No. 12-09
February 2012

WORKING PAPER

TECHNOPANICS, THREAT INFLATION, AND THE DANGER OF AN INFORMATION TECHNOLOGY PRECAUTIONARY PRINCIPLE

By Adam Thierer

MERCATUS CENTER
George Mason University

TECHNOPANICS, THREAT INFLATION, AND THE DANGER OF AN INFORMATION TECHNOLOGY PRECAUTIONARY PRINCIPLE

Adam Thierer[*]

CONTENTS

[*] 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.

I. INTRODUCTION

> *In time we hate that which we often fear*.
>
> — 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 wellbeing 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." These panics are intense public, political, and academic responses to the emergence or use of media or technologies, especially by the young. 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. That has not stopped some from suggesting there are reasons to be particularly fearful of the Internet and new digital technologies. There are various individual and institutional factors 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 Argumentational 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:[1]

- *Fearful Situational Premise*: Here is a situation that is fearful to you.
- *Conditional Premise*: If you carry out A, then the negative consequences portrayed in the fearful situation will happen to you.
- *Conclusion*: You should not carry out A.

This logic pattern here is referred to as *argumentum in terrorem* or *argumentum ad metum*. A closely related variant of this argumentation scheme is known as *argumentum ad baculum*, or an argument based on a threat. *Argumentum ad baculum* literally means "argument to the stick," an appeal to force. Walton outlines the *argumentum ad baculum* argumentation scheme as follows:[2]

- *Conditional Premise*: If you do not bring about A, then consequence B will occur.
- *Commitment Premise*: I commit myself to seeing to it that B comes about.
- *Conclusion*: You should bring about A.

As will be shown, these argumentation devices are at work in many information technology policy debates today even though they

---

1 Douglas Walton, *Fundamentals of Critical Argumentation* (Cambridge: Cambridge University Press, 2006), 285.

2 Ibid., 287.

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 Situational Premise*: Letting kids 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 logical fallacies or be based on myths.[3]

First, the situational 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. 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 prove causation.[4]

---

[3] Adam Thierer, "Fact and Fiction in the Debate over Video Game Regulation," *Progress on Point*, no. 13.7 (Washington, D.C.: The Progress & Freedom Foundation, March 20, 2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985585.

[4] This is often the result of a confusion between probability and outcome. While there may be a low probability that depictions of violence could lead to actual violence, the dispute ought to be about the probability. 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.

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 and, yet, may be difficult to separate or treat as an independent variable. 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.[5] Many children will witness depictions of violence in movies, television, or video games without suffering any negative cognitive impact. Others may be adversely impacted by consumption of such content.

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.

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.[6] It is a variant of "moral panic" theory. Christopher Ferguson, professor at Texas A&M's Department

---

[5] "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." Marjorie Heins, *Not in Front of the Children: "Indecency," Censorship, and the Innocence of Youth* (New York: Hill and Wang, 2011), 228.

[6] Adam Thierer, "Against Technopanics," *Technology Liberation Front*, July 15, 2009, http://techliberation.com/2009/07/15/against-technopanics.

of Behavioral, Applied Sciences, and Criminal Justice, offers the following definition: "A moral panic occurs when a segment of society believes that the behavior or moral choices of others within that society poses a significant risk to the society as a whole."[7] 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 in legal and social policy or even the way the society conceives itself.[8]

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 on "The MySpace Moral Panic," Alice Marwick noted that 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,

---

[7] Christopher J. Ferguson, "The School Shooting/Violent Video Game Link: Causal Relationship or Moral Panic?" *Journal of Investigative Psychology and Offender Profiling*, 5, nos. 1–2, (2008) 25–37, http://onlinelibrary.wiley.com/doi/10.1002/jip.76/abstract.

[8] Stanley Cohen, *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, (London, UK: MacGibbon and Kee, 1972), 9.

> either by controlling young people or the creators or producers of media products.[9]

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."[10] "The first push-back is going to be about kids," she observes. "Is it making our children vulnerable? To predators? To other forms of danger? We will immediately then regulate access."[11] She argues that cultures sometimes adapt more slowly than technologies evolve and that leads to a greater potential for panics.

This pattern has played out for dime novels, comic books, movies, rock-and-roll music, video games, and other types of media or media platforms.[12] While protection of youth is typically a motivating factor, some moral panics and technopanics transcend traditional "it's-for-the-children" rationales 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.

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. 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. Sociologists Erich Goode and Nachman Ben-Yehuda, authors of *Moral Panics: The Social Construction of Deviance*, observe that

> 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, either stiffer penalties or a law enforcement crackdown will be called for. Legislation and law enforcement are two of the

---

[9] Alice Marwick, "The MySpace Moral Panic," *First Monday* 13 nos. 6–2, (June 2008), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2152/1966.

[10] Ben Rooney, "Women and Children First: Technology And Moral Panic," *Wall Street Journal Tech Europe*, July 11, 2011, http://blogs.wsj.com/tech-europe/2011/07/11/women-and-children-first-technology-and-moral-panic.

[11] Ibid.

[12] Robert Corn-Revere, "Moral Panics, the First Amendment, and the Limits of Social Science," *Communications Lawyer* 28, no. 3 (2011).

> most obvious and widely resorted-to efforts to crush a putative threat during a moral panic.[13]

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.[14] 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."[15]

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 development or technology poses to certain classes of the population, especially children, or to society or the economy at large. These rhetorical flourishes are empirically false or at least greatly blown out of proportion relative to the risk in question. 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 "cybersecurity industrial complex."[16]

The fear appeal for cybersecurity can be outlined as follows:

---

[13] Erich Goode and Nachman Ben-Yehuda, *Moral Panics: The Social Construction of Deviance* (Malden, MA: Blackwell Publishing, 1994), 82.

[14] Chaim Kaufmann, "Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War," *International Security* 29 (Summer 2004), 5–48, http://belfercenter.ksg.harvard.edu/files/kaufmann.pdf.

[15] Jane K. Cramer and A. Trevor Thrall, "Framing Iraq: Threat Inflation in the Marketplace of Values," in *American Foreign Policy and the Politics of Fear*, ed. A. Trevor Thrall and Jane K. Cramer (London: Routledge, 2009), 1.

[16] Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy" (working paper, Mercatus Center at George Mason University, Arlington, VA, 2011), 2.

- *Fearful Situational Premise*: Cyber-attacks will be increasingly sophisticated and eventually one could 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,"[17] a "cyber cold war,"[18] a "cyber Katrina,"[19] or even a "cyber 9/11."[20] These analogies are made even though 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.[21]

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,

---

[17] Former Obama Administration Central Intelligence Agency chief Leon Panetta told Congress in February 2011 that "the potential for the next Pearl Harbor could very well be a cyber attack." Richard Serrano, "U.S. Intelligence Officials Concerned about Cyber Attack," *Los Angeles Times*, February 11, 2011, http://www.latimes.com/news/nationworld/nation/la-na-intel-hearing-20110211,0,2209934.story.

[18] Retired Lt. Gen. Harry Raduege, "Deterring Attackers in Cyberspace," *The Hill*, September 23, 2011, http://thehill.com/opinion/op-ed/183429-deterring-attackers-in-cyberspace.

[19] Sen. Olympia Snowe (R-Maine) has argued that "if we fail to take swift action, we, regrettably, risk a cyber Katrina." David Kravets, "Vowing to Prevent 'Cyber Katrina,' Senators Propose Cyber Czar," *Wired Threat Level*, April 1, 2009, http://www.wired.com/threatlevel/2009/04/vowing-to-preve.

[20] Kurt Nimmo, "Former CIA Official Predicts Cyber 9/11," *InfoWars.com,* August 4, 2011, http://www.infowars.com/former-cia-official-predicts-cyber-911.

[21] Rodney Brown, "Cyber Bombs: Data-Security Sector Hopes Adoption Won't Require a 'Pearl Harbor' Moment," *Mass High-Tech Innovation Report*, October 26, 2011, http://www.securityprivacyandthelaw.com/uploads/file/cyber%20bombs.pdf.

Illinois, that resulted in the temporary failure of a water pump.[22] 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."

The Washington Post quickly followed up with an article headlined "Foreign Hackers Targeted U.S. Water Plant in Apparent Malicious Cyber Attack, Expert Says" and claiming that, "The incident was a major new development in cyber-security."[23] Other headlines likened the incident to a "Stuxnet strike" on U.S. soil, referring to the cyber-attack on an Iranian nuclear facility.[24] Media pundits, cybersecurity activists, and congressional lawmakers all quickly pounced on these reports as supposed proof of a serious threat. 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, "The potential attack that took place in Springfield, Illinois, should be a real wakeup call."[25]

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.[26] In fact, a plant contractor, who happened to have been travelling to Russia at the

---

[22] Joe Weiss, "Water System Hack - The System Is Broken," *ControlGlobal.com,* November 17, 2011, http://community.controlglobal.com/content/water-system-hack-system-broken.

[23] Ellen Nakashima, "Foreign Hackers Targeted U.S. Water Plant in Apparent Malicious Cyber Attack, Expert Says," *The Washington Post*, November 18, 2011, http://www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html.

[24] Mark Long, "Stuxnet Strike on U.S. Utility Signals Disturbing Trend," November 21, 2011, *Newsfactor.com,* http://www.newsfactor.com/news/Stuxnet-Hit-on-Utility-Signals-New-Era/story.xhtml?story_id=111003TTUKBI&full_skip=1.

[25] Quoted in Jerry Brito, "Hackers Blow Up Illinois Water Utility . . . . . or Not," *Time Techland*, November 28, 2011, http://techland.time.com/2011/11/28/hackers-blow-up-illinois-water-utility-or-not.

[26] Kim Zetter, "Confusion Center: Feds Now Say Hacker Didn't Destroy Water Pump," *Wired Threat Level*, November 22, 2011, http://www.wired.com/threatlevel/2011/11/scada-hack-report-wrong.

time, had simply logged on remotely to check the plant's systems.[27] His company had helped to create software and systems used to control the plant's equipment. 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.[28]

2. Online Safety Threat Inflation

Threat inflation is also frequently on display in debates over online child safety.[29] Long before the rise of the Internet, threat inflation was a feature of debates about violent or sexual media content in the analog era.[30] Even recently, the titles of major books have decried the "home invasion" of "cultural terrorism"[31] and pleaded with media creators to "stop teaching our kids to kill."[32]

Again, no matter how distasteful 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 as a result of 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.[33]

---

[27] Ellen Nakashima, "Water-Pump Failure in Illinois Wasn't Cyberattack After All," *The Washington Post,* November 25, 2011, http://www.washingtonpost.com/world/national-security/water-pump-failure-in-illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewN_story.html.

[28] Kim Zetter, "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report," *Wired Threat Level*, November 30, 2011, http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved.

[29] Adam Thierer, "Social Networking Websites & Child Protection: Toward a Rational Dialogue," *Progress Snapshot* 2.17 (Washington, D.C.: Progress & Freedom Foundation, June 2006), http://www.pff.org/issues-pubs/ps/2006/ps_2.17_socialnet.pdf.

[30] The most extensive survey can be found in Marjorie Heins, *Not in Front of the Children.*

[31] Rebecca Hagelin, *Home Invasion: Protecting Your Family in a Culture That's Gone Stark Raving Mad* (Nashville, TN: Nelson Current, 2005).

[32] Dave Grossman and Gloria DeGaetano, *Stop Teaching Our Kids to Kill: A Call to Action against TV, Movie & Video Game Violence* (New York: Crown Publishers, 1999).

[33] Robert Corn-Revere, "New Age Comstockery," 4 *CommLaw Conspectus* 173, (Summer 1996).

Unfortunately, the inflated rhetoric surrounding "the Great Cyberporn Panic of 1995"[34] turned out to be based on a single study with numerous methodological flaws.

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."[35] 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. Congress soon passed the Communications Decency Act (CDA), which sought to ban indecent or obscene online content. The Rimm study generated widespread attention and was instrumental in the legislative debate leading up to passage of the law.

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."[36] "Unfortunately for all parties involved," noted Alice Marwick, "Rimm's results were found to be a combination of shoddy social science methodology, questionable research ethics, and wishful extrapolation."[37] "Within weeks after its publication, the Rimm study had been thoroughly discredited," wrote Jonathan Wallace and Mark Mangan, "but the damage had already been done" since lawmakers "had waved the *Time* article around Congress" and "quoted Rimm's phony statistics."[38]

Similarly, a decade later, as social networking sites began growing in popularity in 2005–6, several state attorneys general and lawmakers began claiming that sites like MySpace.com and Facebook represented a "predators' playground," implying that youth could be groomed for abuse or abduction by visiting those sites.[39] Regulatory

---

[34] Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age* (Cambridge, MA: MIT Press, 2003), 259, 259–318.

