The Emergence of the Digital Precautionary Principle

By Carl Gipson
Director, Washington Policy Center's
Technology & Telecommunications Project

June 2011

WASHINGTON POLICY CENTER
Improving lives through market solutions

WASHINGTON
POLICY CENTER
Improving lives through market solutions

The Emergence of the Digital Precautionary Principle

by Carl Gipson
Director, WPC's Technology & Telecommunications Project

June 2011

Contents

The Emergence of the Digital Precautionary Principle

How regulating risk out of the innovation industry would harm economic growth and cause economic and social harm

by Carl Gipson
Director, WPC's Technology & Telecommunications Project June 2011

Key Findings

1. A precautionary principle is emerging in the digital arena.
2. Policymakers should rely on adaptability and resilience, not anticipation, to address problems in the innovation economy.
3. "Prophylactic" rules often end up causing more harm than good.
4. Federal, state and local governments are all susceptible to engaging in precautionary-like behavior.

Introduction: From Laws toward Codes

Air travel is the safest mode of transportation, yet airplanes sometimes crash, killing or injuring scores of passengers.[1] Cars are safer now than they have ever been, yet the Centers for Disease Control and Prevention reported there were 42,000 automobile-related fatalities in 2007 (latest data available). Drug companies spend billions of dollars making their drugs safer and more effective, but thousands of deaths or terrible side effects occur each year.

Would the world be safer or better off without air travel, without automobiles or without penicillin or heart medications? Of course not.

Regulation cannot possibly remove all risk from our daily lives. It is illegal to steal a car, but auto theft remains a problem. It is illegal to assault another human being, but it happens every day in every city. Massive oil spills break both statutory and regulatory laws, but that did not prevent the recent Gulf Oil leak that caused billions of dollars in damage.

It is becoming increasingly difficult to find any areas of industry that are not heavily regulated. Whether the regulatory fiats emanate from the federal government or are more closely homegrown by state or municipal regulators, the number of regulations continues to proliferate at an alarming speed.

As the number of regulations grows, a more disconcerting trend is the type of rules that are being promulgated. Many proposed regulations take an *ex ante* approach to regulating an industry, rather than the previously accepted practice of *ex post* regulatory framework.[2] Essentially, regulators are turning their sights on what they can predict, rather than relying on evidence that justifies a regulatory step to correct a problem in the market.

We are seeing a movement toward prophylactic regulations that do not rely on real scientific or economic evidence.

And we are seeing the emergence of regulations that reflect what might be termed a "digital precautionary principle," where regulators are discouraging innovations in technology by assuming the cost to humans or to the environment of an innovation outweigh the benefits of the new product of service.

[1] In 2010 there were no commercial airline fatalities in the United States.
[2] *Ex Ante* = before the event, *Ex Post* = after the event

What is the Precautionary Principle?

The precautionary principle has been around for several decades, but only in the last ten years has it become more solidified as an actual policy goal. Until now, the precautionary principle has been utilized in the environmental policy arena. While regulation of many industries can take on precautionary-like characteristics, the principle has its strongest roots in environmental policy.

According to Cass Sunstein, Harvard Professor and current Administrator of the Office of Information and Regulatory Affairs in the Obama administration, the precautionary principle is summed up as:

> "Simply put, the [precautionary] principle counsels that we should avoid steps that will create a risk of harm; until safety is established through clear evidence, we should be cautious. In a catchphrase: better safe than sorry."[3]

Another characteristic of the principle is an ignorance of cause and effect. Generally a regulation is written to offset a negative impact—social or economic—caused by a certain action. The precautionary principle turns this relationship on its head and demands that until an action can be proved safe, it is to be banned.

The United Nation's 1992 Rio Declaration states:

> "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation."[4]

In other words, regulators need not rely on actual scientific or economic evidence when crafting rules.

This puts the private market, which must operate under these poorly crafted regulations, at a huge disadvantage. When the evidence of harm to humans or the environment is not set on scientific or economic standards, it is then subject to change based on decisions made in the policy arena. New regulations become subject to the political winds and not evidence-based or peer-reviewed science.

