# The Pollyanna Delusion

**Hal Berghel,** University of Nevada, Las Vegas

*How can we prevent scholarly literature from being misrepresented? By reading and reacting to it. Nowhere is this more critical than with position papers that have the potential to influence government policies.*

Psychologists refer to our tendency to subconsciously emphasize positive thoughts over negative ones as the Pollyanna Principle, according to which people tend to produce a positive bias toward past events, show a propensity to ignore negative stimuli, and have an inclination to react to pleasant stimuli faster than unpleasant. In simple terms, it holds that people prefer to look on the bright side of things even in the face of disconfirming evidence and when doing so isn't in their own best interests. Books have been written about the Pollyanna Principle,[1] and it's been observed in a variety of human endeavors, from mass media, communication, advertising, and marketing, to writing stockholder reports.[2]

There's interesting cognitive psychology behind this principle, along with its close cousins—confirmation bias, cognitive dissonance, and balance theory. This branch of psychology explains much about our nagging political dysfunction, but a related phenomenon exists that has yet to be fully appreciated by the social science community. I'll call this the Pollyanna Delusion, which holds that scholars tend to underappreciate the potential misuse of their scholarly work by partisan and special interests. The latest Pollyanna Delusion candidate is the recent "One Internet" report from the Global Commission on Internet Governance.[3] The subject of this report is nominally the Internet, however, it focuses primarily on politics and the law in which the Internet is ensconced, with scant attention paid to the technology itself. The result is a set of weak observations and policy recommendations that invite misuse by playing into the hands of the power elite who seek to control the Internet for ideological or economic advantage.

## HOW SHOULD THE INTERNET BE GOVERNED?

The report isn't totally without merit, and the topic is certainly important. But the focus of the report is fundamentally misguided. The central question of the report is how the Internet should be governed. The Internet is so important to the world, it's argued, that its governance can no longer be left to a group of well-intentioned techies. "It's governance must ... be based on both formal mechanisms and evolving norms to capitalize on its tremendous


0018-9162/16/$33.00 © 2016 IEEE

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

power to provide economic opportunity and security, while also providing resilience and privacy for all Internet users" (read: the Internet must be sufficiently controlled to optimally serve business and government interests).[3] The report continues, "To realize its full potential, the Internet of the future will need to be open, secure, trustworthy and accessible to all. Safeguarding these attributes requires international cooperation that engages governments, businesses, the technical community and civil society in a shared vision to protect the rights of users, establish norms for responsible public and private use, and ensure the kind of flexibility that will encourage innovation and growth." That's funny. How did the Internet achieve the ubiquity it enjoys without this cooperation between engaged governments and the business community? Ask yourself which of the following is likely to exercise overwhelming control under such new governance: governments, businesses, technical community, civil society? The technical community? Nope. Society? No chance. The control will be in the hands of governments and businesses—just like governance under the proposed Trans-Pacific Partnership, and for the same reasons. Although "One Internet" advises protecting users' rights, it must be understood that such protection will be limited by business and government interests.

The report unfortunately overemphasizes the creation of value for the commercial special interests. And although its recommendations could indeed result in economic, political, commercial, legal, law enforcement, or military value, it won't likely be in the form of net neutrality, proactive positions on anonymity, privacy protections, the absence of censorship, the abolition of invasive and unwanted interference in the form of unsolicited advertisements, and the prohibition of capturing personal information without the affected individual's consent. Only secondary attention is paid to individual rights and constitutional guarantees in this document. Note that the two references found in the preface were both published by corporations (Boston Consulting Group and McKinsey and Company), and both focus on the Internet's value to business.

> The Internet is so important to the world, it's argued, that its governance can no longer be left to a group of well-intentioned techies.

According to "One Internet," we're facing a crisis. (All polemics begin with a crisis—sometimes it's real, but more often, as in this case, it's manufactured.) We purportedly face three possible futures: (1) a broken Internet; (2) a sub-optimal Internet; and (3) an Internet that is "energetic, vigorous and healthy." The latter option comes with an implied happy face of course. Let's parse out these three options.