[35] Philip Elmer-DeWitt, "Cyberporn," *Time*, July 3, 1995.

[36] Jonathan Wallace and Mark Mangan, *Sex, Laws, and Cyberspace* (New York: Henry Holt and Company, Inc., 1996), 127.

[37] Marwick, "The MySpace Moral Panic."

[38] Wallace and Mangan, *Sex, Laws, and Cyberspace*, 151.

[39] Emily Steel and Julia Angwin, "MySpace Receives More Pressure to Limit Children's Access to Site," *Wall Street Journal*, June 23, 2006,

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 that had interactive functionality.[40]

Unsurprisingly, the bill proposing a federal ban on social networks in schools and libraries was titled *The Deleting Online Predators Act*.[41] In 2006, the measure received 410 votes in the U.S. House of Representatives before finally dying in the Senate. It was introduced in the following session of Congress, but did not see another floor vote and was never implemented. During this same period, many states, including Georgia,[42] Illinois,[43] and North Carolina, floated bills that also sought to restrict underage access to social networking sites.[44] None passed, however.

Thus, the fear appeal in this particular case was:

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

Again, this represented a logical fallacy, especially because the premise was based on a myth. Despite the heightened sense of fear aroused by policymakers over this issue, it turned out that there was

---

http://online.wsj.com/public/article/SB115102268445288250-YRxkt0rTsyyf1QiQf2EPBYSf7iU_20070624.html?mod=tff_main_tff_top.

[40] Adam Thierer, "Would Your Favorite Website Be Banned by DOPA? *Technology Liberation Front*, March 10, 2007, http://techliberation.com/2007/03/10/would-your-favorite-website-be-banned-by-dopa.

[41] H.R. 5319, "The Deleting Online Predators Act," 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.

[42] S.B. 59, 149th Gen. Assem., Reg. Sess. (GA, 2007).

[43] S.B. 1682, 95th Gen. Assem. (Ill. 2007).

[44] S.B. 132, 2007 Gen. Assem., Reg. Sess. (N.C. 2007).

almost nothing to the predator panic. 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 boyd.[45] "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."[46]

Generally speaking, the fear about strangers abducting children online was always greatly overstated since it was obviously impossible for them to "snatch" them at a distance. Abduction after Internet contact requires long-term, and usually long-distance, grooming and then meticulous planning about how to commit the crime. This is not to say there were no cases of abduction that involved Internet grooming, but such cases were exceedingly rare and did not represent the epidemic that some suggested.

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 [cases]."[47] 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. The study reported that the vast majority of kidnapping victims were abducted by family, friends of the family, or people who had a close relationships with (or the trust of) the minors. Only 115 of the estimated 260,000 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.[48] Lenore Skenazy, author of *Free-Range Kids: Giving Our*

---

[45] danah michele boyd, "Taken Out of Context, American Teen Sociality in Networked Publics" (doctoral dissertation, University of California, Berkeley, 2008), 266, http://www.danah.org/papers/TakenOutOfContext.pdf.

[46] Ibid.

[47] Andrea J. Sedlak, David Finkelhor, Heather Hammer, and Dana J. Schultz, *National Estimate of Missing Children: An Overview*, National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children (Alexandria, VA: National Center for Missing & Exploited Children, 2002), 7, www.missingkids.com/en_US/documents/nismart2_overview.pdf.

[48] 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. Ohio

Children the Freedom We Had Without Going Nuts with Worry, puts things in perspective: "the chances of any one American child being kidnapped and killed by a stranger are almost infinitesimally small: .00007 percent."[49] 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."[50] This is not to trivialize the seriousness of abduction by family members or known acquaintances since it can be equally traumatic for the child and his family, but these facts make it clear that the panic over strangers using social networks to groom and abduct children was based on a faulty premise.

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

3. Online Privacy Threat Inflation

Privacy is a highly subjective[51] and ever-changing condition.[52]

Missing Children Clearinghouse, *2005 Annual Report,* 4, www.ag.state.oh.us/victim/pubs/2005ann_rept_mcc.pdf.

[49] Lenore Skenazy, *Free-Range Kids: Giving Our Children the Freedom We Had Without Going Nuts with Worry* (San Francisco, CA: Jossey-Bass, 2009), 16.

[50] *The Crime of Family Abduction: A Child's and Parent's Perspective* (Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, May 2010), https://www.ncjrs.gov/pdffiles1/ojjdp/229933.pdf.

[51] "Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves." Jim Harper, "Understanding Privacy—and the Real Threats to It," *Policy Analysis* 520 (Washington, D.C.: Cato Institute, August 4, 2004), www.cato.org/pub_display.php?pub_id=1652. "When it comes to privacy, there are many inductive rules, but very few universally accepted axioms." David Brin, *The Transparent Society* (New York: Basic Books, 1998), 77. "On the social Web, privacy is a global and entirely subjective quality—we each perceive different threats to it." Betsy Masiello, "Deconstructing the Privacy Experience," *IEEE Security & Privacy*, July/August 2009, 70. "Privacy is a matter of taste and individual choice." Michael Fertik, *Comments of Reputation.com, Inc. to the U.S. Department of Commerce*, January 28, 2011, 13, http://www.reputation.com/blog/2011/01/31/reputation-com-comments-commerce-department-privacy-green-paper. "In most conversations, no one knows what anyone else means by 'privacy,' or what information is included in the terms 'personally-identifiable information.'" Larry Downes, "A Market

"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*.[53]

Unsurprisingly, therefore, privacy-related concerns about new digital technologies and online services sometimes prompt extreme rhetorical flourishes. For example, more tailored forms of online advertising and the "tracking" technologies which make them possible are coming under increasing scrutiny today.[54] Some of these concerns are legitimate since online data leakages and breaches can result in serious economic harm to consumers. 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.

Some critics decry the "creepiness" factor associated with online data collection and targeted advertising.[55] While no clear case of harm has been established related to "creepiness," many privacy advocates who oppose virtually any form data collection have elevated this concern to near technopanic levels and are now

---

Approach to Privacy Policy," in *The Next Digital Decade: Essays on the Future of the Internet*, ed. Berin Szoka and Adam Marcus (Washington, D.C.: TechFreedom, 2011), 514, http://nextdigitaldecade.com/ndd_book.pdf#page=510.

[52] "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." Hal Abelson, Ken Ledeen, and Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (Upper Saddle River, NJ: Addison-Wesley, 2008), 68.

[53] Larry Downes, *The Laws of Disruption* (New York: Basic Books, 2009), 69.

[54] See, generally, *The Wall Street Journal's* ongoing "What They Know" series: http://online.wsj.com/public/page/what-they-know-digital-privacy.html.

[55] Mike Isaac, "New Google 'Transparency' Feature Aims to Reduce Ad-Targeting Creepiness," *Wired Gadget Lab*, November 2, 2011, http://www.wired.com/gadgetlab/2011/11/google-ad-transparency-target; and Miranda Miller, "Google+ vs. Facebook: More Passive Aggression & Creepiness in Tech Soap Opera," *Search Engine Watch,* November 9, 2011, http://searchenginewatch.com/article/2123660/Google-vs.-Facebook-More-Passive-Aggression-Creepiness-in-Tech-Soap-Opera.

demanding sweeping regulation of online business practices.[56] The American Civil Liberties Union has likened Facebook's online tracking to "stalking" even though stalking is generally understood to follow from an intent to harm or harass.[57] Others predict even more dire outcomes, employing the rhetoric of a "privacy disaster."[58] Allusions to George Orwell's dystopian novel *1984* and "Big Brother" are quite common.[59] Variants include: "Corporate Big Brother," "Big Brother Inc.,"[60] and "Big Browser."[61]

Comparisons are sometimes drawn to natural disasters or environmental catastrophes, such as a "privacy Chernobyl."[62] "The personal data collected by [online] firms is like toxic waste," says Christopher Soghoian, 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."[63] Of course, in reality, data flows are nothing like Chernobyl or toxic waste since even the worst privacy

---

[56] Adam Thierer, "Techno-Panic Cycles (and How the Latest Privacy Scare Fits In)," *Technology Liberation Front,* February 24, 2011, http://techliberation.com/2011/02/24/techno-panic-cycles-and-how-the-latest-privacy-scare-fits-in.

[57] Chris Conley, "The Social Network is Stalking You," *Blog of Rights*, November 16, 2011, http://www.aclu.org/blog/technology-and-liberty/social-network-stalking-you.

[58] Leslie Harris, "Preventing the Next Privacy Disaster," *Huffington Post*, October 15, 2008, http://www.huffingtonpost.com/leslie-harris/preventing-the-next-priva_b_134921.html.

[59] "Hello, Big Brother: Digital Sensors Are Watching Us," *USA Today*, January 26, 2011, http://www.usatoday.com/tech/news/2011-01-26-digitalsensors26_CV_N.htm.

[60] Scott Cleland and Ira Brodsky, *Search & Destroy: Why You Can't Trust Google Inc.* (St. Louis, MO: Telescope Books, 2011), 48.

[61] Nate Anderson, "Congress, Wary of Amazon's Silk Browser, Demands Answers on Privacy," *Ars Technica*, October 14, 2011, http://arstechnica.com/tech-policy/news/2011/10/congress-wary-of-amazons-silk-browser-demands-answers-on-privacy.ars.

[62] Tim Black, "Are We Heading for 'a Privacy Chernobyl'?" March 15, 2010, http://www.spiked-online.com/index.php/site/article/8310.

[63] Julia Angwin, "How Much Should People Worry About the Loss of Online Privacy?" *The Wall Street Journal*, November 15, 2011, http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html.

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 (through loss of income) or indirectly (through loss of privacy or reputation). But those harms do not approximate death or serious illness as the inflated rhetoric implies.

Similar rhetorical flourishes were heard during the brief technopanic over radio-frequency identification (RFID) technologies in the early 2000s. In the extreme, Katherine Albrecht and Liz McIntyre's books *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move* and *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance* likened RFID to the Biblical threat of the "Mark of the Beast."[64] Legislation was introduced in several states, although none passed.[65] Fears about RFID were greatly exaggerated and the panic largely passed by the late 2000s.[66]

However, similar fear reappeared in the recent debate over wireless location-based services.[67] In Spring 2011, Apple and Google came under fire for retaining location data gleaned by iPhone and Android-based smartphone devices.[68] 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.[69] Of

---

[64] Quoted in Mark Baard, "RFID: Sign of the (End) Times?" *Wired*, June 6, 2006, http://www.wired.com/science/discoveries/news/2006/06/70308.

[65] Declan McCullagh, "Don't Regulate RFID—Yet," *CNet News*, April 30, 2004, http://news.cnet.com/Don%27t%20regulate%20RFID--yet/2010-1039_3-5327719.html.

[66] Jerry Brito, "Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature," *UCLA Journal of Law and Technology* 5 (2004), http://www.lawtechjournal.com/articles/2004/05_041220_brito.php.

[67] Adam Thierer, "Apple, The iPhone And A Locational Privacy Techno-Panic," *Forbes*, May 1, 2011, http://www.forbes.com/sites/adamthierer/2011/05/01/apple-the-iphone-and-a-locational-privacy-techno-panic.

[68] Kashmir Hill, "Apple and Google To Be The Whipping Boys for Location Privacy," *Forbes*, April, 26, 2011, http://www.forbes.com/sites/kashmirhill/2011/04/26/apple-and-google-to-be-the-whipping-boys-for-location-privacy.

[69] Kashmir Hill, "Cool or Creepy? Your iPhone and iPad Are Keeping Track of Everywhere You Go, And You Can See It," *Forbes*, April 20, 2011,

course, if they are sensitive about locational privacy, users can always turn off locational tracking or encrypt and constantly delete their data. Most users won't want to go that far because it would cripple those other 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 most typically the case when large media or information technology firms propose a merger.[70] 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. 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."[71] 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."[72]

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.[73] By April 2002,

---

http://www.forbes.com/sites/kashmirhill/2011/04/20/cool-or-creepy-your-iphone-and-ipad-are-keeping-track-of-everywhere-you-go-and-you-can-see-it.

[70] Adam Thierer, "A Brief History of Media Merger Hysteria: From AOL-Time Warner to Comcast-NBC," *Progress on Point* No. 16.25 (Washington, D.C.: Progress & Freedom Foundation, December 2, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517288.

[71] Norman Soloman, "AOL Time Warner: Calling The Faithful To Their Knees," January 2000, www.fair.org/media-beat/000113.html.

[72] Robert Scheer, "Confessions of an E-Columnist," *Online Journalism Review*, January 14, 2000, www.ojr.org/ojr/workplace/1017966109.php.

