on the Internet failed to provide a comprehensive solution.[126] Congress did not implement the FTC's recommendations for legislation codifying the fair information practices principles that mainly require consent and notice for the collection of personal information. Nor did Congress act to prohibit or restrict commercial profiling and use of cookies.[127]

Unlike cookies, spyware has prompted restrictive legislation and some restrictive case-law.[128] Yet, spyware does not only impact privacy interests. It also impacts the computer's ability to function and its online communication, thereby disrupting regular computer operations and placing a substantial burden on providers' customer support departments. Furthermore, it has also given rise to trademark and copyright disputes.[129] Hence, although spyware legislation may, in effect, eventually restrict some forms of information collection, it does not appear to represent a shift in the legislature's attitude toward online privacy.[130]

Legal regulation was not the only potential mode of regulation for the collection of personal information on the Internet. Two other modes were tried: industry self-regulation and technological solutions. However, neither of these proved effective in containing information collection practices.

Industry self-regulation included two types of measures: privacy policies and certificate programs. Privacy policies that describe modes of collection and use of personal information became prevalent in 2000–

---

[126] *See* Elaine M. Laflamme, *Privacy is Becoming a Company Affair: Protecting Personal Information Means More than Posting Policies on Web Sites*, N.Y. L.J., Jun. 10, 2002, at 6; 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., *In re* DoubleClick Inc. (Aug. 26, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug 26a_02_attach.pdf; Settlement Agreement and Release, *In re DoubleClick, Inc. Privacy Litig*., 154 F. Supp. 2d (S.D.N.Y. 2002) (No. 00-CIV-0641 (NRB)), *available at* http://www.epic.org/privacy/ internet/cookies/dblclkproposedsettlement.pdf (last visited Aug. 29, 2006).

[127] JOSEPH TUROW, AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN 8 (2003), *available at* http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf#search= %22turow%20%22the%20system%20is%20broken%22%22.

[128] *See* CAL. BUS. & PROF. CODE § 22947 (West, Westlaw through Ch. 42 of 2006 Reg. Sess. urgency legislation and Props. 81, 82 and 1A); UTAH CODE ANN. § 13-40-102 (West, Westlaw through 2005 Second Special Session); Washingtonpost.Newsweek Interactive Co. v. Gator Corp., No. Civ.A.02-909-A, 2002 WL 31356645, at *1 (E.D. Va. July 16, 2002). In addition, many states, including the federal government, have new spyware bills. *See* Securely Protect Yourself against Cyber Trespass Act, H.R. 29, 109th Cong. (2005). *See generally* Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283 (2005) (discussing the application of privacy law to spyware).

[129] *See* 1-800 CONTACTS, Inc. v. WhenU.com, Inc., 309 F. Supp. 2d 467 (S.D.N.Y. 2003), *rev'd*, 414 F.3d 400 (2d Cir. 2005); FTC v. Seismic Entm't Prods., No. Civ. 04-377-JD, 2004 WL 2403124, at *2 (D.N.H. Oct. 21, 2004); CTR. FOR DEMOCRACY & TECH., *supra* note 115, at 3.

[130] Privacy concerns were one type of a host of concerns related to spyware that were brought before legislatures. *Cybersecurity and Consumer Data: What's at Risk for the Consumer?: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2003).

2001.[131] Yet, privacy policies were not intended to contain the practice of information collection. Their goal was to give Internet users notice and an option to consent. Whether privacy policies enable effective notice and consent is dubious since it appears that few Internet users read privacy policies.[132]

Certificate programs were another industry effort to self-regulate privacy. Two such programs—TRUSTe and BBB*Online*—were created to dispense privacy seals for web sites that maintained their users' privacy. Yet, few sites applied for the privacy seals. Furthermore, privacy violations by member sites were not investigated or regulated by the seal organizations.[133]

Efforts to regulate information collection through technological means did not provide a resolution to the information collection privacy problem because of the low rate of adoption among individual users. Two main technological solutions are:[134] (i) cookie management systems, the prominent one of which is the Platform for Privacy Preferences (P3P), which enables the user to choose her privacy preferences;[135] and (ii)

---

[131] In 2000, only 22% of a random sample of the busiest sites on the Internet and 51% of the top one hundred sites on the Internet mentioned use of cookies in their privacy policies. FTC, ONLINE PROFILING: A REPORT TO CONGRESS 11 (2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf [hereinafter FTC, ONLINE PROFILING]. However, a study conducted in December 2001 found the following: "Privacy notices are more prevalent, more prominent and more complete. Practically all of the most popular domains and 83% of the Random Sample sites provide some privacy disclosure." And importantly, the study found that the policies were comprehensive. WILLIAM F. ADKINSON, JR. ET AL., PRIVACY ONLINE: A REPORT ON THE INFORMATION PRACTICES AND POLICIES OF COMMERCIAL WEB SITES viii (2002), http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf.

[132] A 2001 Harris Interactive Poll showed that only 3% of users read privacy policies regularly and two-thirds spent little or any time looking at privacy policies. ADKINSON, JR. ET AL., *supra* note 131, at 5.

[133] TRUSTe started in 1997, and by 2002 had only 2000 licensees. BBB*Online* grew from 450 sites in 2000, to 760 sites in 2002. Yet, their overall percentage among web sites remained the same—11%. *See* ADKINSON, JR. ET AL., *supra* note 131, at 24–25; Elec. Privacy Info. Ctr. (EPIC), *Online Profiling Project—Comment*, P994809/Docket 990811219-9219-01, at 9–10 *available at* http://www.epic.org/privacy/internet/profiling_reply_comment.PDF [hereinafter EPIC, *Online Profiling Project*].

[134] A third major technological tool is firewalls. Firewalls, however, guard not only against the collection of personal information, but also against other harms inflicted by viruses, spam, worms and spyware. Consequently, assessing its usage will not reflect willingness to use the technology to prevent the collection of personal information. *See* Home PC Firewall Guide Index, *available at* www.firewallguide.com (last visited Aug. 5, 2006).

[135] P3P tried to resolve the problem of providing effective notice and consent on the Internet. P3P enables the user to choose her privacy preferences. Microsoft.com, Microsoft to Deliver Privacy Tools in Internet Explorer: Company Puts Privacy Controls in the Hands of Surfer, Unveils First Iteration of P3P in Browser (Mar. 21, 2001), http://www.microsoft.com/presspass/press/2001/mar01/03-21privacytoolsiepr.mspx. When a user's browser reaches a site that is P3P enabled, it can match the user's privacy preferences with the site's privacy policy and warn of a mismatch. *See To Review the FTC's Survey of Privacy Policies Posted by Commercial Web Sites: Hearing Before the S. Comm. on Commerce, Sci., and Transp*., 106th Cong. 81–82 (2000) (statement of Daniel J. Weitzner, Technology and Society Domain Leader, World Wide Web Consortium) [hereinafter *FTC's Survey Hearing*]; World Wide Web Consortium (W3C), P3P: The Platform for Privacy Preferences,

anonymizers that allows users to surf anonymously.[136] Studies show that Internet users overall did not adopt these privacy protecting technological tools.[137] Users did not adopt P3P technology despite its easy accessibility. P3P has been incorporated into Internet Explorer, which is used by 50% of Internet users. Yet, 98% of Internet Explorer users did not change the default preferences.[138]

Legal, industry and technological means, hence, failed to effectively regulate the collection of personal information on the Internet. The law, through the series of commercial profiling cases, produced a legal pronouncement permitting collection of personal information on the Internet. Industry self-regulation failed due to the ineffectiveness of notice and consent on the Internet and the commercial lure of personal information collection. Finally, the technological tools did not provide a solution due to their low rate of adoption among Internet users. Yet, the case of genetic discrimination has demonstrated that even in the absence of comprehensive regulation, privacy norms may still prevail. The question, thus, becomes whether social condemnation of the collection of personal information on the Internet has inhibited the practice.

Empirical studies measuring the use of privacy-threatening Internet technologies demonstrate that the practice of collecting personal information and commercial profiling is blooming. Evidence is mixed as to whether social pressure has effectively reduced the collection of

---

http://www.w3.org/P3P/ (last visited Sept. 2, 2006).

[136] *See* TUROW, supra note 127, at 25 (defining anonymizer as software that hides your computer's identity from websites).

[137] A 2003 study that examined users' general application of means to prevent collection of their personal information found that 64% of Internet users never researched how to protect their information on the web. Forty percent said they knew "'almost nothing' about preventing sites from collecting information about them." Twenty-six percent said they knew "a little," while only 9% said they knew "a lot." *Id* at 3. The study also found that less than 23% have used anonymizers at some point. *Id.* at 25.

