Minnesota Journal of Law, Science & Technology

Volume 8 | Issue 2 Article 14

2007

The Role of Diffusion Characteristics in Formulating a General Theory of Law and Technology

Gaia Bernstein

BERNSTEIN G. The Role of Diffusion Characteristics in Formulating a General Theory of Law and Technology. MINN. J.L. SCI. & TECH. 2007;8(2):623-644.

The Role of Diffusion Characteristics in Formulating a General Theory of Law and Technology

Gaia Bernstein*

INTRODUCTION

A general theory of law and technology could provide policy guidelines that improve technology regulators' decision-making. Opponents of such general theory caution that generalizations might prevent the recognition of technological uniqueness, and that the application of broad and indiscriminate principles could impede the identification and appropriate social accommodation of important and novel technologies. To overcome this objection, a general theory of law and technology should provide fine-tuned policy principles that identify the main characteristics differentiating technologies while still providing a common framework that deals with their common attributes.

In this Article, I suggest that the technological characteristics that influence a technology's diffusion—its social adoption process—would provide a constructive foundation for formulating fine-tuned policy guidelines. Policy principles based on the identification of the technological characteristics that influence a technology's diffusion (diffusion characteristics) would not apply narrowly to a specific technology nor would they provide overly broad guidelines relevant to all technologies. Rather, policy guidelines based on diffusion characteristics would be appropriately attuned to both

---

* Associate Professor of Law, Seton Hall University School of Law. This symposium piece was adapted from Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241 (2006).

technological differences and commonalities.

To illustrate my proposal I use case studies of privacy controversies involving two technologies: genetic testing and the Internet. I hope to promote the general theory project by also showing that helpful insights can be derived from the joint study of seemingly very different technologies. The two case studies exhibit paradoxical relationships between privacy protection and technological diffusion. In the case of genetic testing, I focus on genetic discrimination. My analysis of empirical data shows that although genetic discrimination is rare and apparently on the decline, concerns about discrimination preclude individuals from using genetic testing, thereby inhibiting the diffusion of an important new technology. At the same time, my examination of the collection of personal information by commercial entities on the Internet reveals a mirror-image paradox. While use of privacy-threatening devices, such as cookies is on the rise, the increasing privacy threat has not inhibited Internet diffusion.

I suggest that by focusing on diffusion characteristics we could accomplish two goals. First, identification of the diffusion characteristics that made a technology susceptible to the privacy-diffusion paradox could be useful in predicting which technologies are likely to fall prey to a similar paradoxical relationship. Specifically, I argue that genetic testing's preventive and non-triable qualities and the Internet's critical-mass-point quality and decentralized nature made them vulnerable to their respective privacy-diffusion paradoxes.

Second, understanding the role of diffusion characteristics in these controversies could serve to formulate policy guidelines to help resolve both the controversies at issue and future techno-privacy disputes involving similar technologies. I propose that where a technology, like genetic testing, exhibits preventive and non-triable diffusion characteristics, an express and clear-cut privacy protecting law is needed, not necessarily to combat the privacy threat itself, but to alleviate individuals' fears that inhibit them from using the technology. Further, where a technology is centrally diffused, as is genetic testing, efforts to reduce concerns are likely to be most effective when directed at those diffusing the technology, in this case, genetic counselors. I also suggest that when a technology, like the Internet, has a critical mass quality and is decentrally diffused, social norms, in this case non-privacy norms, are quickly entrenched. At that point, both legal and technological measures become less effective. Consequently, in these instances, timing should become an important factor in regulators' decision-making process.

The Article proceeds as follows. Part I presents the two privacy-diffusion paradoxes of genetic discrimination and commercial privacy on the Internet. Part II identifies the diffusion characteristics that made genetic testing and the Internet susceptible to their respective paradoxes. Finally, Part III proposes use of diffusion characteristics as a policy tool to resolve techno-privacy controversies.

