Enhancing Child Safety and 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

Edited by

John Palfrey

danah boyd

Dena Sacco

Carolina Academic Press

Durham, North Carolina

Copyright © 2010
President and Fellows of Harvard College
All Rights Reserved

ISBN: 978-1-59460-776-9
LCCN: 2009941733

Carolina Academic Press
700 Kent Street
Durham, North Carolina 27701
Telephone (919) 489-7486
Fax (919) 493-5668
www.cap-press.com

Printed in the United States of America

Enhancing Child Safety and 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

Directed by the Berkman Center for Internet & Society at Harvard University
Chair: Professor John Palfrey
Co-Director: Dena T. Sacco
Co-Director and Chair, Research Advisory Board: danah boyd
Chair, Technology Advisory Board: Laura DeBonis
Coordinator: Jessica Tatlock

Task Force Members:

AOL/Bebo
Aristotle
AT&T
Berkman Center for Internet & Society at Harvard University (Directors)
Center for Democracy & Technology
Comcast
Community Connect Inc.
ConnectSafely.org
Enough Is Enough
Facebook
Family Online Safety Institute
Google Inc.
IAC
ikeepsafe
IDology, Inc.
Institute for Policy Innovation
Linden Lab
Loopt
Microsoft Corp
MTV Networks/Viacom.
MySpace and Fox Interactive Media
National Center for Missing & Exploited Children
The Progress & Freedom Foundation
Sentinel Tech Holding Corp.
Symantec
Verizon Communications, Inc.
Xanga
Yahoo!, Inc.
Wiredsafety.org

Contents

A Reader's Guide to Enhancing Child Safety xiii
Acknowledgments xix

Cover Letter 3

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 5
Executive Summary 5
I. Introduction 9
II. Methodology 11
A. Development of a Project Plan 11
B. Establishment of Advisory Boards 12
C. Task Force Meetings and Discussions 13
D. Quarterly and Final Reports 14
E. Policy of Open Access to Information 14
III. Summary Report from the Research Advisory Board 15
A. Background 15
B. Background to the Literature Review 16
C. Summary of Literature Review 18
1. Sexual Solicitation and Internet-Initiated Offline Encounters 19
2. Online Harassment and Cyberbullying 21
3. Exposure to Problematic Content 23
4. Different Risks 24
5. Future Research 26
IV. Summary Report from the Technology Advisory Board 26
V. Overview of Online Safety Efforts Made by Social Network Sites 29
VI. Analysis 32
A. Background 32
B. How the Technologies Address Risks Identified by the RAB 34
1. Sexual Solicitation and Internet-Initiated Offline Encounters 34

2. Online Harassment and Cyberbullying 39
3. Exposure to Problematic Content 40
C. A Note on Technologies Not Submitted to the Task Force 41
VII. Recommendations 42
A. Recommendations for the Internet Community 43
B. Recommendations Regarding the Expenditure of Resources 44
C. Recommendations for Parents and Caregivers 45
VIII. Conclusion 46

Appendix A · Joint Statement on Key Principles of Social Networking Safety
North Carolina AG Cooper Announces Landmark Agreement to Protect Kids Online 49
Joint Statement on Key Principles of Social Networking Sites Safety 51
Appendix A: Design and Functionality Changes 58
Appendix B: Design and Functionality Initiatives 61

Appendix B · Task Force Project Plan
Internet Safety Technical Task Force Project Plan 65
I. Background 65
II. Scope 65
III. Structure 67
IV. Systems 68
A. Reports 68
B. Meetings 68
C. Website and Online Workspace 69
V. Communications 69
VI. Intellectual Property 70

Appendix C · Research Advisory Board Literature Review
Online Threats to Youth: Solicitation, Harassment, and Problematic Content 73
1. Introduction 75
1.1 Creation 76
1.2 Scope 76
1.3 A Note on Methodology and Interpretation 78
1.4 Youths Facing Risks 81
1.5 Youth Perpetrators 82
1.6 Adult Perpetrators 82
2. Sexual Solicitation and Internet-Initiated Offline Encounters 83
2.1 Solicitation 84