[138] Microsoft P3P Implementation in Internet Explorer 6.0 and Windows XP: Fact Sheet, *available at* http://www.microsoft.com/presspass/press/2001/mar01/03-21privacytoolsiepr.mspx (last visited Oct. 8, 2006); Ernst & Young, *Enabling P3P: Workshop on Machine Readable Privacy Policies*, at 4, (2004), *available at* www.cdt.org/privacy/20040122enablingp3p.pdf. This was not the first effort to incorporate cookie management into an Internet browser. Its fate, however, resembles those of the previous attempts. In 1996, Netscape created a tool to disable cookies. The default allowed cookies but one could change browser preferences to disable them. By 2000, only 10% had set their browser to reject cookies. TRUST AND PRIVACY ONLINE, *supra* note 106, at 3. In general, utilization of cookies' management technologies remained low. In 2002, only 26% of individuals surveyed could affirmatively ascertain that their browser is not set to accept cookies. *See* The PrivacyPlace.org, *2002 Internet Privacy User Values Survey*, *available at* http://william.stuffle beam.cc/privacySurvey/results/resultsPage.php (last visited Sep. 28, 2006). It should be noted that the main cause of P3Ps failure was lack of adoption among individual users. Adoption of P3P among the most popular web sites has been relatively successful. A 2004 report found that 35% of the top one hundred sites and 18% of the top five hundred sites are P3P enabled. Yet, adoption among sites in general is much lower. A study performed in 2006 found that only about 2.5% of sites in a random survey were P3P enabled. Securityspace, Compact Privacy Policy Report, Sept. 1, 2006, www.securityspace.com.

personally identifiable information and use of cookies. Yet, overall it appears that a vast majority of sites, in particular the popular sites, collect Personally Identifiable Information (PII) that can include personal data such as name, email address or mail address.[139] Similarly, it appears that the majority of sites, in particular the popular sites, are using cookies extensively.[140] Furthermore, where the overall picture of information collection on the Internet is taken into account, the conclusion becomes unambiguous. Cookies have quickly become only one tool among many in the hands of those who desire to collect personal information. The use of such information collection tools is no doubt on the rise. In 1998, 0.664% of web pages contained web bugs, while in 2001, nearly 4% did.[141] In

[139] A 2000 survey, taken as public awareness of online privacy issues was rising, found that almost all sites collect an email address or some other form of PII. *FTC's Survey Hearing*, *supra* note 135, at 21 (prepared statement of Robert Pitofsky, Chairman, FTC). A 2002 survey still found that a very high percentage of sites collect PII. Yet, it revealed a certain reduction in use of PII. In a sample of random sites there was a drop from 97% to 90% while in a sample of popular sites there was a drop from 99% to 96%. ADKINSON, JR. ET AL., *supra* note 131, at 14. At the same time, a 2003 study shows that the collection of PII remains highly popular. Three quarters of P3P enabled sites (that assumingly are relatively privacy conscious sites) collected PII. Simon Byers et al., *Automated Analysis of P3P-Enabled Web Sites* § 4.3 (2003), *available at* http://lorrie.cranor.org/pubs/icec03-final.pdf. About half of these web sites indicated that they share this information with entities other than those who use the data for the purposes for which it was collected. *Id.* § 4.5.

[140] A survey done in 2000—around the time that Internet growth was peaking and controversy regarding use of cookies was erupting—revealed extensive use of cookies among these popular Internet sites. The survey showed that 78% of the top one hundred Internet sites allowed third-party cookies. FTC, ONLINE PROFILING, *supra* note 131, at 11. In addition, a random sample of the busiest sites on the Internet showed that 57% of these sites allowed third-party cookies. *Id.* A later study conducted in December 2001 that was designed to compare to the 2000 study—pointed to a potential reduction. Specifically, it reported that dissemination of personal information between commercial web sites via third party cookies has gone down from 78% to 48% in the top one hundred web sites. The study also showed a drop from 57% to 25% in the random sample of the busiest web sites. ADKINSON, JR. ET AL., *supra* note 131, at viii. However, another series of studies that measured overall use of cookies on the Internet between 2000 and 2006 does not reveal such a reduction, but instead, a dramatic increase in the use of cookies. *See* SecuritySpace.com, Internet Cookie Report, Dec. 1, 2000, http://www.security space.com/s_survey/data/man.200011/cookieReport.html (reporting that 9.5% of servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Dec. 1, 2001, http://www.securityspace.com /s_survey/data/man.200111/cookieReport.html (7.9% of servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Aug. 1, 2002, http://www.securityspace.com/s_survey /data/man.200207/cookieReport.html (14.3 % of the servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Jan. 1, 2003, http://www.securityspace.com/s_survey/data/man.200 212/cookieReport.html (14.3 % of the servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Dec. 1, 2003, http://www.securityspace.com/s_survey/data/man.200311/cookie Report.html (18.9 % of the servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Apr. 1, 2004, http://www.securityspace.com/s_survey/data/man.200403/cookieReport.html (17.5 % of servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Aug. 1, 2004, http://www.securityspace.com/s_survey/data/man.200407/cookieReport.html (18.3 % of servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Feb. 1, 2005, http://www.security space.com/s_survey/data/man.200501/cookieReport.html (17.9 % of servers studied sent cookies); SecuritySpace.com, Internet Cookie Report, Sep. 1, 2006, http://www.securityspace.com/s_survey /data/man.200608/cookieReport.html (24.3% of servers studied sent cookies) The relatively small percentages of cookie usage evidenced stems most likely from the mechanical "crawling" method used to conduct the survey, which does not differentiate between commercial and non-commercial sites. *Id*.

[141] CYVEILLANCE, *supra* note 117, at 4.

2003, 36% of a random sample of consumer oriented sites contained web bugs, while 58% of the most popular sites contained web bugs.[142] Spyware is also becoming increasingly common.[143] In general, it becomes apparent that the practice of collecting personal information has far from tapered off.

Surprisingly, however, concerns about the privacy threat posed by the Internet have not made any evident impact on the diffusion of the technology. Since 2000, users became increasingly aware of the threat to their online privacy through the collection of personal information on the Internet.[144] Yet, between 2000 and 2003, the U.S. online population expanded from eighty-six million in 2000, to one hundred and twenty-six million in 2003.[145] In 2001, 56% of adults in the United States used the Internet, while by 2003, 63% of American adults were online.[146]

Although Internet diffusion was not affected, the public perceived the collection of personal information on the Internet as a privacy threat.[147] Internet users overwhelmingly opposed the specific information collection practices, such as profiling, inter-site sharing, and merging of browsing habits with PII.[148] At the same time, it appears that individuals are

---

[142] Martin et al., *supra* note 117, at 259. Furthermore, reports focusing on the number of web bugs used by popular domains show a significant increase from 2001–2004. For example, 1.2% of Internet sites scanned in 2004 had web bugs planted by Amazon, SecuritySpace.com, Web Bug Site Count Report, Apr. 1, 2004, http://www.securityspace.com/s_survey/data/man.200403/webbug_site.html, while 0.1% of Internet sites scanned in 2001 had web bugs planted by Amazon. SecuritySpace.com, Web Bug Site Count Report, Mar. 1, 2001, http://www.securityspace.com/s_survey/data/man.200102/webbug_site.html. Similarly, Google went up from 0.1% of Internet sites scanned in 2001 to 0.5% in 2004, and Yahoo from 0.2% in 2001 to 0.5% in 2004. *Id.* Furthermore, these studies list the one hundred worst offenders. In 2001, the list included domains that installed bugs in 0.1% of the sites scanned, while in 2004 the list included only sites that installed bugs in 0.2% of the sites scanned. *Id.*

[143] In a 2004 survey, 53% of respondents reported experiencing the effects of spyware on their Internet use. AMERICA ONLINE & NAT'L CYBER SECURITY ALLIANCE, AOL/NCSA ONLINE SAFETY STUDY 4 (2004), *available at* http://staysafeonline.info /pdf/safety_study_v04.pdf.

[144] A survey conducted in 1999 revealed that most users were unaware of the collection of their personal information on the Internet. Alan F. Westin, *Social and Political Dimensions of Privacy*, 59 J. SOC. ISSUES, 431, 445–46 (2003). This changed by 2000, when 79% of Internet users surveyed believed it was common for companies to track web activities. TRUST AND PRIVACY ONLINE, *supra* note 106, at 8.

[145] AMERICAS' ONLINE PURSUITS, *supra* note 109, at ii. Although most Internet growth occurred during 2000 and current growth has tapered off, this is not indicative of any inhibiting effect on Internet diffusion. Many technologies will never reach 100% diffusion.

[146] *Id.*; PEW INTERNET & AMERICAN LIFE PROJECT, MORE ONLINE, DOING MORE 2 (2001), http://www.pewinternet.org/pdfs/PIP_Changing_Population.pdf.

[147] In 2000, the FTC reported that "[n]inety-two percent say they are concerned about threats to their personal privacy when they use the Internet and seventy-two percent say they are very concerned." FTC, ONLINE PROFILING, *supra* note 131, at 14.

[148] A 2000 study found that 89% of respondents opposed merging their PII with their browsing habits, 63% opposed profiling even without use of PII and 91% opposed the sharing of information between web sites. *Id.* at 15. A 2003 study found that 85% were unwilling to accept the way unrelated information about them was merged into profiles. TUROW, *supra* note 127, at 23–24. A third study, however, indicated that when users were offered the option of notice and choice for personalized advertising about 50% were willing to allow commercial profiling. FTC, ONLINE PROFILING, *supra*

unaware of the scope and intricacy of personal information collection and use of such information by commercial entities on the Internet. Although by 2003 a majority of Internet users were aware of the use of cookies, most appear to have a limited understanding of the use of their personal information. A majority of users believe that when a web site has a privacy policy, it will not share their personal information with other web sites or companies.[149] Furthermore, although a majority of users know that web sites collect information about them even if they do not register, they are unaware that unrelated information about them is connected together to form profiles.[150]

Hence, the collection of personal information on the Internet portrays a mirror image of the privacy-diffusion relationship paradox evidenced in the case of genetic discrimination. The use of privacy-threatening Internet devices that enable the collection and use of personal information on the Internet is constantly increasing. Yet, the diffusion of Internet technology is not affected.