I. PRIVACY-DIFFUSION PARADOX MODELS

A. GENETIC DISCRIMINATION

The public is greatly concerned about genetic discrimination by employers and insurers.[1] The media, governmental organizations, and public interest organizations spread genetic discrimination fears.[2] Furthermore, medical professionals, particularly genetic counselors, share these concerns.[3] They play a major role in spreading genetic discrimination fears by warning their patients that genetic testing could result in genetic discrimination.[4] Consequently,

---

1. 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. See VCU CENTER FOR PUBLIC POLICY, VCU LIFE SCIENCES SURVEY: AMERICANS WELCOME SCIENTIFIC ADVANCEMENTS WITH CAUTION (2001), *available at* http://www.vcu.edu/lifesci/images2/survey2001.pdf.

2. *See* COUNCIL FOR RESPONSIBLE GENETICS, GENETIC DISCRIMINATION: POSITION PAPER 1 (2001), *available at* http://www.gene-watch.org/educational/genetic_discrimination.pdf (warning that "an increasing number of healthy individuals have suffered discrimination on the basis of predictive genetic information"); Press Release, Nat'l Human Genome Research Inst., Health Insurance in the Age of Genetics (July 1997), *available at* http://www.genome.gov/10000879 (underscoring data regarding genetic discrimination); Geoffrey Cowley et al., *Flunk the Gene Test and Lose Your Insurance*, NEWSWEEK, Dec. 23, 1996, at 48; GATTACA (Sony Pictures 1997) (depicting a future society of rigid genetic hierarchy). For a description of genetic discrimination concerns, see LORI ANDREWS & DOROTHY NELKIN, BODY BAZAAR: THE MARKET FOR HUMAN TISSUE IN THE BIOTECHNOLOGY AGE 82–101 (2001).

3. *See* Mark A. Hall & Stephen S. Rich, *Laws Restricting Health Insurers' Use of Genetic Information: Impact on Genetic Discrimination*, 66 AM. J. HUM. GENETICS 293, 295-96 (2000).

4. *See* 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, 247-48 (2000).

for many individuals, genetic testing has become synonymous with genetic discrimination.

Nevertheless, a survey I conducted of empirical research on genetic discrimination by insurers and employers revealed that, in fact, genetic discrimination is rare and that despite the growth in the number of available tests, it is on the decline.[5]

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. 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, particularly among pre-symptomatic adults who could test for adult onset diseases.[6]

The current legal regime provides only partial and inconsistent protection from genetic discrimination.[7] It has not played an important part in preventing genetic discrimination.[8] But, more importantly, it 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

5. Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 243, 257-266 (2006).

6. *See, e.g.*, Katherine P. Geer et al., *Factors Influencing Patients' Decisions to Decline Cancer Genetic Counseling Services*, 10 J. GENETIC COUNSELING 25, 30–31 (2001). For a discussion of the relevant literature, see Bernstein, *supra* note 5, at 263-64. Adult onset diseases are genetic diseases that may develop later in life, such as breast cancer, Alzheimer's disease or Huntington's disease.

7. On the federal level, the Health Insurance Portability and Accountability Act and the Americans with Disabilities Act (ADA) provide only partial protection. *See* Health Insurance and Portability Act of 1996, 29 U.S.C. § 1182 (2000); American with Disabilities Act of 1990, 42 U.S.C. §§ 12101–12213 (2000); *see also* 3 EEOC COMPLIANCE MANUAL § 902 (1995); Edward J. Larson, *The Meaning of Human Gene Testing for Disability Rights*, 70 U. CIN. L. REV. 913, 927–28 (2002). On the state level, genetic discrimination protection is comprised of a confusing patchwork of state laws offering inconsistent and partial protection. *See* Paul Steven Miller, *Is There a Pink Slip in My Genes? Genetic Discrimination in the Workplace*, 3 J. HEALTH CARE L. & POL'Y 225, 259–63 (2000); Nat'l Human Genome Research Inst., Genetic Discrimination in Health Insurance, http://www.genome.gov/10002328 (last reviewed Nov. 2006). 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).

8. Hall & Rich, *supra* note 3, at 297, 300-1, 304.

BERNSTEIN G. The Role of Diffusion Characteristics in Formulating a General Theory of Law and Technology. MINN. J.L. SCI. & TECH. 2007;8(2):623-644.

of genetic discrimination laws.[9]

Hence, the findings point 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 regarding the status of privacy protection. Consequently, the law has not been a major factor in inhibiting genetic discrimination, nor has it been successful in alleviating individuals' genetic discrimination concerns, thus failing to facilitate broader adoption of the technology.