[73] 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." Quoted in Thomas Heath, "The Rising

just two years after the deal was struck, AOL-Time Warner had already reported a staggering $54 billion loss.[74] By January 2003, losses had grown to $99 billion.[75] In September 2003, Time Warner decided to drop AOL from its name altogether, and the deal continued to unravel slowly from there.[76] Looking back at the deal, *Fortune* magazine senior editor-at-large Allan Sloan called it the "turkey of the decade."[77] Importantly, the divestitures and downsizing efforts that followed the deal's undoing garnered little attention compared with the hysteria that accompanied the announcement of the deal in 2000.[78]

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."[79] *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.[80] As though he could cover both extremes of the ideological spectrum, Murdoch has not only been compared to Hitler

---

Titans of '98: Where Are They Now?" *The Washington Post*, November 30, 2009, www.washingtonpost.com/wp-dyn/content/article/2009/11/29/AR2009112902385.html?sub=AR.

[74] Frank Pellegrini, *What AOL Time Warner's $54 Billion Loss Means*, April 25, 2002, *Time Online*, www.time.com/time/business/article/0,8599,233436,00.html.

[75] Jim Hu, "AOL Loses Ted Turner and $99 Billion*," CNet News.com*, January 30, 2004, http://news.cnet.com/AOL-loses-Ted-Turner-and-99-billion/2100-1023_3-982648.html.

[76] Jim Hu, "AOL Time Warner Drops AOL from Name," *CNet News.com*, September 18, 2003, http://news.cnet.com/AOL-Time-Warner-drops-AOL-from-name/2100-1025_3-5078688.html.

[77] Allan Sloan, "'Cash for . . . ' and the Year's Other Clunkers," *The Washington Post*, November 17, 2009, www.washingtonpost.com/wp-dyn/content/article/2009/11/16/AR2009111603775.html.

[78] "Break-ups and divestitures do not generally get front-page treatment," notes Ben Compaine, author of *Who Owns the Media?* See Ben Compaine, "Domination Fantasies," *Reason* 28 (January 2004), www.reason.com/news/show/29001.html.

[79] Jack23, "Rupert Murdoch is a Fascist Hitler Antichrist," *DailyKos*, September 7, 2009, www.dailykos.com/story/2009/9/7/778254/-Rupert-Murdoch-is-a-Fascist-Hitler-Antichrist.

[80] Jim Finkle, "Turner Compares Fox's Popularity to Hitler," *Broadcasting & Cable*, January 25, 2005, www.broadcastingcable.com/CA499014.html.

but has been accused of being a Marxist.[81] Meanwhile, Karl Frisch, a Senior Fellow at Media Matters for America, speaks of Murdoch's "evil empire."[82]

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.[83] 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 horribles.[84] 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. In December 2006, News Corp. decided to divest the company to Liberty Media Corporation.[85]

As with the unwinding of the AOL-Time Warner deal, little mention was made in the reporting of the divestiture of DirecTV of the previous round of pessimistic predictions or whether there had

---

[81] Ian Douglas, "Rupert Murdoch is a Marxist," *Telegraph.Co.UK*, November 9, 2009, http://blogs.telegraph.co.uk/technology/iandouglas/100004169/rupert-murdoch-is-a-marxist.

[82] Karl Frisch, *"*Fox Nation: The Seedy Underbelly of Rupert Murdoch's Evil Empire?" *MediaMatters.org*, June 2, 2009, http://mediamatters.org/columns/200906020036.

[83] 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." He continued, "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." Dissenting Statement of Commissioner Jonathan S. Adelstein, *Re: General Motors Corporation and Hughes Electronics Corporation, Transferors, and The News Corporation Limited*, *Transferee*, MB Docket No. 03-124, January 14, 2004, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-330A6.doc.

[84] Jeff Chester, "Rupert Murdoch's Digital Death Star," *AlterNet*, May 20, 2003, www.alternet.org/story/15949.

[85] News Corp , "News Corporation and Liberty Media Corporation Sign Share Exchange Agreement," news release, December 22, 2006, www.newscorp.com/news/news_322.html. A frustrated Murdoch referred to DirecTV as a "turd bird" just before he sold it off. See Jill Goldsmith, "Murdoch Looks to Release Bird," *Variety*, September 14, 2006, www.variety.com/article/VR1117950090.html?categoryid=1236&cs=1.

ever been any merit to the lugubrious lamentations of the critics. The moral of the story seems to be clear: Talk is cheap. Pessimistic critics who use threat inflation to advance their causes are rarely held accountable when their panicky predictions fail to come to pass.

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. At the most basic level, there exist many psychological explanations for why human beings are predisposed toward pessimism and are risk-averse. For a variety of reasons, humans are poor judges of risks to themselves or those close to them. Harvard University psychology professor Steven Pinker, author of *The Blank Slate: The Modern Denial of Human Nature*, notes that:

> 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.[86]

Going beyond this root-cause explanation, 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 the previous insight that the survival instinct combined with poor comparative risk analysis skills lead many people to engage in, or buy into, technopanics.

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

---

[86] Steven Pinker, *The Blank Slate: The Modern Denial of Human Nature* (New York: Penguin Books, 2002), 232.

Crimes Against Children Research Center (CCRC), calls "juvenoia," or ""the exaggerated anxiety about the influence of social change on children and youth."[87] 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. [88]

Many historians, psychologists, sociologists, and other scholars have documented this seemingly never-ending cycle. 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.[89] The late University of North Carolina journalism professor Margaret A. Blanchard once remarked that

> parents 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.[90]

---

[87] David Finkelhor, "The Internet, Youth Deviance and the Problem of Juvenoia" (Durham, NH: Crimes Against Children Research Center, University of New Hampshire, October 22, 2010), http://www.vimeo.com/16900027.

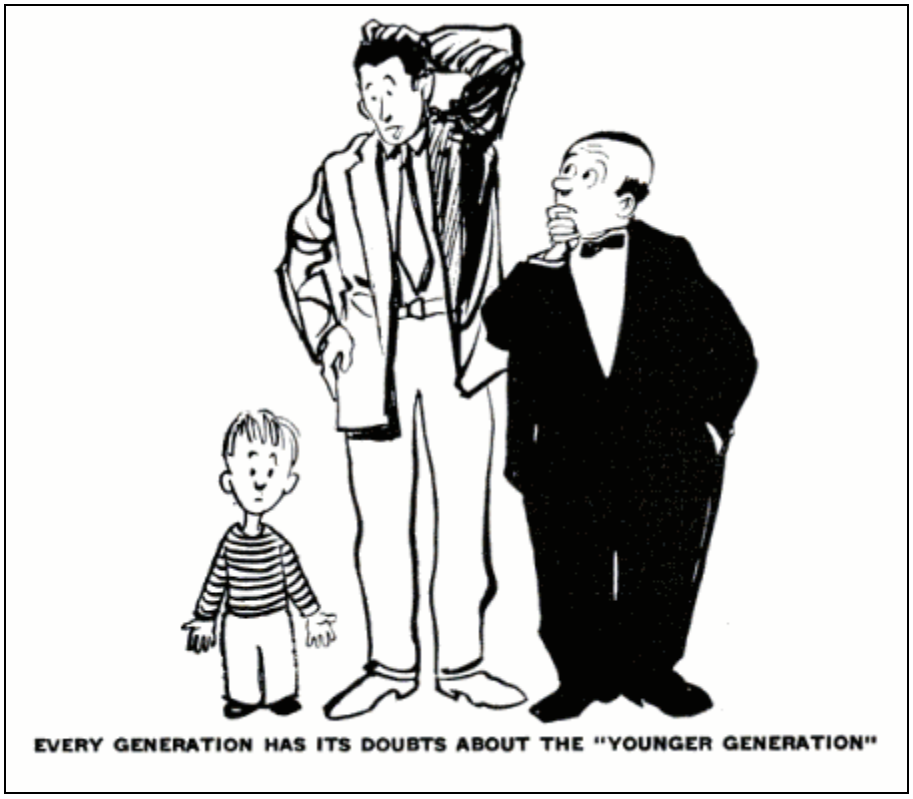
[88] Tyler Cowen, *In Praise of Commercial Culture* (Cambridge, MA: Harvard University Press, 1998), 185.

[89] "Throughout American history, adults have attributed undesirable changes in youth behavior to some aspect of popular culture." Bradford W. Wright, *Comic Book Nation: The Transformation of Youth Culture in America* (Baltimore, MD: The John Hopkins University Press, 2001), 87.

[90] Margaret A. Blanchard, "The American Urge to Censor: Freedom of Expression Versus the Desire to Sanitize Society—From Anthony Comstock to 2 Live Crew," *William and Mary Law Review* 33 (Spring 1992), 743,

Similarly, Thomas Hine, author of *The Rise and Fall of the American Teenager*, argues that, "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."[91]

A 1950 Cartoon from *Life* Magazine



This reoccurring phenomenon was captured nicely by cartoonist Bill Mauldin in a 1950 edition of *Life* magazine. 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." Mauldin, who was 28 at the time, penned an accompanying essay defending his World War II-era generation

---

http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1897&context=wmlr.

[91] Quoted in Nancy Gibbs, "Being 13," *Time*, August 8, 2005, 43.

against attacks for "lacking some of the good old American gambling spirit and enterprise."[92] Of course, this was the same generation of youngsters that Tom Brokaw would eventually label "The Greatest Generation"![93]

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 many unintended consequences.[94] "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*.[95] What parents, guardians, and educators should understand, they argue, "is that the traditional values and common sense that have served them well in the past will be relevant in this new world, too."[96] Thus, while it is certainly true, as Karen Sternheimer notes, that "new technologies elicit fears of the unknown, particularly because they have enabled children's consumption of popular culture to move beyond adult control,"[97] it doesn't follow that prohibition or anticipatory regulation is the best response. 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.

---

92 Bill Maudlin, "The Care & Handling of a Heritage," *Life,* January 2, 1950, http://books.google.com/books?id=TUAEAAAAMBAJ&pg=PA96.

93 Tom Brokaw, *The Greatest Generation* (New York: Random House, 1998).

94 Adam Thierer, "Parents, Kids & Policymakers in the Digital Age: Safeguarding Against 'Technopanics,'" *Inside ALEC* (July 2009), 16–7, http://www.alec.org/am/pdf/Inside_July09.pdf.

95 John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008), 9.

96 Ibid., 10.

97 Karen Sternheimer, *It's Not the Media: The Truth about Pop Culture's Influence on Children* (Boulder, CO: Westview Press, 2003), 38.

In a 1777 essay, the Scottish philosopher and economist David Hume observed that, "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 extensive learning."[98] 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."[99]

What is ironic about such nostalgia is that it is rooted in something typically unknown by the proponent. The poet Susan Stewart argues that nostalgia represents "a sadness without an object, a sadness which creates a longing that of necessity is inauthentic because it does not take part in lived experience. Rather, it remains behind and before that experience."[100] Too often, Stewart observes, "nostalgia wears a distinctly utopian face" and thus becomes a "social disease."[101]

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. "The idea that childhood in the past was comprised of carefree days without worry is a conveniently reconstructed version of history," observes Sternheimer. "This fantasy allows adults to feel nostalgia for a lost idealized past that never was."[102]

The psychological explanation for this is relatively straightforward: people are always more comfortable with what they know relative to that with which they are unfamiliar. Consequently,

---

[98] David Hume, "Of the Populousness of Ancient Nations," in David Hume, *Essays Moral, Political, Literary* (Indianapolis: Liberty Fund 1987, 1777).

[99] Michael Shermer, *The Believing Brain: From Ghosts and Gods to Politics and Conspiracies—How We Construct Beliefs and Reinforce Them as Truths* (New York: Times Books, 2011), 275.

[100] Susan Stewart, *On Longing: Narratives of the Miniature, the Gigantic, the Souvenir, the Collection* (Durham, NC: Duke University Press, 1993), 23.

[101] Ibid.

[102] Sternheimer, *It's Not the Media,* 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.*" Ibid., 32, 34.

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.

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.[103] Stated differently, by its nature, technology disrupts settled matters. "The shock of the new often brings out critics eager to warn us away," notes Dennis Baron.[104] 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 a moral panics or technopanics discussed above. In particular, cultural critics and advocacy groups benefit from the use of nostalgia by playing into, or whipping up, fears that we've lost a better time and then suggesting steps can and should be taken to help us return to that time.

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. "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."[105] 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.[106]

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

---

[103] Adam Thierer, "10 Things Our Kids Will Never Worry About Thanks to the Information Revolution," *Forbes*, December 18, 2011, http://www.forbes.com/sites/adamthierer/2011/12/18/10-things-our-kids-will-never-worry-about-thanks-to-the-information-revolution.

[104] Dennis Baron, *A Better Pencil: Readers, Writers, and the Digital Revolution* (Oxford: Oxford University Press, 2009), 12.