C. *Employer Monitoring of Internet and Email*

Imagine a first-year New York law firm associate working very long hours. Two of the deals she has been working on are closing next week and for the last three weeks she has barely left the office. Still, Christmas is drawing near and she has to buy presents before going home. She has, therefore, resorted to buying them online. She also finds it very efficient to pay her bills and order her groceries online. Her boyfriend is clerking for a judge in Chicago. They have been unable to meet for the last couple of weeks but they correspond regularly through emails. Similarly, since she does not have time for long phone calls, she has been maintaining most of her contacts with her family and friends through email. She vaguely remembers being told at orientation that the law firm may monitor her email and Internet activities. She has not given it much thought recently.

Employer monitoring of email and Internet communications affects a broad range of employees. In the legal profession it pertains not only to first year associates, but also to judges. Despite their initial objections, federal judges' computers are monitored to detect downloading of music,

---

note 106, at 19. At the same time, about 32% to 49% still objected to profiling under these conditions. *Id.*

[149] TUROW, *supra* note 127, at 4.

[150] *Id. See also* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 1052–94 (1999) (discussing the gap between consumers' stated preference for privacy and dearth of action to guard their privacy).

streaming video, pornography and in general reduce computer use that is not related to judicial work.[151]

A large part of our social, professional and consumer lives now takes place through the Internet, email and instant messaging. At the same time, Internet and email have become vital business tools that many employees need to have at their disposal. Employees who spend a large part of their day at work tend to utilize email and Internet for their personal use as well as for business use.[152] At the same time, employers have many incentives to monitor use of Internet and email by employees. These reasons include: (i) avoiding legal liability for sexual harassment through exposure to pornography, or for copyright infringement through music file sharing; (ii) ensuring legal compliance (especially in highly regulated industries); (iii) ensuring productivity by preventing non-work related surfing and emails; (iv) security concerns, such as protecting trade secrets and other confidential information and; (v) preventing overloading of the system with music files or pictorial attachments.[153]

Although there is a general trend toward increased monitoring by employers, email and Internet monitoring is done on a much greater scale than other communications. Extensive email and Internet use can be monitored relatively cheaply through use of software that scans for certain uses. While 19% of major U.S. companies monitor phone conversations of employees in selected job categories and 3% record and review all employees phone conversations, 55% retain and review email communications and 76% monitor Internet communications.[154] Employers who monitor email and Internet use take disciplinary action or terminate employees for a broad range of related activities. The leading reason for disciplinary action or termination is access to pornography. Other reasons

---

[151] Neil A. Lewis, *Rebels in Black Robes Recoil at Surveillance of Computers*, N.Y. TIMES, Aug. 8, 2001, at A1, *available at* LEXIS, News Library, NYT File; Tony Mauro, *Federal Courts Adopt New Online Policies*, LEGAL TIMES, Sept. 24, 2001, at 6, *available at* WL, 9/24/2001 LEGAL TIMES 6.

[152] For example, the majority of employees (74.4%) said that 1% to 10% of their email is personal; 8.8% said that 11% to 25% of their email is personal. In addition, 31% of employees use instant messaging at work. Of those, 58% utilize it for personal use. AM. MGMT. ASS'N & EPOLICY INST., 2004 WORKPLACE E-MAIL AND INSTANT MESSAGING SURVEY 6 (2004), *available at* http://www.epolicyinstitute.com/survey/survey04.pdf [hereinafter 2004 WORKPLACE E-MAIL AND INSTANT MESSAGING SURVEY]. For a report detailing the type of Internet sites employees visit at work., see, Websense, Web@work Survey, 2006 available at http://www.securitymanagement.com/library/websense_technofile0906.pdf#search=%22web%40work%20employer%20survey%20%22.

[153] AM. MGMT. ASS'N, 2001 AMA SURVEY: WORKPLACE MONITORING & SURVEILLANCE: SUMMARY OF KEY FINDINGS 1 (2001), *available at* http://www.amanet.org/research/pdfs/ems_short2001.pdf [hereinafter 2001 AMA WORKPLACE MONITORING SURVEY SUMMARY]; Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474–76 (2002).

[154] AM. MGMT. ASS'N & EPOLICY INST., ELECTRONIC MONITORING & SURVEILLANCE: SURVEY 3, 6 (2005), *available at* http://www.amanet.org/research/pdfs/ems_summary05.pdf [hereinafter 2005 ELECTRONIC MONITORING SURVEY].

include online chatting, gaming, gambling, music downloads, investing or shopping at work, and reading news.[155]

Employers, through Internet and email monitoring, have greater access to their employees' personal lives than they ever had before. Although employees have filed suits arguing that company monitoring of their email and Internet activities violates their privacy, they have consistently lost these cases.[156]

Most of these cases dealt with email privacy. Tort causes of action have generally failed for two reasons. First, the courts found that the employees had no reasonable expectation of privacy in their email and Internet communications. In one action for intrusion upon seclusion, the court declined to find a reasonable expectation of privacy even where the employer assured employees that their email correspondence would remain confidential.[157] Secondly, the courts held that Internet and email monitoring would not constitute a highly offensive invasion of privacy to the reasonable person.[158] Suits were likewise rejected under the Electronic Communications Privacy Act (ECPA) and similar state statutes.[159] Even government employees who receive additional privacy protection under the Fourth Amendment usually failed to win these suits.[160] Plaintiffs have fared equally when the email correspondence at issue was between employees, or included outside correspondence.[161] Plaintiffs failed to win even when the employer accessed a non-work email account, such as a Hotmail account.[162]

Despite the prevalence of Internet monitoring, few cases challenge the practice. Yet, the trend appears to follow the email cases. In one case that concerned Internet use by a government employee, the court held that the employee's Fourth Amendment rights were not violated because, in light

---

[155] Websense, *Web@work Employer Survey 2000: Cyberslacking* 1 (on file with Connecticut Law Review); Websense, *Web@work Employer Survey 2001: Cyberslacking* 1 (on file with Connecticut Law Review); Websense, *Internet Misuse Survey 2002*, (on file with Connecticut Law Review).

[156] *See* KEVIN J. CONNOLLY, LAW OF INTERNET SECURITY AND PRIVACY, § 5.04[A][3] (2004).

[157] Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

[158] *See* Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 at *3–7 (D. Mass. May 7, 2002); *Smyth*, 914 F. Supp. at 101; McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *12 (Tex. Ct. App. May 28, 1999); William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK. L. REV. 91, 110–11 (2003).

[159] *See generally* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623 (E.D. Pa. 2001); F. LAWRENCE STREET & MARK P. GRANT, LAW OF THE INTERNET §2.11 (2)(a)(ii) (2005) (citing Shoars v. Epson Am. Inc., No. SWC II2749, slip op. (Cal. App. Dep't Super. Ct. Dec. 8, 1992)); Corbett, *supra* note 158, at 108–09.

[160] *See* United States v. Monroe, 52 M.J. 326, 327–330 (C.A.A.F. 2000); Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH L. & POL'Y 135, 153 (2003).

[161] *See Garrity*, 2002 U.S. Dist. LEXIS 8343; *Fraser*, 135 F. Supp. 2d 623.

[162] *See* Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 (W.D. Wis. 2002).

of a privacy policy announcing audits of Internet use, he did not have a reasonable expectation of privacy.[163]

The law has, in effect, authorized email and Internet monitoring by employers.[164] These communications are a hybrid between a mailed letter and a phone communication. Yet, the blanket endorsement of employer Internet and email monitoring differs from the legal stand on employer monitoring of regular mail or telephone conversations. Under the ECPA, an employer cannot monitor phone calls when employees have a reasonable expectation of privacy.[165] Monitoring is permissible if consent can be inferred because an employee was notified in advance, or if the employer monitors the phone in the ordinary course of business.[166] The courts, however, have construed these exceptions narrowly, thereby protecting employees' phone privacy.[167] The postal mail receives even stronger privacy protection than the telephone. Under federal statute, the unauthorized opening of another's mail constitutes a criminal offense.[168] In addition, the courts have found that an employer's reading of an employee's private mail comprises a privacy violation under the tort of intrusion upon seclusion.[169]

The business advantages of employee monitoring, combined with its technological feasibility and the absence of legal prohibitions, have lead to a consistent increase in email and Internet monitoring by employers. Email monitoring has been constantly on the rise. In 2005 55% of major U.S. companies monitored or retained email messages compared to 1997, when only 14.9% of major U.S. companies monitored email.[170] As for Internet monitoring, in 2005 76% of major U.S. companies monitored the

---

[163] United States v. Simons, 206 F.3d 392, 395–97, 401 (4th Cir. 2000); *see also* Wagner v. Roth, 780 N.Y.S.2d 42 (N.Y. App. Div. 2004).

[164] *See generally* Michael Rustad & Sandra R. Paulsson, *Monitoring Employee Email and Internet Usage: Avoiding the Omniscient Electronic Sweatshops: Insights from Europe* (Suffolk U. L. Sch. Intell. Prop. Paper No. 6, at 18–45, 2005).

