Minnesota Journal of Law, Science & Technology

Volume 14 | Issue 1 Article 8

2013

Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle

Adam Thierer

Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle

Adam Thierer*

I. INTRODUCTION 311
II. *ARGUMENTUM IN CYBER-TERROREM*: A FRAMEWORK FOR EVALUATING FEAR APPEALS 312
A. Appeals to Fear as an Argumentation Device 312
B. Deconstructing Fear Appeal Arguments: The Violent Media Case Study 313
C. Technopanics 315
D. Threat Inflation 317
1. Cybersecurity Threat Inflation 318
2. Online Safety Threat Inflation 320
3. Online Privacy Threat Inflation 325
4. Economic- and Business-Related Threat Inflation 329
III. REASONS PESSIMISM DOMINATES DISCUSSIONS ABOUT THE INTERNET AND INFORMATION TECHNOLOGY 332
A. Generational Differences 333
B. Hyper-Nostalgia, Pessimistic Bias, and Soft Ludditism 335
C. Bad News Sells: The Role of the Media, Advocates, and the Listener 337
D. The Role of Special Interests and Industry Infighting 338
E. Elitist Attitudes Among Academics and Intellectuals 344
F. The Role of "Third-Person-Effect Hypothesis" 345

* Senior Research Fellow, Mercatus Center at George Mason University. The author wishes to thank the following individuals for helpful thoughts on various drafts of this article: Paul Dragos Aligica, Jerry Brito, Will Rinehart, Adam Marcus, Gregory Conko, and two anonymous reviewers.

IV. TYING IT ALL TOGETHER: FEAR CYCLES 347
V. WHY TECHNOPANICS AND THREAT INFLATION ARE DANGEROUS 350
A. Foster Animosities and Suspicions Among the Citizenry 351
B. Create Distrust of Many Institutions, Especially the Press 351
C. Often Divert Attention from Actual, Far More Serious Risks 351
D. Lead to Calls for Information Control 352
VI. WHEN PANIC BECOMES POLICY: THE RISE OF AN INFO-TECH "PRECAUTIONARY PRINCIPLE" ... 352
A. A Range of Responses to Theoretical Risk 356
B. The Perils of "Playing it Safe" 361
C. Anticipation vs. Resiliency 364
D. Case Studies: Applying the Resiliency Model to Information Technology Issues 368
1. Online Child Safety, Privacy, and Reputation Management 368
2. Cybersecurity 373
3. Market Power and Economic Issues 374
E. Resiliency Makes Even More Sense When Practicality of Control is Considered 376
VII. A FRAMEWORK FOR EVALUATING AND ADDRESSING TECHNOLOGY RISK 379
A. Defining the Problem 380
B. Consider Legal and Economic Constraints 381
C. Consider Alternative, Less Restrictive Approaches 383
D. Evaluate Actual Outcomes 384
VIII. CONCLUSION 385

I. INTRODUCTION

"In time we hate that which we often fear."[1]

— William Shakespeare

Fear is an extremely powerful motivational force. In public policy debates, appeals to fear are often used in an attempt to sway opinion or bolster the case for action. Such appeals are used to convince citizens that threats to individual or social well-being may be avoided only if specific steps are taken. Often these steps take the form of anticipatory regulation based on the precautionary principle.

Such "fear appeal arguments" are frequently on display in the Internet policy arena and often take the form of a full-blown "moral panic" or "technopanic."[2] These panics are intense public, political, and academic responses to the emergence or use of media or technologies, especially by the young.[3] In the extreme, they result in regulation or censorship.

While cyberspace has its fair share of troubles and troublemakers, there is no evidence that the Internet is leading to greater problems for society than previous technologies did.[4] That has not stopped some from suggesting there are reasons to be particularly fearful of the Internet and new digital technologies.[5] There are various individual and institutional factors

---

1. WILLIAM SHAKESPEARE, *Antony and Cleopatra* act 1, sc. 3, line 12, *in* THE COMPLETE WORKS OF WILLIAM SHAKESPEARE 1127, 1132 (Stanley Wells & Gary Taylor eds., Clarendon Press 1986).

2. Adam Thierer, *Parents, Kids, & Policymakers in the Digital Age: Safeguarding Against "Techno-Panics*," INSIDE ALEC (Am. Legislative Exch. Council, D.C.), July 2009, at 16, 16–17 [hereinafter *Safeguarding Against Technopanics*], *available at* http://www.pff.org/issues-pubs/articles/090715-against-technopanics-adam-thierer-Inside-ALEC.pdf. *See also* Josh Constine, *Selling Digital Fear*, TECHCRUNCH (Apr. 7, 2012), http://techcrunch.com/2012/04/07/selling-digital-fear (discussing public panic about availability of private information online).

3. *See Safeguarding Against Technopanics*, *supra* note 2, at 16 ("[S]ocial and cultural debates quickly become political debates.").

4. *See* Adam Thierer, *Fact and Fiction in the Debate over Video Game Regulation*, PROGRESS ON POINT (Progress & Freedom Found., D.C.), Mar. 2006, at 20–21 [hereinafter *Fact and Fiction*], *available at* http://www.pff.org/issues-pubs/pops/pop13.7videogames.pdf (identifying a decrease in youth murder, rape, robbery, assault, alcohol and drug abuse, teen birth rates, high school dropout rates, and suicide rates).

5. *Cf.* Alice E. Marwick, *To Catch a Predator? The MySpace Moral Panic*, FIRST MONDAY (June 2, 2008), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2152/1966 (giving examples of reasons some are fearful of the Internet, but arguing that these reasons are not based on empirical evidence).

at work that perpetuate fear-based reasoning and tactics.

This paper will consider the structure of fear appeal arguments in technology policy debates, and then outline how those arguments can be deconstructed and refuted in both cultural and economic contexts. Several examples of fear appeal arguments will be offered with a particular focus on online child safety, digital privacy, and cybersecurity. The various factors contributing to "fear cycles" in these policy areas will be documented.

To the extent that these concerns are valid, they are best addressed by ongoing societal learning, experimentation, resiliency, and coping strategies rather than by regulation. If steps must be taken to address these concerns, education- and empowerment-based solutions represent superior approaches to dealing with them compared to a precautionary principle approach, which would limit beneficial learning opportunities and retard technological progress.

II. *ARGUMENTUM IN CYBER-TERROREM*: A FRAMEWORK FOR EVALUATING FEAR APPEALS

This section outlines the rhetorical framework at work in many information technology policy debates today, and explains why logical fallacies underlie many calls for regulation. Subsequent sections will show how these logical fallacies give rise to "technopanics" and "fear cycles."

A. APPEALS TO FEAR AS AN ARGUMENTATION DEVICE

Rhetoricians employ several closely related types of "appeals to fear." Douglas Walton, author of *Fundamentals of Critical Argumentation*, outlines the argumentation scheme for "fear appeal arguments" as follows:

- "*Fearful Situation Premise*: Here is a situation that is fearful to you."[6]
- "*Conditional Premise*: If you carry out A, then the negative consequences portrayed in this fearful situation will happen to you."[7]
- "*Conclusion*: You should not carry out A."[8]

---

6. DOUGLAS WALTON, FUNDAMENTALS OF CRITICAL ARGUMENTATION 285 (2006).
7. *Id.*
8. *Id.*

This logic pattern is referred to as *argumentum in terrorem* or *argumentum ad metum*.[9] A closely related variant of this argumentation scheme is known as *argumentum ad baculum*, or an argument based on a threat.[10] *Argumentum ad baculum* literally means "argument to the stick," an appeal to force.[11] Walton outlines the *argumentum ad baculum* argumentation scheme as follows:

- "*Conditional Premise*: If you do not bring about A, then consequence B will occur."[12]
- "*Commitment Premise*: I commit myself to seeing to it that B will come about."[13]
- "*Conclusion*: You should bring about A."[14]

As will be shown, these argumentation devices are at work in many information technology policy debates today even though they are logical fallacies or based on outright myths. They tend to lead to unnecessary calls for anticipatory regulation of information or information technology.

B. DECONSTRUCTING FEAR APPEAL ARGUMENTS: THE VIOLENT MEDIA CASE STUDY

Consider a familiar example of an appeal to fear: Proposals to control children's exposure to violent television, movies, or video games. The argument typically goes something like this:

- *Fearful Situation Premise*: Letting children watch violent television or movies, or play violent video games, will make them violent in real life.
- *Conditional Premise*: If we allow children to play games that contain violent content, then those children will behave aggressively or commit acts of violence later.
- *Conclusion*: We should not let children see violent television or movies, or play violent games.

A closer examination of each of the elements of this argument helps us to understand why appeals to fear may represent

---

9. Bo Bennett, *Logical Fallacies: Appeal To Fear*, LOGICALLY FALLACIOUS, http://www.logicallyfallacious.com/index.php/logical-fallacies/32-appeal-to-fear (last visited Sept. 13, 2012).

10. WALTON, *supra* note 6, at 286.

11. *Id.*

12. *Id.* at 287.

13. *Id.*

14. *Id.*

logical fallacies or be based on myths.[15]

First, the situation and conditional premises may not be grounded in solid empirical evidence. For example, in the above illustration, it remains a hotly disputed issue whether there is any connection between viewing *depictions* of violence and *real-world acts* of violence.[16] In this regard, another logical fallacy could also be at work here: *post hoc ergo propter hoc*. That is, just because A preceded B does not mean that A caused B. Stated differently, "correlation does not necessarily equal causation."[17]

Second, and related to the previous objection, there may be other environmental or societal variables that influence human behavior (in this case, acts of aggression or violence) that must be factored into any discussion of causality. This is true even if it is difficult to separate or treat each factor as an independent variable.[18] For example, what do we know about a violent child's upbringing, mental state, family situation, relationships with other children, and so on?

Third, the premises assume all children react identically to violently-themed media, which is clearly not the case. Every child is unique and has different capabilities and responses to visual stimuli.[19] Many children will witness depictions of violence in movies, television, or video games without suffering any negative cognitive impact.[20] Others may be adversely im-

---

15. *See Fact and Fiction*, *supra* note 4, at 18–19 (discussing the lack of a causal link between violent video games and aggressive behavior in children).

16. *Id.* at 19.

17. *Id.* This is often the result of a confusion between probability and outcome. The dispute ought to be about the probability that a depiction of violence will lead to actual violence. What often happens is the reverse: a particular episode is so upsetting that the fact of exposure to violently themed media is assumed to be the most probable cause, even if it had nothing to do with the incident. *See id.* (noting that there is no clear link between violent video games and actual violence or aggression).

18. *Id.* at 21.

19. *See* MARJORIE HEINS, NOT IN FRONT OF THE CHILDREN: "INDECENCY," CENSORSHIP, AND THE INNOCENCE OF YOUTH 228 (2001) ("Rarely do the debaters note that the same work may induce imitation in some viewers and catharsis in others—or that the same person may respond differently to different violent or sexual content.").

20. *Cf.* Christopher J. Ferguson, *The School Shooting/Violent Video Game Link: Causal Relationship or Moral Panic?*, 5 J. INVESTIGATIVE PSYCHOL. & OFFENDER PROFILING 25, 33 (2008) (discussing school shooters and noting that most children are unaffected by violent video games, but children with existing problems may be "at risk").

pacted by consumption of such content.[21]

Fourth, both the premises and conclusion ignore the possibility of alternative approaches to managing children's media exposure or gradually assimilating them into different types of media experiences. Even if one concedes that viewing *some* depictions of violence may have *some* influence on *some* children, it does not necessarily follow that government should limit or prohibit access to those depictions of violence. There are methods of partially screening content or teaching children lessons about such content that would not demand a sweeping prohibition of all such content in society or even an individual household.[22] This approach to deconstructing fear appeals is useful when analyzing "technopanics."

C. TECHNOPANICS

"Technopanics" are the real-world manifestations of fear appeal arguments. A "technopanic" refers to an intense public, political, and academic response to the emergence or use of media or technologies, especially by the young.[23] It is a variant of "moral panic" theory. Christopher Ferguson, professor of Texas A&M's Department of Behavioral, Applied Sciences, and Criminal Justice, offers the following definition: "A moral panic occurs when a segment of society believes that the behaviour or moral choices of others within that society poses a significant risk to the society as a whole."[24] Authoritative research on moral panic theory was conducted by British sociologist Stanley Cohen in the 1970s. He defined a moral panic as a moment when:

> A condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people; socially accredited experts pronounce their diagnoses and solutions; ways of coping are evolved or . . . resorted to . . . . Sometimes the panic passes over and is forgotten, except in folklore and collective memory; at other times it has more serious and long-lasting repercussions and might produce such changes as those

---

21. *Id.*

22. ADAM THIERER, PARENTAL CONTROLS & ONLINE CHILD PROTECTION: A SURVEY OF TOOLS & METHODS 195 (Version 4.0 2009), *available at* http://www.pff.org/parentalcontrols/Parental%20Controls%20&%20Online%20Child%20Protection%20[VERSION%204.0].pdf.

23. *See Safeguarding Against Technopanics*, *supra* note 2, at 16.

24. Ferguson, *supra* note 20, at 30.

> in legal and social policy or even in the way the society conceives itself.[25]

By extension, a "technopanic" is simply a moral panic centered on societal fears about a particular contemporary technology (or technological method or activity) instead of merely the content flowing over that technology or medium. In a 2008 essay *To Catch a Predator? The MySpace Moral Panic*, Alice E. Marwick noted:

> Technopanics have the following characteristics. First, they focus on new media forms, which currently take the form of computer-mediated technologies. Second, technopanics generally pathologize young people's use of this media, like hacking, file-sharing, or playing violent video games. Third, this cultural anxiety manifests itself in an attempt to modify or regulate young people's behavior, either by controlling young people or the creators or producers of media products.[26]

Genevieve Bell, director of Intel Corporation's Interaction and Experience Research, notes that "moral panic is remarkably stable and it is always played out in the bodies of children and women."[27] She observes, "The first push-back is going to be about kids," which will lead to the questions, "Is it making our children vulnerable? To predators? To other forms of danger? We will immediately then regulate access."[28] She argues that cultures sometimes adapt more slowly than technologies evolve, and that leads to a greater potential for panics.[29]

This pattern has played out for dime novels, comic books, movies, music, video games, and other types of media or media platforms.[30] While protection of youth is typically a motivating factor, some moral panics and technopanics transcend the traditional "it's-for-the-children" rationale for information control. The perceived threat may be to other segments of society or involve other values that are supposedly under threat, such as privacy or security.[31]

---

25. STANLEY COHEN, FOLK DEVILS AND MORAL PANICS: THE CREATION OF THE MODS AND ROCKERS 9 (1972).

26. Marwick, *supra* note 5.

27. Ben Rooney, *Women and Children First: Technology and Moral Panic*," WALL ST. J. TECH EUR. (July 11, 2011, 12:30 PM), http://blogs.wsj.com/tech-europe/2011/07/11/women-and-children-first-technology-and-moral-panic.

28. *Id.*

29. *Id.*

30. Robert Corn-Revere, *Moral Panics, the First Amendment, and the Limits of Social Science*, COMM. LAW., Nov. 2011, at 4, 4.

31. *See id.* at 5 (acknowledging that besides protecting children, other fac-

During all panics, the public, media pundits, intellectuals, and policymakers articulate their desire to "do something" to rid society of the apparent menace, or at least tightly limit it.[32] Thus, the effort (a) *to demonize* and then (b) *to control* a particular type of content or technology is what really defines a true panic.[33] Sociologists Erich Goode and Nachman Ben-Yehuda, authors of *Moral Panics: The Social Construction of Deviance*, observe:

> Whenever the question, "What is to be done?" is asked concerning behavior deemed threatening, someone puts forth the suggestion, "There ought to be a law." If laws already exist addressing the threatening behavior, moral entrepreneurs will call for stiffer penalties or a law-enforcement crack-down. Legislation and law enforcement are two of the most obvious and widely resorted to efforts to crush a putative threat during a moral panic.[34]

Unsurprisingly, a rush to judgment is a common feature of many panics. Such hasty judgments are often accompanied by, or the direct result of, the threat inflation tactics discussed next.

D. THREAT INFLATION

The rhetorical device most crucial to all technopanics is "threat inflation." The concept of threat inflation has received the most attention in the field of foreign policy studies.[35] In that context, political scientists Jane K. Cramer and A. Trevor Thrall define threat inflation as "the attempt by elites to create concern for a threat that goes beyond the scope and urgency that a disinterested analysis would justify."[36]

Thus, fear appeals are facilitated by the use of threat inflation. Specifically, threat inflation involves the use of fear-inducing rhetoric to inflate artificially the potential harm a new

---

tors include political, moral, or religious motives).

32. *See* ERICH GOODE & NACHMAN BEN-YEHUDA, MORAL PANICS: THE SOCIAL CONSTRUCTION OF DEVIANCE 35 (2d ed. 2009).

33. *See id.* at 48 (summarizing a moral panic to include, *inter alia*, heightened concern and hostility towards a behavior and a desire to change the behavior causing the panic).

34. *Id.* at 122.

35. *See, e.g.*, Chaim Kaufmann, *Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War*, INT'L SECURITY, Summer 2004, at 5, 5–6 (analyzing threat inflation leading up to the Iraq War).

36. JANE K. CRAMER & A. TREVOR THRALL, *Introduction: Understanding Threat Inflation*, *in* AMERICAN FOREIGN POLICY AND THE POLITICS OF FEAR: THREAT INFLATION SINCE 9/11 1, 1 (A. Trevor Thrall & Jane K. Cramer eds., 2009).

development or technology poses to certain classes of the population, especially children, or to society or the economy at large.[37] These rhetorical flourishes are empirically false or at least greatly blown out of proportion relative to the risk in question.[38] Some examples of how threat inflation facilitates technopanics follow.

1. Cybersecurity Threat Inflation

Jerry Brito and Tate Watkins of the Mercatus Center have warned of the dangers of threat inflation in cybersecurity policy and the corresponding rise of the "cyber-industrial complex."[39]

The fear appeal for cybersecurity can be outlined as follows:

- *Fearful Situation Premise*: Cyber-attacks will be increasingly sophisticated and eventually one will be catastrophic.
- *Conditional Premise*: If we do not regulate digital networks and technologies soon, we will be open to catastrophic attacks.
- *Conclusion*: Policymakers should comprehensively regulate digital networks and technologies to secure us against attacks.

The rhetoric of cybersecurity debates illustrates how threat inflation is a crucial part of this fear appeal. Frequent allusions are made in cybersecurity debates to the potential for a "digital Pearl Harbor,"[40] a "cyber cold war,"[41] a "cyber Katrina,"[42] or even a "cyber 9/11."[43] These analogies are made even though

---

37. *Safeguarding Against Technopanics*, *supra* note 2, at 16.

38. *Id.* at 17.

39. Jerry Brito & Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy* 1 (Mercatus Ctr., Working Paper No. 11-24, 2011).

40. *See* Richard A. Serrano, *Cyber Attacks Seen as a Growing Threat*, L.A. TIMES, Feb. 11, 2011, at A18 ("[T]he potential for the next Pearl Harbor could very well be a cyber attack.").

41. Harry Raduege, Op-Ed., *Deterring Attackers in Cyberspace*, HILL, Sept. 23, 2011, at 11.

42. David Kravets, *Vowing to Prevent 'Cyber Katrina,' Senators Propose Cyber Czar*, WIRED THREAT LEVEL (Apr. 1, 2009, 3:33 PM), http://www.wired.com/threatlevel/2009/04/vowing-to-preve.

43. Kurt Nimmo, *Former CIA Official Predicts Cyber 9/11*, INFOWARS.COM (Aug. 4, 2011), http://www.infowars.com/former-cia-official-predicts-cyber-911.

these historical incidents resulted in death and destruction of a sort not comparable to attacks on digital networks. Others refer to "cyber bombs" even though no one can be "bombed" with binary code.[44] Michael McConnell, a former director of National Intelligence, said the "threat is so intrusive, it's so serious, it could literally suck the life's blood out of this country."[45]

Again, a rush to judgment often follows inflated threats. For example, in November 2011, a cybersecurity blogger posted details of an alleged Russian cyber-attack on a water utility in Springfield, Illinois, that resulted in the temporary failure of a water pump.[46] Someone at the water utility passed details of the alleged Russian intrusion to the Environmental Protection Agency and the information ended up with the Illinois Statewide Terrorism and Intelligence Center, which issued a report on a "Public Water District Cyber Intrusion."[47]

The Washington Post quickly followed up with an article headlined *Overseas Hackers Hit Water Plant in Illinois, State Says*, and claimed that "the incident was a major new development in cybersecurity."[48] Other headlines likened the incident to a "Stuxnet strike" on U.S. soil, referring to the cyber-attack on an Iranian nuclear facility.[49] Media pundits, cybersecurity

---

44. Rodney Brown, *Cyber Bombs: Data-Security Sector Hopes Adoption Won't Require a 'Pearl Harbor' Moment*, INNOVATION REP. (Mass High Tech, Bos., Mass.), Oct. 26, 2011, at 10, 10, *available at* http://digital.masshightech.com/launch.aspx?referral=other&pnum=&refresh=6t0M1Sr380Rf&EID=1c256165-396b-454f-bc92-a7780169a876&skip=.

45. *Morning Edition*: *Cybersecurity Bill: Vital Need or Just More Rules?* (NPR, Mar. 22, 2012), *available at* http://www.npr.org/templates/transcript/transcript.php?storyId=149099866.

