

Resilience: Building Better Users and Fair Trade Practices in Information

Andrea M. Matwyshyn*

I.	WHAT IS RESILIENCE?	392
A.	<i>Building Resilience in Systems: The Software Ecosystem</i>	393
B.	<i>Building Resilience in Users</i>	397
II.	RESILIENCE, CONTRACTS, AND FAIR TRADE PRACTICES IN INFORMATION.....	401
A.	<i>Resilience and Contracts in Technology-Mediated Spaces</i>	402
B.	<i>Fair Trade Practices, Privacy, and Technology Contracts</i>	404
1.	Experience in Digital Contract: Creating a Plain English “Information License and Security Agreement”	405
2.	Emotion in Digital Contract: Creating a Sense of Transparency in Formation with Summary Labeling.....	407
3.	Modeling: Imposing Digital Reasonableness Standards.....	407
4.	Feedback Loops in Digital Contract: Offering a Live Human to Negotiate and Explain Terms.....	408
III.	CONCLUSION	409

* Andrea M. Matwyshyn is an assistant professor of Legal Studies and Business Ethics at the Wharton School at the University of Pennsylvania; more information about her work is available at <http://www.amatwyshyn.com>. She thanks Marcia Tiersky for comments on this work and can be reached at amatwysh@wharton.upenn.edu.

A long-running joke about the law asserts that that the practice of law would be more pleasant if it weren't for all those pesky clients. In the world of technology, a more terse version of this same sentiment exists: PEBKAC—Problem Exists Between Keyboard and Chair. Technologists often long for “better” users of their products. Naturally, the logical reaction to this type of statement is to encourage developers of products to engage in better usability testing of their products on actual consumers. However, a deeper question may lurk beneath the superficial flippancy of PEBKAC. Is there in fact a way that we can “build better users?” This Article argues that there is. Despite a long running discourse regarding the resilience of infrastructure and networks themselves, a portion of the discussion that has been neglected relates to human resilience—buttressing the resilience of *users* of technology and the role of law in furthering this goal. Borrowing lessons from developmental psychology and securities regulation, this Article expands the concept of resilience into the software and digital contracting ecosystem. It argues that technology law and policy can be tooled in part to adopt an explicit focus on building users' resilience and sense of self-efficacy, particularly in connection with data privacy and information security. Technology law and policy can help to train consumers to be confident users and bounce back from technology problems. With the assistance of strengthened fair trade practices in privacy, contract law offers one avenue for explicit trust-reinforcing mechanisms to assist consumers in becoming more resilient users.

I. WHAT IS RESILIENCE?

Many of us have found ourselves in a situation where we did not understand how a piece of software worked behind the scenes on our machines. We wondered what exactly we had agreed to when we clicked “yes” on the user agreement, whether we could really trust the code, and whether we understood the extent to which data would be collected about us. For some of us, a mild panic followed. Yet, in these moments of privacy “freakout,” we had no one to ask. Reading a privacy policy—to the extent we understood it—likely yielded only more questions. We found ourselves cursing the software product as “creepy” privacy-invasive code. Meanwhile, the technologists who write software frequently feel equally frustrated by the way we, the consumer base that uses their products, interact with these products. In other words, a perception gap exists between the way that builders of technology tools perceive their products and the way that average consumers perceive these same products. The reason for this disconnect can be understood as a deficit of what developmental psychologists might call resilience. This resilience, or ability to recover and flourish in the face of obstacles, is frequently absent on both sides of the software equation—both in the code writing process

itself and in consumers' ability to overcome technology obstacles when using products.

A. *Building Resilience in Systems: The Software Ecosystem*

The concept of resilience has long been prevalent in systems literature. When applied to technological, human, and ecological systems, resilience refers to the ability of the system to restore and maintain itself in a functional state, providing all services, despite disruptive changes to the system.¹ As such, the concept of resilience springs from complexity theory and its focus on dynamic, emergent change and system evolution in response.² “The challenge [to a resilient system] . . . is to conserve the ability to adapt to change, to be able to respond in a flexible way to uncertainty and surprises” and “to identify the properties and processes that shape the future.”³ By definition, resilience involves the ability of a system to evolve in advance of and in response to known vulnerabilities to avoid or minimize their impact. However, this enterprise of anticipation is always limited by human knowledge and other factors.⁴

Resilient systems have been identified to possess three distinct types of properties or processes. First, the system is built with an eye to the future and possesses redundancy, which allows for bouncing back from destabilizing events to come.⁵ In other words, they possess the ability to change. Second, the system demonstrates a shifting balance between stable and unstable forces, with internal controls intended to counterbalance external variability.⁶ This means that the system is still capable of performing when an external force pushes on it. Third, the system demonstrates a dynamic, changing nature that compensates for vulnerability and persists.⁷ In other words, the system possesses the ability to self-correct and return to a normal state.

The concept of resilience has been applied in legal literature to

1. See C. S. Holling & Lance H. Gunderson, *Resilience and Adaptive Cycles*, in PANARCHY: UNDERSTANDING TRANSFORMATIONS IN HUMAN AND NATURAL SYSTEMS 25, 28 (Lance H. Gunderson & C. S. Holling eds., 2002).

2. See, e.g., Barbara A. Cherry, *Institutional Governance for Essential Industries Under Complexity: Providing Resilience Within the Rule of Law*, 17 COMMLAW CONSPECTUS 1, 4–5 (2009). Resilience can be “measured by the magnitude of disturbance that can be absorbed before the system changes its structure by changing the variables and processes that control behavior.” Holling & Gunderson, *supra* note 1, at 28.

3. Holling & Gunderson, *supra* note 1, at 32.

4. See generally ROBERT ROSEN, *LIFE ITSELF: A COMPREHENSIVE INQUIRY INTO THE NATURE, ORIGIN, AND FABRICATION OF LIFE* 67–107 (T.F.H. Allen & David W. Roberts eds., 1991).