[165] *See* Electronics Communications Privacy Act, 18 U.S.C. §§ 2511(2)(d), §2510(5) (2000).

[166] *See id.*

[167] *See, e.g.*, Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

[168] 18 U.S.C. § 1702 (2000).

[169] Vernars v. Young, 539 F.2d 966 (3d Cir. 1976).

[170] 2005 ELECTRONIC MONITORING SURVEY, *supra* note 154; The American Management Association started conducting surveys in 1997. The statistics collected demonstrate the expansion in the scope of email and Internet monitoring, although the focus of the survey varied somewhat over the years. The 2004 survey found that 60% of major U.S. companies used software to monitor external email while 27% used it to monitor internal email. 2004 WORKPLACE E-MAIL AND INSTANT MESSAGING SURVEY, *supra* note 152, at 2. The 2003 survey found that 52% of major U.S. companies engage in some form of email monitoring, while 40% monitor via use of software. AM. MGMT. ASS'N ET AL., 2003 E-MAIL RULES, POLICIES AND PRACTICES SURVEY 2, 4 (2003), *available at* http://www.messagingarchitects.com/policy/articles/Email_Policies_Practices.pdf. The 2001 survey found that storage and review of email messages is done by 46.5% of major U.S. companies. 2001 AMA WORKPLACE MONITORING SURVEY SUMMARY, *supra* note 153, at 1. This was compared to 38.1% in 2000; 27% in 1999; 20.2% in 1998 and 14.9% in 1997. *Id.*

Internet up 45% from 1999 when surveys reported that 31% of companies monitor or restrict Internet use.[171]

The lawsuits demonstrate that many employees believe that employers' email and Internet monitoring threatens their privacy, yet, despite the unprecedented growth of Internet and email monitoring compared to the monitoring of other employee communications modes, such as telephone or mail, there is no indication that Internet or email diffusion has been affected.[172] Potentially, some employees who are aware of monitoring may have limited certain uses of email and Internet at work. Yet, there is no indication that this has had any effect on the overall diffusion of Internet technology.

Hence, the case of employee Internet monitoring resembles the case of the collection of personal information on the Internet. Threats to employees' privacy through monitoring of their Internet and email use are constantly increasing. The law has endorsed the broad monitoring of email and Internet use by employers and in effect pronounced that such actions are not illegal. Yet, the diffusion of Internet technology has been unaffected.

IV. SUSPECT PRIVACY-DIFFUSION RELATIONSHIPS

The relationships between privacy protection and diffusion described in the previous Part give rise for concern. In this Part, I show that the controversies surrounding genetic discrimination, collection of personal information on the Internet and employee email and Internet monitoring involve two suspect privacy-diffusion relationship models. I then turn to identify the technological diffusion characteristics that entrapped genetic testing and the Internet in their respective suspect privacy-diffusion relationships. The identification of the technological diffusion characteristics that make a technology vulnerable to a suspect value protection-diffusion relationship should alert decision-makers charged with the regulation of new technologies to a potential problem.

A. *The Privacy-Diffusion Relationship*

The controversies surrounding genetic discrimination, the collection of personal information on the Internet and monitoring of employees Internet and email use involve pressures on the social structures through which we perceive our privacy. Individuals' objections to the use of their genetic

---

[171] 2005 ELECTRONIC MONITORING SURVEY, *supra* note 154; Vault.com, Survey of Internet Use in the Workplace (1999), http://www.vault.com/surveys/internetuse/employer.jsp?results=4 [hereinafter Vault.com 1999 Survey].

[172] As discussed, Internet diffusion has accelerated during this time period. *See supra* notes 144–46 and accompanying text.

information by insurers and employers and the collection and monitoring of their actions on the Internet by employers and commercial profiling companies evidence these pressures. In all three cases, the new technologies transformed the status quo, thereby creating novel privacy threats.

The employee monitoring case affects the norms of appropriateness that define what information about employees should be revealed to their employers. The Internet enables employees to conduct a broader range of personal affairs from work and to do so in a more efficient way than ever before. At the same time, the technology facilitates employers' monitoring of employees' communications. Internet monitoring can be done in an exceedingly comprehensive and cost-effective way. Consequently, employers have broader access to employees' personal affairs than prior to the advent of Internet and email. Employees' reactions indicate a violation of norms of appropriateness. Many believe that employers' monitoring of their email and Internet constitutes an inappropriate change in the employment relationship.

The collection of personal information by commercial entities on the Internet changes the status quo through a violation of existing norms of appropriateness, norms of information flow and the unauthorized creation of personal information. Commercial entities aggregate bits of information about individual Internet users—amalgamating information from different sources that individuals do not expect to be put together. These bits of information are covertly used to create new profiles about individual users. Commercial profiling companies then use the information derived from the creation of these profiles for purposes of targeted marketing. This is done through the creation of a new flow of information back to the individual, thus changing that person's Internet universe.[173] Surveys of the general public revealed that the public views the new personal collection of information norms exercised by commercial entities as privacy threats.[174]

Finally, use of genetic information by insurers and employers could destabilize the status quo. The public distinguishes use of the newly available, highly personal genetic information by such third parties from use of regular medical information. Genetic information carries significant cultural force, symbolizing for many the actual truth—the very essence of the self.[175] Public opinion surveys show that many individuals believe that use of genetic information is inappropriate, even where use of regular

---

[173] *See* Gaia Bernstein, *Accommodating Technological Innovation: Identity, Genetic Testing and the Internet*, 57 VAND. L. REV. 965, 1014–20 (2004).

[174] FTC, ONLINE PROFILING, *supra* note 131, at 15–16.

[175] DOROTHY NELKIN & M. SUSAN LINDEE, THE DNA MYSTIQUE: THE GENE AS A CULTURAL ICON 38–57 (1995).

medical information may be appropriate. The public conceives the use of genetic information by insurers and employers as a privacy threat. [176]

The examination of the three privacy controversies through the broader privacy-diffusion relationship prism reveals two suspect relationship models that reflect disequilibrium between privacy and diffusion:

Model One—The Genetic Discrimination Model: The privacy threat did not materialize. Genetic discrimination is rare and apparently on the decline. Yet, paradoxically, diffusion of genetic testing is inhibited. Individuals continue to fear genetic discrimination and are, therefore, less likely to test.

Model Two—The Internet Model: The monitoring of employee Internet use and commercial collection of personal information present an alternative suspect relationship. Privacy threats imposed by Internet technology are consistently on the increase. Yet, paradoxically, Internet diffusion has rapidly accelerated.

B. *Susceptible Technologies*

Understanding the characteristics that made genetic testing and the Internet susceptible to these privacy-diffusion relationships is a first step toward the resolution of these paradoxes. Furthermore, technologies are often not as unique as they appear at first blush. Identifying the technological characteristics that entrapped genetic testing and the Internet in these relationships could inform decision-making regarding other technologies that share the same characteristics. Early identification of these characteristics could serve as an important tool in the hands of those in charge of regulating new technologies.

In this Section, I identify four characteristics that affected the diffusion of genetic testing and the Internet and made them susceptible to the described privacy-diffusion relationships. Two diffusion attributes made genetic testing susceptible to the suspect privacy-diffusion relationship manifested in the case of genetic discrimination: (i) its preventive nature; and (ii) its non-triable quality. At the same time, two other diffusion attributes made the Internet susceptible to the second privacy-diffusion relationship: (i) its critical mass point quality; and (ii) its decentralized diffusion process. The identified diffusion characteristics may not be the only factors leading to the development of the two different suspect privacy-diffusion relationships. They do, however, create important

---

[176] *See* NATIONAL CENTER FOR GENOME RESOURCES, NATIONAL SURVEY OF PUBLIC AND STAKEHOLDERS' ATTITUDES AND AWARENESS OF GENETIC ISSUES, 1, 4 (1996) (on file with Connecticut Law Review); Philip Reilly, *Genetic Discrimination*, *in* GENETIC TESTING AND THE USE OF INFORMATION, *supra* note 68, at 106, 118–20.

conditions for the development of these relationships and consequently warrant attention.[177]

1. *Genetic Testing: A Preventive Technology*

Preventive innovations are technologies aimed at avoiding unwanted consequences. The rewards to the individual from adopting a preventive innovation are often delayed in time. The unwanted results may not occur right away or may never occur at all. They are also relatively intangible.[178] Examples of preventive innovations are using car seat belts, adoption of soil conservation practices, being screened for breast cancer, getting inoculations against a disease, flossing one's teeth and testing for HIV/AIDS.[179]

Let us look at the case of car seat belts. In 2001, after decades of government efforts and information campaigns the percent of Americans who buckled up has reached only 73%.[180] In some states, such as Massachusetts, only 51% wear seat belts.[181] When individuals are asked why they do not buckle up they give diverse reasons. Some are teenagers or drunk drivers who are risk takers. Others insist it is their right not to use