### Option 1: A dangerous and broken Internet

Remember that this is an agenda-based report, not peer-reviewed scholarship, so we shouldn't expect much justification for claims. And we aren't disappointed here: Option 1 is the worst-case scenario in which "the costs imposed through the malicious actions of criminals and inadvertent effects of government regulation of the Internet are so high that individuals and companies curtail their usage." Note how this is carefully worded to emphasize that the maliciousness of criminals (*really bad*) and government overregulation (*really, really bad*) will cause individuals and companies to use the Internet less (*horrors*!). What is meant, of course, is that these big-business interests might not derive full profit or value from the resource. Note also, that the report's concern is with government overregulation of business, not with government overregulation of citizens. Internet surveillance of citizens, government censorship, government collusion with cybermercenaries and "pure plays," government exploitation of malware, government harvesting of zero-day attacks to forestall patches that protect netizens, cyberwarfare attacks, violations of civil rights, and the like are discussed with little passion as they're not central to the envisioned forthcoming crisis. Civil libertarians will be nonplussed by this report. And though businesses might fear regulation that could interfere with their business models, the informed public has no such fear because they're not afraid of government overregulation of business, but rather government overreaction and overreach when it comes to their personal liberties.

"One Internet" claims that the global loss stemming from "malicious actions" this year could be as high as $445 billion (though there's no documentation provided). To place this in context (and leaving aside the issue of whether the claim is correct), it pales in comparison to the $4 trillion in encumbrances thus far for the recent wars in Iraq and Afghanistan,[4] or the minimum $14–$43 trillion that the 2007–2008 economic meltdown took out of the economy when lost output and consumption, government

bailouts, and lost opportunity are combined.[5] Additionally, unlike wars and economic meltdowns, the losses due to malicious actors don't fall on the taxpayer. Further, many of these costs are due to business negligence—the accountability for which, as Adam Smith would be the first to point out, the businesses themselves should own. The numbers in this report are somewhere between imaginary and quixotic, and they're offered without means to verify them or place into an appropriate context; as such, they're not credibility inspiring.

> Imagine what the Internet would look like if key decisions about innovation and design were left to politicians, lawyers, and business executives.

### Option 2: Uneven and unequal gains

This second scenario anticipates a moral hazard in which digital dividends are disproportionately distributed among the stakeholders. This is a rehash of the digital divide argument framed in the 1990s amidst the hype for the information superhighway. Some nations could "assert sovereign control through trade barriers, data localization and censorship and by adopting other techniques that fragment the network in ways that limit the free flow of goods, services, capital and data," thereby "increasing inequality and unrest across the board." This Chicken Little/sky-is-falling mantra should be familiar, as it's invoked in virtually every undocumented polemic. It shares memetic qualities with Godwin's Law.

### Option 3: Nirvana is achieved

In this third scenario, the digital world is a happy place. "A healthy Internet produces unprecedented opportunities for social justice, human rights, access to information and knowledge, growth, development and innovation."[3] The expansion of broadband access solves many social ills, and advances such as the Internet of Things (IoT) produce growth in the gross domestic product of player-nations in the tens of trillions of dollars. Thus, through the properly governed Internet, the world is magically transformed into a warm and caring place. As I've argued many times before in this column, technology is, with few exceptions, ethically neutral: It'll be used for good or ill by the power elite. "One Internet" offers the same sort of specious argument as George Shultz did with the dictator's dilemma.[6]

## A NEW SOCIAL COMPACT

Therefore, we're led to believe that option 3 will solve our problems, and in order to realize it, we'll need a new social compact. Here it is in short:[3]

> *There must be a mutual understanding between citizens and their state that the state takes responsibility to keep its citizens safe and secure under the law while, in turn, citizens agree to empower the authorities to carry out that mission, under a clear, accessible legal framework that includes sufficient safeguards and checks and balances against abuses. Business must be assured that the state respects the confidentiality of its data and they must, in turn, provide their customers the assurance that their data is not misused. There is an urgent need to achieve consensus on a social compact for the digital age in all countries. Just how urgent is shown by current levels of concern over allegations of intrusive state-sponsored activities ranging from weakening of encryption to large-scale criminal activity to digital surveillance to misuse of personal data, and even to damaging cyber attacks and disruption.*

It's hard to imagine how a reasonable person could object to this new social compact. It's equally hard to imagine how anyone could implement it. Like the United Nations Universal Declaration of Human Rights, this compact will fall stillborn from the (digital) press. These standards and values, no matter how well-intentioned, won't withstand the inevitable assault from sundry governments, industries, businesses, cultures, religions, nongovernment agencies, and political organizations that find specific principles inconvenient or incompatible with parochial bias. The goal of the compact is notable although its likely effect is negligible. This will play out just like the battle over net neutrality—baby steps forward and backward that are indiscernible through the political smokescreen.