46. Joe Weiss, *Water System Hack - The System Is Broken*, CONTROLGLOBAL.COM (Nov. 17, 2011, 7:42 PM), http://community.controlglobal.com/content/water-system-hack-system-broken; *see also* Ellen Nakashima, *Overseas Hackers Hit Water Plant in Illinois, State Says*, WASH. POST, Nov. 19, 2011, at A3 (adding that the water plant failure occurred in Illinois).

47. Kim Zetter, *Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report*, WIRED THREAT LEVEL (Nov. 30, 2011, 5:54 PM), http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved [hereinafter *Comedy of Errors*]; Kim Zetter, *Confusion Center: Feds Now Say Hacker Didn't Destroy Water Pump*, WIRED THREAT LEVEL (Nov. 22, 2011, 8:12 PM), http://www.wired.com/threatlevel/2011/11/scada-hack-report-wrong [hereinafter *Confusion Center*].

48. Nakashima, *supra* note 46.

49. Mark Long, *Stuxnet Strike on U.S. Utility Signals Disturbing Trend*, NEWSFACTOR (Nov. 21, 2011, 2:20 PM), http://www.newsfactor.com/news/Stuxnet-Hit-on-Utility-Signals-New-Era/story.xhtml?story_id=111003TTUKBI&full_skip=1.

activists, and congressional lawmakers all quickly pounced on these reports as supposed proof of a serious threat.[50] Rep. Jim Langevin (D-RI), founder of the Congressional Cybersecurity Caucus and the sponsor of a bill that would expand regulation of private utilities, claimed that "[t]he potential attack that took place in Springfield, Illinois, should be a real wakeup call."[51]

Following a thorough investigation by the Department of Homeland Security and the Federal Bureau of Investigation, however, it turned out there was no Russian cyber-attack.[52] In fact, a plant contractor, who happened to have been travelling to Russia at the time, had simply logged on remotely to check the plant's systems.[53] His company had helped to create software and systems used to control the plant's equipment.[54] Moreover, the water pump failed for an electrical-mechanical reason unrelated to the consultant logging on from afar, and no serious disruption to service had occurred.[55]

2. Online Safety Threat Inflation

Threat inflation is also frequently on display in debates over online child safety.[56] Long before the rise of the Internet, threat inflation was a feature of debates about violent or sexual media content in the analog era.[57] Even recently, the titles and front covers of major books have decried the "home invasion" of "cultural terrorism,"[58] and pleaded with media creators to "stop teaching our kids to kill."[59]Again, no matter how distasteful

50. *Comedy of Errors*, *supra* note 47.

51. Jerry Brito, *Hackers Blow Up Illinois Water Utility . . . . or Not*, TIME TECHLAND (Nov. 28, 2011), http://techland.time.com/2011/11/28/hackers-blow-up-illinois-water-utility-or-not.

52. *Confusion Center*, *supra* note 47.

53. Ellen Nakashima, *Water-Pump Failure Wasn't Cyberattack*, WASH. POST, Nov. 26, 2011, at A6.

54. *Comedy of Errors*, *supra* note 47.

55. *Id.*

56. Adam Thierer, *Social Networking Websites & Child Protection*, PROGRESS SNAPSHOT (Progress & Freedom Found., D.C.), June 2006, *available at* http://www.pff.org/issues-pubs/ps/2006/ps_2.17_socialnet.pdf.

57. *See generally*, HEINS, *supra* note 19 (providing extensive survey of media impact on children).

58. REBECCA HAGELIN, HOME INVASION: PROTECTING YOUR FAMILY IN A CULTURE THAT'S GONE STARK RAVING MAD 3 (2005) (including on the cover "[s]afeguarding your family from cultural terrorism").

59. DAVE GROSSMAN & GLORIA DEGAETANO, STOP TEACHING OUR KIDS

any particular type of media content may be, no one's home is physically invaded, no violent terrorist acts are committed, and no one is killed by the depiction of violence in the media.

These rhetorical tactics have been adapted and extended as the Internet and digital technology have become ubiquitous. For example, as the Internet expanded quickly in the mid-1990s, a technopanic over online pornography developed just as quickly.[60] Unfortunately, the inflated rhetoric surrounding "the Great Cyberporn Panic of 1995"[61] turned out to be based on a single study with numerous methodological flaws.[62]

A now-famous July 1995 *Time* magazine cover story depicted a child with a horrified look on his face apparently looking at pornography on a computer screen, and the article spoke in panicked tones about "smut from cyberspace."[63] The *Time* story relied largely on a *Georgetown Law Journal* study conducted by Carnegie Mellon University researcher Martin Rimm. Rimm's study reported that 83.5% of online images were pornographic.[64] Congress soon passed the Communications Decency Act (CDA), which sought to ban indecent or obscene online content.[65] The Rimm study generated widespread attention and was instrumental in the legislative debate leading up to passage of the law.[66]

The study was ravaged by other researchers, however, and revealed to be mostly a publicity stunt by Rimm, who had a "history of involvement in media stunts and wild self-promotions."[67] "Unfortunately for all parties involved," noted Alice Marwick, "Rimm's results were found to be a combination of shoddy social science methodology, questionable research

---

TO KILL: A CALL TO ACTION AGAINST TV, MOVIE & VIDEO GAME VIOLENCE at iii (1999).

60. *Cf.* Robert Corn-Revere, *New Age Comstockery*, 4 COMMLAW CONSPECTUS 173, 183–84 (1996) (analyzing the application of the Communications Decency Act to the Internet).

61. MIKE GODWIN, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 259 (rev. & updated ed. 2003).

62. Marwick, *supra* note 5.

63. Philip Elmer-DeWitt, *On a Screen Near You: Cyberporn*, TIME, July 3, 1995 at 38.

64. Marwick, *supra* note 5.

65. *Id.*

66. *Id.*

67. JONATHAN WALLACE & MARK MANGAN, SEX, LAWS, AND CYBERSPACE 127 (1996).

ethics, and wishful extrapolation."[68] "Within weeks after its publication, the Rimm study had been thoroughly discredited," wrote Jonathan Wallace and Mark Mangan, "[b]ut the damage had already been done [since lawmakers] had waved the *Time* article around Congress [and] quoted Rimm's phony statistics."[69]

Similarly, a decade later, as social networking sites began growing in popularity in 2005–06, several state attorneys general and lawmakers began claiming that sites like MySpace and Facebook represented a "predators' playground," implying that youth could be groomed for abuse or abduction by visiting those sites.[70] Regulatory efforts were pursued to remedy this supposed threat, including a proposed federal ban on access to social networking sites in schools and libraries as well as mandatory online age verification, which was endorsed by many state attorneys general. These measures would have impacted a wide swath of online sites and services with interactive functionality.[71]

Unsurprisingly, the bill proposing a federal ban on social networks in schools and libraries was titled *Deleting Online Predators Act of 2006*.[72] In 2006, the measure received 410 votes in the U.S. House of Representatives before finally dying in the Senate.[73] The Bill was introduced in the following session of Congress, but did not see another floor vote and was never implemented.[74] During this same period, many states floated bills that also sought to restrict underage access to so-

---

68. Marwick, *supra* note 5.

69. WALLACE & MANGAN, *supra* note 67, at 151.

70. Emily Steel & Julia Angwin, *MySpace Receives More Pressure to Limit Children's Access to Site*, WALL ST. J., June 23, 2006, at B3.

71. Adam Thierer, *Would Your Favorite Website Be Banned by DOPA?*, TECH. LIBERATION FRONT (Mar. 10, 2007), http://techliberation.com/2007/03/10/would-your-favorite-website-be-banned-by-dopa [hereinafter *Banned by DOPA?*].

72. Deleting Online Predators Act, H.R. 5319, 109th Cong. (2006). *See also* Adam Thierer, *The Middleman Isn't the Problem*, PHILLY.COM (May 31, 2006), http://articles.philly.com/2006-05-31/news/25400396_1_web-sites-social-networking-block-access.

73. 152 CONG. REC. 16,231 (2006) (referring the bill to the Senate Committee on Commerce, Science, and Transportation); 152 CONG. REC. 16,040 (2006) (House vote).

74. 153 CONG. REC. 4,559 (2007) (introducing the bill into the House and referring it to the Committee on Energy and Commerce).

cial networking sites.[75] However, none of the underage access restrictions introduced with these bills were ultimately enacted as law.[76]

The fear appeal in this particular instance was:

- *Fearful Situation Premise*: Predators are out to get your kids, and they are lurking everywhere online.[77]
- *Conditional Premise*: If you allow kids to use social networking sites, predators could get to your kids and abuse them.[78]
- *Conclusion*: You should not allow your kids on social networking sites (and perhaps policymakers should consider restricting access to those sites by children).[79]

Again, this represented a logical fallacy. Despite the heightened sense of fear aroused by policymakers over this issue, it turned out that there was almost no basis for the predator panic.[80] It was based almost entirely on threat inflation. "As with other moral panics, the one concerning MySpace had more to do with perception than reality," concluded social media researcher danah michelle boyd.[81] Furthermore, she states, "As researchers began investigating the risks that teens faced in social network sites, it became clear that the myths and realities of risk were completely disconnected."[82]

Generally speaking, the fear about strangers abducting children online was always greatly overstated, since it is obvi-

---

75. S. 59, 149th Gen. Assemb., Reg. Sess. (Ga. 2007); S. 1682, 95th Gen. Assemb. (Ill. 2007); S. 132, 2007 Gen. Assemb., Reg. Sess. (N.C. 2007) (enacted).

76. The North Carolina bill, as enacted, no longer included the prior access-restriction language. *See* S. 132, 2007 Gen. Assemb., Reg. Sess. (N.C. 2007) (enacted).

77. *E.g.*, Melina Collison, *Internet Safety 101: Rules for Your Children When They Are Using the Internet*, EXAMINER.COM (Aug. 7, 2009), http://www.examiner.com/article/internet-safety-101-rules-for-your-children-when-they-are-using-the-internet.

78. *See, e.g.*, Deleting Online Predators Act, H.R. 5319, 109th Cong. (2006).

79. *See id.*

80. *See* danah michele boyd, Taken Out of Context: American Teen Sociality in Networked Publics 266 (2008) (unpublished Ph.D. dissertation, University of California, Berkeley) (on file with author), *available at* http://www.danah.org/papers/TakenOutOfContext.pdf.

81. *Id.*

82. *Id.*

ously impossible for abductors to directly "snatch" children by means of electronic communication. Abduction after Internet contact requires long-term, and usually long-distance, grooming and meticulous planning about how to commit the crime.[83] This is not to say there were no cases of abduction that involved Internet grooming, but such cases did not represent the epidemic that some suggested.[84]

A 2002 study conducted for the Department of Justice's Office of Juvenile Justice and Delinquency Prevention found that abductions by strangers "represent an extremely small portion of all missing children [incidents]."[85] Although the survey is a decade old and suffers from some data and methodological deficiencies, it remains the most comprehensive survey of missing and abducted children in the United States.[86] The study reported that the vast majority of abducted children were abducted by family members or someone acting on behalf of a family member.[87] Only 115 of the estimated 150,200 abductions—or less than a tenth of a percent—fit the stereotypical abduction scenario that parents most fear: complete strangers snatching children and transporting them miles away.[88] Lenore Skenazy, author of *Free-Range Kids: Giving Our Children the Freedom*

---

83. *Cf.* Samantha Craven et al., *Sexual Grooming of Children: Review of Literature and Theoretical Considerations*, 12 J. SEXUAL AGGRESSION 287, 289 (2006) (describing a study in which forty-five percent of a sample of convicted child sex offenders had employed sexual grooming behaviors, but also noting that this type of offender may be less likely to be reported, identified, and convicted than more aggressive offenders).

84. *Cf.* DANIEL GARDNER, THE SCIENCE OF FEAR: HOW THE CULTURE OF FEAR MANIPULATES YOUR BRAIN 185–86 (2009) (stating that earlier unfounded statistics estimated 50,000 to 75,000 children were kidnapped each year, when in fact, each year only about 115 "stereotypical kidnappings" [defined as "[a] stranger or slight acquaintance takes or detains a child for ransom or with the intention of keeping him or her, or kills the child"] occur in the United States).

85. ANDREA J. SEDLAK ET AL., OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, U.S. DEP'T OF JUSTICE, NATIONAL ESTIMATES OF MISSING CHILDREN: AN OVERVIEW 7 (2002), *available at* www.missingkids.com/en_US/documents/nismart2_overview.pdf.

86. *See* Justine Taylor et al., *An Examination of Media Accounts of Child Abductions in the United States*, JUST. POL'Y J., Fall 2011, at 1, 20.

87. *See* SEDLAK ET AL., *supra* note 85, at 7.

88. *Id.* A 2005 study of cases about missing children in Ohio revealed a similar trend. Of the 11,074 documented missing child cases in 2005, only five involved abduction by strangers compared with 146 abductions by family members. OH. MISSING CHILDREN CLEARINGHOUSE, 2005 ANNUAL REPORT 4 (2005).

We Had Without Going Nuts with Worry, puts things in perspective: "[T]he chances of any one American child being kidnapped and killed by a stranger are almost infinitesimally small: .00007 percent."[89] A May 2010 report by the Department of Justice confirmed that "family abduction [remains] the most prevalent form of child abduction in the United States."[90] These facts are not intended to trivialize the seriousness of abduction by family members or family acquaintances since it can be equally traumatic for the child and his or her family, but they make it clear that the panic over strangers using social networks to groom and abduct children was based on a faulty premise—stereotypical kidnappings, resulting from online grooming by sexual predators, are commonplace.

As with all other technopanics, the "predator panic" eventually ran its course, although some of the aforementioned fears remain in the public consciousness because they are driven by some of the factors outlined in Section III of this article. Section IV of this article also offers some possible explanations for why certain panics die out over time.

3. Online Privacy Threat Inflation

Privacy is a highly subjective[91] and an ever-changing con-

---

89. LENORE SKENAZY, FREE-RANGE KIDS: GIVING OUR CHILDREN THE FREEDOM WE HAD WITHOUT GOING NUTS WITH WORRY 16 (2009).

90. OFFICE OF JUVENILE JUSTICE AND DELINQUENCY PREVENTION, U.S. DEP'T OF JUSTICE, THE CRIME OF FAMILY ABDUCTION: A CHILD'S AND PARENT'S PERSPECTIVE at i (2010), *available at* https://www.ncjrs.gov/pdffiles1/ojjdp/229933.pdf.

91. Betsy Masiello, *Deconstructing the Privacy Experience*, IEEE SECURITY & PRIVACY, Jul.–Aug. 2009, at 70 ("On the social Web, privacy is a global and entirely subjective quality—we each perceive different threats to it."); Jim Harper, *Understanding Privacy—and the Real Threats to It*, *in* POL'Y ANALYSIS, at 1, 1 (Cato Inst., No. 520, 2004), *available at* http://www.cato.org/pubs/pas/pa520.pdf ("Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves."). *See also* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 77 (1998) ("When it comes to privacy, there are many inductive rules, but very few universally accepted axioms."); Larry Downes, *A Market Approach to Privacy Policy*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 509, 514 (Berin Szoka & Adam Marcus eds., 2011) ("In most conversations, no one knows what anyone else means by 'privacy,' or what information is included in the term 'personally-identifiable information."); MICHAEL FERTIK, COMMENTS OF REPUTATION.COM, INC. TO THE U.S. DEPARTMENT OF COMMERCE 13 (2011), *available at* http://www.reputationdefenderblog.com/wp-content/uploads/2011/01/Comments-of-Reputation.com-Inc-to-the-Department-

dition.[92] "Privacy, clearly, evokes an emotional, even visceral, response in most people, making it difficult if not impossible to talk about rationally," notes Larry Downes, author of *The Laws of Disruption*.[93]

Unsurprisingly, therefore, privacy-related concerns about new digital technologies and online services sometimes prompt extreme rhetorical flourishes.[94] For example, more tailored forms of online advertising, and the "tracking" technologies which make them possible, are coming under intense scrutiny today.[95] Some of these concerns are legitimate since online data leaks and breaches can result in serious economic harm to consumers.[96] Other fears are somewhat inflated, however, and can be attributed to a general unfamiliarity with how online advertising works and the role personal information and data collection play in the process.[97]

Some critics decry the "creepiness" factor associated with online data collection and targeted advertising.[98] While no clear

---

of-Commerce-20110128.pdf ("Privacy is a matter of taste and individual choice.").

92. *Cf.* HAL ABELSON ET AL., BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 68 (2008) ("The meaning of privacy has changed, and we do not have a good way of describing it. It is not the right to be left alone, because not even the most extreme measures will disconnect our digital selves from the rest of the world. It is not the right to keep our private information to ourselves, because the billions of atomic factoids don't any more lend themselves into binary classification, private or public.").

93. LARRY DOWNES, THE LAWS OF DISRUPTION 69 (2009).

94. Josh Constine, *Selling Digital Fear*, TECHCRUNCH (Apr. 7, 2012), http://techcrunch.com/2012/04/07/selling-digital-fear.

95. ADAM THIERER, MERCATUS CTR., PUBLIC INTEREST COMMENT ON FEDERAL TRADE COMMISSION REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 11 (2011), *available at* http://mercatus.org/sites/default/files/public-interest-comment-on-protecting-consumer-privacy-do-not-track-proceeding.pdf.

96. *See generally* FRED H. CATE, CTR. FOR INFO. POL'Y LEADERSHIP, INFORMATION SECURITY BREACHES AND THE THREAT TO CONSUMERS 6 (2005) (describing the costs to consumers of "identity-based fraud," a term that encompasses several of the most common misuses of personal information that is lost or stolen in a data breach).

97. THIERER, *supra* note 95, at 11.

98. *See, e.g.*, Mike Isaac, *New Google 'Transparency' Feature Aims to Reduce Ad-Targeting Creepiness*, WIRED GADGET LAB (Nov. 2, 2011, 3:27 PM), http://www.wired.com/gadgetlab/2011/11/google-ad-transparency-target; Miranda Miller, *Google+ vs. Facebook: More Passive Aggression & Creepiness in Tech Soap Opera*, SEARCH ENGINE WATCH (Nov. 9, 2011), http://searchenginewatch.com/article/2123660/Google-vs.-Facebook-More-

case of harm has been established related to "creepiness," some privacy advocates who oppose virtually any form of data collection have elevated this concern to near technopanic levels and are now demanding sweeping regulation of online business practices.[99] Even though stalking is generally understood to follow from an intent to harm or harass, the American Civil Liberties Union has likened Facebook's online tracking to "stalking."[100] Others predict even more dire outcomes, employing the rhetoric of a "privacy disaster."[101] Allusions to George Orwell's dystopian novel *1984* and "Big Brother" are quite common.[102] Variants include "Corporate Big Brother,"[103] "Big Brother Inc.,"[104] and "Big Browser."[105]

Comparisons are sometimes drawn with natural disasters or environmental catastrophes, such as a "privacy Chernobyl."[106] "The personal data collected by [online advertising] firms is like toxic waste," said Christopher Soghoian, then a fellow at the Open Society Institute, because "eventually, there will be an accident that will be impossible to clean up, leaving those whose data has spewed all over the Internet to bear the full costs of the breach."[107] Of course, in reality, data flows are nothing like Chernobyl or toxic waste since even the worst pri-

---

Passive-Aggression-Creepiness-in-Tech-Soap-Opera.

99. Adam Thierer, *Techno-Panic Cycles (and How the Latest Privacy Scare Fits In)*, TECH. LIBERATION FRONT (Feb. 24, 2011), http://techliberation.com/2011/02/24/techno-panic-cycles-and-how-the-latest-privacy-scare-fits-in.

100. *See* Chris Conley, *The Social Network is Stalking You*, BLOG RIGHTS (Nov. 16, 2011, 6:33 PM), http://www.aclu.org/blog/technology-and-liberty/social-network-stalking-you.

101. *See* Leslie Harris, *Preventing the Next Privacy Disaster*, HUFFINGTON POST (Oct. 15, 2008, 3:27 PM), http://www.huffingtonpost.com/leslie-harris/preventing-the-next-priva_b_134921.html.

102. *See e.g.*, Byron Acohido, *Yes, You Are Being Watched: Big Brother's Got Nothing On Today's Digital Sensors*, USA TODAY, Jan. 26, 2011, at 1B.

103. Monica Guzman, *Is Corporate 'Big Brother' Watching Your Blog?*, SEATTLE'S BIG BLOG (July 25, 2008), http://blog.seattlepi.com/thebigblog/2008/07/25/is-corporate-big-brother-watching-your-blog/.

104. SCOTT CLELAND & IRA BRODSKY, SEARCH & DESTROY: WHY YOU CAN'T TRUST GOOGLE INC. 48 (2011).

105. Nate Anderson, *Congress, Wary of Amazon's Silk Browser, Demands Answers on Privacy*, ARSTECHNICA (Oct. 14, 2011, 12:42 PM), http://arstechnica.com/tech-policy/news/2011/10/congress-wary-of-amazons-silk-browser-demands-answers-on-privacy.

106. Tim Black, *Are We Heading for 'a Privacy Chernobyl'?*, SPIKED (Mar. 15, 2010), http://www.spiked-online.com/index.php/site/article/8310.

107. Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy*?, WALL ST. J., Nov. 15, 2011, at B11.

vacy violations or data breaches pose no direct threat to life or health. Again, this is not to minimize the seriousness of data leakages since they can harm people both directly (e.g., through financial loss) or indirectly (e.g., through loss of privacy or reputation), but those harms do not usually approximate death or serious illness, as the inflated rhetoric implies.[108]

Similar rhetorical flourishes were heard during the brief technopanic over radio-frequency identification (RFID) technologies in the early 2000s. In the extreme, RFID was likened to the biblical threat of the "mark of the beast."[109] Legislative bills to regulate privacy-related aspects of RFID technology were introduced in several states, although none passed.[110] Fears about RFID were greatly exaggerated and the panic largely passed by the late 2000s.[111]

However, similar fears reappeared in the recent debate over wireless location-based services.[112] In Spring 2011, Apple and Google came under fire for retaining location data gleaned by iPhone- and Android-based smartphone devices.[113] But these "tracking" concerns were greatly overblown since almost all mobile devices must retain a certain amount of locational information to ensure various services work properly, and this data was not being shared with others.[114] Of course, if users are

---

108. *See generally* CATE, *supra* note 96.

109. *See* Mark Baard, *RFID: Sign of the (End) Times?* WIRED (June 6, 2006), http://www.wired.com/science/discoveries/news/2006/06/70308.

110. *See* Declan McCullagh, *Don't Regulate RFID—Yet*, CNET NEWS (Apr. 30, 2004, 4:00 AM), http://news.cnet.com/Don%27t%20regulate%20RFID--yet/2010-1039_3-5327719.html.

111. *See generally* Jerry Brito, *Relax, Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, 2004 UCLA J.L. & TECH. 5 (2004) (discussing how most fears concerning RFID use is exaggerated).

112. *See* Adam Thierer, *Apple, The iPhone And A Locational Privacy Techno-Panic*, FORBES (May 1, 2011, 5:43 PM), http://www.forbes.com/sites/adamthierer/2011/05/01/apple-the-iphone-and-a-locational-privacy-techno-panic.

113. *See* Kashmir Hill, *Apple and Google to Be the Whipping Boys for Location Privacy*, FORBES (Apr. 26, 2011, 12:32 PM), http://www.forbes.com/sites/kashmirhill/2011/04/26/apple-and-google-to-be-the-whipping-boys-for-location-privacy.

114. *Cf.* Brian X. Chen, *Why and How Apple Is Collecting Your iPhone Location Data*, WIRED GADGET LAB (Apr. 21, 2011, 5:44 PM), http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/ (explaining how and why Apple uses location data, but pointing out that there was no known reason to keep phones' entire location history in an unencrypted file on the device).

sensitive about locational privacy, they can always turn off locational tracking or encrypt and constantly delete their data. Most users probably won't want to go that far because doing so would also cripple useful features and applications.

4. Economic- and Business-Related Threat Inflation

The threat inflation and technopanic episodes documented above dealt mostly with social and cultural concerns. Economic- and business-related concerns also sometimes spawn panicky rhetorical flourishes. This is typically the case when large media or information technology firms propose a merger.[115] The panic in play here is that the expanded reach of modern media platforms will be used in a sinister way by various corporate actors.

For example, when the mega-merger between media giant Time Warner and then Internet superstar AOL was announced in early 2000, the marriage was greeted with a variety of apocalyptic predictions.[116] Syndicated columnist Norman Solomon, a longtime associate of the media watchdog group Fairness & Accuracy in Reporting, referred to the transaction in terms of "servitude," "ministries of propaganda," and "new totalitarianisms."[117] Similarly, University of Southern California Professor of Communications, Robert Scheer, wondered if the merger represented "Big Brother" and claimed, "AOL is the Levittown of the Internet," and "a Net nanny reigning [sic] in potentially restless souls."[118]

Such pessimistic predictions proved wildly overblown. To say that the merger failed to create the sort of synergies (and profits) that were anticipated would be an epic understatement.[119] By April 2002, just two years after the deal was

---

115. *See, e.g.*, Adam Thierer, *A Brief History of Media Merger Hysteria: From AOL-Time Warner to Comcast-NBC*, PROGRESS ON POINT (Progress & Freedom Found., D.C.), Dec. 2, 2009 [hereinafter *Media Merger Hysteria*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517288.

116. *See* Robert Scheer, *Confessions of an E-Columnist*, ONLINE JOURNALISM REV. (Jan. 26, 2002), http://www.ojr.org/ojr/workplace/1017966109.php; Norman Soloman, *AOL Time Warner: Calling The Faithful To Their Knees*, FAIR, http://www.fair.org/media-beat/000113.html (last updated Jan. 2005).

117. *See* Soloman, *supra* note 116.

118. *See* Scheer, *supra* note 116.

119. Looking back at the deal almost ten years later, AOL cofounder Steve Case said, "The synergy we hoped to have, the combination of two members of digital media, didn't happen as we had planned." Thomas Heath, *The Rising*

struck, AOL-Time Warner had already reported a staggering $54 billion one-time loss for "goodwill impairment" on the deal.[120] By January 2003, these losses had grown to $99 billion.[121] In September 2003, Time Warner decided to drop AOL from its name altogether, and the deal continued to unravel slowly from there.[122] Looking back at the deal, *Fortune* magazine senior editor-at-large Allan Sloan called it the "turkey of the decade."[123] Importantly, the divestitures and downsizing efforts that followed the deal's failure to meet its objectives garnered little attention compared with the hysteria that accompanied the announcement of the deal in 2000.[124]

The business dealings of News Corp. Chairman and CEO Rupert Murdoch have also prompted panicked rhetorical scorn at times. The popular blog *The Daily Kos* once likened him to "a fascist Hitler antichrist."[125] *CNN* founder Ted Turner once compared the popularity of the News Corp.'s Fox News Channel to the rise of Adolf Hitler prior to World War II.[126] As though he could cover both extremes of the ideological spectrum, Murdoch has not only been compared to Hitler, but he has also been accused of being a Marxist.[127] Meanwhile, Karl Frisch, a Senior Fellow at Media Matters for America, speaks

---

Titans of '98: Where are They Now?, WASH. POST, Nov. 30, 2009, at A15.

120. Frank Pellegrini, *What AOL Time Warner's $54 Billion Loss Means*, TIME BUSINESS (Apr. 25, 2002), http://www.time.com/time/business/article/0,8599,233436,00.html.

121. *See* Jim Hu, *AOL Loses Ted Turner and $99 Billion,* CNET NEWS (Jan. 30, 2004, 1:37 PM), http://news.cnet.com/AOL-loses-Ted-Turner-and-99-billion/2100-1023_3-982648.html.

122. Jim Hu, *AOL Time Warner Drops AOL from Name*, CNET NEWS (Sept. 18, 2003, 10:58 AM), http://news.cnet.com/AOL-Time-Warner-drops-AOL-from-name/2100-1025_3-5078688.html.

123. Allan Sloan, *'Cash for . . . ' and the Year's Other Clunkers*, WASH. POST, Nov. 17, 2009, at A25.

124. *See* Ben Compaine, *Domination Fantasies*, REASON, Jan. 2004, at 28 ("Break-ups and divestitures do not generally get front-page treatment . . . .").

125. jack23, *Rupert Murdoch is a Fascist Hitler Antichrist*, DAILYKOS (Sept. 7, 2009, 10:14 AM), www.dailykos.com/story/2009/9/7/778254/-Rupert-Murdoch-is-a-Fascist-Hitler-Antichrist.

126. Jim Finkle, *Turner Compares Fox's Popularity to Hitler*, BROAD. & CABLE (Jan. 25, 2005, 11:14 AM), http://www.broadcastingcable.com/CA499014.html.

127. *E.g.*, Ian Douglas, *Rupert Murdoch is a Marxist*, TELEGRAPH, http://blogs.telegraph.co.uk/technology/iandouglas/100004169/rupert-murdoch-is-a-marxist (last updated Nov. 9, 2009).

of Murdoch's "evil empire."[128]

These fears came to a head in 2003 when News Corp. announced it was pursuing a takeover of satellite television operator DirecTV. Paranoid predictions of a potential media apocalypse followed.[129] Jeff Chester of Center for Digital Democracy predicted that Murdoch would use this "Digital Death Star" "to force his programming on cable companies" and a long parade of other horrible actions.[130] Despite the extreme rhetoric, the rebels would get the best of Darth Murdoch since his "Digital Death Star" was abandoned just three years after construction.[131] In December 2006, News Corp. agreed to divest a 38.4 percent share in the company to Liberty Media Corporation.[132]

As with the unwinding of the AOL-Time Warner deal, in the reporting of the divestiture of DirecTV, "little mention was made of the previous round of pessimistic predictions or whether there had ever been any merit to the lugubrious lamentations of the critics."[133] The moral of the story seems to be clear that talk is cheap, and "[p]essimistic critics who use threat inflation to advance their causes are rarely held accountable when their panicky predictions fail to come to pass."[134]

---

128. Karl Frisch, *Fox Nation: The Seedy Underbelly of Rupert Murdoch's Evil Empire?*, MEDIA MATTERS FOR AM. (June 2, 2009, 6:15 PM), http://mediamatters.org/columns/200906020036.

129. Then Federal Communication Commission Commissioner Jonathan Adelstein worried that the deal would "result in unprecedented control over local and national media properties in one global media empire. Its shockwaves will undoubtedly recast our entire media landscape." Press Release, Johnathan S. Adelstein, Commissioner, Fed. Commc'ns Comm'n, Re: General Motors Corporation and Hughes Electronics Corporation, Transferors, and The News Corporation Limited, Transferee, MB Docket No. 03-124 (Jan. 14, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-330A6.doc. Later, he asserted, "With this unprecedented combination, News Corp. could be in a position to raise programming prices for consumers, harm competition in video programming and distribution markets nationwide, and decrease the diversity of media voices." *Id.*

130. Jeff Chester, *Rupert Murdoch's Digital Death Star*, ALTERNET (May 20, 2003), www.alternet.org/story/15949.

131. *See* Press Release, News Corp., News Corporation and Liberty Media Corporation Sign Share Exchange Agreement (Dec. 22, 2006) [hereinafter News Corp.], *available at* http://www.newscorp.com/news/news_322.html. *Cf.* Jill Goldsmith, *Murdoch Looks to Release Bird*, VARIETY (Sept. 14, 2006), http://www.variety.com/article/VR1117950090.html?categoryid=1236&cs=1 (stating that Murdoch referred to DirecTV as a "turd bird" before he sold it off).

132. *See* News Corp., *supra* note 131.

133. *Media Merger Hysteria*, *supra* note 115, at 5.

134. Adam Thierer, *Cybersecurity Threat Inflation Watch: Blood-Sucking*

III. REASONS PESSIMISM DOMINATES DISCUSSIONS ABOUT THE INTERNET AND INFORMATION TECHNOLOGY

There are many explanations for why we see and hear so much fear and loathing in information technology policy debates today.[135] At the most basic level, there exist many psychological explanations for why human beings are predisposed toward pessimism and are risk-averse.[136] For a variety of reasons, humans are poor judges of risks to themselves or those close to them.[137] Harvard University psychology professor Steven Pinker, author of *The Blank Slate: The Modern Denial of Human Nature*, notes:

> The mind is more comfortable in reckoning probabilities in terms of the relative frequency of remembered or imagined events. That can make recent and memorable events—a plane crash, a shark attack, an anthrax infection—loom larger in one's worry list than more frequent and boring events, such as the car crashes and ladder falls that get printed beneath the fold on page B14. And it can lead risk experts to speak one language and ordinary people to hear another.[138]

Going beyond this root-cause explanation, which many others have explored in far more detail,[139] this section considers six specific factors that contribute to the rise of technopanics and threat inflation in the information technology sector. Importantly, however, each of these particular explanations builds on previous insight: Survival instincts combined with poor comparative risk analysis skills lead many people to engage in, or buy into, technopanic.[140]

Weapons!, TECH. LIBERATION FRONT (Mar. 22, 2012), http://techliberation.com/2012/03/22/cybersecurity-threat-inflation-watch-blood-sucking-weapons.

135. *See, e.g.*, GARDNER, *supra* note 84; MICHAEL SHERMER, THE BELIEVING BRAIN: FROM GHOSTS AND GODS TO POLITICS AND CONSPIRACIES—HOW WE CONSTRUCT BELIEFS AND REINFORCE THEM AS TRUTHS 274–75 (2011); BRUCE SCHNEIER, LIARS & OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE 203 (2012).

136. *See* SHERMER, *supra* note 135, at 275 ("*Negativity bias*: the tendency to pay closer attention and give more weight to negative events, beliefs, and information than to positive."). *See generally* GARDNER, *supra* note 84.

137. *See* GARDNER, *supra* note 84, at 10.

138. STEVEN PINKER, THE BLANK SLATE: THE MODERN DENIAL OF HUMAN NATURE 232 (2002).

139. *See id.*; GARDNER, *supra* note 84; SHERMER, *supra* note 135; SCHNEIER, *supra* note 135.

140. *See* GARDNER, *supra* note 84, at 89–101.

A. GENERATIONAL DIFFERENCES

Generational differences certainly account for a large part of the pessimism at work in debates over the impact of technology on culture and society. Parents and policymakers often suffer from what Dr. David Finkelhor, Director of the University of New Hampshire's Crimes Against Children Research Center (CCRC), calls "juvenoia," or "the exaggerated anxiety about the influence of social change on children and youth."[141] George Mason University economist Tyler Cowen has noted:

> Parents, who are entrusted with human lives of their own making, bring their dearest feelings, years of time, and many thousands of dollars to their childrearing efforts. They will react with extreme vigor against forces that counteract such an important part of their life program. The very same individuals tend to adopt cultural optimism when they are young, and cultural pessimism once they have children. Parents often do not understand the new generation of cultural products and therefore see little or no benefit in their children's interest in them.[142]

Additionally, "many historians, psychologists, sociologists, and other scholars have documented this seemingly never-ending cycle of generational clashes."[143] Parents and policymakers sometimes fail to remember that they too were once kids and managed to live with the media and popular culture about which the same fears were expressed.[144] The late University of North Carolina journalism professor Margaret A. Blanchard once remarked:

> [P]arents and grandparents who lead the efforts to cleanse today's society seem to forget that they survived alleged attacks on their morals by different media when they were children. Each generation's adults either lose faith in the ability of their young people to do the same or they become convinced that the dangers facing the new generation are much more substantial than the ones they faced as children.[145]

---

141. Dr. David Finkelhor, Presentation at the University of New Hampshire, Crimes Against Children Research Center, Justice Studies Colloquium: The Internet, Youth Deviance and the Problem of Juvenoia, (Oct. 22, 2010) (video available at http://www.vimeo.com/16900027).

142. TYLER COWEN, IN PRAISE OF COMMERCIAL CULTURE 185 (1998).

143. Adam Thierer, *Why Do We Always Sell the Next Generation Short?*, FORBES (Jan. 8, 2012), http://www.forbes.com/sites/adamthierer/2012/01/08/why-do-we-always-sell-the-next-generation-short.

144. *Cf.* BRADFORD W. WRIGHT, COMIC BOOK NATION: THE TRANSFORMATION OF YOUTH CULTURE IN AMERICA 87 (2001) ("Throughout American history, adults have attributed undesirable changes in youth behavior to some aspect of popular culture.").

145. Margaret A. Blanchard, *The American Urge to Censor: Freedom of Expression Versus the Desire to Sanitize Society—From Anthony Comstock to 2*

Similarly, Thomas Hine, author of *The Rise and Fall of the American Teenager*, argues, "We seem to have moved, without skipping a beat, from blaming our parents for the ills of society to blaming our children . . . . We want them to embody virtues we only rarely practice. We want them to eschew habits we've never managed to break."[146]

This reoccurring phenomenon was captured nicely by cartoonist Bill Mauldin in a 1950 edition of *Life* magazine.[147] His cartoon, which featured an older gentleman looking suspiciously at a middle-aged man who, in turn, stares in puzzlement at a young boy, included the caption, "Every Generation Has Its Doubts about the Younger Generation."[148] Mauldin, who was 28 at the time, penned an accompanying essay defending his World War II-era generation against attacks for "lacking some of the good old American gambling spirit and enterprise."[149] Of course, this was the same generation of youngsters that Tom Brokaw would eventually label "The Greatest Generation!"[150]

A more measured, balanced approach seems prudent since generational fears based on all-or-nothing extremes are rarely good bases for policy. In particular, as discussed in Section V, fear mongering and technopanics could have unintended consequences.[151] "Fear, in many cases, is leading to overreaction, which in turn could give rise to greater problems as young people take detours around the roadblocks we think we are erecting," argue Harvard University law professors John Palfrey and Urs Gasser, authors of *Born Digital: Understanding the First Generation of Digital Natives*.[152] What parents, guardians, and educators should understand, they assert, "is that the traditional values and common sense that have served them well in the past will be relevant in this new world, too."[153] Thus, while it is certainly true, as Karen Sternheimer notes, that

---

Live Crew, 33 WM.& MARY L. REV. 741, 743 (1992).

146. Nancy Gibbs, *Being 13*, TIME, Aug. 8, 2005, at 43.

147. *See* Bill Maudlin, *The Care & Handling of a Heritage*, LIFE, Jan. 2, 1950, at 100.

148. *Id.*

149. *Id.* at 96.

150. *See* TOM BROKAW, THE GREATEST GENERATION (1998).

151. *E.g.*, *Safeguarding Against Technopanics*, *supra* note 2, at 16.

152. JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 9 (2008).

153. *Id.* at 10.

"new technologies elicit fears of the unknown, particularly because they have enabled children's consumption of popular culture to move beyond adult control," it doesn't follow that prohibition or anticipatory regulation is the best response.[154] Section VII will consider alternative approaches.

B. HYPER-NOSTALGIA, PESSIMISTIC BIAS, AND SOFT LUDDITISM

Many of the generational differences discussed above are driven by hyper-nostalgia. Excessive nostalgia can help explain skepticism about many forms of technological change. It can even result in calls for restrictions on technology.

In a 1777 essay, the Scottish philosopher and economist David Hume observed, "The humour of blaming the present, and admiring the past, is strongly rooted in human nature, and has an influence even on persons endued with the profoundest judgment and most extensive learning."[155] Michael Shermer, author of *The Believing Brain*, refers to "the tendency to remember past events as being more positive than they actually were" as the "rosy retrospection bias."[156]

What is ironic about such nostalgia is that it is rooted in something typically unknown by the proponent. The poet Susan Stewart argues that "[n]ostalgia is a sadness without an object, a sadness which creates a longing that of necessity [which] is inauthentic because it does not take part in lived experience. Rather, it remains behind and before that experience."[157] Too often, Stewart observes, "nostalgia wears a distinctly utopian face" and becomes a "social disease."[158]

While referring to nostalgia as a "disease" is a bit hyperbolic, it is clear that a great deal of nostalgia haunts debates about technological change—especially with reference to the impact of change on children.[159] "The idea that childhood in the past was comprised of carefree days without worry is a conveniently reconstructed version of history," observes Sternheimer, and,

---

154. KAREN STERNHEIMER, IT'S NOT THE MEDIA: THE TRUTH ABOUT POP CULTURE'S INFLUENCE ON CHILDREN 38 (2003).

155. DAVID HUME, *Of the Populousness of Ancient Nations*, *in* DAVID HUME, ESSAYS MORAL, POLITICAL, LITERARY 377, 464 (Eugene F. Miller ed., rev. ed. 1987).

156. SHERMER, *supra* note 135, at 275.

157. SUSAN STEWART, ON LONGING: NARRATIVES OF THE MINIATURE, THE GIGANTIC, THE SOUVENIR, THE COLLECTION 23 (1984).

158. *Id.*

159. *Id.*

"[t]his fantasy allows adults to feel nostalgia for a lost idealized past that never was."[160]

The psychological explanation for this is relatively straightforward: People are generally more comfortable with what they know relative to that with which they are unfamiliar. Consequently, the natural instinct of many when presented with new technological developments or forms of media and culture, especially when they are older and more set in their ways, is initially to shun them, or at least to be somewhat suspicious of them.[161]

Many critics fear how technological evolution challenges the old order, traditional values, settled norms, traditional business models, and existing institutions—even as the standard of living generally improves with each passing generation.[162] Stated differently, by its nature, technology disrupts settled matters. "[T]he shock of the new often brings out critics eager to warn us away," notes Dennis Baron.[163] Occasionally, this marriage of distaste for the new and a longing for the past (often referred to as a "simpler time" or "the good old days") yields the sort of moral panics or technopanics discussed above. In particular, cultural critics and advocacy groups can benefit from the use of nostalgia by playing into, or stirring up, fears that we've lost a better time, and then suggesting steps that can and should be taken to help us return to that time.[164]

Again, this tendency is particularly powerful as it relates to children and their upbringing. "Fear that popular culture has a negative impact on youth is nothing new: it is a recurring theme in history," observes Sternheimer.[165] He further states,

---

160. STERNHEIMER, *supra* note 154, at 26. Sternheimer goes on to note, "We often overlook the realities of childhood past and present that defy the assumption that childhood without electronic media was idyllic . . . . So while we mourn the early demise of childhood, the reality is that for many Americans childhood has never lasted *longer*." *Id.* at 32–34.

161. *See* MATT RIDLEY, THE RATIONAL OPTIMIST: HOW PROSPERITY EVOLVES 292 (2010).

162. *See generally* Adam Thierer, *10 Things Our Kids Will Never Worry About Thanks to the Information Revolution*, FORBES (Dec. 18, 2011), http://www.forbes.com/sites/adamthierer/2011/12/18/10-things-our-kids-will-never-worry-about-thanks-to-the-information-revolution.