---

[177] Two additional factors may have contributed to the development of the two privacy-diffusion relationships. First, the Internet privacy-diffusion relationship is likely also a result of the invisible nature of Internet monitoring. Individuals cannot see cookies, web bugs and spyware. Even individuals who are knowledgeable about Internet monitoring are not constantly reminded that commercial entities are monitoring their Internet conduct. Consequently, people are less likely to react to the privacy threat. For a more detailed discussion of the invisible monitoring factor, see, Bernstein, *supra* note 17. Second, the sensitivity of medical information may have contributed to the genetic discrimination privacy-diffusion relationship. Individuals are very sensitive about disclosing their medical information, particularly due to the grave consequences of losing one's insurance. Yet, it appears that individuals' reactions to threats on their personal medical information are also context and technology related. Although Internet users express great concern about the collection of their personal health information on the Internet and take some measures not to disclose their personally identifiable information, the majority of Internet users researches health issues on the Internet. Furthermore, during the period in which the public became aware of privacy concerns on the Internet the percentage of Internet users that sought health Information on the Internet increased from 54% in 2000 to 66% in 2003. *See* CALIFORNIA HEALTHCARE FOUNDATION AND INTERNET HEALTHCARE COALITION, ETHICS SURVEY OF CONSUMER ATTITUDES ABOUT HEALTH WEB SITES 4 (2000), *available at* http://www.chcf.org/topics/view.cfm?itemID=12493; HEALTH PRIVACY PROJECT, HEALTH PRIVACY POLLING DATA (2004), *available at* http://www.healthprivacy.org/usr_doc/poling_data.pdf; PEW INTERNET & AMERICAN LIFE PROJECT, HEALTH INFORMATION ONLINE ii, 3, (2005), available at http://www.pewinternet.org/pdfs/PIP_Healthtopics_May05.pdf.

[178] ROGERS, *supra* note 4, at 991.

[179] *Id.* at 233.

[180] U.S. DEPARTMENT OF TRANSPORTATION, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, SAFETY BELT AND HELMET USE IN 2002—OVERALL RESULTS 3 (2003), *available at* http://www-nrd.nhtsa.dot.gov/pdf/nrd-30/NCSA/Rpts/2002/809-500.pdf.

[181] U.S. DEPARTMENT OF TRANSPORTATION, NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, RESEARCH NOTE: SAFETY BELT USE IN 2002—USE RATES IN THE STATES AND TERRITORIES 3 (2003), *available at* http://www-nrd.nhtsa.dot.gov/pdf/nrd-30/NCSA/RNotes/2003/809-587.pdf.

seat belts. Some state that it wrinkles their clothes or takes too much time. In general, they are all saying that the cost and effort required to wear seat belts is greater than the benefit in the remote chance that they would get involved in an accident.[182]

Genetic testing is also a preventive technology.[183] The goal of the genetic test is to detect the probability for disease in advance in order to take preventive measures where possible or make informed life-decisions. Yet, most genetic diseases are not certain to develop even when an individual carries the genetic mutation.[184] Even if the individual will eventually develop the disease, this could take place well into the future. Such benefits are not tangible and do not provide an immediate reward.

Preventive innovations are characterized by a low diffusion rate—the technology tends to diffuse slowly and relatively few individuals adopt it.[185] Preventive technologies have a lower adoption rate because of their weaker relative advantage.[186] Relative advantage is the most important predictor of a technology's adoption. It is comprised of the economic profitability, social prestige, low initial cost, decrease in comfort, savings in time and effort and the immediacy of the reward.[187] Preventive innovations do not provide an immediate reward. These innovations promise rewards that are distant in time and uncertain in nature. Furthermore, it is difficult to perceive the unwanted event because it is a non-event. Since preventive technologies have a weaker relative advantage, people are less likely to adopt them.

The preventive nature of genetic testing technology exacerbates the privacy threats imposed by the technology. Where the technology is preventive and individuals are already disinclined to adopt it, any additional problem including a privacy threat is likely to play a more significant role. Consequently, genetic testing technology was susceptible to the first privacy-diffusion relationship model, where diffusion is inhibited despite the absence of an actual privacy threat. Other technologies that share the preventive technology characteristic also have a higher likelihood of being entrapped in this relationship.

---

[182] ROGERS, *supra* note 4, at 235.

[183] For a study focusing on the effects of the preventive nature of genetic testing technology, see generally, Armstrong et al., *supra* note 54 at 96.

[184] For example a woman who carries the genetic mutation for breast cancer (BRCA1 or BRCA2) has a 50% to 85% chance of incurring the disease. Memorial Sloan-Kettering Cancer Ctr., Breast/Ovarain Cancer: BRCA1 & BRCA2, http://www.mskcc.org/mskcc/html/8623.cfm (last visited Sept. 12, 2006).

[185] ROGERS, *supra* note 4, at 234–35.

[186] *Id*. at 991.

[187] *Id*. at 232–34.

2. *Genetic Testing: A Non-Triable Technology*

The triability of an innovation is the degree to which a user can experiment with a technology on a limited basis.[188] Users perceive triability as important because it reduces risk and uncertainty about the consequences of using an innovation. It provides adopters a risk free way to explore and experiment with the technology. Experimentation increases users' comfort.[189] Consequently, new ideas that can be divided for trial are generally adopted faster.[190]

Examples of triable technologies, that is, technologies that can be experimented with on a limited basis, are plentiful. One can try the Internet on a library computer, borrow a cellular phone from a friend to check it out or purchase it with a one-month trial period. Similarly one can view a DVD player at a friend's house.

Genetic testing, on the other hand, is a non-triable technology—it does not lend itself to limited experimentation. Most potential users of genetic testing are members of families inflicted by a disease who consider testing for the specific disease that is prevalent in their family. Once they test the information regarding their genetic carrier status is created and can affect self-conceptions or be abused by third-parties. Furthermore, unlike other types of personal information, the created genetic information is immutable.[191] Consequently, users of genetic testing technology are generally first time users or potential adopters. Further, even if an individual would decide to undergo a battery of genetic tests, use of the technology would in most cases still remain a one-time event.

Additionally, there are five typical groups of adopter categories: innovators, early adopters, early majority, late majority and laggards.[192] Genetic testing, due to its slow diffusion rate, is still at the early adopters stage.[193] Earlier adopters of an innovation tend to perceive triability as more important than later adopters. Earlier adopters are more affected by the triability of the technology because their use of the technology serves as a kind of vicarious trial for later adopters.[194] Consequently, users of

---

[188] *Id*. at 249.

[189] *See* Elena Karahanna et al., *Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs*, 23 MIS Q. 183, 185–86 (1999).

[190] ROGERS, *supra* note 4, at 258.

[191] *See* Armstrong et al., *supra* note 54, at 96–97. For a discussion of the potential effects of genetic information on conceptions of the self, see generally, Rochelle Cooper Dreyfuss & Dorothy Nelkin, *The Jurisprudence of Genetics*, 45 VAND. L. REV. 313 (1992).

[192] ROGERS, *supra* note 4, at 282–85.

[193] *See* Michael Hall & Olunfunmilayo I. Olopade, *Confronting Genetic Testing Disparities: Knowledge Is Power*, 293 J. AM. MED. ASSOC. 1783, 1784–85 (2005) (explaining why physicians are reluctant to order genetic testing); Louise Wideroff et al., *Physician Use of Genetic Testing for Cancer Susceptibility: Results of a National Survey*, 12 CANCER EPIDEMIOLOGY, BIOMARKERS & PREVENTION 295 (2003) (describing the limited use of cancer susceptibility tests).

[194] ROGERS, *supra* note 4, at 258.

genetic testing technology are particularly affected by the non-triable nature of the technology.

The non-triable nature of genetic testing technology also exacerbates the privacy threat. First, like preventive technologies, non-triable technologies have a slower diffusion rate.[195] Individuals are less likely to adopt a technology that cannot be tried out. The inability to experiment with a technology aggravates any concerns regarding its ramifications, since once it is used the individual has to bear the full brunt of the implications. In the case of genetic testing, an individual considering whether to test fears that by the act of taking the test she may expose herself to the full consequences of genetic discrimination.

Secondly, potential adopters of a technology are more affected by privacy threats than individuals that already used the technology. Social norms play a greater role when a behavior is new. As the behavior becomes more ritualized, habits begin to exert a stronger influence and the effect of social norms weakens. Thus, experience decreases the influence of social norms.[196] A study that compared pre-adoption and post-adoption behavior found that the social compatibility of a technology affected the decisions of pre-adopters, but did not play a significant role in the decisions of individuals already using the technology.[197] Genetic testing technology cannot be tried on an experimental basis. Its use is usually a one-time event. Consequently, the non-triable nature of the technology affects the type of users: most users of genetic testing are either first time users or potential adopters as opposed to experienced users. Their decisions are, therefore, particularly vulnerable to the privacy threats.

Hence, the non-triable nature of genetic testing technology aggravates the privacy threat. Individuals examining non-triable technologies are extra cautious about the adoption decision. Therefore, genetic testing technology is susceptible to the paradoxical situation evidenced in the case of genetic discrimination where individuals do not adopt the technology despite the actual absence of a privacy threat.

3. *Internet Technology: A Critical Mass Point Technology*

Network effects exist where the value of the good is dependent on the number of individuals who use it. Interactive technologies, such as the telephone, the fax or the Internet, are often characterized by "network effects." The interactive nature of communication technologies creates interdependence between adopters in the system. An interactive communication is of little use to people unless others adopt it. For

---

[195] *See id.*

[196] Ronald Thompson et al., *Influence of Experience on Personal Computer Utilization: Testing a Conceptual Model*, 11 J. MGMT. INFO. SYS. 167, 173, 181–82 (1994).