5. See Holling & Gunderson, *supra* note 1, at 32–33.

6. *Id.*

7. *Id.*

various types of connected systems, including the environmental ecosystem,⁸ tribal sovereignty,⁹ agencies and social trust,¹⁰ human communities¹¹ (such as families¹²), social decay,¹³ disasters,¹⁴ markets and financial systems,¹⁵ technology,¹⁶ and critical infrastructure¹⁷ (such as electrical grids¹⁸ and internet infrastructure¹⁹). This idea of resilience analysis of the software development lifecycle and ecosystem, however, presents a newer undertaking, and one to date almost entirely unexplored in the legal literature.²⁰ The software ecosystem, including the processes of

8. As applied to ecological systems, “[r]esilience is the capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity, and feedbacks.” Brian Walker et al., *Resilience, Adaptability and Transformability in Social-Ecological Systems*, *ECOLOGY & SOC’Y*, Dec. 2004, at 2.

9. See, e.g., Patrice H. Kunesh, *Constant Governments: Tribal Resilience and Regeneration in Changing Times*, 19 *KAN. J.L. & PUB. POL’Y* 8 (2009).

10. See, e.g., Rebecca M. Bratspies, *Regulatory Trust*, 51 *ARIZ. L. REV.* 575 (2009).

11. See, e.g., Barbara Cosens, *Transboundary River Governance in the Face of Uncertainty: Resilience Theory and the Columbia River Treaty*, 30 *J. LAND RESOURCES & ENVTL. L.* 229 (2010). When applied to social systems, resilience is the “ability of human communities to withstand and recover from stresses.” *Id.* at 237 (citing *Resilience Dictionary*, STOCKHOLM RESILIENCE CENTRE, <http://www.stockholmresilience.org/research/whatisresilience/resiliencedictionary.4.aeea46911a3127427980004355.html> (last visited Feb. 22, 2011)).

12. A dichotomy exists between the resilience-building and resilience-reducing potential of particular ecologies, such as families. Families can either assist in coping with change or hamper a child’s ability to adapt. See, e.g., Alastair Ager, *What Is Family? The Nature and Functions of Families in Times of Conflict*, in *A WORLD TURNED UPSIDE DOWN: SOCIAL ECOLOGICAL APPROACHES TO CHILDREN IN WAR ZONES* 39 (Neil Boothby et al. eds., 2006).

13. See, e.g., Lawrence J. Vale & Thomas J. Campanella, *The Cities Rise Again*, in *THE RESILIENT CITY: HOW MODERN CITIES RECOVER FROM DISASTER* 3, 7 (Lawrence J. Vale & Thomas J. Campanella eds., 2005) (differentiating between “protracted socioeconomic decay” and disasters and noting that it is often more difficult for cities to respond with resilience to the former).

14. See, e.g., W. Neil Adger et al., *Social-Ecological Resilience to Coastal Disasters*, 309 *SCI.* 1036 (2005).

15. See, e.g., Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 68 *Fed. Reg.* 17,809 (Apr. 11, 2003), available at <http://www.sec.gov/news/studies/34-47638.htm>.

16. See, e.g., Elizabeth Burleson, *Climate Change Consensus: Emerging International Law*, 34 *WM. & MARY ENVTL. L. & POL’Y REV.* 543, 584 (2010).

17. See, e.g., Bennie G. Thompson, *A Legislative Prescription for Confronting 21st-Century Risks to the Homeland*, 47 *HARV. J. ON LEGIS.* 277, 298 (2010).

18. See, e.g., Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 *VAND. J. TRANSNAT’L L.* 57 (2010).

19. See, e.g., Gregory S. McNeal, *Cyber Embargo: Countering the Internet Jihad*, 39 *CASE W. RES. J. INT’L L.* 789, 802 (2007).

20. Although legal literature hasn’t explored resiliency analysis, computer science has. These basic tenets are: protection from disclosure (confidentiality); protection from alteration (integrity); protection from destruction (availability); who is making the request

software development, deployment, and repair, should be viewed as another type of system that warrants a resilience analysis. Why? The reason for this extension is the avoidability of much consumer harm, particularly with respect to privacy and information security concerns. A significant portion of consumer complaints arise because particular digital products cannot withstand the entirely foreseeable wear and tear of consumer use and foreseeable third party attacks.

What users perceive to be unacceptable, privacy-invasive code frequently surprises even sophisticated companies. However, with adequate resiliency analysis beforehand, most consumer privacy and information security freakouts are entirely avoidable. Two recent examples of this underestimation of consumer reactions involve Google and Facebook. In early 2010, Google launched a product called Buzz.²¹ By external appearances, Buzz seemed to be a type of crossover product between a Facebook-like interface and a Twitter feed. To assist in its adoption, Google decided to repurpose the data in users' Gmail e-mail account contact lists for their individual starter group of "followers" in Buzz, making these lists public by default.²² Almost immediately, public outcry ensued.²³ Gmail address books for some users contained contact information for individuals who were unwelcome "followers."²⁴ In its zealotry to promote Buzz, Google had, according to press accounts, cut short its usual beta testing process and unintentionally triggered the "privacy invasion" sensitivity of some of its users.²⁵ This product shipping decision was subsequently labeled by a Federal Trade Commission (FTC)

(authentication); what rights and privileges the requestor has (authorization); the ability to build historical evidence (auditing); and the management of configuration, sessions, and exceptions. See, e.g., OFFICIAL (ISC)² GUIDE TO THE CISSP CBK (Harold F. Tipton & Kevin Henry eds., 2007); Kristin R. Eschenfelder & Anuj C. Desai, *Software as Protest: The Unexpected Resiliency of U.S.-Based DeCSS Posting and Linking*, 20 INFO. SOC'Y 101 (2004) (demonstrating the proliferation of U.S.-based websites either posting or linking to the DeCSS program over the course of *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001)).

21. *Google Buzz—What Is the Purpose?*, CLEAN CUT MEDIA (Feb. 16, 2010), <http://www.cleancutmedia.com/internet/google-buzz-what-is-the-purpose>; GOOGLE BUZZ, www.google.com/buzz (last visited Feb. 22, 2011).