163. DENNIS BARON, A BETTER PENCIL: READERS, WRITERS, AND THE DIGITAL REVOLUTION 12 (2009).

164. Adam Thierer, *On Nostalgia*, TECH. LIBERATION FRONT (Dec. 28, 2011), http://techliberation.com/2011/12/28/on-nostalgia/.

165. STERNHEIMER, *supra* note 154, at 7.

"Like our predecessors we are afraid of change, of popular culture we don't like or understand, and of a shifting world that at times feels out of control."[166] In this way, generational fears and hyper-nostalgia are closely linked. "There has probably never been a generation since the Paleolithic that did not deplore the fecklessness of the next and worship a golden memory of the past," notes British journalist Matt Ridley.[167]

Economic policy debates are also riddled with hyper-nostalgia. Bryan Caplan, a George Mason University economist and the author of *Myth of the Rational Voter*, has documented the existence of a general "pessimistic bias" among many voters, or "a tendency to overestimate the severity of economic problems and underestimate the (recent) past, present, and future performance of the economy."[168] Much of this is rooted in nostalgia about a supposed golden age of a particular industry or an affinity for certain of types of technology or business models and methods.

C. BAD NEWS SELLS: THE ROLE OF THE MEDIA, ADVOCATES, AND THE LISTENER

"The most obvious reason that doomsday fears get disproportionate public attention is that bad news is newsworthy, and frightening forecasts cause people to sit up and take notice," Julian Simon astutely observed in 1996.[169] That is equally true today.[170] Many media outlets and sensationalist authors sometimes use fear-based rhetorical devices to gain influence or sell books. "Opportunists will take advantage of this fear for personal and institutional gain," notes University of Colorado Law School professor Paul Ohm.[171]

Fear mongering and prophecies of doom have always been with us, since they represent easy ways to attract attention and

---

166. *Id.* at 8.

167. RIDLEY, *supra* note 161, at 292.

168. BRYAN CAPLAN, MYTH OF THE RATIONAL VOTER: WHY DEMOCRACIES CHOOSE BAD POLICIES 44 (2007).

169. JULIAN L. SIMON, THE ULTIMATE RESOURCE 539–40 (1996). *See also id.* at 583 ("It is easier to get people's attention [and television time and printer's ink] with frightening forecasts than with soothing forecasts.").

170. *Cf.* CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 102 (2005) ("Many perceived 'epidemics' are in reality no such thing, but instead the product of media coverage of gripping, unrepresentative incidents.").

171. Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1401 (2008).

get heard. "Pessimism has always been big box office," notes Ridley.[172] It should not be surprising, therefore, that sensationalism and alarmism are used as media differentiation tactics.[173] This is particularly true as it relates to children and online safety.[174] "Unbalanced headlines and confusion have contributed to the climate of anxiety that surrounds public discourse on children's use of new technology," argues Professor Sonia Livingstone of the London School Economics.[175] Therefore, "[p]anic and fear often drown out evidence."[176] Few journalists are willing to buck this trend and present evidence in a dispassionate, balanced fashion.[177]

Sadly, most of us are eager listeners and lap up bad news, even when it is overhyped, exaggerated, or misreported. Shermer notes that psychologists have identified this phenomenon as "negativity bias," or "the tendency to pay closer attention and give more weight to negative events, beliefs, and information than to positive."[178] Negativity bias, which is closely related to the phenomenon of "pessimistic bias" discussed above, is frequently on display in debates over online child safety, digital privacy, and cybersecurity.

D. THE ROLE OF SPECIAL INTERESTS AND INDUSTRY INFIGHTING

Plenty of groups and institutions benefit from peddling bad

---

172. RIDLEY, *supra* note 161, at 294.

173. *See* GARDNER, *supra* note 84, at 165 ("Like corporations, politicians, and activists, the media profit from fear. Fear means more newspapers sold and higher ratings, so the dramatic, the frightening, the emotional, and the worst case are brought to the fore while anything that would suggest the truth is not so exciting and alarming is played down or ignored entirely.").

174. KAREN STERNHEIMER, KIDS THESE DAYS: FACTS AND FICTIONS ABOUT TODAY'S YOUTH 152 (2006) [hereinafter KIDS THESE DAYS] ("On a very basic level, the news media also benefit by telling us emotional stories about the trouble that kids may find themselves in . . . . Bad news about kids encapsulates our fears for the future, gives them a face and a presence, and seems to suggest a solution.").

175. Michael Burns, *UK a 'High Use, Some Risk' Country for Kids on the Web*, COMPUTERWORLD (Oct. 18, 2011), http://news.idg.no/cw/art.cfm?id=F3254BA7-1A64-67EA-E4D5798142643CEF.

176. *Id.*

177. *See, e.g.*, Larry Magid, *Putting Techno-Panics into Perspective*, MERCURY NEWS (July 13, 2012), http://www.larrysworld.com/2012/07/13/putting-technopanic-into-perspective.

178. *See* SHERMER, *supra* note 135, at 275.

news.[179] Many advocacy groups have heartfelt concern about the impact of specific types of technological change. All too often, however, they exaggerate fears and agitate for action because they benefit from it either by directly getting more resources from government, the public, and other benefactors, or indirectly from the glow of publicity that their alarmism generates. Sternheimer notes:

> [A]ctivist groups and nonprofit organizations work to raise awareness and funds for their cause. In the process they may exaggerate the extent of the problem or encourage the public to believe that the problem is growing. . . . While no one disputes the good intentions most of these organizations have, the organizations also have a vested interest in making specific problems seem as scary as possible.[180]

In their work on moral panic theory, Goode and Ben-Yehuda discuss the importance of "moral entrepreneur[s]," who are crusaders that believe something must be done about a wrongdoing and "take steps to make sure that certain rules are enforced."[181] Thus, some institutions structure their operations to perpetuate fears about behaviors or content they believe is immoral, unhealthy, or unsafe. Once such an institutional arrangement is given life, it tends to be self-perpetuating and constantly seeks out new threats—possibly even inflating them in the process—in order to ensure they continue to have a *raison d'être.*[182]

For example, the National Center for Missing & Exploited Children (NCMEC) is a nonprofit entity established by Congress in 1984 that works to prevent the sexual abuse of children.[183] NCMEC's mission is important, and it has provided a vital public service by helping to prevent child abuse and solve

---

179. *See* GARDNER, *supra* note 84, at 165.

180. STERNHEIMER, *supra* note 174, at 151–52.

181. GOODE & BEN-YEHUDA, *supra* note 32, at 160.

182. *See* GARDNER, *supra* note 84, at 150 ("[T]here is really only one way to grab the attention of distracted editors and reporters: Dispense with earnest, thoughtful, balanced, well-researched work and turn the message into a big, scary headline."); SCHNEIER, *supra* note 135, at 201 ("These institutions [police and other law-enforcement bodies] have been delegated responsibility for implementing institutional pressure on behalf of society as a whole, but because their interests are different, they end up implementing security at a greater or lesser level than society would have. Exaggerating the threat, and oversecuring—or at least over-spending—as a result of that exaggeration, is by far the most common outcome.").

183. *Mission and History,* NAT'L CENTER FOR MISSING & EXPLOITED CHILD., http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362 (last visited Sept.18, 2012).

missing children cases. Unfortunately, however, the organization also has a built-in incentive to inflate certain perceived threats since their revenue from both private, and especially public, sources grow as the threats they identify increase.[184] Research by *The Wall Street Journal* statistics columnist Carl Bialik suggests that NCMEC has misused or misreported certain data, including repeatedly asserting that the Internet child porn trade was a business worth $20 billion annually even though the NCMEC could muster no evidence to support the claim.[185] Bialik also showed how NCMEC was inflating data about how many children had been sexually solicited online.[186]

Corporate actors also sometimes benefit from excessive fear mongering.[187] Simply put, fear sells.[188] The economist Bruce Yandle coined the phrase "baptists and bootleggers" to explain the phenomenon of interests with diverging views banding together to advance a regulatory cause, often by using fear tactics.[189] In the context of social regulation, companies occasionally employ fear tactics to increase their visibility and potential to sell goods and services that will supposedly eradicate the supposed threat to society they have identified.[190] For example, many companies produce tools that help people protect their privacy and security as well as their children's online safety.[191] Most of them deserve praise for those innovations.

---

184. *See* Berin Szoka, *If NCMEC's Going to Regulate the Internet for Child Porn, It Should At Least Be Subject to FOIA*, TECH. LIBERATION FRONT (Aug. 9, 2009), http://techliberation.com/2009/08/09/if-ncmec%E2%80%99s-going-to-regulate-the-internet-for-child-porn-it-should-at-least-be-subject-to-foia; Carl Bialik, *Online Warnings Mean Well, but the Numbers Don't Add Up*,WALL ST. J. (Jan. 21, 2005), http://online.wsj.com/public/article/SB110617073758830511-2aJjGHdzDxeGmQglegoKJ9IXwig_20071216.html; Carl Bialik, *Measuring the Child-Porn Trade*, WALL ST. J. (Apr. 18, 2006), http://online.wsj.com/article/SB114485422875624000.html [hereinafter *Child-Porn Trade*].

185. Carl Bialik, *Measuring the Child-Porn Trade*, WALL ST. J. (Apr. 18, 2006), http://online.wsj.com/article/SB114485422875624000.html.

186. *Child-Porn Trade*, *supra* note 184.

187. *See* GARDNER, *supra* note 84, at 14.

188. *Id.* at 13–14 ("Fear sells. Fear makes money. The countless companies and consultants in the business of protecting the fearful from whatever they may fear know it only too well. The more fear, the better the sales.").

189. *See* Bruce Yandle, *Bootleggers and Baptists: The Education of a Regulatory Economist*, AEI J. ON GOV'T & SOC'Y REGULATION, May–June 1983, at 13.

190. *See* GARDNER, *supra* note 84, at 14.

191. *See id.*

Unfortunately, a handful of these vendors occasionally overhype various online concerns and then also overplay the benefits of their particular tool as a silver-bullet solution to those supposed pathologies.[192] Again, bad news sells and, in this case, it sells products and services to fearful citizens. "The opportunities for finding a fear, promoting it, and leveraging it to increase sales are limited only by imagination," notes Daniel Gardner, author of *The Science of Fear*.[193]

For example, when the "stranger danger" and "predator panic" over social networking sites first erupted, some vendors of age-verification technologies attempted to get various lawmakers to mandate the use of their verification technologies,[194] even as doubts were being raised about their effectiveness.[195] These entities clearly stood to benefit from any law or regulation that encouraged or mandated the use of age verification technologies.

Other special interests fire up fears and use threat inflation in an attempt to obtain government contracts.[196] These special interests are also involved in debates over both cybersecurity and child safety. Brito and Watkins argue that "a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War."[197] Similarly, Susan Crawford, a former White House senior advisor on technology policy matters, has noted that "cyberwar hysteria aids consultants" by prompting a cybersecurity bill which if passed "would certainly create work" for many organizations surrounding the D.C. beltway.[198] According to *The Economist* magazine, Stefan Sav-

---

192. KIDS THESE DAYS, *supra* note 174, at 141 ("Business tends to thrive on our notion that we can reduce our anxiety by purchasing its products. Youth phobia is a burgeoning industry, with a variety of products and services geared to address our fears of and fears for young people.").

193. *Id.* at 128.

194. *See* Chris Soghoian, *State Attorneys General Push Online Child Safety Snake Oil*, CNET NEWS (Sept. 24, 2008), http://news.cnet.com/8301-13739_3-10048583-46.html.

195. *See* INTERNET SAFETY TECHNICAL TASK FORCE, BERKMAN CTR. FOR INTERNET AND SAFETY, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES: FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE TO THE MULTI-STATE WORKING GROUP ON SOCIAL NETWORKING OF STATE ATTORNEYS GENERAL OF THE UNITED STATES 10 (2008); Adam Thierer, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, PROGRESS ON POINT (Progress & Freedom Found., D.C.), Mar. 2007, at 14–15.

196. *See* GARDNER, *supra* note 84, at 14.

197. Brito & Watkins, *supra* note 39, at 1.

198. Susan Crawford, *Cyberwar Hysteria Aids Consultants, Hurts U.S.*,

age, a Professor in the Department of Computer Science and Engineering at the University of California, San Diego, says the "security industry sometimes plays 'fast and loose' with the numbers, because it has an interest in 'telling people that the sky is falling.'"[199]

Similarly, in online safety debates, many organizations petition federal, state, and local lawmakers for grants to fund tools or educational curricula they have developed to address these fears.[200]

This sort of corporate fear mongering creates an imbalance of pessimistic perspectives in public policy debates. In essence, a perverse incentive exists for organizations and corporations to tell "bad news stories" to policymakers and the public without reference to the potential long-term gains, or without the broader benefits of technological change ever being taken into account.[201] The late Julian Simon, who was a Senior Fellow at the Cato Institute, noted how this phenomenon was also at work in the context of environmental resource discussions, writing, "There are often special-interest groups that alert us to impending shortages of particular resources such as timber or clean air. But no one has the same stake in trying to convince us that the long-run prospects for a resource are better than we think."[202]

Fear-based tactics are also occasionally employed in economic policy debates. When it suits their interests, corporations and advocacy groups will play up the potential dangers of other sectors or technologies if for no other reason than to divert attention from themselves.[203] Better yet, from their perspective, is the potential for their competitors to be burdened with regulation that might constrain their efforts to innovate, expand,

---

BLOOMBERG (July 24, 2011), http://www.bloomberg.com/news/2011-07-25/cyberwar-hysteria-aids-consultants-hurts-u-s-susan-crawford.html.

199. *Measuring the Black Web: Is Cybercrime As Big As Its Foes Fear?*, ECONOMIST, Oct., 15, 2011, at 69.

200. *See* Nancy Willard, *My Review of I-Safe*, NANCY WILLARD'S WEBLOG (Mar. 13, 2008), http://csriu.wordpress.com/2008/03/13/my-review-of-i-safe.

201. PAUL DRAGOS ALIGICA, PROPHECIES OF DOOM AND SCENARIOS OF PROGRESS: HERMAN KAHN, JULIAN SIMON, AND THE PROSPECTIVE IMAGINATION 20 (2007).

202. SIMON, *supra* note 169, at 583.

203. *See* Adam Thierer, *The Sad State of Cyber-Politics*, CATO POL'Y REP., Nov.–Dec. 2010, at 6–8 [hereinafter *Cyber-Politics*].

and compete.[204] Unfortunately, when companies and other interests employ such tactics, it merely raises the general level of anxiety about information technology and the Internet more broadly.

For example, Microsoft and Google were involved in finger pointing. For years, Google and various other Silicon Valley actors tag-teamed to encourage greater government interest in Microsoft and its supposed market power in the operating systems and web browser sectors.[205] In fact, "Google hammered Microsoft in countless legal and political proceedings here and abroad."[206] But the tables turned in recent years, and Microsoft is now the ringleader of the rising political war against Google.[207] Today, Microsoft "is using against Google the same antitrust playbook" others "once used against it."[208] Whether it is the legal battle over Google Books, Department of Justice reviews of various Google acquisitions, or other policy fights both here and in other countries, Microsoft now hounds Google at every turn.[209] The end result of these Microsoft-Google squabbles has been elevated political and regulatory concern of *all* segments of the market that these companies serve.[210]

Of course, companies seeking to wield the power of government to humble their competitors or gain competitive advantage is nothing new.[211] Long ago, Nobel Prize-winning economist Milton Friedman warned of "the business community's suicidal impulse," or the persistent propensity to persecute one's competitors using regulation or the threat thereof.[212] We have another term for it today: crony capitalism.[213] Again, the result is simply more fear and loathing about all the players

---

204. *See id.*

205. *See id.* at 6.

206. *Id.*; *see also* Alexei Oreskovic & David Lawsky, *Google Joins EU Antitrust Case Against Microsoft*, WIRED (Feb. 25, 2009), http://www.wired.com/techbiz/media/news/2009/02/reuters_us_google_microsoft.

207. *Cyber-Politics*, *supra* note 203, at 6–7.

208. *Id.* at 7.

209. *See* Jason Kincaid, *Microsoft Tells Google to Face the Antitrust Music*, TECHCRUNCH (Feb. 26, 2010), http://techcrunch.com/2010/02/26/microsoft-google-antitrust.

210. *Cyber-Politics*, *supra* note 203, at 7.

211. Milton Friedman, *The Business Community's Suicidal Impulse*, CATO POLICY REPORT, Mar.–Apr. 1999, at 6–7.

212. *Id.*

213. MATTHEW MITCHELL, THE PATHOLOGY OF PRIVILEGE: THE ECONOMIC CONSEQUENCES OF GOVERNMENT FAVORITISM 24 (2012).

and sectors involved, as well as their technologies or platforms.[214]

E. ELITIST ATTITUDES AMONG ACADEMICS AND INTELLECTUALS

Academic skeptics and cultural critics often possess elitist attitudes about the technologies, platforms, or new types of media content that the masses or young adopt before they do. These elitist views are often premised on the "juvenoia" and hyper-nostalgic thinking described above.

This is not unique to the field of information technology, of course. Paul Dragos Aligica of the Mercatus Center notes that in battles over environmental and natural resource policy "many have a sense of intellectual superiority. The better educated believe that they understand what is best for the less educated, in other words, that they know how some others should live their lives."[215] This observation is even more pertinent when the debate shifts to the impact of new technology on culture and learning, issues which are frequently in play in various Internet policy debates.

In his 1995 book *The Vision of the Anointed: Self-Congratulation as a Basis for Social Policy*, Thomas Sowell formulated a model of ideological crusades to expand government power over our lives and economy.[216] "The great ideological crusades of the twentieth-century intellectuals have ranged across the most disparate fields," noted Sowell.[217] What they all had in common, he argued, was "their moral exaltation of the anointed above others, who are to have their different views nullified and superseded by the views of the anointed, imposed via the power of government."[218] These government-expanding crusades shared several key elements which Sowell identified as:

> 1. Assertions of a great danger to the whole society, a danger to which the masses of people are oblivious.

---

214. *See id.* at 29–30.

215. ALIGICA, *supra* note 201, at 20.

216. THOMAS SOWELL, THE VISION OF THE ANOINTED: SELF-CONGRATULATION AS A BASIS FOR SOCIAL POLICY 5 (1995).

217. *Id.*

218. *Id. See also id.* at 123 ("To those with the vision of the anointed, the public serves not only as a general object of disdain, but as a baseline from which to measure their own lofty heights, whether in art, politics, or other fields.").

> 2. An urgent need for government action to avert impending catastrophe.
>
> 3. A need for government to drastically curtail the dangerous behavior of the many, in response to the prescient conclusions of the few.
>
> 4. A disdainful dismissal of arguments to the contrary as uninformed, irresponsible, or motivated by unworthy purposes.[219]

This model can be used in efforts to reshape the Internet economy, or to curb the direction of online culture and speech. Importantly, it is also in the best interest of academics and pundits to propagate such fears and elitist attitudes in an attempt to gain more prominence within their academic circles, in public policy debates, and among press contacts. "Research almost always has ideological foundations," Sternheimer writes, "[i]f not that of the researchers themselves, who want to demonstrate that funding their work is important, then that of the groups that fund the research."[220] The role researchers play in exacerbating technopanics is discussed further in the Section IV.

F. THE ROLE OF "THIRD-PERSON-EFFECT HYPOTHESIS"

A phenomenon that psychologists refer to as the "third-person effect hypothesis" can help explain many technopanics and resulting calls for government intervention, especially as they relate to media policy and free speech issues.[221] More specifically, this phenomenon occurs when many critics "seem to see and hear in media or communications only what they want to see and hear—or what they *don't* want to see or hear."[222] When such critics encounter perspectives or preferences that "are at odds with their own, they are more likely to be concerned about the impact of those [things] on others throughout society."[223] This leads them "to believe that government must "do something" to correct those [perspectives]."[224] In fact, *"[m]any people desire control of culture or technology because they think it will be good for others, not necessarily for them-*

---

219. *See id.* at 5.

220. KIDS THESE DAYS, *supra* note 174, at 152. *See also id.* ("Science is an attempt to get closer to understanding our world, but it is often based on preconceptions about the way the world works.").

221. *See* ADAM THIERER, MEDIA MYTHS: MAKING SENSE OF THE DEBATE OVER MEDIA OWNERSHIP 119–23 (2005).

222. *Id.* at 14.

223. *Id.*

224. *Id.*

selves."[225] The control they desire often has a very specific purpose in mind: "re-tilting" cultural or market behavior or outcomes in their desired direction.

Several of the factors identified above validate a theory known as the "third-person effect hypothesis."[226] The third-person effect hypothesis was first formulated by Columbia Journalism School professor W. Phillips Davison in a seminal 1983 article:

> In its broadest formulation, this hypothesis predicts that people will tend to overestimate the influence that mass communications have on the attitudes and behavior of others. More specifically, individuals who are members of an audience that is exposed to a persuasive communication (whether or not this communication is intended to be persuasive) will expect the communication to have a greater effect on others than on themselves.[227]

Davison used this hypothesis to explain how media critics on both the left and right seemed simultaneously to find "bias" in the same content or reports.[228] In reality, their own personal preferences were biasing their ability to evaluate that content fairly.[229] Davison's article prompted further research by many other psychologists, social scientists, and public opinion experts to test just how powerful this phenomenon was in explaining calls for censorship and other social phenomena.[230] In these studies, the third-person effect has been shown to be the primary explanation for why many people fear—or even want to ban—various types of speech or expression, including news,[231] misogynistic rap lyrics,[232] television violence,[233] video games,[234]

---

225. *Id.*

226. *Id.* at 121.

