Privacy in a Post-Regulatory World:
Lessons from the Online Safety Debates

By Adam Thierer[*]

No matter how well-intentioned, privacy laws and regulations are being increasingly strained by the realities of our modern Information Age, and that fact should influence our strategies for dealing with the challenges posed by ubiquitous social media, Big Data, and the coming "Internet of Things."[1] Specifically, we need to invert the process of how we go about protecting privacy by focusing more on bottom-up solutions—education, empowerment, media literacy, digital citizenship lessons, *etc*.—instead of top-down legalistic solutions or techno-quick fixes.[2] In this regard, we can draw important lessons from the debates over how best to protect children from objectionable online content.[3]

I. NEW REALITIES

Lawmakers and policy advocates who worry about how best to protect online privacy today must contend with the fact that, for better or worse, we now live in a world that is ruthlessly governed by two famous Internet aphorisms. First, "information wants to be free." Sometimes that fact is worth celebrating. "Unfortunately," notes computer scientist Ben Adida, "information replication doesn't discriminate: your *personal data*, credit cards and medical problems alike, also want to be free. Keeping it secret is really, really hard," he correctly notes.[4]

A second well-known Internet aphorism explains why this is the case: "The Net interprets censorship as damage and routes around it," as Electronic Frontier Foundation co-founder John Gilmore once noted.[5] But this insight applies to *all* classes of information. Whether we are talking about copyright policy, cybersecurity, state secrets, pornography, hate speech, or personal information, the reality is always the same: *Any* effort to control information flows will be resisted by many other forces or actors in the online ecosystem. Moreover, once the genie is out of the bottle, it is incredibly hard to get it back in.

These two realities are the byproduct of the Internet's decentralized, distributed nature; the unprecedented scale of modern networked communications; the combination of dramatic

---

[*] *Senior Research Fellow, Mercatus Center, George Mason University.*

1 Adam Thierer, Mercatus Center at George Mason University, *Public Interest Comment to the Federal Trade Commission in the Matter of The Privacy and Security Implications of the Internet of Things* (May 31, 2013), http://mercatus.org/publication/privacy-and-security-implications-internet-things; Adam Thierer, *Can We Adapt to the Internet of Things*? IAPP PRIVACY PERSPECTIVES (June 19, 2013), https://www.privacyassociation.org/privacy_perspectives/post/can_we_adapt_to_the_internet_of_things.

2 Adam Thierer, *Let's Not Place All Our Eggs in the Do Not Track Basket*, IAPP PRIVACY PERSPECTIVES, (May 2, 2013), https://www.privacyassociation.org/privacy_perspectives/post/lets_not_place_all_our_eggs_in_the_do_not_track_basket.

3 Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409 (2013).

4 Ben Adida, *(your) information wants to be free*, Benlog (Apr. 28, 2011, 12:46 AM), http://benlog.com/articles/2011/04/28/your-information-wants-to-be-free.

5 *Quoted in* Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME (Dec. 6, 1993), http://www.chemie.fu-berlin.de/outerspace/internet-article.html.

expansions in computing and processing power (also known as "Moore's Law")[6] alongside a steady drop in digital storage costs; and the rise of widespread Internet access and ubiquitous mobile devices and access.

Compounding matters further still—especially for efforts to protect privacy—is the fact that we are our own worst enemies when it comes to information containment. Ours is a world of unprecedented individual information sharing through user-generation of content and self-revelation of data. On top of that, we now have decentralized peer-on-peer surveillance; new technologies make it easier than ever for us to release information not only about ourselves abut about all those around us.

Traditional information control mechanisms are being strained to the breaking point in this new environment and we need to be discussing how to come to grips with these new realities.

II. A CONVERSATION FEW WANT TO HAVE

Unfortunately, we're not having that conversation today. Or, to the extent we are, we're focused on the wrong set of issues or solutions. Discussions about protecting online privacy and reputation are still predominately tied up with philosophical ("What privacy rights do we have?) and legalistic ("How should we enforce those rights?") debates. Outside of some very narrow contexts (i.e., sensitive health and financial information), consensus about privacy rights has been elusive here in the United States.

The urge to delineate a tidy set of neatly-defined privacy rights and then protect them by law is completely understandable. But it is becoming more of a pipe dream with each passing year. Call me a defeatist, but esoteric metaphysical debates about the nature of our privacy rights and heated policy debates about how to enforce them are increasingly a waste of time.

Moreover, at some point the costs associated with regulatory controls must be taken into account. If we conduct a careful benefit-cost analysis of various regulatory proposals—something that has been woefully lacking on the privacy front in recent years—we find that many complex economic and social trade-offs are at work.[7] Regulation is not a costless exercise and, as noted, there are reasons to doubt it will even be effective if pursued.

III. NEW APPROACHES

We desperately need a new approach and I believe we can find it by examining the debate we have had about online child protectio over the past 15 years.[8] Since the dawn of the commercial Internet in the early 1990s, online safety and access to objectionable content has been a major public policy concern. As a result, countless regulatory schemes and technical

---

[6] "Moore's Law" refers to a statement by Intel co-founder Gordon Moore regarding the rapid pace of semiconductor technology. Moore stated, "The number of transistors and resistors on a chip doubles every 18 months." *Definition of Moore's Law*, PC MAGAZINE ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/47229/moore-s-law, (last visited June 29, 2013).

[7] Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, GEO. MASON UNIV. L. REV. (*forthcoming*, Summer 2013).