22. Jonathan Fildes, *Google Admits Buzz Social Network Testing Flaws*, BBC NEWS, <http://news.bbc.co.uk/2/hi/technology/8517613.stm> (last visited Feb. 22, 2011).

23. See *id.*

24. In one case, an abusive ex-husband was added as a follower to one woman's Buzz feed, much to her dismay. Nick Saint, *Outraged Blogger Is Automatically Being Followed by Her Abusive Ex-Husband on Google Buzz*, BUS. INSIDER (Feb. 12, 2010), <http://www.businessinsider.com/outraged-blogger-is-automatically-being-followed-by-her-abusive-ex-husband-on-google-buzz-2010-2>.

25. Jonathan Fildes, *Google Admits Buzz Social Network Testing Flaws*, BBC NEWS (Feb. 16, 2010), <http://news.bbc.co.uk/2/hi/technology/8517613.stm>.

member as “irresponsible conduct”²⁶ and at least eleven U.S. lawmakers called for an FTC investigation.²⁷ Along similar lines, Facebook found itself in court because of its Beacon program,²⁸ which collected data regarding user behaviors on “partner” websites.²⁹ The Beacon program involved embedded code in partner sites that triggered a post regarding consumer conduct on those partner sites to be posted to some consumers’ Facebook feeds.³⁰ Because some users did not understand how this information was being shared, and they considered the practice an invasion of their privacy.³¹ This confusion resulted in what the media has termed a “public relations disaster”³² and in a class action lawsuit against Facebook that resulted in a settlement in the amount of \$9.5 million.³³

Both companies in question were surprised by the consumer reaction. However, in both cases this surprise was likely avoidable. More extensive usability testing on average consumers likely would have revealed the code’s lack of resilience when embedded into the broader software ecosystem.

That said, the lack of resilience of the developers’ code in the two cases above was only part of the problem. It was undoubtedly exacerbated by some users’ lack of individual resilience. Some consumers poorly adjust to new technology and experience potent emotions of stress and confusion with respect to even small changes in existing software. To understand this parallel consumer resilience side of this dynamic, we now turn to developmental psychology.

26. Emily Steel, *Google Buzz Exemplifies Privacy Problems, FTC Commissioner Says*, WALL ST. J. BLOGS (Mar. 17, 2010, 2:37 PM), <http://blogs.wsj.com/digits/2010/03/17/google-buzz-exemplifies-privacy-problems-ftc-commissioner-says/>.

27. Grant Gross, *Lawmakers Ask for FTC Investigation of Google Buzz*, PCWORLD.COM (Mar. 29, 2010), http://www.pcworld.com/article/192801/lawmakers_ask_for_ftc_investigation_of_google_buzz.html?tk=rss_news.

28. *Lane v. Facebook, Inc.*, No. C 08-3845 RS, 2009 WL 3458198 (N.D. Cal. Oct. 23, 2009).

29. Juan Carlos Perez, *Facebook’s Beacon More Intrusive than Previously Thought*, PCWORLD.COM (Nov. 30, 2007), http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html.

30. See Om Malik, *Is Facebook Beacon a Privacy Nightmare?*, GIGAOM (Nov. 6, 2007), <http://gigaom.com/2007/11/06/facebook-beacon-privacy-issues/>. For a discussion of the public relations problems for Facebook caused by the “Beacon” technology, see Perez, *supra* note 29.

31. See, e.g., Gil Kaufman, *Facebook Bows to User Complaints About Beacon’s Privacy Violation*, MTV.COM (Nov. 30, 2007), <http://www.mtv.com/news/articles/1575455/facebook-bows-user-complaints.jhtml>.

32. Caroline McCarthy, *Facebook Notifies Members About Beacon Settlement*, CNET NEWS (Dec. 3, 2009), http://news.cnet.com/8301-13577_3-10409034-36.html.

33. *Id.*

B. *Building Resilience in Users*

In developmental psychology literature, resilience of humans refers to the process through which a person is exposed to adversity and manages to adapt and function successfully despite setbacks.³⁴ Many factors contribute to the development of resilience, and the process is inherently socially embedded. This means that the resilience of the community and other contexts that the individual experiences can either assist or diminish resilience in the individual. Further, resilience can be learned,³⁵ and individuals functioning under conditions of stress can indeed rise to the occasion, overcoming challenges and succeeding.³⁶ Although methodological variation exists, generally resilience studies look for “risk” factors³⁷ and mitigating “protective” factors that assist with overcoming stressors.³⁸ In particular, the extent to which individuals participate in decision making tends to correlate positively with improved resilience.³⁹ What this means for the software ecosystem is that designing products with greater transparency and user participation in mind will likely yield more resilient users over time.

In other words, “building better users” entails, first and foremost,

34. See, e.g., Corey L. M. Keyes, *Risk and Resilience in Human Development: An Introduction*, 1 RES. HUM. DEV. 223, 224 (2004), http://www.sociology.emory.edu/ckeyes/rhd14_1.pdf.

35. The American Psychological Association identified four factors in particular shared by individuals who tended to be viewed as “resilient”: a) “the capacity to make realistic plans and to carry them out,” b) a positive self-image and confidence in one’s strengths and abilities, c) the ability to communicate skillfully and solve problems, and d) “the capacity to manage strong feelings and impulses.” AM. PSYCHOLOGICAL ASS’N, *Resilience: After a Hurricane*, APA.ORG, <http://www.apa.org/helpcenter/hurricane-resilience.aspx/> (last visited Feb. 22, 2011).

36. For example, in the words of one researcher, “[t]here are kids in families from very adverse situations who really do beautifully, and seem to rise to the top of their potential, even with everything else working against them.” David Gelman, *The Miracle of Resiliency*, NEWSWEEK, Summer 1991, at 44 (quoting Dr. W. Thomas Boyce, Director of Behavioral and Developmental Pediatrics at the University of California, San Francisco).