227. W. Phillips Davison, *The Third-Person Effect in Communication*, 47 PUB. OPINION Q. 1, 3 (1983).

228. *See id.* at 10–11.

229. *See id.* at 11.

230. *See* Douglas M. McLeod et al., *Behind the Third-Person Effect: Differentiating Perceptual Processes for Self and Other*, 51 J. COMM. 678 (2001).

231. *See* Vincent Price et al., *Third-person Effects of News Coverage: Orientations Toward Media*, 74 JOURNALISM & MASS COMM. Q. 525, 525–40 (1997).

232. *See* Douglas M. McLeod et al., *Support for Censorship of Violent and Misogynic Rap Lyrics: An Analysis of the Third-Person Effect*, 24 COMM. RES. 153, 153–74 (1997).

233. *See* Hernando Rojas et al., *For the Good of Others: Censorship and the Third-Person Effect*, 8 INT'L J. PUB. OPINION RES.163, 163–86 (1996).

234. *See* James D. Ivory, Addictive for Whom? Electronic Games, The Third-person Effect, and Contributors to Attitudes Toward the Medium (May 2004) (unpublished paper) *available at* http://filebox.vt.edu/users/

and pornography.[235] In each case, the subjects surveyed expressed strong misgivings about allowing others to see or hear too much of the speech or expression in question, while they greatly discounted the impact of that speech on themselves. Such studies thus reveal the strong paternalistic instinct behind proposals to regulate speech. As Davison notes:

> Insofar as faith and morals are concerned . . . it is difficult to find a censor who will admit to having been adversely affected by the information whose dissemination is to be prohibited. Even the censor's friends are usually safe from the pollution. It is the general public that must be protected. Or else, it is youthful members of the general public, or those with impressionable minds.[236]

It is easy to see how this same phenomenon is at work in various Internet policy debates. Regulatory advocates imagine their preferences are "correct" (i.e., right for everyone) and that the masses are being duped by external forces beyond their control or comprehension, even though the advocates themselves are immune from the brainwashing because they are privy to some higher truth that *hoi polloi* simply cannot fathom. To some extent, this is Sowell's "Vision of the Anointed" at work. In another sense, this phenomenon reminds one of George Bernard Shaw's famous quip, "Critics, like other people, see what they look for, not what is actually before them."[237]

IV. TYING IT ALL TOGETHER: FEAR CYCLES

Combining the notions and explanations outlined in the previous sections, we can begin to think of how "fear cycles" work. Fear cycles refer to the manner in which various individuals and organizations work either wittingly or unwittingly in a mutually reinforcing fashion to perpetuate technopanics.

To illustrate the various forces at work that drive panics in

---

jivory/Ivory20043pGamesICA.pdf.

235. *See* Albert C. Gunther, *Overrating the X-rating: The Third-person Perception and Support for Censorship of Pornography*, 45 J. COMM., Mar. 1995, at 27–38.

236. Davison, *supra* note 227, at 14; *see also* Bob Thompson, *Fighting Indecency, One Bleep at a Time*, WASH. POST, Dec. 9, 2004, at A1 (documenting the process by which the Parents Television Council, a vociferous censorship advocacy group, screens various television programming and revealing that one of the PTC screeners interviewed for the story talked about the societal dangers of various broadcast and cable programs she rates, but then also noted how much she personally enjoys HBO's "The Sopranos" and "Sex and the City," as well as ABC's "Desperate Housewives").

237. GEORGE BERNARD SHAW, THREE PLAYS FOR PURITANS at xxiv (Chicago and New York H. S. Stone and Company) (1901).

the context of violent video games, Chris Ferguson developed what he referred to as the "Moral Panic Wheel."[238] The adjoining image, developed by Ferguson, illustrates that there is no one entity or factor responsible for moral panics or technopanics.[239] Rather, it is the combination of many forces and influences that ultimately bring about such panics. Activist groups and agenda-driven researchers obviously play a part. Ferguson notes that:

> As for social scientists, it has been observed that a small group of researchers have been most vocal in promoting the anti-game message, oftentimes ignoring research from other researchers, or failing to disclose problems with their own research. As some researchers have staked their professional reputation on anti-game activism, it may be difficult for these researchers to maintain scientific objectivity regarding the subject of their study. Similarly, it may be argued that granting agencies are more likely to provide grant money when a potential problem is identified, rather than for studying a topic with the possibility that the outcome may reveal that there is nothing to worry about . . . . (citation omitted)[240]

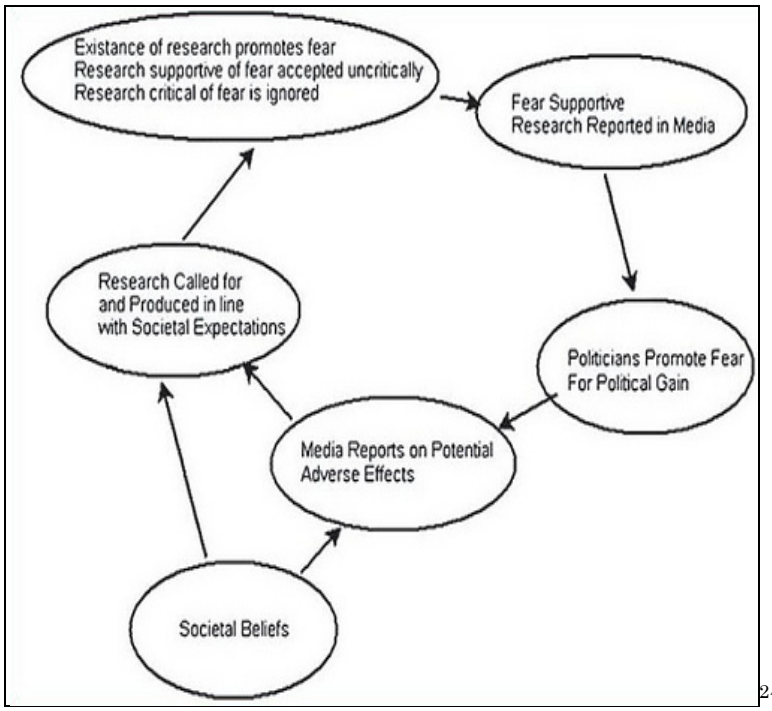
Ferguson points out that the media and politicians also play a key role in agitating the public and fueling overhyped fears, explaining,

> The media dutifully reports on the most negative results, as these results 'sell' to an already anxious public. Politicians seize upon the panic, eager to be seen as doing something particular as it gives them an opportunity to appear to be 'concerned for children'. Media violence, in particular, is an odd social issue with the ability to appeal both to voters on the far right, who typically are concerned for religious reasons, and on the far left, who are typically motivated by pacifism.[241]

Ferguson reiterates that generation gaps are often a key feature of moral panics: "[T]he majority of individuals critical of video games are above the age of 35 (many are elderly) and oftentimes admit to not having directly experienced the games. Some commentators make claims betraying their unfamiliarity."[242]

---

238. Ferguson, *supra* note 20, at 31.
239. *See id.*
240. *Id.* at 30–31.
241. *Id.* at 32–33.
242. *Id.* at 31.



[243]

University of Chicago legal scholar Cass Sunstein has described "fear as wildfire" and explained how "social cascades" contribute to the rapid spread of fear and panic.[244] Through social cascades, he argues, the "people who participate in them are simultaneously amplifying the very social signal by which they are being influenced" as "representative anecdotes and gripping examples move rapidly from one person to another."[245] In this sense, fear is contagious and mutually reinforcing. Hence, the resulting fear cycle.

Aligica notes that Julian Simon developed a similar fear cycle concept in his work debunking panics over environmental or development issues:

> [B]ehind the apocalyptic public opinion beliefs . . . is more rhetoric and psychology. In fact, one could identify a *sui generis* process of circular reasoning in which bad news feeds on itself. The cycle starts with experts or supposed experts repeating the same basic pessimistic assertions. Those assertions are echoed and repeated by mass media that amplifies them exponentially. People start to adopt those views.

---

243. *Id.* at 31.
244. SUNSTEIN, *supra* note 170, at 89–106.
245. *Id.* at 94–95.

> A new cycle starts but this time with the newly gained "everyone knows" status. The media defense that it is just a mere "messenger" does not stand critical scrutiny.[246]

It may be the case that these fear cycles are now accelerating in the technology policy arena but that the severity of each individual panic is somewhat diminished as a result, because:

> [t]hey peak and fizzle out faster . . . Perhaps this is a natural outgrowth of the technological explosion we have witnessed in recent years. Digital innovation is unfolding at a breakneck pace and each new development gives rise to a new set of concerns. Going forward, this could mean we experience more "mini-panics" and fewer of the sort of sweeping "the-world-is-going-to-hell" type panics.[247]

Why do panics pass? Perhaps it is the case that the unique factors that combine to create technopanics tend to dissipate more rapidly over time precisely because technological changes continue to unfold at such a rapid clip. Maybe there is something about human psychology that "crowds out" one panic as new fears arise. Perhaps the media and elites lose interest in the panic *du jour* and move on to other issues.[248] Finally, people may simply learn to accommodate cultural and economic changes. Indeed, some of things that evoke panic in one generation come to be worshiped (or at least respected) in another. As *The Economist* magazine recently noted, "There is a long tradition of dire warnings about new forms of media, from translations of the Bible into vernacular languages to cinema and rock music. But as time passes such novelties become uncontroversial, and eventually some of them are elevated into art forms."[249] These topics and explanations are ripe for future study.

V. WHY TECHNOPANICS AND THREAT INFLATION ARE DANGEROUS

Should we care about technopanics, threat inflation, and fear cycles? Won't they just eventually blow over with the pass-

---

246. ALIGICA, *supra* note 201, at 20 (citation omitted).

247. Adam Thierer, *Technopanic Cycles (and How the Latest Privacy Scare Fits In)*, TECH. LIBERATION FRONT (Feb. 24, 2011), http://techliberation.com/2011/02/24/techno-panic-cycles-and-how-the-latest-privacy-scare-fits-in/.

248. *See* GARDNER, *supra* note 84, at 177 ("When panics pass, they are simply forgotten, and where they came from and why they disappeared are rarely discussed in the media that featured them so prominently.").

249. *No Killer App: The Moral Panic about Video Games is Subsiding*, ECONOMIST, Dec. 10, 2011, at 10.

ing of time? Unfortunately, some panics do not blow over so quickly, and, even when they do pass rapidly, panics and threat inflation can have troubling ramifications.

A. FOSTER ANIMOSITIES AND SUSPICIONS AMONG THE CITIZENRY

First, it should go without saying that continuously elevated states of fear or panic can lead to dangerous tensions throughout society. For example, the recent "stranger danger" panic has led to unfortunate suspicions about the presence of males near children.[250] Similarly, excessive panic over cybersecurity matters can lead to paranoia about the potential danger of visiting certain digital environments or using certain digital tools that are, generally speaking, safe and beneficial to the masses.

B. CREATE DISTRUST OF MANY INSTITUTIONS, ESPECIALLY THE PRESS

Second, technopanics and the use of threat inflation can also result in a "boy who cried wolf" problem for advocacy groups, the government, and the press. When panic becomes the norm, it becomes more difficult for the public to take seriously those people and institutions who perpetuate these panics. This is dangerous for deliberative democracy because "[w]hen a threat is inflated, the marketplace of ideas on which a democracy relies to make sound judgments—in particular, the media and popular debate—can become overwhelmed by fallacious information."[251]

C. OFTEN DIVERT ATTENTION FROM ACTUAL, FAR MORE SERIOUS RISKS

Third, if everything is viewed as a risk, then nothing is a risk. Fear-based tactics and inflated threat scenarios can lead to situations where individuals and society ignore quite serious risks because they are overshadowed by unnecessary panics over nonproblems.[252] "The problem is that both individuals and societies may be fearful of nonexistent dangers or trivial risks—and simultaneously neglect real dangers," writes Sun-

---

250. *See* Wendy McElroy, *Destroying Childhood to Save Children*, FREEMAN (Dec. 6, 2011), http://www.thefreemanonline.org/headline/destroying-childhood-to-save-children.

251. Brito & Watkins, *supra* note 39, at 2.

252. *See* SUNSTEIN, *supra* note 170, at 105.

stein.[253] This problem is discussed in more detail in Section VI.

D. LEAD TO CALLS FOR INFORMATION CONTROL

Finally, technopanics, threat inflation, and fear cycles are dangerous because they encourage policymakers to adopt far-reaching controls on information flows and the information economy more generally. In each of the case studies presented above, increased regulation of communication platforms was the primary solution proposed by elites, academics, regulatory advocates, special interests, or policymakers. Such information control could stifle free speech, limit the free flow of ideas, and retard social and economic innovation.

The next section explores how we might be witnessing the rise of a "precautionary principle" for some information technology policy matters. The adoption of a precautionary principle would restrict progress in this arena until technology creators or proponents can demonstrate new tools are perfectly safe.

For these reasons, it is vital that public policy debates about information technology not be driven by technopanics and threat inflation. According to Ohm, "[t]o date, the fear mongers have had the upper hand, shaping policy through sound bites and unfounded anecdotes."[254] Such claims must be countered with hard evidence and dispassionate reasoning before they do serious damage to the information economy and human welfare through the increasing adoption of precautionary principle-based public policies in this arena.

VI. WHEN PANIC BECOMES POLICY: THE RISE OF AN INFO-TECH "PRECAUTIONARY PRINCIPLE"

What is likely to happen if fear-based tactics come to be taken more seriously by policymakers? Stated differently, if public policies are guided by such pessimistic predictions, what course of action should we expect governments to pursue?

When it comes to technological progress, the pessimistic creed often is "better safe than sorry."[255] This response is gen-

---

253. *Id.*

254. Ohm, *supra* note 171.

255. Jonathan H. Adler, *The Problems with Precaution: A Principle Without Principle*, AM. MAG. (May 25, 2011), http://www.american.com/archive/2011/may/the-problems-with-precaution-a-principle-without-principle.

erally known as "the precautionary principle."[256] When applied in a public policy setting, the precautionary principle holds that since every technology and technological advance could pose some theoretical danger or risk, public policies should prevent people from using innovations until their developers can prove that they won't cause any harms.[257] In other words, the law should mandate "play it safe" as the default policy toward technological progress. Journalist Ronald Bailey has summarized this principle as "anything new is guilty until proven innocent."[258]

Although this principle is most often discussed in the field of environment law, it is increasingly on display in Internet and information technology policy debates.[259] Indeed, the logical extension of the technopanic mentality outlined above would be the preemptive prohibition of many forms of technological change in order to stave off perceived threats to culture, learning, traditions, social norms, the economy, institutions, professions, or traditional ways of doing business—in short, to stave off just about anything.[260]

The child safety and privacy policy fields are rife with examples of new innovations being preemptively micromanaged or discouraged. Section II discussed the *Deleting Online Predators Act*, a 2006 measure to ban access to social networking sites in schools and libraries, which received 410 votes in the U.S. House of Representatives before dying in the Senate.[261] A decade earlier, under the *Communications Decency Act*, Congress attempted to sanitize the Internet from "indecent" and "obscene" content.[262]

Lately, the precautionary principle mindset has gained the

---

256. *Id.*

257. *Id.*

258. Ronald Bailey, *Precautionary Tale*, REASON (Apr. 1999), http://reason.com/archives/1999/04/01/precautionary-tale.

259. *See* Julian Morris, *Introduction*, *in* RETHINKING RISK AND THE PRECAUTIONARY PRINCIPLE at viii-ix (Julian Morris ed., 2000) (discussing and refuting the precautionary principal in that context).

260. Adam Thierer, *Prophecies of Doom & the Politics of Fear in Cybersecurity Debates*, TECH. LIBERATION FRONT (Aug. 8, 2011), http://techliberation.com/2011/08/08/prophecies-of-doom-the-politics-of-fear-in-cybersecurity-debates/.

261. Deleting Online Predators Act, H.R. 5319, 109th Cong. (2006).

262. Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L. J. 51, 53 (1996).

most steam in the field of privacy policy. For example, in late 2011, Amazon announced a new tablet computer, the Kindle Fire, to compete against Apple's iPad and other devices.[263] The Kindle Fire takes advantage of Amazon's sophisticated cloud computing platform to offer users a faster and more efficient browsing experience, as Amazon's servers do all the heavy lifting in terms of information processing.[264] Of course, that also meant Amazon would possess more information about user's web-surfing habits and interests, which immediately raised privacy concerns.[265] Some lawmakers were quick to raise questions and hint that perhaps such innovation wasn't even needed. At one hearing in October 2011, Representatives Joe Barton and Ed Markey lambasted Amazon's move to offer this new feature to consumers. Barton compared online data collection to the forcible quartering of military soldiers in one's home, and Markey spoke in Orwellian terms of Amazon's "Big Browser" ambitions.[266] These lawmakers didn't seem to care that no consumer would be forced to spend $200 for the devices, or that the Kindle Fire's cloud-based browser features could be turned off entirely.[267] Instead, their attitude was summarized by Barton's dismissive belief that "enough is enough,"[268] which was followed up with a letter to Amazon from Markey asking a series of threatening questions about the browser's functions.[269]

This is reminiscent of the hostile reaction that briefly fol-

---

263. *See* Chenda Ngak, *Is the Kindle Fire HD a Threat to Apple iPad, Google Nexus 7?*, TECHTALK (Sept. 7, 2012, 10:49 AM), http://www.cbsnews.com/8301-501465_162-57508218-501465/is-the-kindle-fire-hd-a-threat-to-apple-ipad-google-nexus-7/ (comparing the Kindle Fire to the Apple iPad).

264. Tom Cheredar, *Kindle Fire Uses a New Silk Web Browser to Boost Efficiency*, VENTURE BEAT (Sept. 28, 2011, 8:07 AM), http:// venturebeat.com/2011/09/28/amazon-kindle-silk-browser.

265. Nate Anderson, *Your Internet Data: More Like Redcoats Living in Your Home or Black Gold in the Ground?*, ARSTECHNICA (Oct. 13, 2011, 4:55 PM), http://www.arstechnica.com/tech-policy/news/2011/10/your-internet-data-more-like-redcoats-living-in-your-home-or-black-gold-in-the-ground.ars [hereinafter *Your Internet Data*].

266. *Id.*; Anderson, *supra* note 105.

267. Doug Gross, *Reviews: Kindle Fire HD Good, but not Quite an iPad*, CNNTECH, http://www.cnn.com/2012/09/12/tech/mobile/consumer-reports-kindle-fire-hd/index.html (last updated Sept. 12, 2012, 11:32 AM); Anderson, *supra* note 265.

268. Cheredar, *supra* note 264.

269. *Your Internet Data, supra* note 265.

lowed the debut of Google's Gmail service in 2004.[270] It too raised new privacy concerns and led to calls for prohibition before it had even debuted.[271] At a time when Yahoo! mail (then the leading webmail provider) offered customers less than 10 megabytes of email storage, Gmail offered a then unprecedented gigabyte of storage that would grow over time (to over 7 GB in 2011).[272] Instead of charging "users for more storage or special features, Google paid for the service by showing advertisements next to each email 'contextually' targeted to keywords in that email—a far more profitable form of advertising than 'dumb banner' ads previously used by other webmail providers."[273] Some privacy advocates howled that Google was going to "read users' emails," and led a crusade to ban such algorithmic contextual targeting.[274] In essence, they wanted to impose their own subjective values (and fears) on everyone else.[275]

Interestingly, however, the frenzy of hysterical indignation about Gmail was followed by a collective cyber yawn; users increasingly understood that algorithms, not humans, were doing the "reading" or "tracking," and that, if they didn't like it, they didn't have to use it.[276] By mid-2012, roughly 425 million people around the world were using Gmail, and it has a steadily growing share of the webmail market.[277] People adapted their privacy expectations to accommodate the new service. Luckily, policymakers never acted upon the fears of the critics or else this innovative free service might never have been made available to consumers.

---

270. Adam Thierer, *Lessons from the Gmail Privacy Scare of 2004*, TECH. LIBERATION FRONT (Mar. 25, 2011), http://techliberation.com/2011/03/25/lessons-from-the-gmail-privacy-scare-of-2004.

271. *Id.*

272. Adam Thierer, *Avoiding a Precautionary Principle for the Internet*, FORBES (Mar. 11, 2012, 2:04 PM), http://www.forbes.com/sites/adamthierer/2012/03/11/avoiding-a-precautionary-principle-for-the-internet/ [hereinafter *Avoiding a Precautionary Principle*].

273. Thierer, *supra* note 270.

274. *See* Letter from Chris Jay Hoofnagle, Assoc. Dir., Elec. Privacy Info. Ctr., Beth Givens, Dir., Privacy Rights Clearinghouse, & Pam Dixon, Exec. Dir., World Privacy Forum, to Bill Lockyer, Cal. Attorney Gen., (May 3, 2004), *available at* http://www.epic.org/privacy/gmail/agltr5.3.04.html.

275. *See* email from Adam Thierer to Declan McCullaugh (Apr. 30, 2004, 6:40 PDT), *available at* http://lists.jammed.com/politech/2004/04/0083.html.

276. *Avoiding a Precautionary Principle*, *supra* note 272.

277. Dante D'Orazio, *Gmail Now Has 425 Million Total Users*, VERGE (June 28, 2012), http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users.

Regardless of the context or issue, applying a precautionary principle mindset to information technology concerns will result in a greatly diminished capacity for experimentation, learning, and progress.[278] This is not to say new technologies pose no risks. Rather, as did our ancestors, we must learn to adapt to new tools and use them wisely without taking extreme steps in the face of the risks they pose. The following sections explore how that can be accomplished.