### Aspirations and interests

Let no one discourage well-intentioned lofty aspirations. They become problematic, however, when they feed sophistry—especially in the hands of big business and big government. There's an analogy here to the mythical STEM crisis about which I've written before. No one is opposed to STEM education, but many of us are opposed to drowning the issue in the 3-Hs (hype, hyperbole, and hubris) with the ultimate goal of addressing the "crisis" (a nonexistent shortage of STEM workers) with taxpayer money. In reviewing the literature, we easily see that proponents base no claims on publicly accessible data.[7] So it will be with this "One Internet" report." Special interests—public and private—will use the fact that this report speaks of a need for a new Internet governance model as a justification

for seeking self-serving control of the resource. In all likelihood, these special interests will never read beyond the preface, and this report will come to mean whatever the special interests find convenient. I've pulled several of these lofty aspirations from the report as examples.

**Example 1.** "Governments should not create or require third parties to build back doors or compromise encryption standards, as these efforts would weaken the Internet and fundamentally undermine trust." A driving force behind the zero-day black market is the US government. How can anyone take this proposed principle seriously in light of the revelations of Edward Snowden?

**Example 2.** "The Commission urges member states of the United Nations to agree not to use cyber technology to attack the core infrastructure of the Internet. Governments seeking a peaceful and sustainable Internet should adopt and respect norms that help to reduce the incentive for states to use cyber weapons." Does Stuxnet ring a bell? Even the governments that supported this commission won't agree to this principle whenever it becomes inconvenient.

**Example 3.** "Businesses or other organizations that transmit and store personal data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Institutions should demonstrate accountability and provide compensation in the case of a security breach." And how will this happen? The US House and Senate could as easily pass accountability legislation as make cows fly, and the suggestion that ISPs and telecoms would voluntary subscribe to such accountability is just silly.

**Example 4.** "Manufacturers and vendors of information and communication technologies (ICT) should follow the principle of privacy and security by design, when developing new products, paying particular attention to embedding security in the burgeoning IoT. They must be prepared to accept legal liability for the quality of the technology they produce." This is what the anti-smoking crusade has been saying since the 1930s, yet big tobacco companies refused to admit the hazards of smoking for 75 years and still aren't prepared to accept legal liability for misrepresenting the health hazards of their product. This is like saying that the petroleum industry should be held accountable for climate change. The money, power, and influence are firmly on the opposite side of these issues.

So when "One Internet" calls on "... governments, private corporations, civil society, the technical community and individuals together to create a new social compact for the digital age," it should be taken as a cry in the wilderness. There's no incentive for policy makers to pay more than lip service to this call. But, reinforcing the Pollyanna Delusion, don't underestimate the enormous incentive to use the imprimatur to mislead the public into tacit support or blind faith in misguided and counterproductive policies. Policy makers at large respond to the power of special interests, and there are no powerful special interests behind any of these lofty goals.

## THE POLLYANNA DELUSION, RELOADED

As readers of this column and "Aftershock" know, several of us have discussed the Pollyanna Delusion in connection with the STEM crisis myth and the undocumented claims of a shortage of H-1B visas in high tech.[8–10] As another illustration, consider the SAIC report of the failure of Diebold AccuVote TS voting machines to comply with the State of Maryland Information Security Policy. Although the most damaging parts of the SAIC report were largely redacted by the State of Maryland before public release, enough survived for the reader to get the gist that there were several hundred security weaknesses discovered, 25 of which were judged critical. These two sentences say it all: "[The] AccuVote-TS voting system is not compliant with State of Maryland Information Security Policy & Standards .... The system, as implemented in policy, procedure, and technology, is at high risk of compromise." (Read more at www.ballot-integrity.org/docs/SAIC_Report.pdf.)