There are many critiques of the precautionary principle, but chief among the concerns is that it ignores the cost/benefit relationship in favor of only cost. No benefits are taken into account. If a technological improvement betters the lives of millions but imposes minor costs on others, that improvement would be banned, despite the fact that it does far more good than harm.

Precautionary Principle Expands to the ICT Industry

The information and communications technology (ICT) industry has been one of the most dynamic and growing industries in human history. It has seen tremendous growth both in the United States and globally over the past several decades.

[3] Cass R. Sunstein, "The Paralyzing Principle," Regulation, Winter 2002-2003, page 32.
[4] "Rio Declaration on Environment and Development," The United Nations Conference on Environment and Development, Principle 15 (1992).

But it is not just about dollars and cents; ICT is also responsible for dramatic gains in productivity. According to The Information Technology & Innovation Foundation, the ICT industry in the U.S. is responsible for two-thirds of total factor growth in productivity between 1995 and 2002 and virtually all of the growth in labor productivity.[5]

However, regulators are increasing their scrutiny of the ICT industry and subjecting it to more *ex ante* types of regulations that are not based on scientific or economic evidence. The case studies in this report will show that minimal, if any, economic or scientific evidence or analysis was used to justify proposed regulations, both in statute and administrative code.

In none of the cases mentioned below is there a cost/benefit analysis that asks: "Do the benefits of this regulation outweigh the costs? Are the costs acceptable? Are we better off without regulating in this area? What does the science say?"

Shouldn't We Want Regulations that Protect People?

We do. However, in regulatory policy, more is not always better. And proposed rules must result in more benefits than the costs they impose.

Private industry is constantly engaged in the risky business of turning investments into profit. One cannot easily achieve greater wealth without incurring greater risk.

Therefore, entrepreneurs in the technology industry are constantly seeking the next breakthrough technology that can be monetized in order to achieve a return on investment. It goes without saying that many of the risky ventures in the ICT industry have succeeded in the last four decades (Microsoft, Google, Facebook, Amazon.com, etc.) while many more have failed (pets.com, Friendster, GlobalCrossing, InfoSpace, etc.).

In the ICT industry, innovation happens fast and there is no time to wait for government regulations to catch up. This is why it is important that existing laws reflect a few cornerstone ideas, such as strong property rights (intellectual property as well), rule of law and fair competition (e.g. antitrust law).

Regulations are policymakers' way to engage in risk mitigation for their constituents or the environment. The concepts of innovation and risk mitigation do not have to always end up in conflict, but they often result in an acrimonious relationship. This is due to the delicate balance policymakers face between industry innovations and their constituents asking for regulations they believe will keep them safe.

Unfortunately, policymakers and regulators often attempt to impose rules on services that simply can't be regulated (as hard as that is for some regulators to understand).

Not only do we have to consider the question, "*Should* this be regulated?"

[5] Robert D. Atkinson and Andrew S. McKay, "Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution," March 2007, available at http://itif.org/publications/digital-prosperity-understanding-economic-benefits-information-technology-revolution

we must also ask ourselves "*Can* this be regulated?" In the ICT industry this is extremely important, as many of the existing regulations governing technology are based on systems that have been obsolete for more than a generation, and only serve to hold back improvements (see the Net Neutrality case study below or the rise of Cloud Computing[6]).

Adaptability and Resilience Present a Better Alternative

As many others have shown, a substantial problem with the precautionary principle, especially as it is applied to technology, is its restrictiveness. According to the precautionary principle, if an action by industry imposes both benefits and costs it should therefore be restricted, regardless of whether benefits outweigh the costs. Likewise, if restricting that same action imposes inverted benefits and costs, it too should be restricted, regardless of overall human impact.

Aaron Wildavsky, author of *Searching for Safety,* advocated for a "strategy of resilience" rather than the more traditional risk-aversion theory that much regulation is based upon.[7]

"A strategy of resilience … requires reliance on experience with adverse consequences once they occur in order to develop a capacity to learn from the harm and bounce back. Resilience, therefore, requires the accumulation of large amounts of generalizable resources … that can be used to craft solutions to problems that the people involved did not know would occur."[8]

Part of the problem in dealing with new technology is the fear that tends to be associated with its emergence without fully appreciating its corresponding benefits. As previously stated, the ICT industry has produced trillions of dollars in economic growth in the United States and exponentially more value throughout the globe.