A. A RANGE OF RESPONSES TO THEORETICAL RISK

In thinking about how humans and society more generally respond to technological risk, it is useful to step back and consider one of the oldest technologies: a hammer.

A hammer is a remarkably useful tool. It dates from the Stone Age and has been adapted throughout human civilization to serve a broad array of needs.[279] George Basalla, author of *The Evolution of Technology*, notes that "[i]n 1867 Karl Marx was surprised to learn, as well he might have been, that five hundred different kinds of hammers were produced in Birmingham, England, each one adapted to a specific function in industry or the crafts."[280] An astonishing variety of hammers continues to be produced today, and they are used to accomplish a wide range of tasks by everyone from professional builders to specialized carpenters, and to average citizens.[281]

Of course accidents are also possible with hammers. As this author can attest, hammers may miss targets, smash fingers, and even break knuckles. Worse yet, on some rare occasions, hammers have been wielded by madmen to maim and even to kill people or animals.[282]

---

278. *Avoiding a Precautionary Principle*, *supra* note 272.

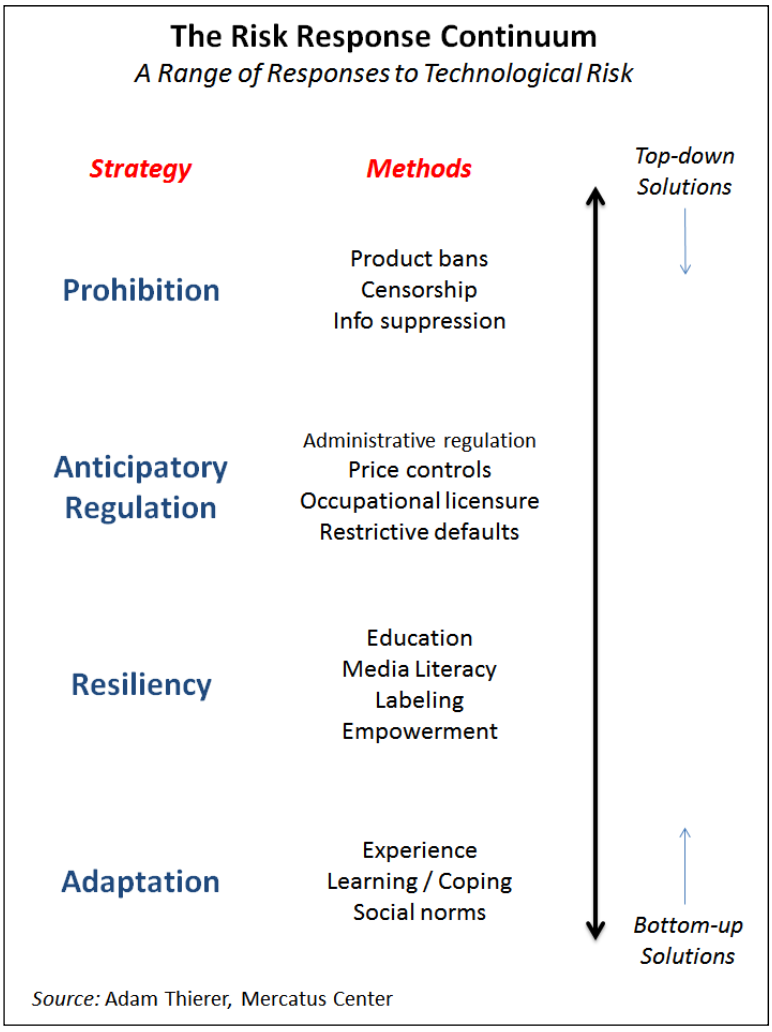
279. *See* 2 Edward H. Knight, KNIGHT'S AMERICAN MECHANICAL DICTIONARY 1052 (1884) ("Many [hammers] are found in the relics of the stone age, before man had learned the use of metal . . . .").

280. GEORGE BASALLA, THE EVOLUTION OF TECHNOLOGY 2 (1988).

281. *See* HENRY PETROSKI, THE EVOLUTION OF USEFUL THINGS 126–29 (1992).

282. *See Two Black Teens Fueled by Hate From Al Sharpton Brutally Beat a White Man in Sanford, FL*, DIVIDED STATES (Apr. 3, 2012), http://www.dividedstates.com/two-black-teens-from-sanford-fl-brutally-beat-white-man-with-a-hammer/; Liz Collin, *Minn. Woman Accused of Killing Cat with Hammer*, CBS MINN. (Feb. 24, 2011, 7:23 AM), http://minnesota.cbslocal.com/2011/02/24/minn-woman-accused-of-killing-cat-with-hammer/.

What then should we do about hammers in light of their clearly dangerous potential? Should we ban them? License their use? Require educational courses? Affix warning stickers? When it comes to the risk that hammers or any technology pose to individuals and society, we might think of a continuum of possible responses that looks like this:



283

283. Adam Thierer, *Journalists, Technopanics & the Risk Response Continuum*, TECH. LIBERATION FRONT (July 15, 2012), http://techliberation.com/2012/15/journalists-technopanics-the-risk-the-response-continuum/ [hereinaf-

Each possible approach to dealing with risks posed by new technology is summarized below:

1. *Prohibition*: Prohibition is an attempt "to eliminate potential risk through suppression of technology, product or service bans, information controls, or outright censorship."[284] As applied to technology, such strategies are generally known as "the precautionary principle," which holds that, "since every technology and technological advance could pose some theoretical danger or risk, public policies should prevent people from using innovations until their developers can prove that they won't cause any harms."[285] In other words, the precautionary principle suggests that—either at the individual or society-wide level—"play it safe" should be the default disposition toward technological progress.[286] Like the next strategy, anticipatory regulation, prohibition represents a *risk mitigation* strategy that focuses on *top-down* solutions, but the solutions tend to be far more sweeping.
2. *Anticipatory Regulation*: Anticipatory regulation would include any public policy action short of prohibition that attempts to deal with technological risk by controlling or curbing the uses of that technology.[287] There exists a diverse array of possible regulatory strategies and precautionary safeguards that can be very context-specific, including: administrative regulation and sanctions, government ownership or licensing controls, or restrictive defaults.[288] Anticipatory regulation can sometimes lead to prohibition, although it is equally likely that prohibition will give way to regulation when efforts to completely ban a specific type of technological

---

ter *Risk Response Continuum*].

284. *Id.*

285. *Avoiding a Precautionary Principle*, *supra* note 272. *See also* Adrian Vermeule, *Precautionary Principles in Constitutional Law*, 4 J. LEGAL ANALYSIS 181, 182 ("[N]ew technologies and policies should be rejected unless and until they can be shown to be safe.").

286. *Avoiding a Precautionary Principle*, *supra* note 272; Alder, *supra* note 255.

287. Frieder Naschold, *Techno-Industrial Innovation and Technology Assessment: The State's Problems with Its New Role*, *in* STATE POLICIES AND TECHNO-INNOVATION 65, 75–76 (Ulrich Hilpert ed., 1991).

288. *Risk Response Continuum*, *supra* note 283.

risk prove futile.[289] Like prohibition, anticipatory regulation is a *risk mitigation* strategy that is more top-down in nature, but not nearly as sweeping or restrictive in character.

3. Resiliency: Resiliency-based strategies address technological "risk through education, awareness building, transparency and labeling, and empowerment steps and tools."[290] Resilience represents "the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances."[291] Resiliency-based strategies can be undertaken by civilizations, companies, communities, institutions, and individuals.[292] Compared to the first two strategies, which focused on *top-down risk mitigation*, resiliency represents a form of *risk adaptation* that focuses on *bottom-up* strategies.[293] But, unlike a strategy of pure adaptation, resilient strategies encourage more active steps by various institutions and individuals to prepare for technological risk.[294] This may include some public policies to facilitate the educational- and empowerment-based strategies mentioned; although, they cannot be unnaturally forced upon individuals or institutions from above.[295]
4. Adaptation: Adaptation entails learning to live with technological risks "through trial-and-error experimentation, experience, coping mechanisms, and social norms," which "often begin with, or evolve out of, resiliency-based efforts."[296] It would be overly simplistic to refer to adaptation as a "just get over it" strategy, although that is the way it is sometimes conceptualized. The essence of adaptation lies in the *bottom-up, organ-*

---

289. *See generally* Mark Thorton, *Alcohol Prohibition Was a Failure* (Cato Inst., Policy Analysis No. 157, 1991) *available at* http://www.cato.org/publications/policy-analysis/alcohol-prohibition-was-failure.

290. *Risk Response Continuum*, *supra* note 283.

291. ANDREW ZOLLI & ANN MARIE HEALY, RESILIENCE: WHY THINGS BOUNCE BACK 7 (2012).

292. *Id.* at 6.

293. *Risk Response Continuum*, *supra* note 283.

294. ZOLLI & HEALY, *supra* note 291, at 211.

295. *Id.* ("This capacity cannot simply be imposed from above—instead it must be nurtured in the social structures and relationships that govern people's everyday lives.").

296. *Risk Response Continuum*, *supra* note 283.

> *ic, and evolutionary* coping mechanisms that individuals and societies develop to deal with technological risks.

Despite the risk associated with hammers, society has generally chosen to rely on the fourth strategy: adaptation. We expect people to be responsible with hammers and, if it comes to it, to learn from their mistakes.

We have adopted the same disposition toward many other potentially dangerous tools, including knives, saws, drills, heat guns, soldering irons, and rope. There are no restrictions on the sale or use of these tools, no special permits or licenses are needed for their use, and governments don't even bother requiring courses about how to use them safely. In other words, we choose *not* to "play it safe" as the precautionary principle would counsel. Societies do not prohibit or regulate the use of these tools, but instead expect people to learn how to use them responsibly—potentially at great risk to themselves and others.

At the opposite end of this spectrum, there are some tools or technologies for which prohibition is potentially the right answer. For example, most citizens are not allowed to possess uranium.[297] The potential costs associated with its unrestricted use are considered unbearable due to the potential for catastrophic destruction or loss of life. Thus, most governments throughout the world impose the ultimate "play it safe" strategy and ban private ownership of such a "weapon of mass destruction."

Those are extreme cases, however. Most policy debates about how society manages technological risk come down to a battle between anticipatory regulation versus resiliency strategies. The urge for precautionary steps often dominates discussions about how to manage risk.[298] The default assumption in the minds of many remains "play it safe."[299] There are serious perils for society from a rigid application of that principle, however, especially from its application to information technology.[300]

---

297. *Uranium Recovery: What We Regulate*, U.S. NUCLEAR REG. COMMISSION, http://www.nrc.gov/materials/uranium-recovery.html (last updated July 23, 2012).

298. Alder, *supra* note 255.

299. *Id.*

300. *Id.*

For purposes of this discussion, the risk taker is generally assumed to be society as a whole, acting through political agents. The risk continuum outlined above will vary by individual actors, who may adopt strategies at an individual or household level that would not likely make as much sense if adopted in a collective fashion and imposed from above on all actors. Stated differently, there is a different choice architecture at work when risk is managed in a localized manner as opposed to a society-wide fashion. Leaving the decision about how to manage risk at the level of the individual, household, or the organization, may result in risk-mitigation strategies that would not be as effective if instituted as a legal or regulatory solution.

For example, outright prohibition of certain digital technologies or forms of media content may be a sensible and effective strategy for some individuals and families who wish to curtail undesirable online interactions, or material they find annoying, offensive, intrusive, or "creepy." Prohibition will likely be far less sensible or effective when imposed on all citizens.

As explained next, when risk-avoidance decisions are made at the governmental level for the whole society, it forecloses the opportunities for experimentation with varying risk-mitigation strategies and new forms of technological change.

B. THE PERILS OF "PLAYING IT SAFE"

The precautionary principle rests on the assumption that it is possible to forestall risk or prevent harm without serious cost to society.[301] There is no free lunch, however. "Playing it safe" sounds sensible until it becomes evident how that disposition limits progress and prosperity.[302]

The problem with the precautionary principle, notes Kevin Kelly, editor of *Wired* magazine, is that because "every good produces harm somewhere . . . [and therefore,] by the strict logic of an absolute precautionary principle[,] no technologies would be permitted."[303] Under an information policy regime guided at every turn by a precautionary principle, digital innovation and technological progress would become impossible because social tradeoffs and economic uncertainly would be considered unacceptable.

---

301. *Id.*
302. *Id.*
303. KEVIN KELLY, WHAT TECHNOLOGY WANTS 247–48 (2010).

Cass Sunstein has done pioneering work on risk analysis and the precautionary principle in particular.[304] "If the burden of proof is on the proponent of the activity or processes in question," he argues, "the Precautionary Principle would seem to impose a burden of proof that cannot be met."[305] The problem is that one cannot prove a negative. An innovator cannot prove the absence of harm, but a critic or regulator can always prove that *some* theoretical harm exists. Consequently, putting the burden of proof on the innovator when that burden can't be met essentially means no innovation is permissible. Meanwhile, forestalling innovation because of theoretical risk means other risks develop or go unaddressed.

New technologies help society address problems that are associated with older technologies and practices, but also carry risks of their own.[306] A new drug, for example, might cure an old malady while also having side effects. We accept such risks because they typically pale in comparison with the diseases new medicines help to cure. While every technology, new or old, has some risks associated with it, new technologies almost always make us safer, healthier, and smarter, because through constant experimentation we discover better ways of doing things.[307]

That is why Aaron Wildavsky, author of the seminal 1988 book *Searching for Safety*, warned of the dangers of "trial *without* error"—the precautionary principle approach—compared to trial and error.[308] Wildavsky argued that:

> The direct implication of trial without error is obvious: If you can do nothing without knowing first how it will turn out, you cannot do anything at all. An indirect implication of trial without error is that if trying new things is made more costly, there will be fewer departures from past practice; this very lack of change may itself be dangerous in forgoing chances to reduce existing hazards . . . Existing hazards will continue to cause harm if we fail to reduce them by taking advantage

304. SUNSTEIN, *supra* note 170, at 34.

305. Cass Sunstein, *The Paralyzing Principle*, REG., Winter 2002-2003 at 34; s*ee also id.* ("The most serious problem with the Precautionary Principle is that it . . . is a crude and sometimes perverse method of promoting various goals . . . . A rational system of risk regulation certainly takes precautions . . . [and does] not adopt the Precautionary Principle.").

306. *See* Henry I. Miller & Gregory Conko, *Precaution without Principle*, 19 NATURE BIOTECHNOLOGY 302, 302 (2001).

307. *Id.*

308. AARON WILDAVSKY, SEARCHING FOR SAFETY 38 (1988).

of the opportunity to benefit from repeated trials.[309]

Simply stated, life involves *and requires* that some level of risk be accepted for progress to occur. Technology analyst Bret Swanson of Entropy Economics, L.L.C. has applied this same principle to business affairs. "The world is inherently risky and uncertain. Bad things happen. We don't know if investments or startups will succeed. When risk and uncertainty are decentralized, however, we get lots of experimentation and lots of small failures. We learn and move on, better prepared for the next try," he correctly notes.[310] This is equally true for social policy: w*illingness to experiment, and even to fail, is what yields learning and progress.*

The importance of failure to social learning and economic progress cannot be overstated.[311] For both the individual and society, "the ability to adapt requires an inner confidence that the cost of failure is a cost we will be able to bear," writes *Financial Times* senior columnist Tim Harford.[312] For without a "willingness to risk failure," he says, "we will never truly succeed."[313] "Innovation and change imply also insecurity and risk, for few changes fail to affect some people adversely," observe economic historians Nathan Rosenberg and L.E. Birdzell, Jr.[314]

By contrast, the precautionary principle destroys social and economic dynamism.[315] It stifles experimentation and the resulting opportunities for learning and innovation.[316] While some steps to anticipate or to control unforeseen circumstances and "to plan for the worse" are sensible, going overboard with precaution forecloses opportunities and experiences that offer valuable lessons for individuals and society.[317]

---

309. *Id.*

310. *See* Bret Swanson, *Banning Risk is Our Biggest Risk*, FORBES (Aug. 30, 2011) http:// www.forbes.com/sites/bretswanson/2011/08/30/banning-risk-is-our-biggest-risk.

311. *See* ZOLLI & HEALY, *supra* note 291, at 13 ("Regular, modest failures are actually *essential* to many forms of resilience—they allow a system to release and then reorganize some of its resources.").

312. TIM HARFORD, ADAPT: WHY SUCCESS ALWAYS STARTS WITH FAILURE 262 (2011).

313. *Id.*

314. NATHAN ROSENBERG & L.E. BIRDZELL, JR., HOW THE WEST GREW RICH: THE ECONOMIC TRANSFORMATION OF THE INDUSTRIAL WORLD 266 (1986).

315. *See* Miller & Conko, *supra* note 306, at 302.

316. *See id.*

317. *See id.*

Worse yet, a rigid application of the precautionary principle could misallocate societal resources and lead to *more* risk. "The real danger of the precautionary principle," argue Henry I. Miller and Gregory Conko, "is that it distracts consumers and policymakers from known, significant threats to human health and often diverts limited public health resources from those genuine and far greater risks."[318] In essence, the principle contradicts itself because it ignores tradeoffs and opportunity costs. As Sunstein cogently argues, "[R]egulation sometimes violates the Precautionary Principle because it gives rise to *substitute risks*, in the form of hazards that materialize, or are increased, as a result of regulation."[319] Regrettably, such tradeoffs are rarely taken into account.

C. ANTICIPATION VS. RESILIENCY

Importantly, Wildavsky explained how the precautionary principle also downplays the important role of resiliency in human affairs.[320] Resiliency in the context of risk could be considered both an individual disposition and a societal method of coping with change.[321] It could entail an individual or society doing nothing in the face of technological change or risk, in which case it would more accurately be described as an adaptation approach. More often, resiliency involves efforts by individuals and institutions (including governments) to educate people better to understand and deal with technological change or risk.[322]

Resiliency theory, like the precautionary principle itself, has its roots in the field of environmental science.[323] "Resilience is a core concept used by ecologists in their analysis of popula-

---

318. *Id.*

319. SUNSTEIN, *supra* note 170, at 32 (emphasis in original).

320. *See* WILDAVSKY, *supra* note 308.

321. *See* ZOLLI & HEALY, *supra* note 291, at 260 ("While there's no single recipe for every circumstance, every journey toward greater resilience begins with continuous, inclusive, and honest efforts to seek out fragilities, thresholds, and feedback loops of a system … Doing so calls us to greater mindfulness . . . just as true for organizations and communities as it is for people.").

322. *Id.* at 6.

323. *See* Marco A. Janssen & Elinor Ostrom, *Resilience, Vulnerability, and Adaptation: A Cross-Cutting Theme of the International Human Dimensions Programme on Global Environmental Change*, 16 GLOBAL ENV'T CHANGE 237, 239 (2006) (explaining the importance of the theory to early environmental changes).

tion ecology of plants and animals and in the study of managing ecosystems," note Marco A. Janssen and Elinor Ostrom.[324] The Resilience Alliance, an international research organization comprised of scientists and practitioners from many disciplines who collaborate to explore the dynamics of social-ecological systems, defines a resilient ecosystem as one that "can withstand shocks and rebuild itself when necessary." [325] They add that "resilience in social systems has the added capacity of humans to anticipate and plan for the future."[326]

Through constant experimentation, humans learn valuable lessons about how the world works, how better to determine which risks are real versus illusory or secondary, and how to assimilate new cultural, economic, and technological change into our lives.[327] A rigid precautionary principle would preclude this learning progress and leave us *more* vulnerable to the most serious problems we might face as individuals or a society. "Allowing, indeed, encouraging, trial and error should lead to many more winners, because of (a) increased wealth, (b) increased knowledge, and (c) increased coping mechanisms, i.e., increased resilience in general," concluded Wildavsky.[328] Again, these principles are equally applicable to the field of information technology.

What does a strategy of resiliency mean in practice? Consider a case study that has nothing to do with information policy: playground safety.

Playgrounds are places of great joy and adventure for children, but they also have the potential to be risky environments for kids. Fearing the potential for serious injuries—and lawsuits—many school and park administrators have removed jungle gyms and other tall structures from playgrounds in recent years.[329] And why not? Again, better to be safe than sorry, at least according to the logic of the precautionary principle.

---

324. *Id.*

325. *Resilience*, RESILIENCE ALLIANCE (Oct. 29, 2002, 15:33:18), http://www.resalliance.org/index.php/resilience.

326. *Id.*

327. *See* ZOLLI & HEALY, *supra* note 291, at 23 ("The resilience frame suggests a different, complementary effort to mitigation: to redesign our institutions, embolden our communities, encourage innovation and experimentation, and support our people in ways that will help them be prepared to cope with surprises and disruptions, even as we work to fend them off.").