37. “A risk factor is an individual attribute, individual characteristic, situational condition, or environmental context that increases the probability’ of an undesirable outcome.” Laura Greenberg, *Compensating the Lead Poisoned Child: Proposals for Mitigating Discriminatory Damage Awards*, 28 B.C. ENVTL. AFF. L. REV. 429, 455 (2001) (quoting Howard B. Kaplan, *Toward an Understanding of Resilience: A Critical Review of Definitions and Models*, in RESILIENCE AND DEVELOPMENT: POSITIVE LIFE ADAPTATIONS 17, 37 (Meyer D. Glantz & Jeannette L. Johnson eds., 1999)).

38. See, e.g., Michael Rutter, *Psychosocial Resilience and Protective Mechanisms*, in RISK AND PROTECTIVE FACTORS IN THE DEVELOPMENT OF PSYCHOPATHOLOGY 181, 181 (Jon Rolf et al. eds., 1993).

39. See, e.g., The Consortium on the School-Based Promotion of Social Competence, *The School-Based Promotion of Social Competence: Theory, Research, Practice, and Policy*, in STRESS, RISK, AND RESILIENCE IN CHILDREN AND ADOLESCENTS: PROCESSES, MECHANISMS, AND INTERVENTIONS 268 (Robert J. Haggerty et al. eds., 1994).

convincing consumers that they can master a technology before them and guiding them in doing so. As such, the development of resilience in humans is inherently bound up with the concept of self-efficacy, which refers to an individual's beliefs about his control and ability to successfully perform a given task or behavior.⁴⁰ Empirical evidence offers support for the connection between self-efficacy perceptions and resilience; there tends to be a correlation in many contexts, such as in academic performance, between the strength of an individual's beliefs about the capability of success and actual success.⁴¹ Even when controlling for ability levels in the specific task, some research demonstrates that students who do not believe they can achieve a goal are, in fact, less likely to do so than their peers who do believe they can achieve that goal.⁴² Unlike the concept of self-esteem, self-efficacy pertains to narrow, specific, and concrete goals and varies within humans from task to task. No one is good at everything. I may be a good photographer, but my tennis abilities leave much to be desired; for another person the two tasks' success levels may be reversed.

The leading theory on self-efficacy is found in the work of Albert Bandura. According to Bandura, when individuals select which tasks to undertake and decide whether to persevere "in the face of obstacles or aversive experiences," they do so based on their perceptions of self-efficacy.⁴³ People develop self-efficacy for a specific task, such as mastering a new technology product, in four ways:⁴⁴

1. Through personal experience;
2. From physiological and/or emotional reactions to an event;
3. Through vicarious experiences or modeling;
4. From feedback from their social environment.

Through these mechanisms, people either adopt a resilient approach to obstacles, mustering feelings of self-efficacy to learn and work through

40. For a discussion of self-efficacy see, for example, ALBERT BANDURA, *SELF-EFFICACY: THE EXERCISE OF CONTROL* (1997).

41. See Barry J. Zimmerman, *A Social Cognitive View of Self-Regulated Academic Learning*, 81 J. EDUC. PSYCHOL. 329, 331 (1989) (offering data suggesting that perceptions of high self-efficacy are positively correlated with persistence and achievement in an academic context).

42. *Id.*

43. Albert Bandura, *Self-Referent Thought: A Developmental Analysis of Self-Efficacy*, in *SOCIAL COGNITIVE DEVELOPMENT: FRONTIERS AND POSSIBLE FUTURES* 200, 201 (John H. Flavell & Lee Ross eds., 1981); see *infra* pp. 9–11; see also, e.g., Albert Bandura, *Social Cognitive Theory of Self-Regulation*, 50 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 248, 257–58 (1991), <http://www.des.emory.edu/mfp/Bandura1991OBHDP.pdf> (concluding that confidence in self-efficacy positively influences choices, aspirations, effort, perseverance, and stress levels).

44. For a discussion of self-efficacy determinants, see, for example, Michael Hunter Schwartz, *Teaching Law Students to Be Self-Regulated Learners*, 2003 MICH. ST. L. REV. 447, 456 (2003).

new obstacles or they fail to persevere.⁴⁵

Personal experience plays an important cumulative role in learning resilience. A user's history of technology learning is likely to impact self-efficacy in new technology tasks; it brings a backdrop of success or failure to all new technology situations users enter. For Bandura, "partial mastery experiences" predict "subsequent performance of threatening tasks that [an individual has] never done before."⁴⁶ Perhaps more dramatically, "[a]rbitrarily instilled beliefs of inefficacy discourage . . . coping behavior even when the opportunity to exercise personal control exists. In contrast, instilled perceived efficacy largely overrides ostensible external constraints on the exercise of personal control . . ."⁴⁷ In other words, when it comes to technology, peoples' negative prior experiences with code prime their future experiences. Stated another way, cumulative learning episodes can create either a virtual circle of self-reinforcing technology success or a vicious circle of self-priming technology failure.

In a similar vein, as in all things human, emotion plays a role in learning and control. Some consumers reach a point in their interactions with technology where they become overwhelmed with frustration and a feeling of lack of control; they have a negative emotional reaction to code they cannot seem to understand and simply give up on learning more. Research in self-efficacy theory indicates a possible relationship between anxiety of this sort and low self-efficacy.⁴⁸ In other words, when consumers experience anger or stress over malfunctioning software, their sense of self-efficacy likely diminishes. People who value a goal but develop low self-efficacy with respect to their ability to achieve it, in turn, can become despondent, depressed, and disengaged. Then, viewing the disengagement as failure, they feel powerless in achieving the goal, creating a self-reinforcing negative cycle. As a consequence, they may shy away from another attempt to master the task.⁴⁹ This negative dynamic then further diminishes the likelihood of success with a particular task.

Third, self-efficacy can be bolstered by observational learning from

45. See, e.g., Zimmerman, *supra* note 41, at 331 (offering data suggesting that perceptions of high self-efficacy are positively correlated with persistence and achievement in an educational context).