[8] *See generally* ADAM THIERER, PROGRESS & FREEDOM FOUND., PARENTAL CONTROLS & ONLINE CHILD PROTECTION: A SURVEY OF TOOLS & METHODS (Version 4.0) (2009), http://www.pff.org/parentalcontrols.

solutions have been proposed. But those efforts were largely abandoned over time as policymakers and online safety advocates came to realize that legal hurdles and practical realities meant a new approach to dealing with access to objectionable online content was needed.

Between 2000 and 2010, six major online safety task forces or blue ribbon commissions were formed to study these concerns and consider what should be done to address them, including legal and technical solutions. Three of these task forces were convened by the United States federal government and issued reports in 2000,[9] 2002[10] and 2010.[11] Another was commissioned by the British government in 2007 and issued in a major report in March 2008.[12] Finally, two additional task forces were formed in the U.S. in 2008 and concluded their work, respectively, in December of 2008[13] and July of 2009.[14]

Altogether, these six task forces heard from hundreds of experts and produced thousands of pages of testimony and reports on a wide variety of issues related to online safety. While each of these task forces had different origins and unique membership, what is striking about them is the general unanimity of their conclusions. In particular, the overwhelming consensus of these expert commissions was that there is no single "silver-bullet" technological solution or regulatory quick-fix to concerns about access to objectionable online content. Many of the task forces cited the rapid pace of change in the digital world when drawing that conclusion.

Instead, each of the task forces concluded that education should be the primary solution to most online child safety concerns. Specifically, these task forces consistently stressed the importance of media literacy, awareness-building efforts, public service announcements, targeted intervention techniques, and better mentoring and parenting strategies.

As part of these efforts to strive for "digital citizenship," experts stressed how vital it is to teach both children and adults smarter online hygiene (sensible personal data use) and "Netiquette" (proper behavior toward others), which can further both online safety and digital privacy goals.[15] More generally, as part of these digital literacy and citizenship efforts, we must do more

---

[9] COPA Commission, REPORT TO CONGRESS (Oct. 20, 2000), www.copacommission.org.

[10] Computer Science and Telecommunications Board, National Research Council, YOUTH, PORNOGRAPHY AND THE INTERNET (2002), http://www.nap.edu/openbook.php?isbn=0309082749.

[11] Online Safety and Technology Working Group, YOUTH SAFETY ON A LIVING INTERNET (June 4, 2010), http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf.

[12] Byron Review, SAFER CHILDREN IN A DIGITAL WORLD: THE REPORT OF THE BYRON REVIEW (Mar. 27, 2008), http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.

[13] 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 (Dec. 31, 2008), http://cyber.law.harvard.edu/pubrelease/isttf.

[14] PointSmart, ClickSafe, TASK FORCE RECOMMENDATIONS FOR BEST PRACTICES FOR CHILD ONLINE SAFETY (July 2009), http://www.pointsmartreport.org.

[15] Common Sense Media, Digital Literacy and Citizenship in the 21st Century: Educating, Empowering, and Protecting America's Kids 1 (2009), www.commonsensemedia.org/sites/default/files/CSM_digital_policy.pdf; Anne Collier, *From users to citizens: How to make digital citizenship relevant*, NET FAMILY NEWS, (Nov. 16, 2009, 2:23 PM), www.netfamilynews.org/2009/11/
from-users-to-citizen-how-to-make.html; Nancy Willard, *Comprehensive Layered Approach to Address Digital*

to explain the potential perils of over-sharing information about ourselves and others while simultaneously encouraging consumers to delete unnecessary online information occasionally and cover their digital footprints in other ways.

These education and literacy efforts are also important because they help us adapt to new technological changes by employing a variety of coping mechanisms or new social norms. These efforts and lessons should start at a young age and continue on well into adulthood through other means, such as awareness campaigns and public service announcements.

IV. THE ROLE OF PRIVACY PROFESSIONALS & THE DIGITAL DESIGNERS OF THE FUTURE

Finally, education and digital citizenship efforts are essential not only because they teach consumers how to navigate new information environments and challenges but also because they can guide the actions of current or future *producers* of new digital technologies.

We've spent a great deal of time in recent years encouraging digital innovators to institute "privacy by design" when contemplating their new products. But *real* privacy by design should be a state of mind and a continuous habit of action that influences how designers think about the impact of their products and services before and after creation.

The role of privacy professionals is equally vital. As Deirdre Mulligan and Kenneth Bamberger have noted, increasingly, it is what happens "on the ground"—the day-to-day management of privacy decisions through the interaction of privacy professionals, engineers, outside experts and regular users—that is really important. They stress how "governing privacy through flexible principles" is the new norm.[16]

We should continue to consider how we might achieve "privacy by design" before new services are rolled out, but the reality is that "privacy on the fly" through those "flexible principle" may become even more essential.

V. CONCLUSION

So, while law and regulation will likely continue to be pursued and, at the margin, may be able to help with egregious privacy and security harms, the reality is that, outside narrow exceptions such as health and financial information, the case for regulatory control becomes harder to justify as the costs will almost certainly exceed the benefits.

That's why it is so essential to have a good backup plan for when control is impossible or simply too costly. Education is the strategy with the most lasting impact. Education and digital literacy provide skills and wisdom that can last a lifetime, enhancing resiliency. Specifically, education can help teach both kids and adults how to behave in—or respond to—a wide variety of situations. Rethinking privacy from the bottom-up and engaging citizens in this way will ultimately serve us better than the top-down approaches being pursued today.

Citizenship and Youth Risk Online, CTR. FOR SAFE & RESPONSIBLE INTERNET USE (2008), *available at* http://digitalcitizen.wikispaces.com/file/view/yrocomprehensiveapproach.pdf.

[16] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).