This wealth has not been generated without some major risks on the part of investors, employers, employees and their indirect connections. This is coupled with the more existential problem regulators face, which is, regulating unknowable future innovations. Promulgating rules requires significant resources, and a robust and dynamic industry, because of its constantly changing variables, requires even more resources, which are scarce to begin with. Therefore, the cost of regulating in a proscriptive way is higher than regulating in a way that handles known circumstances (i.e. it is easier and requires fewer resources to deal with known factors, rather than to guess about the future).

---

[6] More information on cloud computing and the need to reform the Electronic Computing Privacy Act of 1986 is available at: http://cei.org/coalition-letters/coalition-letter-urging-congress-update-privacy-laws

[7] See "Risk and Safety," Library of Economics and Liberty, at www.econlib.org/library/Enc/RiskandSafety.html

[8] Ibid. Risk aversion is a psychological term used to describe the phenomenon that "a great many people care more about avoiding loss than they do about making gains. Therefore, they will go to considerable lengths to avoid losses, even in the face of high probabilities of making considerable gains."

Case Studies

Radio Frequency Identification Device Legislation

In 2007, legislators in Washington introduced HB 1031, which targeted electronic communications devices. While the original intent was to implement consumer protections against unauthorized access and use of consumer information by companies by targeting Radio Frequency Identification Devices (RFID), the legislation would have impacted the wireless phone industry as well.

HB 1031, as originally proposed would have:[9]

- Required that a person selling, issuing, or distributing items containing an electronic communication device must post a notice and label the item
- Allowed a consumer to request access to any personal information gathered through an electronic communication device and to contest, amend or seek to remove the information
- Prohibited a person from combining or linking a consumer's personal information with information gathered from an electronic communication device
- Prohibited disclosure to third parties of information gathered by an electronic communications device
- Created civil and criminal penalties

While the legislation was supposed to target RFID devices, which were relatively new in 2007, the proposal defined electronic communications devices as "any device that can transfer signs, signals, writing, images, sound, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include: a written or oral communication; a tone-only paging device; or a communication from a tracking device."

This broad definition, if enacted, would have caught wireless phones in the mix. And while mobile data and broadband were certainly in existence in early 2007 when this bill was introduced, there was no way crafters of this bill could have anticipated the rapid growth in wireless broadband, specifically location-based applications and services (foursquare, Yelp, Facebook check-in, etc.).[10] Nor could policymakers have anticipated the emerging technology of Near Field Communications (NFC), which will enable consumers to use their cell phones as a mobile wallet.

HB 1031 would not necessarily have banned such technologies from Washington state, but it would have created severe complications for the businesses and consumers who currently benefit from the aggregation and dissemination of certain types of data, some personal, much of it not.

Would a mobile phone user have to specifically opt-in their information every time they checked in on Facebook or foursquare? Would a company have to construct a mechanism so that a user could access his own data and change it,

[9] The version of HB1031 that eventually passed the state legislature in 2008 focused on the illegal capture and misuse of data from/using an RFID device and made that action a Class C Felony. It was watered down significantly from the original proposal.

[10] For an in-depth look at third-party collection practices, see The Wall Street Journal's "What They Know" series, available at: http://online.wsj.com/public/page/what-they-know-digital-privacy.html

perhaps diluting the usefulness of the information? Would the benefits of trading certain information for free services have entered the discussion?

What regulators should be asking themselves in this situation is, "What, if any, harm has happened in this area that existing consumer protection laws do not already address?" Concrete evidence to justify further rulemaking, rather than conjecture, should be the guiding consideration.

Simply regulating a technology in the name of consumer protection does not guarantee criminals will not try to break the law in the future. Establishing data protection standards—already being done by private standards organizations—and enforcing the current criminal laws will benefit consumers and businesses while still providing the full benefits of new technology.

Cell Phone Radiation Concerns

The city of San Francisco implemented its own version of the Precautionary Principle back in 2003. It states, "Where threats of serious or irreversible damage to people or nature exist, lack of full scientific certainty about cause and effect shall not be viewed as sufficient reason for the City to postpone measures to prevent the degradation of the environment or protect the health of its citizens."