46. Albert Bandura, *Self-Efficacy Mechanism in Human Agency*, 37 AM. PSYCHOLOGIST 122, 128 (1982). Thus, "[e]nactive attainments provide the most influential source of efficacy information because [they] can be based on authentic mastery experiences[;] [s]uccesses heighten perceived self-efficacy[,] repeated failures lower it" *Id.* at 126 (emphasis omitted).

47. BANDURA, *supra* note 40, at 268.

48. See generally S. Lloyd Williams, *Self-Efficacy, Anxiety, and Phobic Disorders*, in SELF-EFFICACY, ADAPTATION, AND ADJUSTMENT: THEORY, RESEARCH, AND APPLICATION 69 (James E. Maddux ed., 1995).

49. *Id.*

the groups around the person, modeling on the behaviors of “similar others.”⁵⁰ In other words, people who work or live in environments with people who demonstrate strong computer skills and efficacy with code are probably more likely to develop strong technology skills themselves. “Seeing similar others perform successfully can raise efficacy expectations in observers who then judge that they too possess the capabilities to master comparable activities.”⁵¹ Modeling has three major effects.⁵² First, it teaches a learner to acquire and perform new responses or skills from observation.⁵³ Second, it serves to inhibit fear responses because the learner sees that the model does not suffer negative consequences. To the contrary, the learner is potentially emboldened when she sees that such behavior often results in positive consequences.⁵⁴ Third, a “facilitation of responses” happens because the learner can emulate the model’s cues.⁵⁵ Seeing someone similar engage in a behavior leads a learner to believe that he or she has the ability to engage in the same conduct. Social models demonstrate what is possible, thereby changing what the learner believes she too can accomplish—an instilling of feelings of self-efficacy. In other words, technology modeling and technology mentorship helps consumers learn to help themselves.

Learning self-efficacy and, in turn, becoming resilient are cumulative, meaning that episodes of success and failure and environmental inputs blend to evolve an individual’s beliefs of self-efficacy.⁵⁶ We construct a belief in our ability to succeed with increasingly challenging tasks based on our ability—and by observing others’ ability—to finish similar but less difficult tasks.⁵⁷ In essence, this is a form of human self-regulation, which,

50. *See* Bandura, *supra* note 46, at 126–27.

51. *Id.*

52. *See* GERALD COREY, THEORY AND PRACTICE OF COUNSELING AND PSYCHOTHERAPY 293–94 (5th ed. 1996) (relying on Bandura’s research).

53. *Id.* at 293.

54. *Id.* at 294.

55. *Id.*

56. *See* Bandura, *supra* note 46, at 124. According to Bandura, models can serve to instruct, motivate, disinhibit, inhibit, socially facilitate, and arouse emotion in a process of vicarious reinforcement. *See id.* at 126–27. Essentially, development is viewed as a process of quantitative change, during which learning episodes gradually accumulate over time. *See id.* Although Social Learning Theory does not directly address historical or cultural context, it reflects the tradition of Vygotsky and the contextualist approach by recognizing the dialectical process of a person who is working within and shaped by an environment; a triadic reciprocal determinism occurs among behavior, cognitive factors, and the environment. *See* LIONEL NICHOLAS, INTRODUCTION TO PSYCHOLOGY 136–38 (2009). There is no endpoint to development, and universal behaviors are rare. Thus, children are developmentally malleable but only within constraints of biology and environment, an environment replete with technology. *See id.*

57. *See id.* at 128.

Bandura argues, is contingent on learning.

Finally, feedback loops matter. Learning, argues Bandera, requires extensive feedback loops to correct for problems that ensue from individual interpretations of situations. These feedback loops are necessarily social: to extend the cognitive capabilities of the individual through tools and resources, learners need inputs for correction of misguided conduct. In order for even those who are “good self-regulators” “[t]o enhance their competency, they have to figure out what information they lack, how best to frame their inquiry, from whom to seek assistance, and how to overrule any social hesitancy they feel to do so.”⁵⁸ This is where law can enter the conversation and offer additional feedback loops.

II. RESILIENCE, CONTRACTS, AND FAIR TRADE PRACTICES IN INFORMATION

As I have argued elsewhere, successfully regulating technology means a primary focus on regulating the humans building and interacting with the technology, rather than the products themselves.⁵⁹ Technology specific regulation is doomed to failure as the pace of innovation outstrips the law. Human conduct, on the other hand, particularly when framed in terms of traditional legal approaches, is a finite and regulable universe of possibilities. If we stipulate that both innovation in code and consumer protection are equally important social goals, we can reframe the conversation around regulating conduct of both sets of humans involved in the code ecosystem in their relation to each other—both the humans who *write* the code and the humans who *use* the code. The discussion in Section I above articulated that resilience in systems is characterized by redundancy, a shifting balance between stable and unstable forces limited by internal controls, and a dynamic nature that compensates for change and then persists. The above discussion of the developmental psychology literature leads us to the conclusion that four core elements—experience, emotion, modeling, and feedback loops—are integral to building resilience in consumers. When we consider these four core elements, we can begin to construct a user-centered model for consumer protection in technology spaces.⁶⁰ Legal approaches, therefore, should focus on enhancing resilience

58. BANDURA, *supra* note 40, at 231.

59. Andrea M. Matwyshyn, *Technology, Commerce, Development, Identity*, 8 MINN. J. L. SCI. & TECH. 515 (2007).

60. Though we frequently anthropomorphize it, technology does not really have a life of its own at present. It is a creation by humans for humans; humans give technology its animating features. Even emergent unintended technology consequences are, nevertheless, at some point caused in fact by humans authoring code and, potentially, proximately caused by other humans interacting with that code. But, first and foremost, the reason that anyone writes or uses code is developmental—code authorship or use is a type of act of creative

on both sides of commercial relationships between the imperfect humans creating technology and the imperfect humans using technology. The natural starting point for such a legal undertaking is contract law.