[105] Sternheimer, *It's Not the Media*, 7–8.

[106] Matt Ridley, *The Rational Optimist: How Prosperity Evolves* (New York: Harper Collins, 2010), 292.

general "pessimistic bias" among many voters, or "a tendency to overestimate the severity of economic problems and underestimate the (recent) past, present, and future of the economy."[107] 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.[108] That is equally true today.[109] 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.[110]

Fear mongering and prophecies of doom have always been with us, since they represent easy ways to attract attention and get heard. "Pessimism has always been big box office," notes Ridley.[111] This is even more true in the midst of the modern information age cacophony. Breaking through all the noise is hard when competition for our eyes and ears is so intense. It should not be surprising, therefore, that sensationalism and alarmism are used as media differentiation tactics. This is particularly true as it relates to kids and

---

[107] Bryan Caplan, *Myth of the Rational Voter* (Princeton, NJ: Princeton University Press, 2007), 44.

[108] Julian Simon, *The Ultimate Resource 2* (Princeton, NJ: Princeton University Press, 1996), 539–40. Simon adds, "It is easier to get people's attention (and television time and printer's ink) with frightening forecasts than soothing forecasts." Ibid., 583.

[109] "Many perceived 'epidemics' are in reality no such thing, but instead the product of media coverage of gripping, unrepresentative incidents." Cass Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge: Cambridge University Press, 2005), 102.

[110] Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online," *UC Davis Law Review* 41, no. 4 (2008), 1401.

[111] Ridley, *The Rational Optimist*, 294.

online safety.[112] "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. "Panic and fear often drown out evidence."[113]

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."[114] 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 news. 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 directly from getting more resources from government, the public, and other benefactors or indirectly from the glow of publicity that their alarmism generates. Sternheimer notes that

> activist 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

---

[112] "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." Karen Sternheimer, *Kids These Days: Facts and Fictions about Today's Youth* (Lanham, MD: Rowman & Littlefield Publishers, Inc., 2006), 152.

[113] Michael Burns, "UK a 'High Use, Some Risk' Country for Kids on the Web," *Computerworld*, October 18, 2011, http://news.idg.no/cw/art.cfm?id=F3254BA7-1A64-67EA-E4D5798142643CEF.

[114] Shermer, *The Believing Brain*, 275.

> interest in making specific problems seem as scary as possible.[115]

In their work on moral panic theory, Goode and Ben-Yehuda discuss the importance of "moral entrepreneurs," who are "crusaders who believe that some members of the society are willfully engaged in immoral and therefore damaging behavior and are not being sufficiently punished for it. Something must be done, they believe, to discourage or eliminate such behavior."[116] 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.*[117]

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.[118] NCMEC's mission is important, and it has provided a vital public service by helping to prevent child abuse and solve 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 grows as the threats they identify increase.[119] Research by *The Wall Street Journal* statistics columnist

---

[115] Karen Sternheimer, *Kids These Days*, 151–2.

[116] Goode and Ben-Yehuda, *Moral Panics*, 80.

[117] Security expert Bruce Schneier has noted that in the case of police and other law-enforcement bodies, "these institutions 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 over-securing—or at least over-spending—as a result of that exaggeration, is by far the most common outcome." Bruce Schneier, *Liars & Outliers: Enabling the Trust that Society Needs to Thrive* (New York: John Wiley & Sons, Inc., 2012), 203.

[118] "The National Center for Missing & Exploited Children Mission and History," http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362 (*accessed December 20, 2011*).

[119] Berin Szoka, "If NCMEC's Going to Regulate the Internet for Child Porn, It Should At Least Be Subject to FOIA," *Technology Liberation Front*, August 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. Chris

Carl Bialik has documented how NCMEC misused or misreported certain data, including repeatedly asserting that Internet child porn trade was a business worth $20 billion annually even though it could muster no evidence to support the claim.[120] Bialik also showed how NCMEC was inflating data about how many children had been sexually solicited online.[121]

Corporate actors also sometimes benefit from excessive fear mongering. 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.[122] In the context of social regulation, companies occasionally employ fear tactics to increase their visibility and potentially to sell goods and services that will supposedly eradicate the supposed threat to society they have identified. For example, many companies produce tools that help people protect their privacy and security as well as their children's online safety. Most of them deserve praise for those innovations. 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. Again, bad news sells and, in this case, it sells products and services to fearful citizens.

For example, when the "stranger danger" and "predator panic" over social networking sites first erupted, some vendors of age-verification technologies attempted to exacerbate such fears in an attempt to get various lawmakers to mandate the use of their verification technologies,[123] even as doubts were being raised about

---

Soghoian, "Editorial: It's Time for a Child Porn Czar," *CNet*, December 9, 2008, http://news.cnet.com/8301-13739_3-10118923-46.html.

[120] Carl Bialik, "Measuring the Child-Porn Trade," *Wall Street Journal*, April 18, 2006, http://online.wsj.com/article/SB114485422875624000.html.

[121] Carl Bialik, "Online Warnings Mean Well, But the Numbers Don't Add Up," *Wall Street Journal*, January 21, 2005, http://online.wsj.com/public/article/SB110617073758830511-2aJjGHdzDxeGmQglegoKJ9IXwig_20071216.html.

[122] Bruce Yandle, "Bootleggers and Baptists — The Education of a Regulatory Economist," *Regulation* 3, no. 3 (1983), 12–6.

[123] Chris Soghoian, "State Attorneys General Push Online Child Safety Snake Oil," *CNet News.com*, September 24, 2008, http://news.cnet.com/8301-13739_3-10048583-46.html.

their effectiveness.[124] 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. This is clearly at work 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."[125] Similarly, Susan Crawford, a former White House senior advisor on technology policy matters, has noted the emergence of "cyberwar hysteria aids consultants" who "would certainly create work" for many organizations surrounding the D.C. Beltway.[126] As Stefan Savage, a Professor in the Department of Computer Science and Engineering at the University of California, San Diego, told *The Economist* magazine, the cybersecurity industry sometimes plays "fast and loose" with the numbers because it has an interest in "telling people that the sky is falling."[127]

Similarly, in online safety debates, many organization petition federal, state, and local lawmakers for grants to fund tools or educational curricula they have developed to address these fears.[128]

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

---

[124] Internet Safety Technical Task Force, *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*, December 31, 2008, 10, http://cyber.law.harvard.edu/pubrelease/isttf; and Adam Thierer, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions," (Washington, D.C.: Progress & Freedom Foundation, March 2007) *Progress on Point* No. 14.5, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976936.

[125] Brito and Watkins, "Loving the Cyber Bomb?" 1.

[126] Susan Crawford, "Cyberwar Hysteria Aids Consultants, Hurts U.S." *Bloomberg,* July 24, 2011, http://www.bloomberg.com/news/2011-07-25/cyberwar-hysteria-aids-consultants-hurts-u-s-susan-crawford.html.

[127] "Measuring the Black Web," *The Economist,* October, 15, 2011, http://www.economist.com/node/21532263.

[128] Nancy Willard, "My Review of I-Safe," *Nancy Willard Weblog*, March 13, 2008, http://csriu.wordpress.com/2008/03/13/my-review-of-i-safe.

to the potential long-term gains or without the broader benefits of technological change ever being taken into account. 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."[129]

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. Better yet, from their perspective, is the potential for their competitors to be burdened with regulation that might constrain their efforts to innovate, expand, and compete.[130] 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, during the height of the "predator panic," MySpace was the leading social networking site and the company feeling most of the heat from policymakers. Unsurprisingly, MySpace attempted to shift some of that focus toward its emerging rival, Facebook, and suggested policymakers take a closer look at its practices, implying that the newer platform posed more risks for kids. Facebook responded by simply pointing fingers back at MySpace. Generally speaking, this simply raised the overall level of concern about social networking sites and kids' safety in general and resulted in more political pressure on *both* companies and the entire social media sector.

Another recent example of this same sort of finger pointing involves Microsoft and Google. 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. Google hammered Microsoft in

---

[129] Julian Simon, *The Ultimate Resource 2*, 583.

[130] Adam Thierer, "The Sad State of Cyber-Politics," *Cato Policy Report*, (Washington, D.C.: Cato Institute, November/December 2010), http://www.cato.org/pubs/policy_report/v32n6/cpr32n6-1.html.

countless legal and political proceedings here and abroad.[131] But the tables turned in recent years, and Microsoft is now the ringleader of the rising political war against Google. Today, Microsoft is using against Google the same antitrust playbook others once used against it. 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.[132] 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.

Of course, companies seeking to wield the power of government to humble their competitors or gain competitive advantage is nothing new. 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.[133] We have another term for it today: crony capitalism. Again, the result is simply more fear and loathing about all the players and sectors involved, as well as their technologies or platforms.

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

---

[131] Alexei Oreskovic and David Lawsky, "Google Joins EU Antitrust Case against Microsoft," *Reuters*, February 25, 2009, http://www.wired.com/techbiz/media/news/2009/02/reuters_us_google_microsoft.

[132] Jason Kincaid, "Microsoft Tells Google to Face the Antitrust Music," *TechCrunch*, February 26, 2010, http://techcrunch.com/2010/02/26/microsoft-google-antitrust.

[133] Milton Friedman, "The Business Community's Suicidal Impulse," *Cato Policy Report*, (Washington, D.C.: Cato Institute, March/April 1999), http://www.cato.org/pubs/policy_report/v21n2/friedman.html.

they understand what is best for the less educated, in other words, that they know how some others should live their lives."[134] 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. "The great ideological crusades of the twentieth-century intellectuals have ranged across the most disparate fields," noted Sowell.[135] 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."[136] These government-expanding crusades shared several key elements, which Sowell identified as: (1) assertion of a great danger to the whole society, a danger to which the masses of people are oblivious; (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; and (4) a disdainful dismissal of arguments to the contrary as uninformed, irresponsible, or motivated by unworthy purposes.

This model is frequently on display with various 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, "If not that of the researchers themselves, who want to demonstrate that funding their

---

[134] Paul Dragos Aligica, *Prophecies of Doom and Scenarios of Progress: Herman Kahn, Julian Simon, and the Prospective Imagination* (New York: The Continuum International Publishing Group, 2007), 10.

[135] Thomas Sowell, *The Vision of the Anointed: Self-Congratulation as a Basis for Social Policy* (New York: Basic Books, 1995), 5.

[136] Sowell adds, "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." Ibid., 123.

work is important, then that of the groups that fund the research."[137] 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.[138] Simply stated, many critics sometimes 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. 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. They come to believe that government must "do something" to correct those perspectives. *Many people desire control of culture or technology because they think it will be good for others, not necessarily for themselves*. 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 know as the "third-person effect hypothesis." 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

---

[137] Sternheimer, *Kids These Days,* 152. She continues, "science is an attempt to get closer to understanding our world, but it is often based on preconceptions about the way the world works."

[138] For an explanation of how the third-person effect serves as a powerful explanation for the heated reaction that followed a modest Federal Communications Commission effort to liberalize media ownership rules in 2003–4, see Adam Thierer, *Media Myths: Making Sense of the Debate over Media Ownership* (Washington, D.C.: The Progress & Freedom Foundation, 2005), 119–23, www.pff.org/issues-pubs/books/050610mediamyths.pdf.

> persuasive) will expect the communication to have a greater effect on others than on themselves.[139]

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. In reality, their own personal preferences were biasing their ability to evaluate that content fairly. 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.[140] 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,[141] misogynistic rap lyrics,[142] television violence,[143] video games,[144] and pornography.[145] 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

---

[139] W. Phillips Davison, "The Third-Person Effect in Communication," *Public Opinion Quarterly* 47, no.1 (1983), 3.

[140] For the best overview of third-person effect research, see Douglas M. McLeod, Benjamin H. Detenber, and William P. Eveland., Jr., "Behind the Third-Person Effect: Differentiating Perceptual Processes for Self and Other," *Journal of Communication* 51, no. 4 (2001), 678–95.

[141] Vincent Price, David H. Tewksbury, and Li-Ning Huang, "Third-person Effects of News Coverage: Orientations Toward Media," *Journalism & Mass Communications Quarterly* 74, no. 3 (1997), 525–40.

[142] Douglas M. McLeod, William P. Eveland, and Amy I. Nathanson, "Support for Censorship of Violent and Misogynic Rap Lyrics: An Analysis of the Third-Person Effect," *Communications Research* 24 (1997), 153–74.

[143] Hernando Rojas, Dhavan V. Shah, and Ronald J. Faber, "For the Good of Others: Censorship and the Third-Person Effect," *International Journal of Public Opinion Research* 8 (1996), 163–86.