B. INTERNET PRIVACY

With the advent of the Internet to popular use, web sites and commercial-profiling companies began collecting personal information, through use of cookies, spyware, and the less well-known web bugs. Their goal was to target advertising at Internet users and sometimes to transform Internet sites to match a visitor's interests and financial ability.[10]

Commercial collection of personal information on the Internet reached public awareness in 1999–2000.[11] Yet, despite mounting public pressure, courts have not found commercial profiling through use of cookies as compromising individuals' privacy.[12] Further, legislative responses focused only on spyware and the settlements reached between government agencies and collectors of personal information on

---

9. Hall & Rich, *supra* note 4, at 253.

10. *See* CTR. FOR DEMOCRACY & TECH., GHOSTS IN OUR MACHINES: BACKGROUND AND POLICY PROPOSALS ON THE "SPYWARE" PROBLEM 2 (2003); Microsoft, Understanding Cookies, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx (last visited Mar. 28, 2007).

11. *See, e.g.*, *Amid Protests, DoubleClick and Abacus Announce Plans for $1 Billion Merger*, ELECTRONIC ADVERTISING & MARKETPLACE REP., June 29, 1999 (describing concerns that a merger of an online marketing firm with a consumer data tracking information firm would threaten online privacy); Joseph Gallivan, *Privacy Group Calls for DoubleClick Nix*, N.Y. POST, June 22, 1999, at 39. 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).

12. *See* In re Toys R Us, Inc., Privacy Litig., No. M-00-1381, 2001 U.S. Dist. LEXIS 16947, at *18, *27 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A., Inc., 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001); In re DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y 2001).

the Internet failed to provide a comprehensive solution.[13] Consequently, the law, in effect, produced a legal pronouncement permitting collection of personal information on the Internet.

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.[14]

Unsurprisingly, the findings of a survey I have conducted of empirical data measuring the use of privacy-threatening Internet technologies revealed that the practice of collecting personal information and commercial profiling is booming.[15] At the same time, it appears that concerns about the privacy threat posed by the Internet have not made any evident impact on the diffusion of the technology. In the period between 2000-2003, when users became increasingly aware of the threat to their Internet privacy, the U.S. online population expanded

---

13. *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 S6; JOSEPH TUROW, ANNENBERG PUB. POL'Y CTR., 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. An agreement between the Attorneys' General of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick, Inc. provides an example of states' response to problems with the collection of personal information. *See* Agreement between the Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington, and Doubleclick Inc., In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (No. 00 Civ 0641 NRB), *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a_02_attach.pdf; Press Release, Office of the N.Y. State Attorney Gen., Major Online Advertisers Agrees to Privacy Standards for Online Tracking: Company to Increase Visibility and Verify Data Collection Practices (Aug. 26, 2002), *available at* http://www.oag.state.ny.us/press/2002/aug/aug26a_02.html; For legislation and case law restricting use of spyware see CAL. BUS. & PROF. CODE § 22947 (West 2007); UTAH CODE ANN. § 13-40-102 (West 2005); Washingtonpost.Newsweek Interactive Co., LLC., et al., v. The Gator Corp., No. Civ.A.02-909-A, 2002 WL 31356645, at *1 (E.D. Va. July 16, 2002). In addition, many states and the federal government have new spyware bills. *See* Securely Protect Yourself against Cyber Trespass Act, H.R. REP. NO. 109-32 (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).

14. Bernstein, *supra* note 5, at 268-70.

15. *Id.* at 270-2.

BERNSTEIN G. The Role of Diffusion Characteristics in Formulating a General Theory of Law and Technology. MINN. J.L. SCI. & TECH. 2007;8(2):623-644.

from eighty-six million in 2000, to one hundred and twenty-six million in 2003.[16]

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.