A. *Resilience and Contracts in Technology-Mediated Spaces*

The primary law of the code ecosystem since its inception has always been contract law. Despite a greater volume of litigation with respect to high profile intellectual property in technology spaces, ultimately, contract law is currently a more potent framework for legal ordering than is intellectual property law in such spaces. But for very limited circumstances, contract law is not preempted even by copyright law when an agreement exists between the parties.⁶¹ As *ProCD, Inc. v. Zeidenberg* explained,⁶² where a contract between the parties exists, regardless of whether the subject matter is copyrightable, contract law is not preempted.⁶³

expression that intends to expand the capabilities of the author or user with a technological appendage to his or her being. Though perhaps this reflects a melodramatic framing of the deeper social meaning of, for example, a flying pig screensaver, even the creation of this code with arguably limited social impact still reflects an act of self-realization for the coder. It reflects an act of human generativity. Generativity—a developmental psychology concept arising from the work of Erik Erikson—refers to the human desire to create something greater than yourself that survives your own lifetime. See ERIK H. ERIKSON, *CHILDHOOD AND SOCIETY* 231 (1950). Professor Zittrain has eloquently argued that devices and code are inherently generative. See JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT* 69–70 (2008). I respectfully submit they are not truly generative in the traditional meaning of the term. Driven by the current limitations of artificial intelligence research, only humans can be generative at present—code is merely a line of symbols in the absence of a human to author it, animate it with values, or give it derivative life.

61. In *Rano v. Sipa Press, Inc.*, the 9th Circuit held that copyright preempted state law relating to the termination at will of a license with an indefinite duration because when “California law and federal law are in direct conflict, federal law must control.” *Rano v. Sipa Press, Inc.*, 987 F.2d 580, 585 (9th Cir. 1993). Assignability of a licensee’s rights would provide another preemption basis because under federal law such rights cannot be assigned in a nonexclusive license without the consent of the licensor. See *CFLC, Inc. v. Cadtrak Corp.*, 89 F.3d 673, 679 (9th Cir. 1996). Cf. *Chamberlain v. Cocola Assocs.*, 958 F.2d 282, 285 (9th Cir. 1992) (applying a California statute regarding transfer of a tangible object in the case of a transfer of the intangible rights to use an object).

62. 86 F.3d 1447 (7th Cir. 1996). *ProCD, Inc. v. Zeidenberg* was the first appellate ruling dealing with the enforceability of shrinkwrap licenses, and it held that the contract restrictions ProCD placed on the use of a noncopyrightable database were not preempted by copyright law. See *id.* at 1454–55; see also *DaimlerChrysler Servs. N. Am., LLC v. Summit Nat’l, Inc.*, 144 F. App’x. 542 (6th Cir. 2005) (holding that copyright defenses are irrelevant to contract enforcement); *Davidson & Assocs. v. Jung*, 422 F.3d 630, 632, 639 (8th Cir. 2005) (holding that a license is not preempted by fair use); *Altera Corp. v. Clear Logic, Inc.*, 424 F.3d 1079, 1089–90 (9th Cir. 2005) (finding that copyright law does not preempt contract enforcement); *Bowers v. Baystate Techs, Inc.*, 320 F.3d 1317, 1323–26 (Fed. Cir. 2003) (holding that copyright law did not preempt the plaintiff’s contractual claims).

63. The court opined that

enforcement . . . would not withdraw any information from the public domain. . . .

More importantly, however, contract law is critical because it is arguably the field of law most aimed at fostering resilience in the marketplace: it is intended to create a safety net of commercial trust and to assist parties in bouncing back from relationship failures. At its most basic level, contract law involves one set of imperfect persons successfully interacting with another set of imperfect persons to generate a sense of control over the exchange.

A concern for the four core elements of developing resilience in humans are also represented in contract law—the same four elements I have argued should be fostered in users of technology. For example, contract law reflects a concern over imbalanced cumulative learning between the parties in its disparate treatment of sophisticated contracting parties and unsophisticated parties in the Uniform Commercial Code.⁶⁴ Emotions of bargaining parties are considered through doctrines such as duress and coercion, where one party can exert psychological influence unfairly over another. Modeling issues arise, rather obviously, in the perennial debate over form contracting. Companies frequently use industry-wide contracts, and their lawyers “borrow” forms from each other or reuse the same form contract with numerous clients. Finally, contract is heavily driven through crafting feedback loops through various doctrines related to breach, remedies, and warranties on a going forward basis, seeking to preserve the relationship whenever possible.

So, is the resilience problem in information contracting solved because of the resilience of contract law itself? No. The existing inherent resilience-fostering nature of contract law is being undercut in new technology contexts, particularly with respect to privacy and information security. Due to certain unique characteristics, rather than bolstering both systemic and individual resilience, technology-mediated contracting instead damages resilience on both sides of the relationship between the code creator and the consumer user. In previous work, I empirically demonstrated that terms of use and end user license agreements online—the contracts that shift risk from the authors of code to users—were becoming progressively more draconian in favor of drafters.⁶⁵ I argued that the results indicate that current Internet contracting constructions do not

Everyone remains free to copy and disseminate all 3,000 telephone books that have been incorporated into ProCD's database. Anyone can add SIC codes and zip codes. ProCD's rivals have done so. Enforcement of the shrinkwrap license may even make information more readily available, by reducing the price ProCD charges to consumer buyers.

ProCD, Inc., 86 F.3d at 1455.

64. See, e.g., U.C.C. § 2-207(2) (treating merchants differently).

66. Andrea M. Matwyshyn, *Mutually Assured Protection: Toward Development of Relational Internet Data Security and Privacy Contracting Norms*, in *SECURING PRIVACY IN THE INTERNET AGE 73* (Anupam Chander et al. eds., 2008).

successfully reconcile the needs of code creators and consumers in a way that is likely to lead to improved trust and growth in the digital marketplace.⁶⁶ My predictions in that work appear to have been correct, at least with respect to privacy and information security.