Nevertheless, thanks to a judicious amount of neoliberal spin, Diebold morphed this report into "The thorough system assessment conducted by SAIC verifies that Diebold voting stations provides an unprecedented level of election security. ... Voters in the State of Maryland can now rest assured that they will participate in highly secure and accurate elections." This disconnect from reality is a common byproduct of spin cycles and shows just how easy it is to morph reports into phantasmagorical nonsense that is then taken as gospel by the unprepared. The Pollyanna Delusion can only be neutralized when knowledgeable scientists stay abreast of seemingly innocuous polemics that are used to support bad policy by unthinking politicians and bureaucrats.

If critically reviewed by computer professionals and technologists, "One Internet" will be seen for what it is. As with other conclusion-directed reports, the challenge isn't so much to get knowledgeable professionals to provide correct interpretations, but just to get them to read it. It's too easy for all of us to dismiss such reports as irrelevant contrivances of external constituencies, but that isn't the way policy makers will look at it. Most of them will never read any of it and will choose to rely on the interpretations provided by staffers, partisans, and representatives of special interests. To the typical elected official, the credibility lies not in the words but the imprimatur: it was produced by a

commission, so it must be true. If the lobbyists the politicians listen to say that this report supports a certain piece of legislation, no further investigation is required. Thus, absent computing professionals inserting themselves into the limited public discussion, such reports go unchallenged.

If the list of Global Commission on Internet Governance advisors is an accurate indication, the group is largely a collection of political wonks, lawyers, and nontechnical members of professional societies, with a sprinkling of academics with computing backgrounds. It's what one might expect from this mix: the operative principle being that the Internet is now too important to leave in the care, custody, and control of the people who designed it, built it, and made it the success that it is.

On the contrary, I submit that the Internet is as successful as it is because the policy makers, politicians, lawyers, business executives, and nontechnical folks were largely isolated from the major decision making in the first place. Imagine what the Internet would look like if key decisions about innovation and design were left to politicians, lawyers, and business executives.

The "One Internet" report is just another example of serviceable therapeutic rhetoric in service to special interests. It's important for academics to recognize that no matter how eminently ignorable such reports are, they're capable of being effectively misused by policy makers to the detriment of both technology and society. We need to be attuned to the likelihood that our well-intentioned scholarship can be misused for partisan policy objectives that are inconsistent with the scholarship. Let's start with actually reading the report!

## REFERENCES

1. M.W. Matlin and D. J. Stang, *The Pollyanna Principle: Selectivity in Language, Memory and Thought*, Schenkman Publishing, 1979, 226 pp.
2. H. Hildebrandt and R. Snyder, "The Pollyanna Hypothesis in Business Writing: Initial Results, Suggestions for Research," *J. Business Comm.*, vol. 18, no. 1, 1981, pp. 5–15.
3. "The Global Commission on Internet Governance—One Internet," report, The Centre for International Governance Innovation, 2016; www.ourinternet.org/report.
4. D. Trotta, "Iraq War Costs U.S. More than $2 Trillion," Reuters, 14 Mar. 2013; www.reuters.com/article/us-iraq-war-anniversary-idUSBRE92D0PG20130314.
5. D. Luttrell, T. Atkinson, and H. Rosenblum, "Assessing the Costs and Consequences of the 2007–09 Financial Crisis and Its Aftermath," *Economic Letter*, Federal Reserve Bank of Dallas, 11th District, vol. 8, no. 7, Sept. 2013; www.dallasfed.org/assets/documents/research/eclett/2013/el1307.pdf.
6. H. Berghel, "The Dictator's (False) Dilemma," *Computer*, vol. 49, no. 7, 2016, pp. 40–43.
7. *Achieving Systemic Change—A Sourcebook for Advancing and Funding Undergraduate STEM Education*, C.L. Fry, ed., Assoc. Am. Colleges and Universities, 30 Oct. 2014; www.aacu.org/sites/default/files/files/publications/E-PKALSourcebook.pdf.
8. R. Charette, "The STEM Anxiety Business," *Computer*, vol. 49, no. 3, 2016, pp. 82–87.
9. N. Matloff, "The H-1B Visa Controversy," *Computer*, vol. 49, no. 7, 2016, pp. 88–93.
10. H. Berghel, "STEM Crazy," *Computer*, vol. 48, no. 9, 2015, pp. 75–80.

**HAL BERGHEL** is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.