II. USE OF DIFFUSION CHARACTERISTICS TO IDENTIFY TECHNOLOGICAL SUSCEPTIBILITY

Understanding the characteristics that made genetic testing and the Internet susceptible to these privacy-diffusion relationships is a first step toward resolving the privacy paradoxes of genetic discrimination and the Internet. Furthermore, technologies are often not as unique as they appear at first blush. Identifying the technological characteristics that created the genetic testing and Internet privacy-diffusion 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 Part, I identify two diffusion characteristics that made genetic testing susceptible to its problematic diffusion-privacy relationship: (i) its preventive nature and (ii) its non-triable quality. I also point to two different diffusion characteristics that made Internet technology vulnerable to its respective privacy-diffusion relationship: (i) its critical mass quality and (ii) its decentralized nature.[17]

---

16. *See* MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, AMERICAS' ONLINE PURSUITS: THE CHANGING PICTURE OF WHO'S ONLINE AND WHAT THEY DO ii (2003), *available at* http://www.pewinternet.org/pdfs/PIP_Online_Pursuits_Final.PDF.

17. 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, Gaia Bernstein, *When New Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 VILL. L. REV. 921 (2006). Second, the sensitivity of

A. 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.[18] 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.[19]

Genetic testing is also a preventive technology.[20] 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.[21] Even if the individual will eventually develop the disease, this could take place well into the future.

---

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 research 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* CA. HEALTHCARE FOUND. 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 & AM. LIFE PROJECT, HEALTH INFORMATION ONLINE ii, 3, (2005), *available at* http://www.pew internet.org/pdfs/PIP_Healthtopics_May05.pdf.

18. EVERETT M. ROGERS, DIFFUSION OF INNOVATIONS 234-36 (5th ed. 2003).

19. *Id.* at 233.

20. For a study focusing on the effects of the preventive nature of genetic testing technology, see generally Katrina Armstrong et al., *Early Adoption of BRCA1/2 Testing: Who and Why*, 5 GENETICS IN MED. 92, 96 (2003).

21. 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 Apr. 28, 2007).

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.[22] Preventive technologies have a lower adoption rate because of their weaker relative advantage. Relative advantage is one of the most important predictors of a technology's adoption.[23] Relative advantage 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.[24] Preventive innovations do not provide an immediate reward, but instead 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 paradox, 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.

B. 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.[25] 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.[26] Consequently, new ideas that can be divided for

22. ROGERS, *supra* note 18, at 233–35.

23. *Id* at 233.

24. *Id*. at 232–34.

25. *Id*. at 258 (while Rogers refers to the concept as "trialability" I prefer to use the similar term "triability").

26. *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).

trial are generally adopted faster.[27]

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, their genetic carrier status is created and can affect self-conceptions or be abused by third-parties.[28] Furthermore, unlike other types of personal information, the created genetic information is immutable.[29] 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.[30] Genetic testing, due to its slow diffusion rate, is still in the early-adopter stage.[31] 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.[32] Consequently, users of 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

27. ROGERS, *supra* note 18, at 258.

28. Armstrong et al., *supra* note 20, at 95-97. 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).

29. While an individual may be able to change her credit rating she will never be able to change her genetic information.

30. ROGERS, *supra* note 18, at 282–85.

31. *See* Michael Hall & Olunfunmilayo I. Olopade, *Confronting Genetic Testing Disparities: Knowledge Is Power*, 293 J. AM. MED. ASS'N 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).

32. ROGERS, *supra* note 18, at 258.

rate.[33] 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 be tested, fears that by the act of taking the test she may expose herself to the full consequences of genetic discrimination.

Second, 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.[34] 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.[35] 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.

It appears that 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.

C. INTERNET TECHNOLOGY: A CRITICAL MASS POINT TECHNOLOGY

Network effects exist where the value of the good is

---

33. *See id.*

34. 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).

35. Karahanna et al., *supra* note 26

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 instance, the telephone became more desirable once it became more widespread and there were additional people to call.[36] Network effects become prominent as a critical mass of people starts using a technology.[37]

Once the critical mass point is reached, the rate of adoption accelerates.[38] Thus, when a technology reaches the critical mass point, social norms regarding its use become quickly entrenched.[39] 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.[40]

36. *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); M. Lynne Markus, *Toward a "Critical Mass" Theory of Interactive Media*, *in* ORGANIZATIONS AND COMMUNICATION TECHNOLOGY 194 (Janet Fulk & Charles Steinfield eds., 1990).