How do we assess the legal implications of this dynamic? Although it is tempting to simply argue in favor of technology contract essentialism, technology-mediated contracts are not really special contracts; instead, they should be analyzed as contracts executed under special circumstances that diminish party resilience, particularly when a bargaining power imbalance already exists. The next question, therefore, is how can we shift the dynamics of technology-mediated contracting back in favor of fostering resilience? As a thought exercise, using the four core elements of building resilience identified previously, let us analyze four common consumer laments regarding understanding data privacy and information security and its relationship to the traditional resilience of contract law. This in turn may help identify a set of guidelines for “fair trade practices” in information that bolsters resilience. Such guidelines, if authored by the FTC, would provide meaningful guidance for code creators on avoiding an unfair trade practices inquiry from the FTC with respect to data privacy and information security practices.

B. *Fair Trade Practices, Privacy, and Technology Contracts*

As the examples of Google Buzz and Facebook Beacon demonstrated, consumer privacy freakouts can be swift and brutal. Why? As the FTC has correctly identified, the core deficit for consumers is a missing sense of control.⁶⁷ This feeling of lack of control and, correspondingly, diminished resilience, is driven by two dynamics: weakened communication and

66. *Id.* In particular, my sample did not reflect a balance being struck between predictable mitigation of liability for content providers and assumption of obligations to securely treat user data. Instead, the content of the terms of use and privacy policies analyzed reflected an inherently irreconcilable tension in legal strategy adopted in the two constructions: the terms of use tended to reflect a nonrelational approach best suited to a one-shot game of adversaries, while the privacy policies tended to reflect a more relational approach with a continuing obligation to maintain data in accordance with security promises, reflecting an iterated game of commercial partners.

Id. at 81. Another developing tension that was noted was one of contractual interpretation. Browsewrap terms of use are usually not deemed enforceable, but privacy policies in the same browsewrap construction are being enforced by the FTC and private actors as contracts (at least in legal approach, if not explicitly). *See id.* at 77–80.

67. FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010), <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>; *see also* Press Release, Fed. Trade Comm’n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), *available at* <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.

bolstered data mining. Perhaps counterintuitively, technology mediated spaces present an impoverished contracting medium when compared to real space. Second, technology-mediated spaces involve far greater data collection medium capabilities when compared with real space; this collection may frequently exceed the scope of information a consumer believes herself to be knowingly volunteering. In order to restore consumers' sense of control and foster resilience, a feedback loop can be implemented by the FTC through articulating additional fair trade practices in information. Such a set of guidelines might include four elements: a single, plain English user agreement that embodies all relevant terms, a summary label, contractual enforcement using a "reasonable digital consumer" standard, and a transparency requirement to reasonably answer all consumer privacy and security inquiries.

1. Experience in Digital Contract: Creating a Plain English "Information License and Security Agreement"

The experience of an average consumer with respect to digital contracting today goes something like this: "I tried to read a EULA once, it was really long and I couldn't understand anything in it. It included references to a bunch of other agreements too. I gave up and just clicked 'yes' because I needed to use the product. Now I just click 'yes' on every contract that pops up. Besides, although I care about privacy, all these companies are just going to follow me around and abuse my data anyway. There's no point to even reading a privacy policy."

Fatalistic default acceptance of terms presented to consumers is the norm in digital contracting. Even consumers who wish to invest the time to understand the contract before them are unlikely to be able to do so. Coupled with the inability to ask questions, this dynamic leaves consumers feeling helpless, without meaningful control and choice, and clicking "yes" on every agreement that appears before them on a screen in a Pavlovian clicking behavior.

Particularly because of the difficulty in understanding companies' data privacy and security practices, consumers require a single point of information regarding companies' practices. As I have argued elsewhere,⁶⁸ even assuming for the sake of argument that a consumer can understand the plain face meaning of the terms of the contract, the consumer cannot necessarily verify what particular code is in fact doing on her system. Code can hide itself and its functionalities in elaborate ways. Without full clear disclosure to eliminate this information imbalance, a fair meeting of the

68. See Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 112-13 (2010).

minds on information collection terms in a contract is not feasible.

Terms of use agreements and privacy policies as separate agreements is merely an unfortunate artifact of early Internet law.⁶⁹ These two antiquated contract constructions should be replaced with a single contract form where privacy and security promises are conspicuous, material terms of the user license agreement. Consequently, a breach of these terms obviously presents a material breach of the agreement in its entirety and offers a consumer recourse in the relationship for contract breach.⁷⁰

In addition to creating a single contract, a “Plain English” requirement in digital contract language would greatly assist consumers’ sense of control over information exchanges and, consequently, foster resiliency. Plain English requirements have been instituted in situations where a disclosure need was pressing, but the subject matter at hand was inherently complicated. For example, in securities regulation, the Securities and

69. See, e.g., Matwyshyn, *supra* note 66, at 77–79.

70. In fact, a business benefit may also arise for the code creator from such a simplified construction. Particularly in large organizations, it is common to find a “lack of cooperation among attorneys, businesspeople, and technologists The lawyers drafting terms of use may be inadequately sensitive” to the technology in question. *Id.* at 83. “Meanwhile, privacy policies are sometimes written by marketing departments or technologists who may be unaware of the legal implications of particular contract presentation on the user interface[.]” for example. *Id.* Therefore, when these two contracts are analyzed together, they may, at present, not effectively accomplish either liability limitation or user disclosure in their current dual presentation. *Id.* For example, in Internet contracting contexts, terms of use are generally written by attorneys who zealously attempt to limit their clients’ liability to the greatest extent possible but may not really understand the website. However, because no negotiation of these terms occurs, they remain in their original, unnegotiated format when the website goes live. These terms of use, meanwhile, are considered unsightly legal verbiage by the designers of websites and are tucked away in inconspicuous places. The effect of these actions on legal enforceability generally goes un contemplated: the lawyers have been excluded from the business decision loop. Privacy policies, on the other hand, are generally written at least in part by the public relations department of business enterprises. As such, the legally binding effect of these privacy promises is frequently not understood by the businesspeople involved in their creation. Thus, terms of use and privacy policies are not necessarily thought about as being inherently interrelated by businesspeople and attorneys. The standard content of terms of use, such as user indemnification provisions, may be set aside by some U.S. courts. In the United States, challenges could be brought on the basis of substantive unconscionability (for example, user indemnification provisions), embodying offline problems of form contracts of adhesion, procedural unconscionability with regard to formation uncertainty, as well as other formation issues arising from inadequate user notice and consent and the absence of negotiation. See *id.* at 80–81, 83. Most terms of use would almost certainly be set aside in their entirety or at least in substantial part if challenged in the European Union. The European Union’s grounds for invalidation of terms-of-use content include violation of, among other directives, the European Union Directive on Distance Contracts and the Directive on Unfair Terms. See, e.g., James R. Maxeiner, *Standard-Terms Contracting in the Global Electronic Age: European Alternatives*, 28 *YALE J. INT’L L.* 109, 111–13 (2003). Clearly, multijurisdictional unenforceability of terms of use is a suboptimal outcome from the perspective of both technologists and lawyers within an entity attempting to limit liability on a global basis.