With this mentality, the City passed a cell phone radiation disclosure law in June 2010, despite the lack of any scientific evidence. The Federal Communications Commission, the World Health Organization and National Cancer Institute all disputed the City's assertion that there was any link between cell phone usage and brain cancer.

The city's response? "It's information that's out there if you're willing to look hard enough," according to a city spokesman.

The city ordinance requires retailers of cell phones to display:

1. The SAR (specific absorption rate) value of that phone and the maximum allowable SAR value for cell phones set by the FCC
2. A statement explaining what SAR is
3. A statement that additional educational materials regarding SAR values and cell phone use are available from the cell phone retailer

The city ordinance even dictates the font and font size ("Arial or equivalent, no smaller than 8 point") of the display.

The CTIA, the trade association for wireless companies, filed a lawsuit against the city ordinance. A decision on the case is pending.

One short passage from the lawsuit takes aim at what might be categorized as the city's approach to precautionary rulemaking in this area:

> "By enacting the Ordinance, the City is, in its own words, seeking to 'take a lead role' in 'the next frontier of consumer safety' and expects the Ordinance will 'encourage telephone manufacturers to redesign their devices to function at lower radiation levels,' despite the fact that devices

functioning at existing RF [Radio Frequency] levels already fully comply with the FCC established safety standards for RF emissions."[11]

In May 2011 the city backed away from the regulation as passed and is considering an alternative regulation, one that would most likely move away from the SAR label requirement.[12] One reason is that SAR measures *peak* radiation emission from a handset instead of the *average* emission levels. Therefore, a customer wishing to minimize radiation exposure could actually end up purchasing a handset that emits a higher average level of radiation when the handset with the higher peak rate actually emits lower overall radiation.

This is just one of the unintended consequences of such a rule. Even though no data exist suggesting a strong correlation between SAR levels emitted from phones and cancer rates, a consumer could rely on faulty measuring statistics to purchase the handset that actually poses more of a threat.

Other governmental bodies have entertained proposals to follow San Francisco in labeling cell phones as potentially harmful to human health. The state of California considered a similar proposal that would have required warning labels on packages and in user guides about potential radiation exposure. Legislators in Maine introduced a bill requiring similar warning labels, including a warning against use of a cell phone by pregnant women.

A bill was introduced in the Oregon Legislature to require a warning label on both sides of the cell phone retail packaging and on the device itself, occupying up to 30% of the surface to read:

> "WARNING: This is a radio-frequency (RF), radiation emitting device that has nonthermal biological effects for which no safety guidelines have yet been established. Controversy exists as to whether these effects are harmful to humans. Exposure to RF radiation may be reduced by limiting your use of this device and keeping away from head and body."

None of these other proposals have been enacted into law yet

Net Neutrality

There are numerous definitions of "network neutrality" but a common explanation is data that flows over the Internet should not be subjected to filters that could prioritize or censor any particular type of information. In other words, data should flow freely.

In October 2009 the Federal Communications Commission (FCC) issued a Notice of Proposed Rule Making, essentially kicking off the Net Neutrality skirmish. There are many complex policy and network architectural issues at play, but the bottom line is, "How much, if any, of the Internet should be regulated by the federal government or FCC?"

On one hand, consumer advocate groups and Internet content providers (e.g. Google) asked for a highly regulated Internet, which would require Internet Service Providers (e.g. Comcast) to treat their own property, the pipes through which Internet data flows, as nothing more than dumb pipes where no data could

[11] See "CTIA – The Wireless Association v. The City and County of San Francisco, California," United States District Court.

[12] Heather Knight, "S.F. put cell phone radiation law on hold," *San Francisco Chronicle*, May 6, 2011.

be prioritized nor blocked.

Internet Service Providers, on the other hand, wanted to continue to operate their networks using network congestion management practices, in order to manage increasing data demands that sometimes outstrip available transmission space (aka bandwidth).

This issue relates to the digital precautionary principle due to, as technology author Larry Downes put it, the FCC's reliance on "prophylactic" rules in the finalized order published in late 2010.[13]

What is most troubling, other than the FCC's insistence that it had the legal authority to issue this order despite a U.S. District Court saying it does not, is that the new rules on this industry will carry many unknowns and will lead to unintended consequences. This is in stark contrast to the known benefits already provided by the growth of the Internet economy over the last few decades. Government regulators are willing to crimp economic and social expansion on the assumption that ISP network congestion management and paid prioritization of data constitutes an even bigger threat.