[197] Karahanna et al., *supra* note 189.

instance, the telephone became more desirable once it became more widespread and there were additional people to call.[198] Network effects become prominent as a critical mass of people starts using a technology.[199]

Once the critical mass point is reached, the rate of adoption accelerates.[200] Thus, when a technology reaches the critical mass point, social norms regarding its use become quickly entrenched.[201] Moreover, a technology that diffuses rapidly and is extensively adopted is less likely to be abandoned. The telephone, for example, has become such an integral part of our professional and personal lives, that it is practically impossible for an individual to unilaterally discontinue use of the phone.[202]

The Internet technology is considered a network effects technology. The desirability of the Internet is dependent on the number of people who use it.[203] Although the Internet existed for decades before it became generally used, once it reached its critical mass point in 1990, its adoption rate accelerated exponentially.[204] In 1990, about four million users used the Internet worldwide, while by 2002, that number had grown to 544 million users worldwide.[205] Privacy-threatening uses of the Internet became common in the second half of the 1990s, at the time that Internet diffusion was already growing at an exponential pace. Consequently, non-privacy norms were quickly entrenched. Furthermore, at this point, when

---

[198] *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 Effects*, 86 CAL. L. REV. 479, 481, 483 (1998); Markus, *supra* note 18.

[199] Technologies characterized by network effects that reach critical mass also manifest a different demand curve. Demand does not grow as price decreases, but instead as demand grows the price may increase. *See* Nicholas Economidas & Charles Himmelberg, *Critical Mass and Network Size with Application to the US Fax Market* 1 (Stern School of Business, N.Y.U., Discussion Paper No. EC-95-11, 1995), *available at* http://raven.stern.nyu.edu/networks/95-11.pdf.

[200] ROGERS, *supra* note 4, at 343–45. For example, the fax boom started in 1983 when the price for faxes was reduced dramatically. Yet, diffusion was slow until 1987 when the critical mass point was reached. From that point on, however, diffusion accelerated at a rapid pace. *Id.*

[201] A social norm regarding use of a technology exists when it is effective in directing behavior regarding the technology. *See* Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643, 1661–66 (1996).

[202] Rogers notes that the critical mass effect could theoretically accelerate discontinuance. He points out that if people would stop responding to emails others may decide that email is no longer an effective mode of communication. However, he concludes that such a rejection of email is unlikely today due to the breadth of its spread. *See* ROGERS, *supra* note 4, at 352. For a comprehensive discussion of the integration of the telephone into American lives, see, CLAUDE S. FISCHER, AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940 (1992).

[203] *See* Mark Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT. L. REV. 1257, 1281 (1998).

[204] The Internet was not an overnight success. It was invented long before it reached critical mass. Several potential dates for the "conception" of the Internet include: the 1964 invention of packet switching; the 1969 commencement of operation of the ARPAnet; or 1989 when commercial Internet service providers started offering services to the general public. *See* Gisle Hannemyr, *The Internet as Hyperbole: A Critical Examination of Adoption Rates*, 19 INFO. SOC. 111, 114 (2003).

[205] ROGERS, *supra* note 4, at 343–44, 346.

millions became dependent on email and Internet for every day use, privacy threats, no matter how intensive, were unlikely to cause people to abandon the technology. It became impossible for individuals to unilaterally discontinue use of a communication mode utilized by so many others. Hence, the critical mass point quality made the Internet susceptible to the second suspect privacy-diffusion relationship, where diffusion accelerated despite extensive privacy threats.

4. *Internet Technology: A Decentralized Technology*

A technology's diffusion process can be either centralized or decentralized. Innovations that are centrally diffused emerge from an expert source that diffuses the innovation to potential adopters who accept or reject the innovation. For example, genetic testing is a centrally diffused innovation—the medical profession, primarily genetic counselors which administer the tests, control its diffusion.[206]

Other technologies have decentralized diffusion processes. In these cases, the diffusion emerges horizontally via peer networks—there is no central expert group in charge of coordinating diffusion. Furthermore, diffusion is accompanied by a high degree of reinvention of the innovation. Users of the technology, in the process of adopting and implementing the technology, act to change and modify it. Members of the user system have the ability to make sound decisions about how the diffusion system should be managed.[207]

The Internet is a prime example of an innovation, which has a decentralized diffusion process. From its inception, the Internet was diffused and developed by its users and not controlled by a central group of experts.[208] The absence of a controlling group that upholds privacy norms, combined with the ability of any user to transform the Internet's architecture, led to the development and spread of privacy-infringing tools, such as cookies and spyware. Hence, the decentralized nature of the Internet amplified the effect of its critical mass point quality (and related network effects) in producing a quick entrenchment of commercial non-privacy norms, thereby increasing its susceptibility to the second suspect privacy-diffusion relationship.[209]

---

[206] *Id.* at 394–98.

[207] *See id.* at 180, 394–398; DUNCAN J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE 50–55 (2003); Brian Butler & Deborah E. Gibbons, *Power Distribution as a Catalyst and Consequence of Decentralized Technology Diffusion*, *in* INFORMATION SYSTEMS INNOVATION AND DIFFUSION: ISSUES AND DIRECTIONS 4–5, 12–13 (Tor J. Larson & Eugene McGuire eds., 1997).

[208] *See* Steven R. Salbu, *Who Should Govern the Internet: Monitoring and Supporting a New Frontier*, 11 HARV J.L & TECH. 429, 435–36 (1998); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 832 (2004).

[209] *See* STEVEN A. HETCHER, NORMS IN A WIRED WORLD 245, 250, 274 (2004) (describing the creation of privacy-threatening norms).

V. POLICY IMPLICATIONS

The two suspect privacy-diffusion relationship models exhibit a divergence from the general preference for a balance between diffusion and privacy protection. As discussed, society generally rejects extensive diffusion and widespread adoption of a new technology that significantly erodes privacy. At the same time, society also disfavors the inhibition of the diffusion of important technologies due to privacy threats.

In this Part, I assess potential resolutions to the genetic discrimination and Internet suspect privacy-diffusion relationships. My objective in this Part goes beyond inquiring whether the suspect relationships are indeed dysfunctional, and proposing specific resolutions. Decision-makers dealing with the regulation of new technologies often assess each new technology in isolation. Yet, there are definite patterns in the co-evolution of technology and society. These patterns can be used to identify similar problems confronted by other new technologies. I propose that undertaking a generalized approach that looks beyond a specific technology can be an important tool in improving decision-making regarding the regulation of new technologies.[210] In particular, I suggest that such an approach would be useful in resolving and preventing problematic privacy-diffusion relationships. Other technologies that share the technological diffusion characteristics that made genetic testing and the Internet susceptible to their respective suspect privacy-diffusion relationships may also be entrapped in these relationships. The identification of the technological diffusion attributes that made genetic testing and the Internet vulnerable to these suspect relationships can be helpful in preventing other technologies from becoming entrapped in the same situations. At the same time, the conclusions I present here are based on privacy controversies involving only two technologies. Consequently, I seek to provide an initial framework for incorporating technological diffusion attributes into technology specific legal decision-making that I expect would be refined with further study of additional technologies.[211]

A. *Regulating Preventive, Non-Triable and Centrally Diffused Technologies*

Technologies that are preventive and non-triable exacerbate privacy threats and are, therefore, prone to the first suspect privacy-diffusion

---

[210] *See* LAWRENCE H. TRIBE, CHANNELING TECHNOLOGY THROUGH LAW 6 (1973); Arie Rip & Johan W. Schot, *Identifying* Loci *for Influencing the Dynamics of Technological Development*, *in* SHAPING TECHNOLOGY, GUIDING POLICY: CONCEPTS, SPACES AND TOOLS 155, 155 (Knut H. Sørensen & Robin Williams eds., 2002).

[211] This Article's case study methodology renders the framework preliminary. Future work that will inquire into additional case studies will be crucial in refining and finessing the conclusions set forth.

relationship. These technologies are more likely to be entrapped in a situation where, although a privacy threat does not exist, individuals perceive a risk and are consequently reluctant to use the technology.

Where a technology's diffusion attributes make it likely that a perception of a privacy threat will affect its diffusion, the expressive role of the law in dispelling such misperceptions is of particular importance. The law has an expressive function that is distinguished from its coercive function. The law's coercive function affects behavior through enforcement by force, while the law's expressive function operates by sending a message. It expresses normative principles and symbolizes societal values. These moralizing features affect behavior.[212] The law's expressive effect publicizes a societal consensus. Where the law publicizes a consensus that a certain behavior is required in order to comply with an abstract internalized norm, the violation of the concrete obligation induces behavioral change by producing guilt.[213]

In the case of genetic discrimination, the law failed to influence the public's risk assessment. The general public apparently did not perceive enough consensus in the partial and inconsistent protection afforded by state laws. Concerned genetic counselors specifically pointed to the narrow scope of available legal protections. [214]

Decision-makers charged with the regulation of new technologies make decisions that can be divided into three categories according to their effects on users' perceptions of risk. The first category includes instances where the law undertakes a clear-cut express restriction on uses of the technology that threaten privacy. The second category includes cases where the law undertakes a hesitant stance that includes inconsistent restrictions on privacy-threatening uses of the technology. In these cases prohibitions are often combined with inaction or even contradictory statements that may be interpreted as a legal endorsement of these privacy-threatening uses.[215] This ambiguous stance produces uncertainty that may inhibit use of the technology. Finally, the law may endorse a blanket clear-cut express legal pronouncement not to restrict certain privacy-threatening uses of the technology.[216]

---

[212] *See* Anderson & Pildes, *supra* note 13, at 1508; McAdams, *supra* note 13, at 398; Steven D. Smith, *Expressivist Jurisprudence and the Depletion of Meaning*, 60 MD. L. REV. 506, 510, 515 (2001).