[144] James D. Ivory, "Addictive for Whom? Electronic Games, The Third-person Effect, and Contributors to Attitudes Toward the Medium." Paper presented to the Communication and Technology Division at the annual conference of the International Communication Association, New Orleans, LA, (May 2004), http://filebox.vt.edu/users/jivory/Ivory20043pGamesICA.pdf.

[145] Albert C. Gunther, "Overrating the X-rating: The Third-person Perception and Support for Censorship of Pornography," *Journal of Communication* 45, no. 1 (1995), 27–38

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.[146]

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 the *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."[147]

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 the context of violent video games, Chris Ferguson developed what he

---

[146] Davison, "The Third-Person Effect,"14. Along these lines, a December 2004 *Washington Post* article documented the process by which the Parents Television Council, a vociferous censorship advocacy group, screens various television programming. 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." Apparently, in her opinion, what's good for the goose is not good for the gander! See Bob Thompson, "Fighting Indecency, One Bleep at a Time," *The Washington Post*, December 9, 2004, www.washingtonpost.com/wp-dyn/articles/A49907-2004Dec8.html.

[147] George Bernard Shaw, *Three Plays for Puritans* (1901), xxiv.

referred to as the "Moral Panic Wheel."[148] The adjoining image, developed by Ferguson, illustrates that there is no one entity or factor responsible for moral panics or technopanics. 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.[149]

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

> 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.[150]

Ferguson reiterates that generation gaps are often a key feature of moral panics: "the 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

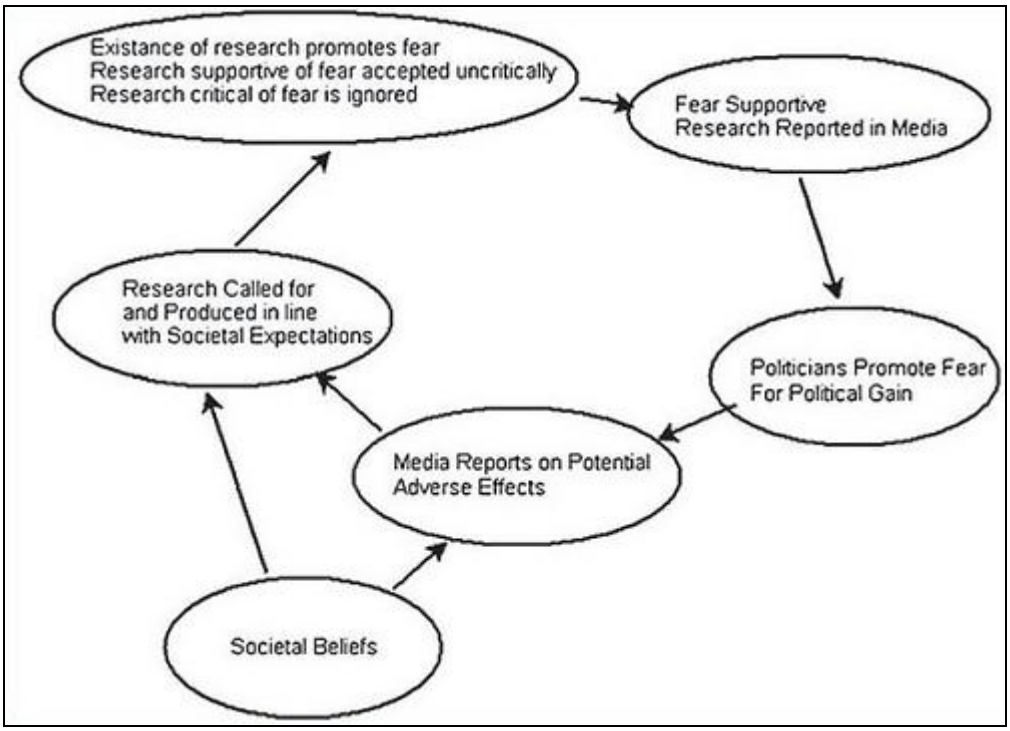
---

[148] Christopher J. Ferguson, "The School Shooting/Violent Video Game Link: Causal Relationship or Moral Panic?" *Journal of Investigative Psychology and Offender Profiling*, 5, nos. 1–2 (2008) 25–37, http://onlinelibrary.wiley.com/doi/10.1002/jip.76/abstract.

[149] Ibid., 30–1.

[150] Ibid., 32–3.

make claims betraying their unfamiliarity," he says.[151]



University of Chicago legal scholar Cass Sunstein, who currently serves as Administrator of the White House Office of Information and Regulatory Affairs, has described "fear as wildfire" and explained how "social cascades" contribute to the rapid spread of fear and panic. 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."[152] 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:

---

[151] Ibid., 31.

[152] Cass Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge: Cambridge University Press, 2005), 94–5.

> Behind the apocalyptic public opinion beliefs . . . is more rhetoric and psychology. In fact, once 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. 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.[153]

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 they 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; 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" panics we have seen in the past.[154]

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. 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,

---

[153] Aligica, *Prophecies of Doom*, 20.

[154] Adam Thierer, "Technopanic Cycles (and How the Latest Privacy Scare Fits In)," *Technology Liberation Front,* February 24, 2011, http://techliberation.com/2011/02/24/technopanic-cycles-and-how-the-latest-privacy-scare-fits-in.

and eventually some of them are elevated into art forms."[155]

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 passing 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.[156] 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 "when 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," argue Brito and Watkins.[157]

---

[155] "No Killer App: The Moral Panic about Video Games is Subsiding," *The Economist*, December 10, 2011, http://www.economist.com/node/21541166.

[156] Wendy McElroy, "Destroying Childhood to Save Children," *The Freeman*, December 6, 2011, http://www.thefreemanonline.org/headline/destroying-childhood-to-save-children.

[157] Brito and Watkins, "Loving the Cyber Bomb," 2.

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. "The problem is that both individuals and societies may be fearful of nonexistent dangers or trivial risks—and simultaneously neglect real dangers," writes Sunstein.[158] 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. "To date, the fear mongers have had the upper hand, shaping policy through sound bites and unfounded anecdotes," writes Ohm.[159] 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.

---

[158] Cass Sunstein, *Laws of Fear*, 105.

[159] Ohm, "The Myth of the Superuser," 1401.

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." This response is generally known as "the precautionary principle." 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. In other words, the law should mandate "play it safe" as the default policy toward technological progress. Journalist Ronald Bailey has summarized this principle: "anything new is guilty until proven innocent."[160]

Although this principle is most often discussed in the field of environment law,[161] it is increasingly on display in Internet and information technology policy debates. 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 just about anything.

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. A decade earlier, under the *Communications Decency Act*, Congress attempted to sanitize the

---

[160] Ronald Bailey, "Precautionary Tale*," Reason*, April 1999, http://reason.com/archives/1999/04/01/precautionary-tale.

[161] For a comprehensive discussion and refutation of the precautionary principle in that context, see: Julian Morris, ed., *Rethinking Risk and the Precautionary Principle* (Oxford, UK: Butterworth-Heinemann, 2000).

Internet from "indecent" and "obscene" content.[162]

Lately, the precautionary principle mindset has gained the 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. The Kindle Fire takes advantage of Amazon's sophisticated cloud computing platform to offer users a faster, more efficient browsing experience by letting Amazon's servers to do all the heavy lifting in terms of information processing.[163] Of course, that also means Amazon will possess more information about user's websurfing habits and interests, which immediately raised privacy concerns. 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 (R-TX) and Ed Markey (D-MA) 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,[164] and Markey spoke in Orwellian terms of Amazon's "Big Browser" ambitions.[165] 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. Instead, their attitude was summarized by Barton's dismissive belief that "enough is enough," which was followed up with a letter to Amazon from Markey asking a series of threatening questions about the browser's functions.

This is reminiscent of the hostile reaction that briefly followed the

---

[162] Robert Cannon, "The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway," 49 *Federal Communications Law Journal* 51, (November 1996), http://www.cybertelecom.org/cda/cannon2.htm.

[163] Tom Cheredar, "Kindle Fire Uses a New Silk Web Browser to Boost Efficiency," *Mobile Beat,* September 28, 2011, http://venturebeat.com/2011/09/28/amazon-kindle-silk-browser.

[164] Nate Anderson, "Your Internet Data: More Like Redcoats Living in Your Home or Black Gold in the Ground?," *Ars Technica*, October 13, 2011, http://arstechnica.com/tech-policy/news/2011/10/your-internet-data-more-like-redcoats-living-in-your-home-or-black-gold-in-the-ground.ars.

[165] Nate Anderson, "Congress, Wary of Amazon's Silk Browser, Demands Answers on Privacy," *Ars Technica*, October 14, 2011, http://arstechnica.com/tech-policy/news/2011/10/congress-wary-of-amazons-silk-browser-demands-answers-on-privacy.ars.

debut of Google's Gmail service in 2004. It, too, raised new privacy concerns and led to calls for prohibition before it had even debuted.[166] 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). Rather than charging some 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. Some privacy advocates howled that Google was going to "read users' email," and led a crusade to ban such algorithmic contextual targeting.[167] In essence, they wanted to impose their own subjective values (and fears) on everyone else.[168]

Interestingly, however, the frenzy of hysterical indignation about Gmail was followed by a collective cyberyawn: 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. As of October 2011, nearly 260 million people around the world were using Gmail, and it has a steadily growing share of the webmail market.[169] 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.

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

---

[166] Adam Thierer, "Lessons from the Gmail Privacy Scare of 2004," *Technology Liberation Front,* March 25, 2011, http://techliberation.com/2011/03/25/lessons-from-the-gmail-privacy-scare-of-2004.

[167] See Letter from Chris Jay Hoofnagle, Electronic Privacy Information Center, Beth Givens, Privacy Rights Clearinghouse, Pam Dixon, World Privacy Forum, to California Attorney General Lockyer, May 3, 2004, http://epic.org/privacy/gmail/agltr5.3.04.html.

[168] See email from Adam Thierer to Declan McCullaugh on Politech email discussion group, April 30, 2004, http://lists.jammed.com/politech/2004/04/0083.html.

[169] Daniel Terdiman, "Microsoft Aiming to Clean Up Hotmail User's Inboxes," *CNET News*, October 3, 2011, http://news.cnet.com/8301-13772_3-20114975-52/microsoft-aiming-to-clean-up-hotmail-users-inboxes.

progress. This is not to say new technologies pose no risks. Rather, as did our ancestors, we must learn to adapt to our 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. George Basalla, author of *The Evolution of Technology*, notes that "In 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."[170] 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 to average citizens.[171]

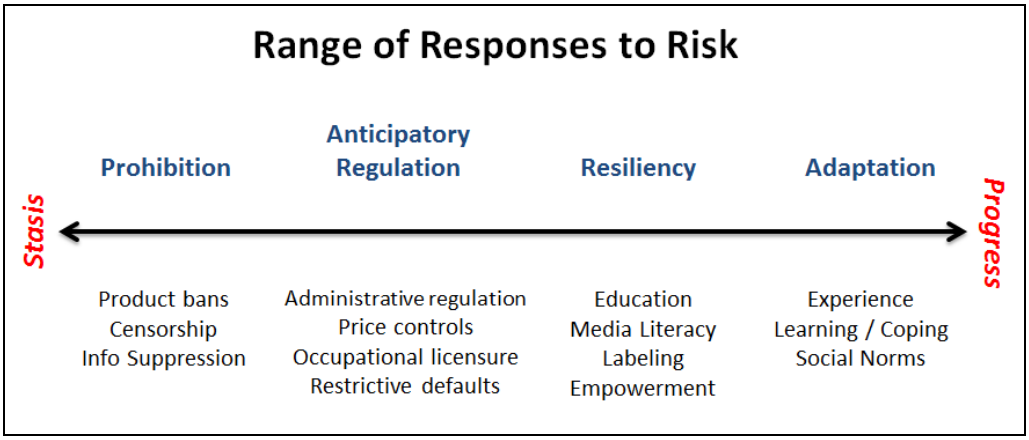
Of course, accidents are also possible with hammers. As this author can attest, hammers may miss targets, smash fingers, and even break knuckles. Worse yet, on some rare occasions, hammers have been wielded by mad men to maim and even to kill people or animals.

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:

---

[170] George Basalla, *The Evolution of Technology* (Cambridge: Cambridge University Press, 1988), 2.

[171] Henry Petroski, *The Evolution of Useful Things* (New York: Vintage Book, 1992), 126–9.



To summarize each possible approach to dealing with risks posed by new technology:

1. Prohibition

Prohibition attempts to eliminate potential risk through suppression of technology, product or service bans, information controls, or outright censorship.

2. Anticipatory Regulation

Anticipatory regulation controls potential risk through preemptive, precautionary safeguards, including administrative regulation, government ownership or licensing controls, or restrictive defaults. Anticipatory regulation can lead to prohibition, although that tends to be rare, at least in the United States.