Rather than accept the known social and economic benefits of a growing Internet industry and deal with concerns as they arise (ex post regulation), the FCC is attempting to place a one-size-fits-all regulatory regime on top of a dynamic and fast-changing sector. A better option would be a policy of resiliency or adaptation, as mentioned earlier.

A net neutrality "resiliency" policy would establish certain rules that focus on both intellectual and physical property and provide incentives for increased competition, as well as protect consumers from anti-competitive behavior by using existing antitrust law.

It would be better for the Department of Justice or the Federal Trade Commission to regulate, if need be, on a basis that targets discrimination against users that harms competition or the users themselves. Regulating agencies would be able to do this under existing federal antitrust law and would not have to go through the onerous process of conjuring up new rules on which to base their actions. This route would rely on a more effective case-by-case strategy that otherwise would be difficult to regulate beforehand.

There are parts of the FCC's order that are good and would be unlikely to alter or denigrate the user's experience or cause ISPs to lose revenue, such as a transparency in network management practices. But the "prophylactic" rules, which prohibit blocking of content applications or non-harmful devices, or prohibit "unreasonable" data discrimination, attempt to clairvoyantly regulate problems that have not yet arisen.

Given the few anecdotal stories the FCC provided as evidence that a corporate takeover of the Internet was underway, backers of net neutrality essentially fear the unknown drawbacks of *not* implementing new rules more than they do the known benefits of continuing the status quo. Backers of net neutrality have essentially asked for these "prophylactic" rules in order to avoid

[13] See "Chairman Genachowski and his Howling Commissioners: Reading the Net Neutrality Order (Part I)," at http://techliberation.com/2010/12/30/chairman-genachowski-and-his-howling-commissioners-reading-the-net-neutrality-order-part-i/

a future that they *assume* will happen, but about which very little or no evidence actually exists.

Conclusion

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

Regulators also face a daunting challenge. So often they are expected to regulate industries in order to protect or enhance human health or environmental safety based on incomplete facts or on speculation. No one, regulator or investor, has a crystal ball. No one can truly see the benefits and costs and all the trial and error that takes place on a daily basis. That is why trying to regulate the future, especially in the technology industry, is so futile.

That does not mean there should be no regulations put in place to promote safety or enhance competition. Basic principles of intellectual property, fair competition and privacy are the bedrock of our economic freedom and growth. But regulating specific technologies will lead to situations where the government picks technological winners and losers, despite government's inability to foresee what kinds of unintended consequences will come about because of its regulatory decisions.

As these three case studies show, the precautionary problem does not just pertain to the federal government, but to state and local governments as well. Allowing the precautionary principle to seep into the digital space will result in unquantifiable opportunity costs. Attempts to regulate risk out of existence are not only impossible, but actually lead to new risks. Taken to its logical conclusion, 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.

About the Author

Carl Gipson is Director of the Center for Small Business at Washington Policy Center. He also directs WPC's technology and telecommunications policy research. He regularly writes opinion pieces, legislative memos, policy notes, and is the author of *Reviving Washington's Small Business Climate*, *24 Ways to Improve Washington's Small Business Climate*, *A Citizen's Guide to Initiative 920: The Estate Tax*, and other publications. Carl appreas regularly in print and broadcast media across the state addresses chambers of commerce and other civic groups. He was a columnist for *The Olympian* in 2003 and received his bachelor's degree in political science from Western Washington University in 2001.

About Washington Policy Center

Chairman	**Greg Porter**
President	**Dann Mead Smith**
Vice President for Research	**Paul Guppy**
Communications Director	**John Barnes**

For more information contact Washington Policy Center:

PO Box 3643
Seattle, WA 98124
p 206-937-9691
f 206-624-8038
wpc@washingtonpolicy.org
www.washingtonpolicy.org

Washington Policy Center is a 501(c)(3) non-profit research and education organization that promotes sound public policy based on free-market solutions. Nothing here should be construed as an attempt to aid or hinder the passage of any legislation before any legislative body.

WASHINGTON
POLICY CENTER
Improving lives through market solutions