328. WILDAVSKY, *supra* note 308, at 103.

329. John Tierney, *Grasping Risk in Life's Classroom*, N.Y. TIMES, July 19, 2011, at D1.

Not everyone agrees. Dr. Ellen Sandseter, a professor of psychology at Queen Maud University in Norway, has conducted research that suggests a little playground risk is a good thing for children.[330] "Children need to encounter risks and overcome fears on the playground," she told *The New York Times*.[331] Additionally, she asserts,

> Climbing equipment needs to be high enough, or else it will be too boring in the long run. Children approach thrills and risks in a progressive manner, and very few children would try to climb to the highest point for the first time they climb. The best thing is to let children encounter these challenges from an early age, and they will then progressively learn to master them through their play over the years.[332]

The *Times* article that cited Sandseter goes on to explain how learning, experimentation, and experience builds resiliency into children that can help them later in life:

> While some psychologists—and many parents have worried that a child who suffered a bad fall would develop a fear of heights, studies have shown the opposite pattern: A child who's hurt in a fall before the age of 9 is less likely as a teenager to have a fear of heights.[333]

This explains why an overly cautious approach to playground safety is counterproductive. It could create life-long anxieties and phobias that would discourage normal play, experimentation, learning, and joy. "Overprotection might thus result in exaggerated levels of anxiety [for children]," Sandseter notes in a recent study with Leif Kennair.[334] "Overprotection through governmental control of playgrounds and exaggerated fear of playground accidents might thus result in an increase of anxiety in society. We might need to provide more stimulating environments for children, rather than hamper their development," they explain.[335]

We can apply this rule more generally beyond playgrounds. Tim Gill, author of *No Fear: Growing Up in a Risk Averse Society*, puts it best:

> It is worth reminding ourselves of two truths about how children grow up to be confident, resilient, responsible people. First, they have to be

---

330. *Id.*

331. *Id.*

332. *Id.* at D3.

333. *Id.*

334. Ellen Beate Hansen Sandseter & Leif Edward Ottesen Kennai, *Children's Risky Play from an Evolutionary Perspective: The Anti-Phobic Effects of Thrilling Experience*, 9 EVOLUTIONARY PSYCHOL. 257, 275 (2011).

335. *Id.*

> given the chance to learn from their mistakes. Second, the best classroom for learning about everyday life is indisputably the real world, beyond home and school. Rather than having a nanny state, where regulation, control and risk aversion dominate the landscape, we should embrace a philosophy of resilience.[336]

Indeed, there are other potential unintended consequences associated with what some have referred to as "surplus safety."[337] If aggressive play on playgrounds is discouraged, it certainly will not help alleviate the growing childhood obesity problem.[338] A recent study of thirty-four daycare centers by five pediatric researchers confirmed that "[s]ocietal priorities for young children—safety and school readiness—may be hindering children's physical development."[339] In particular, the researchers found that "[s]tricter licensing codes intended to reduce children's injuries on playgrounds rendered playgrounds less physically challenging and interesting. . . . Because children spend long hours in care and many lack a safe place to play near their home, these barriers may limit children's only opportunity to engage in physical activity."[340]

Reduced playground time might also affect the sociability of youth by diminishing interaction opportunities and the resulting learning experiences.[341] It also might limit the ability of children to explore and learn from nature.[342] The same is true of information environments. Sternheimer argues:

> The innocence that we like to believe used to exist in the world is revisionist history: children have always faced both natural and human danger, and they have always needed to learn how to cope with both. Attempts to shield children from information will not protect them in

---

336. Tim Gill, *Cotton Wool Revolution: Instilling Resilience in Children is a Vital Lesson but Only Makes Sense in a Supportive Society*, GUARDIAN, Oct. 30, 2007, at 30.

337. *See* Shirley Wyver et al., *Ten Ways to Restrict Children's Freedom to Play: The Problem of Surplus Safety*, 11 CONTEMP. ISSUES IN EARLY CHILDHOOD 263, 277 (2010).

338. *See* Alice G. Walton, *New Playgrounds Are Safe—and That's Why Nobody Uses Them*, ATLANTIC (Feb. 1, 2012, 11:06 AM), http://www.theatlantic.com/health/archive/2012/02/new-playgrounds-are-safe-and-thats-why-nobody-uses-them/252108.

339. Kristen A. Copeland et al., *Societal Values and Policies May Curtail Preschool Children's Physical Activity in Child Care Centers*, 129 PEDIATRICS 265, 265 (2012).

340. *Id.* at 265, 270.

341. *Id.* at 266, 269.

342. *See id.* at 268 (explaining that exposure to nature is a possible benefit of kids being outside).

the end.[343]

Resiliency is the superior approach, she argues, since "parents can never fully protect or control their children. By insisting that they can and should, we deprive kids of an important opportunity for learning to navigate the outside world and learning to make appropriate decisions."[344]

D. CASE STUDIES: APPLYING THE RESILIENCY MODEL TO INFORMATION TECHNOLOGY ISSUES

With the preceding framework in mind, we can next consider how choosing resiliency and adaptation strategies over anticipatory regulation or prohibition is also a wise strategy as it pertains to specific Internet and information technology issues. To reiterate, this is not to rule out the possibility that anticipatory regulation or even prohibition might be advisable in certain limited circumstances. But such determinations will be highly case-specific and must be based on evidence of clear harm or market failure. Also, different values and constitutional rights may need to be considered that would trump other risk analysis considerations. Even then, the other costs associated with anticipatory regulation must be considered and planned for. These issues are discussed at greater length in Section VII.

For the reasons articulated above, however, the presumption should be in favor of allowing greater experimentation with new information technologies, and encouraging adaptation and resiliency strategies over more restrictive alternatives. The following case studies explain how.

1. Online Child Safety, Privacy, and Reputation Management

Collecting information and learning from online sites clearly has great value to children. More generally, children also benefit from being able to participate in online interactions because they learn essential social skills.[345] As a recent MacArthur Foundation study of online youth Internet use concluded:

> Contrary to adult perceptions, while hanging out online, youth are

343. STERNHEIMER, *supra* note 154, at 27.

344. *Id.* at 23.

345. MIZUKO ITO ET AL., LIVING AND LEARNING WITH NEW MEDIA: SUMMARY OF FINDINGS FROM THE DIGITAL YOUTH PROJECT 2 (2008) ("[W]hile hanging out online, youth are picking up basic social and technological skills they need to fully participate in contemporary society.").

> picking up basic social and technological skills they need to fully participate in contemporary society. Erecting barriers to participation deprives teens of access to these forms of learning. Participation in the digital age means more than being able to access "serious" online information and culture.[346]

Nonetheless, fears persist about youth and online environments. The greatly overblown "predator panic" discussed earlier is the most obvious example. As noted previously, when social networking sites such as MySpace and Facebook began gaining prominence in the mid-2000s, some state attorneys general proposed mandatory online age verification, and legislation was floated in Congress that would have banned access to social networking sites in publicly funded schools and libraries.[347] Similarly, when concerns about online cyberbullying arose, regulatory solutions were the kneejerk response.[348]

Ultimately, such "legislate and regulate" responses are not productive (or constitutional) approaches to online safety concerns.[349] The better approach might be labeled "educate and empower," which is a resiliency-based approach centered around media literacy and "digital citizenship" strategies.[350] The focus should be on encouraging better social norms and coping strategies. We need to assimilate children gradually into online environments and use resiliency strategies to make sure they understand how to cope with the challenges they will face in the digital age.[351] Teaching our kids smarter online hygiene and "Netiquette" is vital. "Think before you click" should be lesson number one. They should also be encouraged to delete unnecessary online information occasionally.[352]

---

346. *Id.* at 2.

347. See Steel & Angwin, *supra* note 70, at B3; *Banned by DOPA?*, *supra* note 71.

348. Berin Szoka & Adam Thierer, *Cyberbullying Legislation: Why Education is Preferable to Regulation*, PROGRESS ON POINT (Progress & Freedom Found., D.C.), June 2009, at 2, *available at* www.pff.org/issues-pubs/pops/2009/pop16.12-cyberbullying-education-better-than-regulation.pdf.

349. For one example, see generally *id*.

350. *Digital Literacy and Citizenship in the 21st Century: Educating, Empowering, and Protecting America's Kids*, WHITE PAPER (Common Sense Media, San Francisco, Cal.), June 2009 at 1, 4, [hereinafter *Digital Literacy*] *available at* http://www.commonsensemedia.org/sites/default/files/CSM_digital_policy.pdf.

351. Rebecca Newton & Emma Monks, *Who's Minding the E-Children: Why Kids Can Sensibly Participate on the Net*, GAMER DAILY NEWS http://www.gamersdailynews.com/articlenav-2984-page-1.html (last visited Aug. 28, 2012).

352. Anne Collier, *'Delete Day': Students Putting Messages That Matter*

In recent years, many child safety scholars and child development experts have worked to expand traditional online education and media literacy strategies to place the notion of digital citizenship at the core of their lessons.[353] Online safety expert Anne Collier defines digital citizenship as "critical thinking and ethical choices about the content and impact on oneself, others, and one's community of what one sees, says, and produces with media, devices, and technologies."[354] Common Sense Media, a prominent online safety organization, notes:

> Digital literacy programs are an essential element of media education and involve basic learning tools and a curriculum in critical thinking and creativity.
>
> Digital Citizenship means that kids appreciate their responsibility for their content as well as their actions when using the Internet, cell phones, and other digital media. All of us need to develop and practice safe, legal, and ethical behaviors in the digital media age. Digital Citizenship programs involve educational tools and a basic curriculum for kids, parents, and teachers.[355]

Stephen Balkam, CEO of the Family Online Safety Institute, explains these concepts in practical terms:

> Just as we teach our kids to help at the scene of an accident, or to report a crime and to get involved in their local community, so we need to encourage similar behavior online. To report abusive postings, to alert a grownup or the service provider of inappropriate content, to not pile on when a kid is being cyberbullied, to be part of the solution and not the problem.
>
> We need to use what we've learned about social norms to align

---

Online, NETFAMILYNEWS.ORG (May 6, 2011, 2:41 PM), http://www.netfamilynews.org/?p=30376.

353. Marsali Hancock et al., *From Safety to Literacy: Digital Citizenship in the 21st Century*, THRESHOLD MAG., Summer 2009, at 4; Anne Collier, *From Users to Citizens: How to Make Digital Citizenship Relevant*, NETFAMILYNEWS.ORG (Nov. 16, 2009, 2:23 PM), http://www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; Larry Magid, *We Need to Rethink Online Safety*, HUFFINGTON POST, Jan. 22, 2010, www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html; Nancy Willard, *Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online*, CTR. FOR SAFE & RESPONSIBLE INTERNET USE (Nov. 2008), http://csriu.org/PDFs/yrocomprehensiveapproach.pdf; *Online Safety 3.0: Empowering and Protecting Youth*, CONNECTSAFELY.ORG, www.connectsafely.org/Commentaries-Staff/online-safety-30-empowering-and-protecting-youth.html (last visited Aug. 28, 2012).

354. Anne Collier, *A Definition of Digital Literacy & Citizenship*, NETFAMILYNEWS.ORG (Sept. 15, 2009), www.netfamilynews.org/2009/09/definition-of-digital-literacy.html.

355. *Digital Literacy*, *supra* note 350, at 1 (emphasis omitted).

> kids and ourselves with the positive examples of responsible behavior, rather than be transfixed and drawn towards the portrayals of the worst of the web. It may be true that one in five kids have been involved in sexting, but that means the vast majority exercise good judgment and make wise choices online. The social norms field is ripe with possibilities and guidance in how to foster good digital citizenship.[356]

This approach should be at the center of child safety debates going forward. As online safety educator Nancy Willard notes, responsible digital citizens:

- Understand the risks
- Know how to avoid getting into risk, detect if they are at risk, and respond effectively, including asking for help
- Are responsible and ethical
- Do not harm others
- Respect the privacy and property of others
- Pay attention to the well-being of others
- Make sure their friends and others are safe
- Report concerns to an appropriate adult or site
- Promote online civility and respect.[357]

Only by teaching our children to be good cybercitizens can we ensure they are prepared for life in an age of information abundance.

Many of these same principles and strategies can help us address privacy concerns for both kids and adults. "Again, the solution is critical thinking and digital citizenship," argues online safety expert Larry Magid.[358] He continues, "We need educational campaigns that teach kids how to use whatever controls are built-in to the browsers, how to distinguish between advertising and editorial content and how to evaluate whatever information they come across to be able to make informed choices."[359]

Companies also have an important role to play in creating "well-lit neighborhoods" online where kids will be safe and oth-

---

356. Stephen Balkam, *21st Century Citizenship*, HUFFINGTON POST (Feb. 8, 2010, 5:24 PM), www.huffingtonpost.com/stephen-balkam/21st-century-citizenship_b_453316.html.

357. Willard, *supra* note 353, at 1–2.

358. Larry Magid, *Digital Citizenship and Media Literacy Beat Tracking Laws and Monitoring*, SAFEKIDS.COM (Aug. 29, 2011), http://www.safekids.com/2011/08/29/digital-literacy-critical-thinking-accomplish-more-than-monitoring-tracking-laws.

359. *Id.*

ers can feel their privacy is relatively secure. Many companies and trade associations are also taking steps to raise awareness among their users about how they can better protect their privacy and security.[360] Online operators should also be careful about what (or how much) information they collect—especially if they primarily serve young audiences. Most widely trafficked social networking sites and search engines already offer a variety of privacy controls and allow users to delete their accounts.[361]

Many other excellent online safety- and privacy-enhancing tools already exist for people seeking to safeguard their child's online experiences or their own online privacy.[362] A host of tools are available to block or limit various types of data collection, and every major web browser has cookie-control tools to help users manage data collection.[363] Many nonprofits—including many privacy advocates—offer instructional websites and videos explaining how privacy-sensitive consumers can take steps to protect their personal information online.[364]

---

360. *See* ADAM THIERER, MERCATUS CTR., PUBLIC INTEREST COMMENT ON FEDERAL TRADE COMMISSION REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 9 (2011) [hereinafter PUBLIC INTEREST COMMENT], *available at* http://mercatus.org/sites/default/files/public-interest-comment-on-protecting-consumer-privacy-do-not-track-proceeding.pdf ("[S]ome companies appear to be competing on privacy. . . . [O]ne company offers an Internet search service . . . as being . . . more privacy-sensitive . . . . [I]n response to Google's decision to change its privacy policies . . . Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.").

361. *See id.* at 7 ("The private sector has taken steps to enhance user privacy and security as well. . . . Google and Facebook have improved authentication mechanisms to give users stronger protection against compromised passwords. Also, privacy-enhancing technologies . . . have given users additional tools to encrypt their information in transit.").

362. *Id.* at 24, 24–28.

363. Importantly, just as most families leave the vast majority of parental control technologies untapped, many households will never take advantage of these privacy-enhancing empowerment tools. That fact does not serve as proof of "market failure" or the need for government regulation, however. What matters is that the tools exist for those who wish to use them, not the actual usage rates of those tools. Adam Thierer, *Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies*, PROGRESS ON POINT (Progress & Freedom Found., D.C.), Feb. 27, 2009, at 1, *available at* http://www.pff.org/issues-pubs/pops/2009/pop16.5parentalcontrolsmarket.pdf.

364. Privacy Rights Clearinghouse, *Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social*, PRIVACYRIGHTS.ORG (Aug. 2012), https://www.privacyrights.org/social-networking-privacy.

Taken together, this amounts to a "layered approach" to online safety and privacy protection. Only by using many tools, methods, strategies, social norms, and forms of market pressure can we ensure youngsters are safe online while they learn to cope with new technology and adapt to the changing world around them.

Importantly, education and empowerment efforts such as these have the added advantage of being more flexible than government regulation, which can lock in suboptimal policies and stifle ongoing innovation.[365] To the extent government plays a role, it should be to facilitate learning and resiliency through educational and empowerment-based solutions, not heavy-handed, silver-bullet regulatory solutions. For example, the Federal Trade Commission hosts a collaborative effort with other federal agencies called "OnGuard Online," which represents a savvy approach to raising awareness about various online threats.[366]

2. Cybersecurity

As noted earlier, the technopanic mentality developing around cybersecurity and cyberwar is generally overblown.[367] That does not mean, however, that no cyberattacks will ever occur. Some already have and others will likely occur in the future.

Recent work by Sean Lawson, an assistant professor in the Department of Communication at the University of Utah, has underscored the importance of resiliency as it pertains to cybersecurity. "Research by historians of technology, military historians, and disaster sociologists has shown consistently that modern technological and social systems are more resilient than military and disaster planners often assume," he writes.[368] He continues, "Just as more resilient technological

---

365. *See* THE PRESIDENT'S COUNCIL ON COMPETITIVENESS, THE LEGACY OF REGULATORY REFORM: RESTORING AMERICA'S COMPETITIVENESS at ix (1992) ("The nation has learned through experience, however, that government regulation often creates more problems than it 'solves.'"); *see also* Robert W. Hahn, *Regulation: Past, Present, and Future*, 13 HARV. J.L. & PUB. POL'Y 167, 228 (1990) ("Inflexible social regulations that place strict, detailed limits on firms' behavior also frequently stifle innovation and impose unnecessary costs.").

366. ONGUARD ONLINE, http://www.onguardonline.gov (last visited Sept. 5 2012).

367. Crawford, *supra* note 198.

368. Sean Lawson, *Beyond Cyber Doom: Cyber Attack Scenarios and the Evidence of History* 31 (Mercatus Ctr., Working Paper No. 11-01, Jan. 2011),

systems can better respond in the event of failure, so too are strong social systems better able to respond in the event of disaster of any type."[369]

Education is a crucial part of building resiliency in this context as well. People and organizations can prepare for potential security problems in a rational fashion if given even more information and better tools to secure their digital systems and to understand how to cope when problems arise.[370]

Of course, "[m]ost Internet service providers (ISPs) and other players already take steps to guard against malware and other types of cyberattacks, and they also offer customers free (or cheap) security software."[371] "Corporations, including software vendors, antimalware makers, ISPs, and major websites such as Facebook and Twitter, are aggressively pursuing cyber criminals," notes Roger Grimes of *Infoworld*.[372] "These companies have entire legal teams dedicated to national and international cyber crime. They are also taking down malicious websites and bot-spitting command-and-control servers, along with helping to identify, prosecute, and sue bad guys," he says.[373]

Thus, while it is certainly true that "more could be done" to secure networks and critical systems, panic is unwarranted because much is already being done to harden systems and educate the public about risks.[374] Various digital attacks will continue, but consumers, companies, and others organizations are learning to cope and become more resilient in the face of those threats.

3. Market Power and Economic Issues

In a general sense, resiliency and adaptation are applicable to debates about the economic impact of information technology

---

available at http://mercatus.org/publication/beyond-cyber-doom.

369. *Id.* at 29.

370. *Id.* at 29 ("[I]f the worst should occur, average citizens must be empowered to act in a decentralized, self-organized way to help themselves and others.").

371. *Avoiding a Precautionary Principle*, *supra* note 272.

372. Roger Grimes, *The Cyber Crime Tide is Turning*, PCWORLD (Aug. 9, 2011, 3:23 PM), http://www.pcworld.com/article/237647/the_cyber_crime_tide_is_turning.html.

373. *Id.*

374. Adam Thierer, *Don't Panic Over Looming Cybersecurity Threats*, FORBES (Aug. 7, 2011, 7:53 PM), http://www.forbes.com/sites/adamthierer/2011/08/07/dont-panic-over-looming-cybersecurity-threats.

just as they were applicable to debates about the impact of previous waves of technological change and creative destruction. If we want economic progress to occur, we must learn to cope with structural shifts in an economy, industrial disruptions, sectoral realignments, and job displacements. "Opponents of change," notes Rob Atkinson, "want a world in which risk is close to zero, losers are few, and change is glacial and controlled."[375] Yet, as he correctly argues, that would stifle progress and prosperity:

> There is no doubt that in a society buffeted by the winds of change risk that such a world has significant appeal. But the result of living in such a world would mean that our incomes will go up much more slowly and technological progress to improve health, protect the environment, and improve our lives would slow down significantly. If we want more, we have to risk more. It is as simple as that.[376]

This is why the precautionary principle mentality is so dangerous for a free and innovative economy. Carl Gipson, a technology policy analyst formerly with the Washington Policy Center, correctly asserts:

> Our society and our economy benefit from risk takers. People who risk their financial wellbeing, their time, their energy or their future are willing to take a chance to change the world for the better. And as a society we are better off for their ability and willingness to engage in risky but productive behavior.[377]

A resiliency-based approach to economic change leaves sufficient breathing room for risk takers to be entrepreneurial and discover better, cheaper, and more innovative ways of doing things. By contrast, concludes Gipson, "strict adherence to a precautionary principle in the technology industry would rob our society and economy of countless innovations, because the accompanying risks far outweigh the supposed benefits."[378]

A resiliency mindset also helps us understand why "market power" claims are often too casually bandied about by some pessimists and why patience and humility "in the face of market uncertainty is the more sensible disposition . . . ."[379]

---

375. ROBERT D. ATKINSON, THE PAST AND FUTURE OF AMERICA'S ECONOMY 201 (2004).

376. *Id.*

377. CARL GIPSON, THE EMERGENCE OF THE DIGITAL PRECAUTIONARY PRINCIPLE 9 (2011).

378. *Id.*

379. Adam Thierer, *The Rule Of Three: The Nature of Competition In The Digital Economy*, FORBES (June 29, 2012), http://www.forbes.com/sites/adamthierer/2012/06/29/the-rule-of-three-the-nature-of-competition-in-the-digital-economy/.

Schumpeterian creative destruction has been rapidly eroding "market power" in the digital economy.[380] While some Internet critics fear the worst about growing "information empires,"[381] the truth is that their reign is usually brief as new digital services and platforms rapidly displace each another.[382] Rash interventions aimed at alleviating every short-term hiccup will do far more harm than good.