3. Resiliency

Resiliency addresses risk through education, awareness building, transparency and labeling, and empowerment steps and tools.

4. Adaptation

Adaptation involves learning to live with risk through trial-and-error experimentation, experience, coping mechanisms, and social norms. Adaptation strategies often begin with, or evolve out of, resiliency-based efforts.

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. Most citizens are not allowed to possess bazookas or uranium, for example. The potential costs associated with their 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 "weapons 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. The default assumption in the minds of many remains "play it safe." There are serious perils for society from a rigid application of that principle, however, especially from its application to information technology.

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. There is no free lunch, however. "Playing it safe" sounds sensible until it becomes evident how that disposition limits progress and prosperity.

The problem with the precautionary principle, notes Kevin Kelly, editor of *Wired* magazine, is that because "every good produces harm somewhere . . . by the strict logic of an absolute precautionary principle no technologies would be permitted."[172] 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.

Cass Sunstein has done pioneering work on risk analysis and the precautionary principle in particular.[173] "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."[174] The problem is that one cannot prove a

---

[172] Kevin Kelly, *What Technology Wants*, 247–8.

[173] Sunstein, *Laws of Fear*.

[174] Cass Sunstein, "The Paralyzing Principle," *Regulation* (Washington, D.C.: Cato Institute, Winter 2002-2003), 34, http://www.cato.org/pubs/regulation/regv25n4/v25n4-9.pdf. "The most serious problem with the Precautionary Principle is that it offers no guidance – not that it is wrong, but that it forbids all courses of action, including inaction," Sunstein says. "The problem is that the Precautionary Principle, as applied, is a crude and sometimes perverse method of promoting various goals, not least because it might be, and has been, urged in situations in which the principle threatens to injure future generations and harm rather than help those who are

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. 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.

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. 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 of the opportunity to benefit from repeated trials.[175]

Simply stated, life involves *and requires* that some level of risk be accepted for progress to occur. Technology analyst Bret Swanson of Entropy Economics, LLC, 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

---

most disadvantaged. A rational system of risk regulation certainly takes precautions. But it does not adopt the Precautionary Principle." Ibid., 33, 37.

[175] Aaron Wildavsky, *Searching for Safety* (New Brunswick, CT: Transaction Books, 1988), 38.

experimentation and lots of small failures. We learn and move on, better prepared for the next try," he correctly notes.[176] This is equally true for social policy: *willingness 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. 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. For without a "willingness to risk failure," he says, "we will never truly succeed."[177] "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.[178]

By contrast, the precautionary principle destroys social and economic dynamism. It stifles experimentation and the resulting opportunities for learning and innovation. 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.

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."[179] In essence, the principle contradicts itself because it ignores tradeoffs and opportunity costs. As Sunstein cogently argues, "regulation sometimes violates the Precautionary Principle because it gives rise to *substitute risks*, in the form of hazards that materialize, or are

---

[176] Bret Swanson, "Banning Risk is Our Biggest Risk," *Forbes*, August 30, 2011, http://www.forbes.com/sites/bretswanson/2011/08/30/banning-risk-is-our-biggest-risk.

[177] Tim Harford, *Adapt: Why Success Always Starts with Failure* (New York: Farrar, Strauss and Giroux: 2011), 262.

[178] Nathan Rosenberg and L.E. Birdzell, Jr., *How the West Grew Rich: The Economic Transformation of the Industrial World* (New York: Basic Books, 1986), 266.

[179] Henry I. Miller and Gregory Conko, "Precaution without Principle," *Nature Biotechnology* 19 (April 2011), 302, http://www.ask-force.org/web/Regulation/Miller-Precaution-without-Principle-2001.pdf.

increased, as a result of regulation."[180] 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. Resiliency in the context of risk could be considered both an individual disposition and a societal method of coping with change. 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.

Resiliency theory, like the precautionary principle itself, has its roots in the field of environmental science. "Resilience is a core concept used by ecologists in their analysis of population ecology of plants and animals and in the study of managing ecosystems," note Marco A. Janssen and Elinor Ostrom.[181] 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 resilience as the "capacity of a system to absorb disturbance, undergo change and still retain essentially the same function, structure, identity, and feedbacks."[182] "A resilient ecosystem can withstand shocks and rebuild itself when necessary," they add. "Resilience in social systems has the added capacity of humans to anticipate and plan for the future."[183]

---

[180] Sunstein, *Laws of Fear*, 32 [emphasis in original].

[181] Marco A. Janssen and Elinor Ostrom, "Resilience, Vulnerability, and Adaptation: A Cross-Cutting Theme of the International Human Dimensions Programme on Global Environmental Change," *Global Environmental Change* 16 (2006) 237–239, http://www.public.asu.edu/~majansse/pubs/gecedit2006.pdf.

[182] Resilience Alliance, http://www.resalliance.org/index.php/about_ra. Definition is from Brian Walker, C. S. Holling, Stephen R. Carpenter, and Ann Kinzig, "Resilience, Adaptability and Transformability in Social–Ecological Systems," *Ecology and Society* 9 (2004), 5, http://www.ecologyandsociety.org/vol9/iss2/art5.

[183] Resilience Alliance, "Resilience," http://www.resalliance.org/index.php/resilience.

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. 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.[184] 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. And why not? Again, better to be safe than sorry, at least according to the logic of the precautionary principle.

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. "Children need to encounter risks and overcome fears on the playground," she told *The New York Times*. "Climbing equipment needs to be high enough, or else it will be too boring in the long run,"[185] she argues. "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

---

[184] Wildavsky, *Searching for Safety*, 103.

[185] John Tierney, "Can a Playground Be Too Safe?" *The New York Times*, July 18, 2011, http://www.nytimes.com/2011/07/19/science/19tierney.html?_r=1. See also Ellen Beate Hansen Sandseter, "Categorising Risky Play—How Can We Identify Risk-taking in Children's Play," *European Early Childhood Education Research Journal* 15 (June 2007), 237–52.

years."[186]

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."[187]

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.[188] "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.[189]

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 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.[190]

Indeed, there are other potential unintended consequences

---

[186] Ibid. May need to move down citation on final copy.

[187] Ibid.

[188] Ellen Beate Hansen Sandseter, and Leif Edward Ottesen Kennai, "Children's Risky Play from an Evolutionary Perspective: The Anti-Phobic Effects of Thrilling Experience," *Evolutionary Psychology* 9 (2011), 275, http://www.epjournal.net/filestore/EP092572842.pdf.

[189] Ibid.

[190] Tim Gill, "Cotton Wool Revolution," *The Guardian*, October 30, 2007, http://www.guardian.co.uk/commentisfree/2007/oct/30/comment.comment1.

associated with what some have referred to as "surplus safety."[191] If aggressive play on playgrounds is discouraged, it certainly will not help alleviate the growing childhood obesity problem.[192] A recent study of 34 daycare centers by five pediatric researchers confirmed that "societal priorities for young children—safety and school readiness—may be hindering children's physical development."[193] In particular, the researchers found that "stricter 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."[194]

Reduced playground time might also affect the sociability of youth by diminishing interaction opportunities and the resulting learning experiences. It also might limit the ability of children to explore and learn from nature.

The same is true of information environments. "The innocence that we like to believe used to exist in the world is revisionist history," Sternheimer argues, because "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 the end."[195] 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

---

[191] Shirley Wyver, Paul Tranter, Geraldine Naughton, Helen Little, Ellen Beate Hansen Sandseter and Anita Bundy, "Ten Ways to Restrict Children's Freedom to Play: The Problem of Surplus Safety," *Contemporary Issues in Early Childhood* 11 (2010), 263–77.

[192] Alice G. Walton, "New Playgrounds Are Safe—and That's Why Nobody Uses Them," *The Atlantic*, February 1, 2012, http://www.theatlantic.com/health/archive/2012/02/new-playgrounds-are-safe-and-thats-why-nobody-uses-them/252108.

[193] Kristen A. Copeland, Susan N. Sherman, Cassandra A. Kendeigh, Heidi J. Kalkwarf, and Brian E. Saelens, "Societal Values and Policies May Curtail Preschool Children's Physical Activity in Child Care Centers," *Pediatrics*, 129, no. 2 (February 2011), 1, http://pediatrics.aappublications.org/content/early/2012/01/02/peds.2011-2102.

[194] Ibid.

[195] Sternheimer, *Kids These Days,* 27.

deprive kids of an important opportunity for learning to navigate the outside world and learning to make appropriate decisions."[196]

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, other 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. As a recent MacArthur Foundation study of online youth Internet use concluded:

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

[196] Sternheimer, *Kids These Days,* 23.

> means more than being able to access "serious" online information and culture.[197]

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.com 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.[198] Similarly, when concerns about online cyberbullying arose, regulatory solutions were the kneejerk response.[199]

Ultimately, such "legislate and regulate" responses are not productive (or constitutional) approaches to online safety concerns. The better approach might be labeled "educate and empower," which is a resiliency-based approach centered around media literacy and "digital citizenship" strategies. 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.[200] Teaching our kids smarter online hygiene and "Netiquette" is vital. "Think before you click" should be lesson #1. They should also be encouraged to delete

---

[197] The MacArthur Foundation, *Living and Learning with New Media: Summary of Findings from the Digital Youth Project* (Chicago, IL: The MacArthur Foundation, November 2008), 2, http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

[198] Emily Steel and Julia Angwin, "MySpace Receives More Pressure to Limit Children's Access to Site," The *Wall Street Journal*, June 23, 2006, http://online.wsj.com/public/article/SB115102268445288250-YRxkt0rTsyyf1QiQf2EPBYSf7iU_20070624.html?mod=tff_main_tff_top.

[199] Berin Szoka and Adam Thierer, "Cyberbullying Legislation: Why Education is Preferable to Regulation," *Progress on Point* 16.2 (Washington, D.C.: The Progress & Freedom Foundation, June 19, 2009), www.pff.org/issues-pubs/pops/2009/pop16.12-cyberbullying-education-better-than-regulation.pdf.

[200] Rebecca Newton and Emma Monks, "Who's Minding the E-Children: Why Kids Can Sensibly Participate on the Net," *Gamer Daily News* (August 2011), http://www.gamersdailynews.com/articlenav-2984-page-1.html.

unnecessary online information occasionally.[201]

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.[202] 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."[203] Common Sense Media, a prominent online safety organization, notes that "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," it notes, "means that kids appreciate their responsibility for their content as well as their actions when using the Internet, cell phones, and other digital media. This is part of an effort 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."[204]

Stephen Balkam, CEO of the Family Online Safety Institute,

---

[201] Anne Collier, "'Delete Day': Students Putting Messages That Matter Online," NetFamilyNews.org, May 6, 2011, http://www.netfamilynews.org/?p=30376.

[202] Nancy Willard, *Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online*, (Eugene, OR: Center for Safe and Responsible Internet Use, November 2008), www.cyberbully.org/PDFs/yrocomprehensiveapproach.pdf; Anne Collier, "From Users to Citizens: How to Make Digital Citizenship Relevant," *Net Family News*, November 16, 2009, www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; Larry Magid, "We Need to Rethink Online Safety," *The Huffington Post*, January 22, 2010, www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html; Anne Collier and Larry Magid, ConnectSafety.org, *Online Safety 3.0: Empowering and Protecting Youth*, 2009, www.connectsafely.org/Commentaries-Staff/online-safety-30-empowering-and-protecting-youth.html; and Marsali Hancock, Rebecca Randall, and Alan Simpson, "From Safety to Literacy: Digital Citizenship in the 21st Century," *Threshold*, Summer 2009.

[203] Anne Collier, "A Definition of Digital Literacy & Citizenship," *Net Family News*, September 15, 2009, www.netfamilynews.org/2009/09/definition-of-digital-literacy.html.

[204] Common Sense Media, *Digital Literacy and Citizenship in the 21st Century: Educating, Empowering, and Protecting America's Kids* (San Francisco, CA: Common Sense Media, June 2009), 1, www.commonsensemedia.org/sites/default/files/CSM_digital_policy.pdf.

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 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.[205]

This approach should be at the center of child safety debates going forward. As online safety educator Nancy Willard notes, responsible digital citizens: (1) understand the risks: they know how to avoid getting into risk, detect if they are at risk, and respond effectively, including asking for help; (2) are responsible and ethical: they do not harm others, and they respect the privacy and property of others; (3) pay attention to the wellbeing of others: they make sure their friends and others are safe, and they report concerns to an appropriate adult or site; and, (4) promote online civility and respect.[206] 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. "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

---

[205] Stephen Balkam, *21st Century Citizenship*, The Huffington Post, Feb. 8, 2010, www.huffingtonpost.com/stephen-balkam/21st-century-citizenship_b_453316.html.