Exchange Commission (SEC) promulgated a Plain English Rule with respect to prospectuses.⁷¹ The SEC believed that “using plain English . . . will lead to a better informed [] market . . . in which” consumers “can more easily understand . . . disclosure”⁷² Parallel improvements should happen in the data privacy and information security contracting context.

2. Emotion in Digital Contract: Creating a Sense of Transparency in Formation with Summary Labeling

It is not uncommon to hear a consumer say with frustration: “I didn’t even see that there were terms of use linked on the bottom of that website. How was I supposed to know I was bound by them? And what are all these links to other contracts? I can’t possibly read forty screens of ten-point font on a slow-loading smartphone.”

Although obscure presentations of terms without an affirmative act of assent are unlikely to be enforced, these same terms, if merely incorporated by reference in another more obvious set of terms, are likely to be deemed enforceable. The task of reading multiple cross-referenced linked documents, potentially on a small mobile device, is limiting, at best. At worst, it is taking advantage of a crippled user interface. In order for consumers to understand the totality of the terms to which they are bound, a potentially promising transparency approach is mandating a one-page summary of all material terms—modeled on the spirit of a summary prospectus—as the first screen of all digital agreements. In the language of the SEC, the rationale behind the requirement of a summary prospectus is to offer concise standardized information to consumers, which allows them to compare terms across products.⁷³ The information market requires similar disclosure structures to build consumer resilience.

3. Modeling: Imposing Digital Reasonableness Standards

Particularly with respect to privacy settings on social network websites such as Facebook, a common consumer lament is: “There are way too many privacy settings, and they change the presentation constantly. I can’t keep up, and I have no clue whether what I’m doing will actually set the preferences the way I want them to be. No average person can figure this out in a reasonable amount of time.”

If the ability to set privacy settings is offered, these settings—as selected by the consumer—should constitute a material term of the agreement. Correspondingly, a material unilateral alteration of the terms

71. SEC Plain English Disclosure, 17 C.F.R. pts. 228–30, 239, 274 (2008).

72. *Id.*

73. SEC Enhanced Disclosure and New Prospectus Delivery Options for Registered Open-End Management Investment Companies, 17 C.F.R. pts 230, 232, 239, 274 (2008).

may constitute a breach of contract. Any alteration in interface that changes the spirit of consumer preferences will be perceived by a consumer as “unfair:” technology-mediated contracting lacks the back-and-forth consumers take for granted in real space. Although most consumers never negotiate the agreements they sign, the potential for negotiability appears to exist, at least superficially, in most cases. A human hands over a document for signature; presumably this human can engage in some degree of negotiation or at least answer questions about the contract. Although this person’s incentives are not aligned with those of the consumer, psychologically, for a consumer, this person serves as a type of model with respect to the relationship. This, in turn, likely fosters feelings of self-efficacy and control. In digital spaces, no other human appears present, and this modeling aspect of the exchange is lost.

As I have argued elsewhere, technological skills vary dramatically across users, and this distribution is multi-modal, not necessarily “map[ping] onto chronological age.”⁷⁴ As such, the imposition of a reasonableness standard for contracts in technology spaces accommodates this variation. Creating contracts that a reasonable consumer—as determined by empirical testing—can understand has a type of modeling function. The imposition of this “reasonable digital consumer” standard would perform a modeling function for consumers less skilled than average, urging them to improve and offering a target for their development.

4. Feedback Loops in Digital Contract: Offering a Live Human to Negotiate and Explain Terms

A final lament of many a user goes something like this: “None of my friends understand any of this stuff, either. I don’t have anyone to ask for help with understanding a EULA or privacy policy, or anyone to ask questions of regarding what the company is doing with my information.” In other words, consumers lack a feedback loop: they are asking social guidance in interpreting the situation. Companies rarely have a real-time virtual point of contact for inquiries about EULAs and privacy policies. However, they frequently have real-time shopping assistance. In other words, the possibility exists for the drafter to provide real-time feedback on contracts in technology-mediated spaces. However, even without real-time assistance, consumer questions regarding data privacy and information security, particularly subsequent to a known data breach, should be promptly answered through other means. Based on this author’s experience, consumer inquiries regarding privacy and security inquiries are sometimes ignored even by large, reputable companies.

74. Matwyshyn, *supra* note 59, at 540.

III. CONCLUSION

Applying the concept of resilience, this Article has explored the possibility of crafting improved guidelines for fair trade practices in information contracts. Without meaningful guidance to improve data privacy and technology contracts, code creators have inadequate incentives to write more user-friendly and privacy-sensitive code. They believe their contracts to protect them from almost all liability, and that users are powerless to negotiate. Creators can impose their products on consumers on their own terms—terms which, as I have argued elsewhere, may be unconscionable from the perspective of a reasonable consumer.⁷⁵ Stating the argument another way, using language reflecting the spirit of the SEC's Plain English Rule, contracting practices that may have started out embodying the traditional resilience of contract law have crept into the realm of potentially embodying unfair trade practices. Using the language of developmental psychology, the current state of affairs in digital contracting actively erodes resilience rather than building it, an undesirable result that hampers the future of the information technology marketplace.

75. See generally Andrea M. Matwyshyn, *Technoconsen(t)us*, 85 WASH. U. L. REV. 529 (2007).