[213] See McAdams, *supra* note 13, at 400–09.

[214] *See* Hall & Rich, *supra* note 56, at 252–53.

[215] Complex privacy balancing schemes and legal efforts to regulate indirectly, for example, through changing market incentives, also fall under this category.

[216] The collection of personal information on the Internet and employee monitoring case studies evidenced this type of legal reaction. In these cases, the law expressly proclaimed that these uses of the Internet do not constitute a privacy threat. *See supra* Sections III.B–C.

The law regulating genetic discrimination reflects the second approach; the patchwork of state laws and weak federal protections produces a hesitant and contradictory approach. This creates an uncertainty that inhibits the use of genetic testing technology.

Rules in the first category—rules providing clear-cut and express restrictions—are more likely to influence individuals' risk perceptions regarding the use of technologies that are preventive and non-triable. Imposing a legal rule that sends a clearer message and clarifies an emerging norm consensus is important in engaging with potential users' risk assessment.[217] The expressive function of the law has a significant role in regulating technology. The mere exercise of centralized control can allay public fears regarding potential threatening uses of a new technology. Individuals are often afraid of the unknown and, therefore, are put at ease when legal principles are exercised to govern new technologies. People are reassured by the mere existence of limits that the technology is under control.[218] The law's expressive function plays a particularly important role when dealing with preventive technologies. A study on AIDS testing, another preventive technology, stressed the importance of addressing not only the threat itself but also the perception of risk, that is, the attitudes and beliefs about the threat among those who are potential users. It acknowledged that reducing the actual level of risk would not necessarily reduce the perceived risk.[219]

The need to influence the public perception of risk is, therefore, particularly crucial in the case of preventive and non-triable technologies, such as genetic testing. A clear legal message, in lieu of a partial and inconsistent one, would be helpful in alleviating public fears.[220] Specifically, the failure of the current patchwork of state and federal laws in affecting individuals' public fears points to the need for a comprehensive federal statute. The clear message embodied in such a statute would allay public fears and misperceptions that are currently impeding the diffusion of genetic testing technology. [221]

---

[217] *See* Scott, *supra* note 15, at 1925–26.

[218] *See* Moses, *In Vitro Fertilization*, *supra* note 10, at 527–28.

[219] *See* Scott Burris, *Driving the Epidemic Underground? A New Look at Law and the Social Risk of HIV Testing*, 12 AIDS & PUB. POL'Y J. 66 (1997).

[220] Commentators generally advocate that legal regulation is more effective in the form of "gentle nudges" over "hard shoves." *See generally* Kahan, *supra* note 21; Sarah E. Waldeck, *Using Male Circumcision to Understand Social Norms as Multipliers*, 72 U. CIN. L. REV. 455 (2003). Yet, the change advocated here is not targeted at coercing the behavior of those who impose a threat. It does not propose stricter sanctions. It is aimed at those who should feel protected by the laws by sending a clearer message of the social consensus.

[221] Geer et al., *supra* note 88, at 30–31. *See also* Greely, *supra* note 61, at 1500; Hall & Rich, *supra* note 56, at 252–53. Rothstein and Hornung warn that discrimination would take place once more individuals learn that they are at a genetically increased risk of serious illness and purchase additional life insurance. *See* Mark A. Rothstein & Carlton A. Hornung, *Public Attitudes*, *in* GENETICS AND LIFE INSURANCE: MEDICAL UNDERWRITING AND SOCIAL POLICY 1 (Mark A. Rothstein ed., 2004). One

A third distinctive diffusion attribute of genetic testing technology is its centralized diffusion process. The medical profession, particularly genetic counselors, serves as the gatekeepers of the technology. As such, it has enormous influence on the diffusion of the technology.[222] In the case of a similarly centrally diffused medical technology—the technology of artificial insemination in humans—the medical profession was the main force that controlled the social acceptance of the technology. During the 1950s, the medical profession employed tactics that enabled the practice of artificial insemination to expand despite legal pronouncements of the practice as adultery and the child as illegitimate.[223] Consequently, when a technology is centrally diffused, intervention measures should target the group that controls the diffusion process. Intervention measures seeking to dispel a misperception of risk should follow a similar course. Education regarding the scope of legal protection measures and the actual risk should be focused at that group.

Applying this insight to the case of genetic discrimination—genetic professionals are currently playing a major role in spreading fears and concerns regarding genetic discrimination. Their knowledge about the law is limited and their distrust is broad. When questioned about their concerns, genetic counselors repeatedly pointed out the desirability of a federal law to replace the current anxiety-provoking patchwork of state laws.[224] Consequently, intervention efforts should focus on promoting awareness among genetic professionals. These efforts should involve (i) education regarding the relevant laws, in particular should a comprehensive genetic discrimination federal law be enacted; and (ii) dispelling the disinformation regarding current practices of genetic discrimination. Since genetic testing technology is centrally diffused, concentrating resources on the group that controls diffusion is likely to prove particularly effective.

B. *Regulating Critical Mass and Decentralized Technologies*

Technologies that are characterized by a critical mass point (and related network effects) and decentralized diffusion are prone to the second suspect privacy-diffusion relationship where diffusion accelerates despite an extensive privacy threat. A rapidly diffusing technology accompanied

---

should not rule out the possibility that a federal statute's success in resolving the immediate problem of under-utilization of genetic testing technology would prompt insurers to discriminate. However, the existence of a comprehensive federal statute would be effective in resolving the problem of discrimination as well.

[222] For the influence of moderators in the diffusion of new technologies, see Joshua Mark Greenberg, From Betamax to Blockbuster: Mediation in the Consumption Junction (Aug. 2004) (unpublished Ph.D. dissertation, Cornell University) (on file with Connecticut Law Review).

[223] Bernstein, *supra* note 10, at 1079–83.

[224] Hall & Rich, *supra* note 56, at 252–53.

by a transformation of privacy norms is not necessarily problematic. A change in the social structures that affect privacy posits the situation as suspect and warranting increased scrutiny. Yet, whether the disequilibrium should be remedied depends on decision-makers' conception of privacy.[225]

A comprehensive scrutiny of this suspect-diffusion relationship would consist of an evaluation on both the individual and societal level. The individual inquiry would focus on the cost-benefit analysis employed by users. The examination may reveal that individual users determined that the advantages of a technology outweigh the privacy erosion. A subsequent inquiry would then determine the implications of privacy destabilization for society as a whole.

Let us look at the Internet privacy controversies. The Internet transformed existing norms of appropriateness and flow thereby changing the social structures through which we conceive our privacy. At the same time, the diffusion of the Internet accelerated, thereby spreading the privacy threats. This privacy-diffusion relationship is suspect and warrants increased scrutiny. Yet, whether the suspect relationship would be deemed dysfunctional could be resolved by applying the two-tiered approach.

Americans repeatedly assert the importance of privacy. Yet, users' disinclination to use privacy enhancing technologies, such as P3P, suggests a cost-benefit analysis that favors the advantages of easy Internet use over privacy protection.[226] At the same time, it is unclear whether individuals in fact conduct a cost-benefit analysis when dealing with privacy. Individuals may be unaware of the extent of privacy threats occurring.[227] Internet monitoring, whether conducted by commercial companies or employers, is invisible. Even where Internet users are notified that they are monitored, the surveillance's invisibility has two effects. First, individuals are not consciously reminded of the monitoring on a day-by-day basis. Secondly, the extent of monitoring that takes place is unknown. Hence, decision-makers could conclude that the privacy-diffusion relationship is not the product of rational decision-making.

The second inquiry could also point to the existence of a dysfunctional privacy-diffusion relationship, depending on the privacy conception held by decision-makers. Several commentators have pointed out the

---

[225] Helen Nissenbaum suggests that under certain circumstances a value inquiry would be required. *See* Nissenbaum, *supra* note 48, at 146–47.

[226] For additional critiques of P3P, see, Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 71–100; Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy—Control and Fair Information Privacy*, 2000 WIS. L. REV. 743, 754–55.

[227] *See* TRUST AND PRIVACY ONLINE, *supra* note 109, at 25.

significance of privacy as a public value.[228] Priscilla Regan argued that privacy serves public interests, as it is essential for the proper functioning of a democratic system. First, privacy is an important condition for the rights that are essential for a democracy, such as freedom of speech and association and the restraint on the arbitrary power of government. Second, some commonality is necessary to unite a political system. The development of commonality requires privacy because the more people know about each other, the harder it is to develop a commonality. Third, privacy is important to the development of trust in government.[229] In addition, Paul Schwartz argues that Internet privacy is vital for the development of deliberative democracy online.[230] If decision-makers recognize a potential public value for privacy, they are unlikely to dismiss an accelerated diffusion rate accompanied by an increasing privacy threat as a legitimate individual choice.