[206] Nancy Willard, *Comprehensive Layered Approach*, 1–2.

choices."[207]

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

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.[208] 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.[209] 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.

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

---

[207] Larry Magid, "Digital Citizenship and Media Literacy Beat Tracking Laws and Monitoring," *SafeKids.com,* August 29, 2011, http://www.safekids.com/2011/08/29/digital-literacy-critical-thinking-accomplish-more-than-monitoring-tracking-laws.

[208] Adam Thierer, *Public Interest Comment on Protecting Consumer Privacy in an Era of Rapid Change* (Arlington, VA: Mercatus Center at George Mason University, February 18, 2011), 24–8, http://mercatus.org/publication/public-interest-comment-protecting-consumer-privacy-era-rapid-change.

[209] 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* 16.5 (Washington, D.C.: Progress & Freedom Foundation, February 27, 2009), http://www.pff.org/issues-pubs/pops/2009/pop16.5parentalcontrolsmarket.pdf.

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.[210] 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.[211]

2. Cybersecurity

As noted earlier, the technopanic mentality developing around cybersecurity and cyberwar is generally overblown. 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.[212] "Just as more resilient technological 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."[213]

---

[210] "The nation has learned through experience, however, that government regulation often creates more problems than it 'solves.'" The President's Council on Competitiveness, *The Legacy of Regulatory Reform: Restoring America's Competitiveness* (September 1992), ix. See also Robert W. Hahn, "Regulation: Past, Present, and Future," *Harvard Journal of Law & Public Policy* 13, no.1 228: "Inflexible social regulations that place strict, detailed limits on firms' behavior also frequently stifle innovation and impose unnecessary costs."

[211] http://www.onguardonline.gov.

[212] Sean Lawson, *Beyond Cyber Doom: Cyber Attack Scenarios and the Evidence of History* (Arlington, VA: Mercatus Center at George Mason University, January 25, 2011), 31, http://mercatus.org/publication/beyond-cyber-doom.

[213] Ibid., 29.

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 tools better to secure their digital systems and to understand how to cope when problems arise.

Of course, most 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. "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*.[214] "These companies have entire legal teams dedicated to national and international cybercrime. 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.[215]

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.[216] 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 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

---

[214] Roger Grimes, "The Cyber Crime Tide is Turning," *Infoworld*, August 9, 2011, http://www.pcworld.com/article/237647/the_cyber_crime_tide_is_turning.html.

[215] Ibid.

[216] Adam Thierer, "Don't Panic Over Looming Cybersecurity Threats," *Forbes*, August 7, 2011, http://www.forbes.com/sites/adamthierer/2011/08/07/dont-panic-over-looming-cybersecurity-threats.

change is glacial and controlled."[217] 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.[218]

This is why the precautionary principle mentality is so dangerous for a free and innovative economy. Carl Gibson, a technology policy analyst formerly with the Washington Policy Center, correctly asserts that "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." He continues, "And as a society we are better off for their ability and willingness to engage in risky but productive behavior."[219] 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 Gibson, "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."[220]

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. Schumpeterian creative destruction has been rapidly eroding "market power" in the digital economy.[221] While some Internet critics fear the worst about growing

---

[217] Robert D. Atkinson, *The Past and Future of America's Economy* (Cheltenham, UK: Edward Elgar, 2004), 201.

[218] Ibid.

[219] Carl Gibson, "The Emergence of the Digital Precautionary Principle," (Seattle, WA: Washington Policy Center, June 2011) *Policy Brief*, 9.

[220] Ibid.

[221] Joseph Schumpeter, *Capitalism, Socialism and Democracy* (New York: Harper Perennial, 1942, 2008), 84.

"information empires,"[222] the truth is that their reign is usually brief as new digital services and platforms rapidly displace each another.[223] 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. 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. 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.

The movement of binary bits across electronic networks and digital distribution systems creates unique problems for information control efforts, even when that control might be socially desirable. In particular, efforts to control spam, objectionable media content, hate speech, copyrighted content, and even personal information are greatly complicated by five phenomena unique to the information age. Each of these phenomena is facilitated by the underlying drivers of the information revolution: digitization; dramatic expansions in computing and processing power ("Moore's Law"); a steady drop of digital storage costs; the rise of widespread Internet access; and the ubiquity of mobile devices and Internet access.

1. Media and Technological Convergence

First, content platforms and information distribution outlets are blurring together today thanks to the rise of myriad new technologies and innovations. New digital communication tools and entities generally ignore or reject the distribution-based distinctions and limitations of the past. In other words, convergence means that

---

[222] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (New York: Alfred A. Knopf, 2010).

[223] Adam Thierer, "Of 'Tech Titans' and Schumpeter's Vision," *Forbes*, August 22, 2011, http://www.forbes.com/sites/adamthierer/2011/08/22/of-tech-titans-and-schumpeters-vision.

information is increasingly being "unbundled" from its traditional distribution platform and can find many paths to consumers.[224]

For example, a piece of personal information voluntarily uploaded to a blog can be reproduced instantaneously on other blogs or on a social networking site (such as Facebook, LinkedIn, or MySpace), sent to Twitter (where it could be retweeted countless times), or sent directly to others via email or text messages. Again, this can, and often does, happen within minutes, even seconds. If the information in question contains a picture or video, it can also be reproduced across countless sites virtually instantaneously.

As a result of media and technological convergence, it is now possible to disseminate, retrieve, or consume the same content and information via multiple devices or distribution networks. When copying costs are essentially zero and platforms are abundant, information can flow across communications and media platforms seamlessly and instantly.

In this way, technological convergence complicates efforts to create effective information control regimes. This is will be just as true for privacy regimes as it is for other regulatory efforts.

2. Decentralized, Distributed Networking

Second, information creation, curation, storage, and dissemination are increasingly highly decentralized and distributed in nature. Milton Mueller, author of *Networks and States: The Global Politics of Internet Governance*, notes that:

> 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.[225]

---

[224] Henry Jenkins, founder and director of the Massachusetts Institute of Technology Comparative Media Studies Program and author of *Convergence Culture: Where Old and New Media Collide*, defines 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." Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York: New York University Press, 2006), 2.

[225] Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: The MIT Press, 2010), 4.

For example, controlling information flows by shutting down a website, blog, or social networking site is often ineffective since the information in question could be hosted in multiple places and might have been copied and reproduced by countless individuals who perpetuate the information by uploading it elsewhere.[226] The current debate over Wikileaks and control of state secrets demonstrates how challenging it can be to put information back into the bottle once it is released.[227]

By contrast, controlling information in the past could have been accomplished by smashing a printing press, cutting power to a broadcast tower, or confiscating communications devices. While imperfect, such measures—or even less extreme regulatory measures—were often reasonably effective at controlling information flows. But this was facilitated by the highly centralized nature of those older systems or networks. The highly decentralized

---

[226] "Short of unplugging the Internet, it is difficult to control its networking capabilities because they can always be redirected to a backbone somewhere else on the planet. True, it is possible to block access to some designated sites, but not the trillions of e-mail messages and the millions of web sites in constant process of renewal . . . The best governments can do to enforce their legislation is to prosecute a few unfortunate culprits who are caught in the act, while millions of others enjoy their merry ride over the web . . . While a few of the messengers are punished, the messages go on, most of them surfing the ocean of global, seamless, communication." Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2009), 113.

[227] "WikiLeaks copycats are quickly proliferating around the globe, beyond the U.S. government's effective reach." Jack Goldsmith, "Why the U.S. shouldn't try Julian Assange," *The Washington Post*, February 11, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/10/AR2011021006324.html. Similarly, *The Wall Street Journal* columnist Daniel Henninger has argued that, "There is one certain fix for the WikiLeaks problem: Blow up the Internet. Short of that, there is no obvious answer." Daniel Henninger, "WikiLeaks R Us," *The Wall Street Journal,* December 2, 2010, http://online.wsj.com/article/SB10001424052748704594804575648983975942008.html. For a more technical explanation of why it is probably impossible to shut down Wikileaks, see Danny Sullivan, "Why Wikileaks Will Never Be Closed or Blocked," *Search Engine Land*, December 8, 2010, http://searchengineland.com/why-wikileaks-will-never-be-closed-58226. See also Joby Warrick and Rob Pegoraro, "WikiLeaks Avoids Shutdown as Supporters worldwide Go on the Offensive," *The Washington Post*, December 8, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/08/AR2010120804038.html.

character of modern digital technologies complicates efforts to centralize information control. Hierarchical or top-down regulatory schemes must contend with the atomization of information and its mercurial nature within these modern digital systems.

3. Unprecedented Scale of Networked Communications

Third, in the past, the reach of speech and information was limited by geographic, technological, cultural, and language considerations. Today, by contrast, media flows across the globe at the click of a button because of the dramatic expansion of Internet access and broadband connectivity. Commentary and personal information that appears on a blog or a Twitter account in Tunisia is just as visible in Toledo or Tokyo. Offshore hosting of content also makes it harder than previously to know where content originates or is stored.[228]

While restrictions by government are certainly still possible, the scale of modern speech and content dissemination greatly complicates government efforts to control information flows.

4. Explosion of the Overall Volume of Information

Fourth, the volume of media and communications activity taking place today also complicates regulatory efforts. In simple terms, there is just too much stuff for regulators to police today relative to the past. "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," notes Downes.[229] Mueller concurs: "the sheer volume of transactions and content on the Internet often overwhelms the capacity of traditional government processes to respond" to developments in this space.[230] Almost a decade ago, a blue ribbon panel assembled by the National Research Council to examine the regulation objectionable content had already concluded that the "volume of information on the Internet is so large—and changes so rapidly—that it is simply impractical for human beings to evaluate

---

[228] "The bits are everywhere; there is simply no locking them down, and no one really wants to do that anymore." Abelson, Ledeen, and Lewis, *Blown to Bits*, 68.

[229] Larry Downes, *The Laws of Disruption*, 69.

[230] Mueller, *Networks and States*, 4.

every discrete piece of information for inappropriateness."[231]

The problem has only grown larger since then. IDC's 2009 report, *The Digital Universe Ahead — Are You Ready*?[232] offers the following snapshot of the digital "data deluge" that is upon us:

- In 2009, despite the global recession, the Digital Universe set a record. It grew by 62% to nearly 800,000 petabytes. A petabyte is a million gigabytes. Picture a stack of DVDs reaching from the earth to the moon and back.
- In 2010, the Digital Universe will grow almost as fast to 1.2 million petabytes, or 1.2 zettabytes.
- This explosive growth means that by 2020, our Digital Universe will be 44 times as big as it was in 2009. Our stack of DVDs would now reach halfway to Mars.

The Global Information Industry Center's report on *How Much Information*? also reports:

> In 2008, Americans consumed information for about 1.3 trillion hours, an average of almost 12 hours per day. Consumption totaled 3.6 zettabytes and 10,845 trillion words, corresponding to 100,500 words and 34 gigabytes for an average person on an average day. A zettabyte is 10 to the 21st power bytes, a million million gigabytes. These estimates are from an analysis of more than 20 different sources of information, from very old (newspapers and books) to very new (portable computer games, satellite radio, and Internet video). Information at work is not included.[233]

In February, 2011, Martin Hilbert and Priscila Lopez of the University of Southern California reported their finding that "in 2007, humankind sent 1.9 zettabytes of information through broadcast technology such as televisions and GPS. That's equivalent to every

---

[231] Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, D.C.: National Academy Press, 2002), 187.

[232] John Gantz and David Reinsel, "The Digital Universe Ahead—Are You Ready?" *IDC*, May 2010, http://idcdocserv.com/925.

[233] *How Much Information? 2009 Report on American Consumers* (report, Global Information Industry Center, UC San Diego, January 2010), http://hmi.ucsd.edu/howmuchinfo_research_report_consum.php.

person in the world receiving 174 newspapers every day."[234]

This "volume problem" for information control efforts will only grow more acute in coming years, especially when user-generated content, the next consideration, is taken into account.

5. User-Generation of Content and Self-Revelation of Data

Finally, in this new world in which every man, woman, and child can be a one-person publishing house or self-broadcaster, restrictions on information uploading, downloading, or subsequent aggregation or use will be become increasingly difficult to devise and enforce.[235] This is particularly relevant to any discussion of privacy regulation since millions of individuals are currently placing online massive volumes of personal information about themselves and others. The rapid rise of data self-revelation leads many scholars to puzzle about the existence of a so-called "privacy paradox." "People value their privacy, but then go out of their way to give it up," notes Downes.[236]

Regardless, slowing such information flows through public policy steps will be remarkably challenging since many people voluntarily continue to release and widely distribute their personal information. Moreover, because of the highly connected nature of social networks and the sheer volume of information sharing that takes place across them, absolute privacy control is an impossible task. For example, Facebook says users submit around 650,000 comments on the 100 million pieces of content served up *every minute* on its site.[237] And Hilbert and Lopez found that "humankind shared 65 exabytes of information in 2007, the equivalent of every person in the world

---

[234] Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information," *Science*, February 10, 2011, http://annenberg.usc.edu/News%20and%20Events/News/110210Hilbert.aspx.