37. 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 ECONOMIDES & CHARLES HIMMELBERG, CRITICAL MASS AND NETWORK SIZE WITH APPLICATION TO THE US FAX MARKET 1 (Stern School of Business, N.Y. Univ., Discussion Paper No. EC-95-11, 1995), *available at* http://raven.stern.nyu.edu/networks/95-11.pdf.

38. ROGERS, *supra* note 18, 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.*

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

40. 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 18, at 353. 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).

Internet technology is considered a network effects technology. The desirability of the Internet is dependent on the number of people who use it.[41] 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.[42] In 1990, about 4 million users used the Internet worldwide, while by 2002, that number had grown to 544 million users worldwide.[43] 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 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 problematic privacy-diffusion relationship, where diffusion accelerated despite extensive privacy threats.

D. 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.[44] For example, genetic testing is a centrally diffused innovation—the medical profession, primarily genetic counselors who administer the tests, control its diffusion.

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. Further, diffusion is accompanied by a

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

42. 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).

43. ROGERS, *supra* note 18, at 343-47.

44. *Id.* at 394–98.

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.[45]

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.[46] 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 problematic privacy-diffusion relationship.[47]

III. DIFFUSION CHARACTERISTICS AS A POLICY TOOL

The two privacy-diffusion paradoxes exhibit a divergence from the general preference for a balance between diffusion and privacy protection. 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.[48]

In this Part, I assess potential resolutions to the genetic discrimination and Internet privacy-diffusion relationships. My objective goes beyond proposing specific resolutions. Decision-makers dealing with the regulation of new

---

45. *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).

46. *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).

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

48. Bernstein, *supra* note 5, at 251-53.

technologies often assess each new technology in isolation. Yet, there are definite patterns in the co-evolution of technology and society that 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.[49] 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 privacy-diffusion relationships may also be entrapped in these relationships. Policy solutions based on 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 would be refined with further study of additional technologies.

A. REGULATING PREVENTIVE NON-TRIABLE AND CENTRALIZED TECHNOLOGIES

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

---

49. *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).

while the law's expressive function operates by sending a message. It expresses normative principles and symbolizes societal values. These moralizing features affect behavior.[50] 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.[51]

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 legal protection. Concerned genetic counselors specifically pointed to the narrow scope of available legal protections.[52]

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.[53] This ambiguous stance produces uncertainty that may inhibit use of the technology. Finally, the third category includes cases where the law may endorse a blanket clear-cut express legal pronouncement not to restrict certain privacy-threatening uses of the technology.[54]

The law regulating genetic discrimination reflects the

---

50. *See* Elizabeth S. Anderson & Richard H. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503, 1508 (2000); Richard H. McAdams, *The Origin, Development and Regulation of Norms*, 96 MICH. L. REV. 338, 398 (1997); Steven D. Smith, *Expressivist Jurisprudence and the Depletion of Meaning*, 60 MD. L. REV. 506, 510, 515 (2001).

51. *See* McAdams, *supra* note 50, at 400–09.

52. *See* Hall & Rich, *supra* note 4, at 252–53.

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

54. The collection of personal information on the Internet evidenced this type of legal reaction. In this case, the law expressly proclaimed that this use of the Internet does not constitute a privacy threat.

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—those 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.[55] The expressive function of the law plays 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.[56]

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.[57]

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 help to alleviate public fears.[58] Specifically, the failure of the current

---

55. *See* Elizabeth S. Scott, *Social Norms and the Legal Regulation of Marriage*, 86 VA. L. REV. 1901, 1925-26 (2000).

56. *See* Lyria Bennett Moses, *Understanding Legal Responses to Technological Change: The Example of In Vitro Fertilization*, 6 MINN. J. L. SCI. & TECH. 505, 527-28 (2005).

57. *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).

58. Commentators generally advocate that legal regulation is more effective in the form of "gentle nudges" over "hard shoves." *See generally* Dan M. Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. CHI. L. REV. 607 (2000); 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

patchwork of state and federal laws to allay individuals' public fears points to the need for a comprehensive federal statute. The clear message embodied in such a statute would alleviate public fears and misperceptions that are currently impeding the diffusion of genetic testing technology. [59]

A third distinctive diffusion attribute of genetic testing technology is its centralized diffusion process. The medical profession, particularly genetic counselors, serves as the gatekeeper of the technology. It has enormous influence on the diffusion of the technology.[60] 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.