E. RESILIENCY MAKES EVEN MORE SENSE WHEN PRACTICALITY OF CONTROL IS CONSIDERED

Resiliency is a "particularly sensible approach to dealing with risk in light of the growing futility associated with efforts to prohibit or control information flows."[383] Increasingly, it is too challenging and costly to bottle up information flows. This was true in the era of media and information scarcity, with its "physical and analog distribution methods of information dissemination."[384] However, "the challenge of controlling information in the analog era paled in comparison to the far more formidable challenges governments face in the digital era when they seek to limit information flows."[385]

More specifically, relative to the analog era, information control efforts today are complicated by several factors unique to the Information Age, including:

- Digitization of information, which makes data replication much easier and more reliable;[386]
- Falling storage costs and growing storage capacity, which has made information backup and retrieval easier;
- Dramatic expansions in computing/processing pow-

380. JOSEPH SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY 84 (2008).

381. *See* TIM WU, THE MASTER SWITCH 7–8 (2010).

382. Adam Thierer, *Of 'Tech Titans' and Schumpeter's Vision*, FORBES (Aug. 22, 2011, 12:31 PM), http://www.forbes.com/sites/adamthierer/2011/08/22/of-tech-titans-and-schumpeters-vision.

383. *Avoiding a Precautionary Principle*, *supra* note 272.

384. PUBLIC INTEREST COMMENT, *supra* note 360, at 7.

385. *Id.*

386. NICHOLAS NEGROPONTE, BEING DIGITAL 228 (1995) ("[Digital] bits will be borderless, stored and manipulated with absolutely no respect to geopolitical boundaries.").

er, which is driven by "Moore's Law";[387]

- Ongoing convergence of media platforms and information technologies, which means information can travel over multiple channels and get to citizens more easily than in the past;[388]
- Decentralized, distributed networks, which lack a central point of control;[389]
- Rapid growth in the overall volume of information being distributed and accessed; which means there is exponentially more data with which policymakers must contend;[390] and,
- Explosive growth of user-generated content and user self-revelation of data, which means information control efforts must grapple with more than just "professional" content creation and distribution methods and networks.[391]

The end result of these new developments and technological realities, as David Friedman of Santa Clara Law School has

---

387. Adam Thierer, *Sunsetting Technology Regulation: Applying Moore's Law to Washington*, FORBES (Mar. 25, 2012, 12:56 PM), http://www.forbes.com/sites/adamthierer/2012/03/25/sunsetting-technology-regulation-applying-moores-law-to-washington.

388. HENRY JENKINS, CONVERGENCE CULTURE: WHERE OLD AND NEW MEDIA COLLIDE 2 (2006) (defining convergence as "the flow of content across multiple media platforms, the cooperation between multiple media industries, and the migratory behavior of media audiences who will go almost anywhere in search of the kinds of entertainment experiences they want").

389. MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 4 (2010) ("Combined with liberalization of the telecommunications sector, the Internet protocols decentralized and distributed participation in and authority over networking and ensured that the decision-making units over network operations are no longer closely aligned with political units.").

390. DOWNES, *supra* note 93, at 69 ("Since 1995 the sheer volume of information—personally identifiable and otherwise—that has become digitized and can be cheaply transported around the world has grown by orders of magnitude.").

391. Yochai Benkler notes:

> The material requirements for effective information production and communication are now owned by numbers of individuals several orders of magnitude larger than the number of owners of the basic means of information production and exchange a mere two decades ago. . . . Individuals can reach and inform or edify millions around the world. Such a reach was simply unavailable to diversely motivated individuals before . . . .

YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 4 (2006).

noted, is that "[o]nce information is out there, it is very hard to keep track of who has it and what he has done with it."[392] "The uncertainties and dislocations from new technology can be wrenching," observes *The Wall Street Journal*'s L. Gordon Crovitz, "but genies don't go back into bottles."[393] "The explosive growth is still happening," note Abelson, Ledeen, and Lewis.[394] They additionally note, "Every year we can store more information, move it more quickly, and do far more ingenious things with it than we could the year before."[395]

Again, this has implications for how we manage technological risk. When the possibility of societal information control or regulation is diminished—or proves too costly—resiliency and adaptation strategies become even more attractive alternatives.[396] In the absence of controls, information will be able to flow even more freely on interconnected, ubiquitous digital networks.[397] Getting those information genies back in their bottles would be an enormous challenge.

Moreover, the burdens on the administration or enforcement of modern information-control efforts can be significant and are as important as the normative considerations at play.[398] The increased complications associated with information-control efforts means that the economic and social costs of regulation will often exceed the benefits.[399]

Consequently, a strategy based on building resiliency will focus on more cost-effective education and empowerment-based

---

392. DAVID D. FRIEDMAN, FUTURE IMPERFECT: TECHNOLOGY AND FREEDOM IN AN UNCERTAIN WORLD 62 (2008).

393. L. Gordon Crovitz, Op-Ed., *Optimism and the Digital World*, WALL ST. J., Apr. 21, 2008, at A15.

394. HAL ABELSON ET AL., BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 3 (2008).

395. *Id.*

396. *See generally* Julien Mailland, Note, *Freedom of Speech, the Internet, and the Costs of Control: The French Example*, 33 N.Y.U. J. INT'L L. & POL. 1179, 1198–99 (2001) (describing the French government's attempts at controlling decentralized internet networks).

397. *See generally id.* at 1200–01 (describing how isolating a source in country A might require disconnecting the entire nation from the network in country B).

398. *Id.*

399. *See id.* at 1213–14 (noting the potential economic harm stemming from applying traditional regulations to the different circumstances inherent to the internet).

strategies.[400] This allows for trial and error, and encourages sensible and measured responses to the challenges posed by technological change.[401] These approaches will teach lessons and values that will accommodate future disruptive changes in our culture and economy.[402]

"These technologies are inevitable. And they will cause some degree of harm," notes Kevin Kelly, "Yet their most important consequences—both positive and negative—won't be visible for generations."[403] Thus, we must learn to "count on uncertainty" and appreciate the benefits of ongoing experimentation and innovation. This doesn't mean we shouldn't try to foresee problems associated with new technologies or address some of them preemptively, but that it should be done without resisting new technologies or technological change altogether. "The proper response to a lousy technology is not to stop technology or to produce no technology," Kelly argues, "It is to develop a better, more convivial technology."[404]

Kelly's formulation is remarkably similar to the "bad speech/more speech principle" from First Amendment jurisprudence.[405] This principle states that the best solution to the problem of bad speech, such as hate speech or seditious talk, is more speech to counter it instead of censorship.[406] Kelly advocates the use of this principle: when it comes to technology, society should find ways to embrace it, to soften its blow, or to counter it with new and better technology rather than to ban or restrict it.[407] This principle represents the smart way forward.

VII. A FRAMEWORK FOR EVALUATING AND ADDRESSING TECHNOLOGY RISK

Regardless of the issue, the following four-part framework

---

400. *Avoiding a Precautionary Principle*, *supra* note 272.

401. *Id.*

402. *Id.*

403. KELLY, supra note 303, at 261.

404. *Id.* at 263.

405. *See, e.g.*, Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring) ("If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.").

406. *See* Adam Thierer, *Do We Need a Ministry of Truth for the Internet?*, FORBES (Jan. 29, 2012, 11:46 PM), http://www.forbes.com/sites/adamthierer/2012/01/29/do-we-need-a-ministry-of-truth-for-the-internet.

407. *See* KELLY, *supra* note 303, at 262 ("We can only shape technology's expression by engaging with it, by riding it with both hands around its neck.").

should be used to analyze the risks associated with new technological developments and to determine the proper course of action.[408]

A. DEFINING THE PROBLEM

The first step involves defining the problem to be addressed and determining whether harm or market failure exists.[409] These are two separate inquires. Defining the problem is sometimes easier said than done—what is it that we are trying to accomplish?

It is vital that "harm" or "market failure" not be too casually defined.[410] Harm is a particularly nebulous concept as it pertains to online safety and digital privacy debates where conjectural theories abound. Some cultural critics insist that provocative media content "harms" us or our kids.[411] Critical views on restricting objectionable forms of media only emphasize that "harm" can be very much "in the eye of the beholder." It is important to keep in mind that no matter how objectionable some media content or online speech may be, none of it poses a *direct* threat to adults or children.[412]

Likewise, some privacy advocates claim that advertising is inherently "manipulative" or that more targeted forms of marketing and advertising are "creepy" and should be prohibited.[413]

---

408. *See* RICHARD WILLIAMS & JERRY ELLIG, REGULATORY OVERSIGHT: THE BASICS OF REGULATORY IMPACT ANALYSIS 2 (2011), *available at* http://mercatus.org/sites/default/files/Mercatus-Regulatory-Impact-Analysis-Toolkit.pdf (detailing a four-part analytical framework for examining regulatory impact).

409. *See id.*

410. *See generally* Steven Horwitz, *The Failure of Market Failure*, FREEMAN (Dec. 8, 2011), http://www.thefreemanonline.org/headline/failure-of-market-failure (arguing that the definition of "market failure" is problematic because of its variety of meanings).

411. *See, e.g.*, Robert Zaid, *Harms of Social Media*, ARTICLESBASE (July 13, 2012), http://www.articlesbase.com/information-technology-articles/harms-of-social-media-6052928.html (discussing the harms of instant feedback and online bullying).

412. *But see id.* (noting that new media harms result from psychological pressures not immediate, impending danger).

413. *See generally* Mike Masnick, *Getting Past the Uncanny Valley in Targeted Advertising*, TECHDIRT (Feb. 17, 2012, 7:39 PM), http://www.techdirt.com/blog/innovation/articles/20120217/03044617792/getting-past-uncanny-valley-targeted-advertising.shtml (discussing the creepiness of targeted advertising).

"But creating new privacy rights cannot be justified simply because people feel vague unease," notes Solveig Singleton, formerly of the Cato Institute.[414] If harm in this context is reduced to "creepiness" or even "annoyance" and "unwanted solicitations" as some advocate, it raises the question of whether the commercial Internet as we know it can continue to exist. Such an amorphous standard leaves much to the imagination and opens the door to creative theories of harm, which are sure to be exploited.[415] In such a regime, harm becomes highly conjectural instead of concrete. This makes credible cost-benefit analysis virtually impossible since the debate becomes purely emotional instead of empirical.[416]

Turning to economic considerations, accusations of consumer "harm" are often breezily tossed about by many policymakers and regulatory advocates without any reference to actual evidence proving that consumer welfare has been negatively impacted.[417] "Market failure" claims are also rampant even though many critics are sometimes guilty of adopting a simplistic "big is bad" mentality.[418] Regardless, a high bar must be established before steps are taken to regulate information and digital technologies based on market failure allegations.

B. CONSIDER LEGAL AND ECONOMIC CONSTRAINTS

The second step is to identify constitutional constraints and conduct a cost-benefit analysis of government regulation.[419]

---

414. SOLVEIG SINGLETON, PRIVACY AS CENSORSHIP: A SKEPTICAL VIEW OF PROPOSALS TO REGULATE PRIVACY IN THE PRIVATE SECTOR 8 (1998), *available at* http://www.cato.org/pubs/pas/pa-295.pdf.

415. Adam Thierer, *On "Creepiness" as the Standard of Review in Privacy Debates*, TECH. LIBERATION FRONT (Dec. 13, 2011), http://techliberation.com/2011/12/13/on-creepiness-as-the-standard-of-review-in-privacy-debates.

416. PUBLIC INTEREST COMMENT, *supra* note 360, at 2–3.

417. *See* DANIEL CASTRO, STRICTER PRIVACY REGULATIONS FOR ONLINE ADVERTISING WILL HARM THE FREE INTERNET 2–3 (2010), *available at* http://www.itif.org/files/2010-privacy-regs.pdf (explaining the negative impact of regulations created because of misconceptions about targeted advertising).

418. *But see, e.g.*, Scott Cleland, *Where's the Market for Online Privacy?*, PRECURSOR BLOG (Jan. 31, 2012, 12:17), http://precursorblog.com/content/wheres-market-online-privacy.

419. *See generally* Letter from Richard Williams, Dir. of Policy Research, Mercatus Ctr at George Mason Univ., to Cass Sunstein, Office of Info. & Regulatory Affairs (June 11, 2012) (on file with the Mercatus Center), *available at* http://mercatus.org/sites/default/files/Williams-2012-response-to-OMB-Report.pdf (commenting on the costs and benefits of federal regulations).

If harm or market failure can be demonstrated, the costs associated with government action must be considered.[420] Evaluating the costs could show that government may not effectively address the problem even when there is harm or a market failure. Regulation is not a costless exercise, and sometimes its benefits are artificially inflated.[421] Further, Gardner notes that "[t]he public often demands action on a risk without giving the slightest consideration to the costs of that action."[422] Yet, because government action entails both economic and social tradeoffs it follows that proposed rules should always be subjected to a rigorous cost-benefit analysis.

Of course, not all legal solutions entail the same degree of cost or complexity as approaches using direct regulation. Can the problem be dealt with through traditional common law methods? Can contracts, property rights, antifraud statutes, or anti-harassment standards help?

Again, consider privacy harms. Instead of trying to implement cumbersome, top-down privacy directives based on amorphous assertions of privacy "rights," the Federal Trade Commission (FTC) should "hold[] companies to [the] promises" they make when it comes to the personal information they collect and what they do with it.[423] The FTC has already brought and settled many privacy and data security cases involving its role in policing "unfair or deceptive acts or practices."[424] Recently, the FTC has brought enforcement actions against Google and

---

420. *See* GARDNER, *supra* note 84, at 83 ("[R]egulations can also impose costs on economic activity, and since wealthier is healthier, economic costs can, if they are very large, put more lives at risk than they keep safe.").

421. SHERZOD ABDUKADIROV & DEEMA YAZIGI, INFLATED BENEFITS IN AGENCIES' ECONOMIC ANALYSIS 2 (2012), *available at* http://mercatus.org/sites/default/files/InflatedBenefits_MOP112.pdf.

422. GARDNER, *supra* note 84, at 83.

423. Berin Szoka, *FTC Enforcement of Corporate Promises & the Path of Privacy Law*, TECH. LIBERATION FRONT (July 13, 2010), http://techliberation.com/2010/07/13/ftc-enforcement-of-corporate-promises-the-path-of-privacy-law.

424. 15 U.S.C. § 45 (2006); *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 273 (2011) ("[S]ince 1996 the FTC has actively used its broad authority under Section 5 of the FTC Act, which prohibits 'unfair or deceptive practices,' to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.").

Facebook.[425] Both companies agreed through a consent decree to numerous privacy policy changes and must also undergo privacy audits for the next twenty years.[426] Again, no new law was needed to accomplish this. The FTC's authority was more than sufficient.

Of course, information technology is, by definition, tied up with the production and dissemination of speech. Consequently, First Amendment values may be implicated and limit government action in many cases.

C. CONSIDER ALTERNATIVE, LESS RESTRICTIVE APPROACHES

The third step involves an assessment of the effectiveness of alternative approaches to addressing the perceived problem.

Because preemptive, prophylactic regulation of information technology can be costly, complicated, and overly constraining, less-restrictive approaches should be considered.[427] Empowerment-, education-, awareness-building strategies can be particularly effective, as well as being entirely constitutional. As noted previously, these strategies can help build resiliency and ensure proper assimilation of new technologies into society.

If regulation is still deemed necessary, transparency and disclosure policies should generally trump restrictive rules. For example, after concerns were raised about wireless "bill shock"—abnormally high phone bills resulting from excessive texting or data usage—FCC regulators hinted that regulation may be needed to protect consumers.[428] Eventually, the wireless industry devised a plan to offer their customers real-time alerts before exceeding their monthly text or data allotments.[429] Although these concessions weren't entirely voluntary, this

---

425. *See* Alex Howard, *Google Reaches Agreement with FTC on Buzz Privacy Concerns*, GOV 2.0 (Mar. 30, 2011, 11:38 AM), http://gov20.govfresh.com/google-reaches-agreement-with-ftc-on-buzz-privacy-concerns; Brent Kendall, *Facebook Reaches Settlement with FTC on Privacy Issues*, WALL ST. J. (Nov. 29, 2011, 1:29 PM), http://online.wsj.com/article/BT-CO-20111129-710865.html.

426. Kashmir Hill, *So, What Are These Privacy Audits That Google And Facebook Have To Do For The Next 20 Years?*, FORBES (Nov. 30, 2011, 2:29 PM), http://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years.

427. *See generally* Szoka, *supra* note 423 (suggesting the FTC use a case-by-case process).

428. Amy Schatz, *Cellphone Users to Get Billing Alerts Under New Voluntary Standards*, WALL ST. J., Oct. 17, 2011, at B3.

429. *Id.*

transparency-focused result is nonetheless superior to cumbersome rate regulation or billing micromanagement by regulatory officials.[430] Many wireless operators already offered text alerts to their customers before the new notification guidelines were adopted, but the additional transparency more fully empowers consumers.[431]

Transparency and disclosure are also the superior options for most online safety and privacy concerns. Voluntary media content ratings and labels for movies, music, video games, and smart phone apps have given parents more information to make determinations about the appropriateness of content they or their children may want to consume.[432] Regarding privacy, consumers are better served when they are informed about online privacy and data collection policies of the sites they visit and the devices they utilize.[433]

D. EVALUATE ACTUAL OUTCOMES

Finally, if and when regulatory solutions are pursued, it is vital that actual outcomes be regularly evaluated and, to the extent feasible, results be measured.[434] To the extent regulatory policies are deemed necessary, they should sunset on a regular basis unless policymakers can justify their continued existence.[435] Moreover, even if regulation is necessary in the short-term, resiliency and adaptation strategies may emerge as their

---

430. *See generally* Katy Bachman, *Wireless Companies Stave Off Regulation with New Usage Alerts*, ADWEEK (Oct. 17, 2011), http://www.adweek.com/news/technology/wireless-companies-stave-regulation-new-usage-alerts-135869 (noting that compliance is ensured partially through the implicit threat of mandatory regulation).

431. *See, e.g.*, *id.*

432. ADAM THIERER, PARENTAL CONTROLS & ONLINE CHILD PROTECTION: A SURVEY OF TOOLS & METHODS 19, 41–42 (2009), *available at* http://www.pff.org/parentalcontrols/Parental%20Controls%20&%20Online%20Child%20Protection%20[VERSION%204.0].pdf.

433. *See id.* at 22.

434. RANDALL LUTTER, HOW WELL DO FEDERAL REGULATIONS ACTUALLY WORK? THE ROLE OF RETROSPECTIVE REVIEW 1 (2012), *available at* http://mercatus.org/sites/default/files/Regulatory-Retrospective-Review-Summary.pdf.

435. Adam Thierer, *Sunsetting Technology Regulation: Applying Moore's Law to Washington*, FORBES (Mar. 25, 2012, 12:56 PM), http://www.forbes.com/sites/adamthierer/2012/03/25/sunsetting-technology-regulation-applying-moores-law-to-washington.

benefits become more evident over time.[436]

VIII. CONCLUSION

This paper explains why pessimistic prognostications dominate so many discussions about the future of the Internet and digital technology today. It boils down to a combination of individual attitudes and institutional dynamics.[437] Fear-based reasoning and tactics are used by both individuals and institutions to explain or cope with complicated social, economic, or technological change. Other times, however, these fears are being intentionally inflated by activists, academics, or policymakers in an attempt to expand their own power or influence. In this sense, we would be wise to remember H.L. Mencken's famous quip that "the whole aim of practical politics is to keep the populace alarmed (and hence clamorous to be led to safety) by an endless series of hobgoblins, most of them imaginary."[438]

After careful reflection and evaluation, most fears surrounding new information technologies are based on logical fallacies and inflated threats that lead to irrational technopanics and fear cycles. There are many psychological and sociological explanations for why humans are predisposed to being pessimistic and risk-averse.[439] Nonetheless, most of these fears are not justified when empirical evidence is dispassionately considered. When there *is* something to these fears, alternative methods are often available to cope with the problems brought on by technological change.

If these fears and the fallacies that support them are not exposed and debunked, it is possible that a precautionary-principle mindset will take root in the information technology arena. If so, prohibition and anticipatory regulation will be increasingly proffered as solutions. Resiliency and adaption

---

436. *See id.* (proposing that all technology proposals have a sunset provision).

437. *See* Adam Thierer, *Book Review: "Resilience: Why Things Bounce Back" by Zolli and Healy*, FORBES (Aug. 26, 2012, 10:40 AM), http://www.forbes.com/sites/adamthierer/2012/08/26/book-review-resiliency-why-things-bounce-back-by-zolli-and-healy.

438. H.L. MENCKEN, IN DEFENSE OF WOMEN 53 (1922).

439. *See generally* GARDNER, *supra* note 84, at 59–86 (detailing misconceptions of catastrophic events, such as meteors or volcanic eruptions, and how we evaluate them based on emotion rather than logic); MICHAEL SHERMER, THE BELIEVING BRAIN: FROM GHOSTS AND GODS TO POLITICS AND CONSPIRACIES—HOW WE CONSTRUCT BELIEFS AND REINFORCE THEM AS TRUTHS 274–76 (2011) (listing common biases and beliefs).

strategies are generally superior to more restrictive approaches because they leave more breathing room for continuous learning and innovation through trial-and-error experimentation. Even when that experimentation may involve risk and the chance of mistake or failure, the result of such experimentation is wisdom and progress. As Friedrich August Hayek concisely wrote, "Humiliating to human pride as it may be, we must recognize that the advance and even preservation of civilization are dependent upon a maximum of opportunity for accidents to happen."[440]

440. F. A. HAYEK, THE CONSTITUTION OF LIBERTY 29 (1960).