[235] "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," notes Yochai Benkler. He continues, "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* (New Haven, CT: Yale University Press, 2006), 4

[236] Downes, *The Laws of Disruption,* 79.

[237] Ken Deeter, "Live Commenting: Behind the Scenes," Facebook.com, February 7, 2011, http://www.facebook.com/note.php?note_id=496077348919.

sending out the contents of six newspapers every day."[238] Not all of that shared information was personal information, of course, but much of it probably was.

This problem will be exacerbated by the increasing ubiquity of mobile devices that capture and reproduce information instantaneously. For example, practically every teenager today carries a powerful digital "sensor" or surveillance technology in his pocket today: his mobile phone.[239] Teenagers use their phones to record audio and video of themselves and the world around them and instantaneously share it with all mankind. They also use geolocation technologies to pinpoint the movement of themselves and others in real time. Meanwhile, new translation tools and biometric technologies are becoming widely available to consumers. Tools such as Google Goggles, available for many smartphones, let users snap pictures of anything they see and have it identified by Google's search engine, with information almost instantly provided to the user.[240] Eventually, these technologies will merge with "wearable computing" technologies in which biometric buttons on our shirts or coats will feed live streams of our daily movements and interactions into social networking sites and databases. We'll use them to record our days and play them back later, or perhaps to just instantly scan and recognize faces and places in case we cannot remember them.

Such technologies and ubiquitous information sharing activities are not going away; they are growing rapidly and will be commonplace in short order. As a result, mountains of intimate data will be created, collected, collated, and cataloged about us *and by us* on a daily basis.

When combined with the other four factors discussed above—the convergence of media and technology, decentralized and distributed networking, the unprecedented scale of networked communications, and the explosion of the overall volume of information—the unprecedented individual information sharing and user generation of content makes information control efforts and especially privacy control efforts significantly more difficult. Digital marketing

---

[238] Hilbert and Lopez, "The World's Technological Capacity."

[239] "Young people are turning to mobile devices in droves. They use them to post more information about themselves and their friends into the ether." Palfrey and Gasser, *Born Digital*, 62.

[240] http://www.google.com/mobile/goggles/#text.

professional Bhavishya Kanjhan notes that increasingly it is "the action of a user [that is] rendering . . . privacy controls ineffective. The human element is the weakest link in the chain."[241]

F. Implications for Anticipatory Regulation vs. Resiliency Strategies

The end result of these developments, as David Friedman of Santa Clara Law School has noted, is that "once information is out there, it is very hard to keep track of who has it and what he has done with it."[242] "The uncertainties and dislocations from new technology can be wrenching," observes *The Wall Street Journal's* Gordon Crovitz, "but genies don't go back into bottles."[243] "The explosive growth is still happening," note Abelson, Ledeen, and Lewis. "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."[244]

Again, this has implications for how we manage technological risk. When the possibility of information control or anticipatory regulation is greatly diminished or proves exorbitantly costly for society, resiliency and adaptation strategies become even more attractive alternatives. Information will increasingly flow freely on interconnected, ubiquitous digital networks. Getting those information genies back in their bottles would be an enormous challenge.

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

Consequently, a strategy based on building resiliency will focus on more cost-effective education and empowerment-based strategies that allow for trial and error and encourage sensible, measured responses to the challenges posed by technological change. Those

---

[241] Bhavishya Kanjhan, "Online Privacy is Dead and It Is a Good Thing," *Social Media Today*, June 14, 2010, http://socialmediatoday.com/index.php?q=SMC/206725.

[242] David Friedman, *Future Imperfect: Technology and Freedom in an Uncertain World* (Cambridge, MA: Cambridge University Press, 2008), 62.

[243] L. Gordon Crovitz, "Optimism and the Digital World," *The Wall Street Journal,* April 21, 2008, http://online.wsj.com/article/SB120873501564529841.html.

[244] Abelson, Ledeen, and Lewis, *Blown to Bits*, 3.

approaches will teach lessons and values that will accommodate future disruptive changes in our culture and economy.

"These technologies are inevitable. And they will cause some degree of harm," notes Kelly, "Yet their most important consequences—both positive and negative—won't be visible for generations."[245] 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 can 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."[246]

Kelly's formulation is remarkable similar to the "bad speech/more speech principle" from the field of First Amendment jurisprudence. That 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.[247] That's the same principle that Kelly advocates that society embrace when it comes to technology: Don't seek to ban or restrict it; find ways to embrace it, soften its blow, or counter it with new and better technology. It represents the smart way forward.

VII. A FRAMEWORK FOR EVALUATING AND ADDRESSING TECHNOLOGY RISK

Regardless of the issue, the following four-part framework should be used to analyze the risks associated with new technological developments and determine the proper course of action.[248]

A. Defining the Problem

The first step involves defining the problem to be addressed and determining whether harm or market failure exists. These are two

---

[245] Kevin Kelly, *What Technology Wants* (New York: Viking, 2010), 261.

[246] Ibid., 263.

[247] Adam Thierer, "Do We Need a Ministry of Truth for the Internet?" *Forbes*, January 29, 2012, http://www.forbes.com/sites/adamthierer/2012/01/29/do-we-need-a-ministry-of-truth-for-the-internet.

[248] This framework is based on Richard Williams and Jerry Ellig, "Regulatory Oversight: The Basics of Regulatory Impact Analysis" (working paper, Mercatus Center at George Mason University, Arlington, VA, 2011), http://mercatus.org/publication/regulatory-oversight.

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.[249] Harm is a particular 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. Many moral panics have come and gone through the years as critics looked to restrict speech or expression they found objectionable. In cases such as these, "harm" is very much an eye-of-the-beholder issue. 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.

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. "But creating new privacy rights cannot be justified simply because people feel vague unease," notes Solveig Singleton, formerly of the Cato Institute.[250] If harm in this context is reduced to "creepiness" or even "annoyance" and "unwanted solicitations" as some advocate, it raises the question 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.[251] In such a regime, harm becomes highly conjectural instead of concrete. This makes credible cost-benefit analysis virtually impossible since the debate becomes purely about emotion instead of anything empirical.[252]

---

[249] Steven Horwitz, "The Failure of Market Failure," *The Freeman*, December 8, 2011, http://www.thefreemanonline.org/headline/failure-of-market-failure.

[250] Solveig Singleton, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector," *Policy Analysis* 295, (Washington, D.C.: Cato Institute, January 22, 1998), 8, http://www.cato.org/pubs/pas/pa-295.html.

[251] Berin Szoka and Adam Thierer, "Targeted Online Advertising: What's the Harm Where Are We Heading," *Progress on Point* No. 16.2, (Washington, D.C.; Progress & Freedom Foundation, June 2009), http://www.scribd.com/doc/12597638/Targeted-Online-Advertising-Whats-the-Harm-Where-Are-We-Heading.

[252] Adam Thierer, *Public Interest Comment on Protecting Consumer Privacy in an Era of Rapid Change* (Arlington, VA: Mercatus Center at George Mason University, February 18, 2011), 24–8, http://mercatus.org/publication/public-interest-comment-protecting-consumer-privacy-era-rapid-change.

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. "Market failure" claims are also rampant even though many critics are sometimes guilty of adopting a simplistic "big is bad" mentality. Regardless, a high bar must be established before steps are taken to regulate information and digital technologies based upon market failure allegations.

B. Consider Legal and Economic Constraints

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

If harm or market failure can be demonstrated, the costs associated with government action must be considered. Even where there is harm and a market failure, it does not necessarily follow that government can effectively address the problem. Proposed rules should always be subjected to rigorous cost-benefit analysis. Regulation is not a costless exercise. All government action entails tradeoffs, both economic and social.

Of course, not all legal solutions entail the same degree of cost or complexity as direct regulatory approaches. 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 upon amorphous assertions of privacy "rights," the Federal Trade Commission (FTC) should hold companies to the promises or claims they make when it comes to the personal information they collect and what they do with it.[253] The agency has already brought and settled many privacy and data security cases involving its authority under Section 5 of the Federal Trade Commission Act to police "unfair and deceptive practices."[254] Recently the FTC has brought enforcement actions

---

[253] Berin Szoka, "FTC Enforcement of Corporate Promises & the Path of Privacy Law," *Technology Liberation Front,* July 13, 2010, http://techliberation.com/2010/07/13/ftc-enforcement-of-corporate-promises-the-path-of-privacy-law.

[254] "Since 1996 the Federal Trade Commission has actively used its broad authority under Section 5 of the FTC Act, which prohibits 'unfair or deceptive practices,' to

against Google[255] and Facebook.[256] Both companies agreed through a consent decree to numerous privacy policy changes, and they must also undergo privacy audits for the next 20 years.[257] Again, no new law was needed to accomplish this. The FTC's plenary 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, it is often wise to consider alternative, less restrictive approaches. Education and awareness-building strategies can be particularly effective, as well as being entirely constitutional. Empowerment-based strategies are also useful. 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"—

---

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." Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Ground and On the Books," *Stanford Law Review* 63 (January 2011), 127, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385.

[255] Alex Howard, "Google Reaches Agreement with FTC on Buzz Privacy Concerns," *Gov20.Govfresh*, March 30, 2011, http://gov20.govfresh.com/google-reaches-agreement-with-ftc-on-buzz-privacy-concerns.

[256] Brent Kendall, "Facebook Reaches Settlement with FTC On Privacy Issues," *The Wall Street Journal*, November 29, 2011, http://online.wsj.com/article/BT-CO-20111129-710865.html.

[257] Kashmir Hill, "So, What Are These Privacy Audits That Google And Facebook Have To Do For The Next 20 Years?" *Forbes*, November 30, 2011, 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.

abnormally high phone bills resulting from excessive texting or data usage—FCC regulators hinted that regulation may be needed to protect consumers. Eventually, the wireless industry devised a plan to offer their customers real-time alerts before they go over monthly text or data allotments.[258] Although these concessions weren't entirely voluntary, this transparency-focused result is nonetheless superior to cumbersome rate regulation or billing micromanagement by regulatory officials.[259] 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.

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 smartphone apps have given parents and others more information to make determinations about the appropriateness of content they may want to consume.[260] 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.

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. To the extent regulatory policies are deemed necessary, they should sunset on a regular basis unless policymakers can justify their continued existence. Moreover, even if regulation is necessary in the short-term, resiliency and adaptation

---

[258] Amy Schatz, "Cellphone Users to Get Billing Alerts under New Voluntary Standards," *The Wall Street Journal*, October 17, 2011, http://online.wsj.com/article/SB10001424052970203658804576635053172551850.html#ixzz1b42SjtiX.

[259] Steve Largent, president and CEO of CTIA-The Wireless Association, admitted that the notification guidelines will help the industry "avoid costly regulation." Katy Bachman, "Wireless Companies Stave Off Regulation with New Usage Alerts," *AdWeek*, October 17, 2011, http://www.adweek.com/news/technology/wireless-companies-stave-regulation-new-usage-alerts-135869.

[260] Adam Thierer, *Parental Controls & Online Child Protection: A Survey of Tools*, Version 4.0 (Washington, D.C.: Progress & Freedom Foundation, Summer 2009), http://www.pff.org/parentalcontrols.

strategies may emerge or become more evident over time.

VIII. CONCLUSION

This paper has endeavored to explain 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. Fear-based reasoning and tactics are used by both individuals and institutions to explain or cope with complicated social, economic, or technological change.

Most of those fears 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 redisposed toward pessimism and are risk-averse.[261] Nonetheless, most of these fears are generally not justified when empirical evidence is dispassionately considered. When there is something to these fears, alternative methods are often available to individuals and society 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 a precautionary principle mindset will increasingly take root in the information technology arena. If so, prohibition and anticipatory regulation increasingly will be proffered as solutions. Resiliency and adaption strategies are generally superior to more restrictive approaches because they leave more breathing room for continuous learning and innovation through trial and error experimentation. Wisdom and progress are the result of such experimentation, even when it involves risk and the chance for mistakes and failure. As F.A. Hayek 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."[262]

---

[261] A survey of these biases can be found in Shermer, *The Believing Brain*, 274-6; and Bruce Schneier, *Liars & Outliers: Enabling the Trust that Society Needs to Thrive* (New York: John Wiley & Sons, Inc., 2012), 217–8.

[262] F.A. Hayek, *The Constitution of Liberty* (London: Routledge, 1960, 1990), 29.