This insight can be applied to the case of genetic discrimination. Genetic professionals currently play 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 to the desirability of a federal law to replace the current anxiety-provoking patchwork of state laws.[61] Consequently, intervention efforts should focus on promoting awareness among genetic professionals. These efforts should involve: (i) education regarding the relevant

---

those who should feel protected by the laws by sending a clearer message of the social consensus.

59. *See* Geer et al., *supra* note 6, at 30–31. *See also* Henry T. Greely, *Genotype Discrimination*: *The Complex Case for Some Legislative Protection*, 149 U. PA. L. REV. 1483 (2001); Hall & Rich, *supra* note 4, 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 generally* 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 should not rule out the possibility that a federal statute's success in resolving the immediate problem of under-utilization of genetic testing technology might prompt insurers to discriminate. However, the existence of a comprehensive federal statute would be effective in resolving the problem of discrimination as well.

60. 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).

61. Hall & Rich, *supra* note 4, at 252–53.

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 paradox where diffusion accelerates despite an extensive privacy threat.

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 is of the essence.[62] 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.[63]

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 is the preferred choice.[64]

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

63. 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, *supra* note 56, at 515-17. 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.

64. *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 of 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 63, at 169–70. *See generally* Benjamin, *supra* note 63. For commentators criticizing the wait-and-see approach, see generally 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, *supra* note 56.

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.[65] The law tends to be more effective in influencing social norms when a new rule is consistent with community expectations.[66]

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 and 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 the law's legitimacy and reduces its effectiveness.[67]

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. An initial time period exists 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.[68]

Consequently, express legal prohibitions on uses of a technology that threaten privacy are less effective once social

---

65. Kahan, *supra* note 58, at 608; Scott, *supra* note 55, at 1926–28.

66. Scott, *supra* note 55, at 1926–28.

67. *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 & Econ., Working Paper No. 6, June 2005), *available at* http://ssrn.com/abstract=740184; Stuart P. Green, *Plagiarism, Norms and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights*, 54 HASTINGS L.J. 167, 173, 236-38 (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).

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

norms are entrenched. Decision-makers considering regulation to restrict uses of technologies that have a critical mass point and decentralized diffusion process need to particularly focus on the issue of timing. Yet, early intervention should not be promoted 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.[69]

Non-privacy norms became entrenched, in the case of the Internet, after 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.[70] Yet, with the benefit of hindsight these efforts have failed.[71] Decision-makers have not, to this point, restricted commercial profilers' or employers' ability to use privacy-threatening Internet devices. As discussed, such measures are likely to be less effective now due to the current entrenchment of non-privacy norms.[72] 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 earlier stage when the problematic privacy-diffusion relationship can be more effectively resolved.

IV. CONCLUSION

In this Article, I have used two techno-privacy controversies to show that diffusion characteristics could be

---

69. Others have suggested manipulation of the underlying social norms. *See, e.g.*, Depoorter et al., *supra* note 67, at 13–14.

70. 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); FED. TRADE COMM'N, FINAL REPORT OF THE FEDERAL TRADE. COMMISSION ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY (2000), *available at* http://www.ftc.gov/acoas/papers/acoasfinal1.pdf.

71. *See* CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY SELF REGULATION: A DECADE OF DISAPPOINTMENT (2005), *available at* http://www.epic.org/reports/decadedisappoint.pdf.

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

BERNSTEIN G. The Role of Diffusion Characteristics in Formulating a General Theory of Law and Technology. MINN. J.L. SCI. & TECH. 2007;8(2):623-644.

useful as a policy tool in the resolution and potential prevention of future controversies involving technologies that share the same diffusion characteristics. This Article is based on limited case studies and, therefore, can offer only an initial formulation for the use of diffusion characteristics. My hope is that I have demonstrated that a middle-ground exists between treating each technology as unique and therefore deserving special treatment and the formulation of overly broad principles that bluntly erode the very novelty we want to promote.