Where decision-makers view technologies that are characterized by a critical mass point and decentralized diffusion as entrapped in a problematic privacy-diffusion relationship, the timing of the intervention becomes of the essence.[231] Decision-makers generally have two main intervention options: early intervention at the outset of diffusion or the adoption of a wait-and-see approach to evaluate the effects of the technology before regulating.[232]

The early intervention approach carries with it the obvious hazards of regulating the unknown—groping in the dark before informed decisions can be made. Consequently, in many instances the wait-and-see approach would constitute the preferred choice.[233] Under some conditions, however,

---

[228] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1 (2003); Robert Post, *The Social Foundations of Privacy*: *Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).

[229] Regan, *supra* note 39, at 225–27.

[230] *See* Schwartz, *supra* note 47, at 1607.

[231] For an in-depth discussion of the appropriate timing for intervention for purposes of privacy protection, see generally, Bernstein, *supra* note 17.

[232] S*ee generally* ROGER B. DWORKIN, LIMITS: THE ROLE OF THE LAW IN BIOETHICAL DECISION MAKING 169–71 (1996); Stuart Minor Benjamin, *Proactive Legislation and the First Amendment*, 99 MICH. L. REV. 281, 320 (2000); Moses, *In Vitro Fertilization*, *supra* note 10, at 515–17. I should note that a legal pronouncement not to restrict technological uses may be misperceived as a wait-and-see stand. Such pronouncements, however, constitute legal actions that not only affect social norms but also require direct legal action should later legal change be desired.

[233] *See* Hernan Galperin & François Bar, *The Regulation of Interactive Television in the United States and the European Union*, 55 FED. COMM. L.J. 61 (2002) (describing the wait–and-see approach taken by American regulators with regard to interactive television); Mark A. Lemley & Lawrence Lessig, *The End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001) (describing the FCC's wait–and-see approach regarding the regulation of cable Internet access). For commentators supporting the wait–and-see approach, see DWORKIN, *supra* note 232, at 169–70; Benjamin, *supra* note 232. For commentators criticizing the wait-and-see approach, see Matthew Fagin et al., *Beyond Napster: Using Antitrust Law to Advance and Enhance Online Music Distribution*, 8 B.U. J. SCI. & TECH. L. 451 (2002); Moses, *In Vitro Fertilization*, *supra* note 10.

the wait-and-see approach could prove problematic. Stuart Benjamin cautions that in certain circumstances, the costs of waiting can be prohibitive. The costs can be particularly high when the change will be difficult to reverse. He defines these circumstances as instances where there would be irreparable substantial harm and where the harm would not be minor, although it need not be inevitable.[234] Where suspect privacy-diffusion relationships are at stake, the nature of the harm depends on the effects on privacy. But, most importantly, the difficulty of reversibility is related to the diffusion attributes, specifically to the critical mass point and decentralized diffusion qualities.

We have seen that social norms related to the use of technologies that are characterized by a critical mass point and decentralized diffusion process tend to become quickly entrenched. Law and social norms literature demonstrates that a legal rule is less likely to be effective where it departs substantially from the prevailing norm. For example, a compulsory attendance statute that required school attendance until age twenty-one is likely to be ineffective in influencing parental commitment norms.[235] Conversely, the law tends to be more effective in influencing social norms when a new rule is consistent with community expectations.[236] Along these lines, Lawrence Lessig distinguishes between offensive and defensive uses of social meaning.[237] An offensive use of a social meaning construction aims to change existing social meanings, while a defensive use seeks to conserve an existing social meaning that would have otherwise changed.[238] Lessig explains that defensive social meaning construction is more likely to be accomplished than offensive construction. The reason is that instead of having to overcome existing structures of social stigma, the structures of social stigma are already built in.[239]

Recent attempts to regulate social norms in the area of intellectual property underscore these insights. Studies showed that laws criminalizing the misappropriation of various forms of intellectual property are ineffective. Despite prohibitive laws, the unauthorized use of software, taping of music CDs and videotapes continues on a large scale. It appears that people do not conceive this behavior as immoral. The disparity between social norms of morality and the law affects its legitimacy and reduces its effectiveness.[240]

---

[234] *See* Benjamin, *supra* note 232, at 321–31

[235] Scott, *supra* note 15, at 1926–28; Kahan, *supra* note 21, at 608.

[236] Scott, *supra* note 15, at 1926–28.

[237] *See* Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943 (1995).

[238] *Id.* at 986–87.

[239] *Id.* at 999.

[240] *See* Ben Depoorter 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 &

In the case of new technologies, the cost of the lost opportunity to intervene is particularly high because of the additional flexibility available when a new technology first enters society. New technologies, especially those enveloped in a revolutionary aura, tend to enter society with a relatively clean slate. There is a time period in which uses and social norms surrounding the innovation are in flux. However, after a certain point they stabilize and reach a certain closure. From that point onward, change is less likely.[241]

Consequently, express legal prohibitions on uses of a technology that threaten privacy are less effective once social norms are entrenched. Decision-makers considering regulation to restrict uses of technologies that have a critical mass point and decentralized diffusion process would need to particularly heed to the issue of timing. Yet, my goal here is not to promote early intervention across the board. The uncertainties accompanying early intervention suggest that such a course should be pursued infrequently. I suggest however, that where technologies manifest the characteristics of critical mass point and decentralized diffusion decision-makers should include timing as an important factor in their decision-making.[242]

Looking back at the Internet privacy scenarios, we have seen that non-privacy norms became entrenched. In the case of the Internet, the non-privacy norms preceded the critical mass point. While the critical mass point was reached in 1990, non-privacy norms emerged around the mid-1990s. Many academics and policy makers advocated resorting to self-regulation and market resolutions.[243] Yet, with the benefit of hindsight these efforts have failed.[244] Decision-makers have not, to this point, restricted commercial profilers' or employers' ability to use privacy-threatening Internet devices. As discussed, at this point, such measures are likely to be less effective due to the current entrenchment of non-privacy

---

Econ., Working Paper No. 6, 2005), *available at* http://www.law.ugent.be/grond/casle/nudges%20final.pdf; Stuart 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, at 173, 236–38 (2002). *See also* Lior Jacob Strahilevitz, *Charismatic Code, Social Norms and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505 (2003).

[241] *See* WIEBE E. BIJKER, OF BICYCLES, BAKELITES AND BULBS 84–85 (1995).

[242] Others have suggested manipulation of the underlying social norms. *See*, *e.g.*, Depoorter et al., *supra* note 240, at 13–14.

[243] For examples of such proposals, see Steven A. Hetcher, *The Emergence of Website Privacy Norms*, 7 MICH. TELECOMM. & TECH. L. REV. 97, 122 (2001); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1371–72, 1387 (1996); FTC, FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY (2000), http://www.ftc.gov/acoas/papers/acoasfinal1.pdf.

[244] *See* Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, Electronic Privacy Information Center (2005), *available at* http://www.epic.org/reports/decadedisappoint.pdf.

norms.[245] Had decision-makers been aware of the sensitivity of the timing decision due to the critical mass point quality and the decentralized diffusion process, they may have elected a different route. This emphasizes the need to identify the relevant diffusion attributes at an early stage in which the suspect privacy-diffusion relationship can be more effectively resolved.

VI. CONCLUSION

In this Article, I pointed out the importance of expanding the techno-privacy debate beyond its traditional focus on the need and appropriate measures to protect privacy. I demonstrated that tensions stemming from an imbalance between technological diffusion and privacy protection often underlie controversies involving new technologies and privacy. Consequently, I argued for the need to introduce diffusion considerations into legal decision-making.

I examined controversies involving genetic testing, the Internet and the value of privacy through the broader privacy-diffusion prism. The study uncovered two suspect privacy-diffusion relationship models that exhibit a divergence from the general social preference for a balance between privacy and diffusion. The genetic discrimination model evidenced one state of disequilibrium where the privacy threat did not materialize; yet, paradoxically the diffusion of genetic testing technology was inhibited. Conversely, the Internet model presented another form of imbalance where privacy threats increased, yet, Internet diffusion accelerated.

I proceeded to identify the technological characteristics that affected the diffusion process of genetic testing and the Internet and made them susceptible to their respective suspect relationships. I demonstrated that the diffusion characteristics of preventability, non-triability, critical mass point and decentralization made genetic testing and the Internet vulnerable to their respective privacy-diffusion imbalances. Further, I argued that these technological diffusion characteristics are shared by other technologies, and therefore insights derived from these case studies can be applied across technologies.

Finally, I proposed that decision-makers charged with the regulation of new technologies could resolve and even prevent such privacy-diffusion imbalances by incorporating diffusion characteristics into their decision-making process. I suggested that where a technology is preventive and non-triable, the expressive role of the law becomes increasingly important and the formulation of express and clear restrictions would be most effective in influencing individuals' risk perception. Further, I posited that

---

[245] *See* Bernstein, *supra* note 17 (comparing the effectiveness of children Internet privacy regulation and spam regulation).

where a technology is centrally diffused, targeting legal and educational measures at the group that controls the technology's diffusion would be particularly effective. Last, I proposed that where a technology is characterized by a critical mass point and decentralized diffusion process, social norms become quickly entrenched, and therefore timing becomes of the essence. Accordingly, I suggested that in these cases, decision-makers should carefully consider the timing factor in their decision-making process.