2.2 Offline Contact 86
2.3 Victims 88
2.4 Perpetrators 89
3. Online Harassment and Cyberbullying 90
3.1 Victims 91
3.2 Perpetrators 93
3.3 Overlaps in Victimization and Perpetration 94
3.4 Offline Connections 95
3.5 Connections to Solicitation 96
4. Exposure to Problematic Content 96
4.1 Pornography 97
4.2 Violent Content 99
4.3 Other Problematic Content 99
5. Child Pornography 101
5.1 Child Pornography Offenders 102
5.2 Child Pornography and Sexual Solicitation 102
6. Risk Factors 104
6.1 Online Contact with Strangers 104
6.2 Posting of Personal Information 105
6.3 Sharing of Passwords 107
6.4 Depression, Abuse, and Substances 107
6.5 Poor Home Environment 108
6.6 Intensity of Online Participation 109
7. Genres of Social Media 110
7.1 Chatrooms and Instant Messaging 110
7.2 Blogging 111
7.3 Social Network Sites 112
7.4 Multiplayer Online Games and Environments 113
7.5 Multimedia Communications 114
8. Future Research 115
8.1 Minor-Minor Solicitation and Sexual Relations 116
8.2 Problematic Youth-Generated Content 116
8.3 Impact on Less-Visible Groups 117
8.4 Interplay Between Socioeconomic Class and Risk Factors 118
8.5 Photographs and Video in Online Harassment and Solicitation 118
8.6 Intersection of Different Mobile and Internet-based Technologies 119
8.7 Online Activities of Registered Sex Offenders 119
8.8 Continued Research, New Methodologies, and Conceptual Clarity 119

9. Understanding Research Methodologies (Appendix A) 120
9.1 Samplings 121
9.2 Response Rates 122
9.3 Prevalence 123
9.4 Sources of Bias 123
9.5 Constructs 124
9.6 Question Wording 124
9.7 Causality and Complexity 125
9.8 Qualitative Methodologies 125
9.9 Funding Sources 126
9.10 Underreporting of Incidents 126
10. References 126

Appendix D · Technology Advisory Board Report
Executive Summary 149
Introduction 150
Process and Methodology 151
Technology Advisory Board Members and Observers 151
Soliciting, Collecting, and Evaluating Submissions 152
Soliciting 152
Collecting 152
Evaluating 153
Analysis 154
Age Verification/Identity Authentication 155
Category Description 155
Commentary 156
Conclusion 157
Filtering/Monitoring/Auditing 157
Category Description 157
Commentary 158
Conclusion 159
Text Analysis 160
Category Description 160
Commentary 160
Conclusion 161
Biometrics 162
Category Description 162
Commentary 162
Conclusion 163
Other: Individual Identification 163

Category Description 163
Commentary 163
Conclusion 164
Case Study: icouldbe.org 164
Conclusions 165
Exhibits to Appendix D
1. TAB Member and Observer Bios 171
2. Submission Template 183
Internet Safety Technical Task ForceTechnology Submission Template 183
3. Intellectual Property Policy 189
Intellectual Property Policy for the Internet Safety Technical Task Force 189
No Confidentiality of Contributions 189
Copyrighted Materials 189
Patents 190
Trade Secrets 190
Intellectual Property Created by the Task Force 190
4. Alphabetical List of Technology Submissions 193

Appendix E · Submissions from Social Network Sites
Internet Technical Safety Taskforce — Request for Input Bebo and AOL 197
Statement to the Technical Advisory Board from Community Connect, Inc. 209
Facebook 215
Google/orkut 222
Loopt, Inc. 225
Viacom/MTV Networks 231
Fox Interactive Media/MySpace 234
Yahoo! 262

Appendix F · Statements from Members of the Task Force
AOL and Bebo's Statement Regarding the Internet Safety Technical Task Force's Final Report 271
Aristotle International 273
AT&T 275
Center for Democracy & Technology 277
Comcast 279
ConnectSafely 281

Enough Is Enough 283
Family Online Safety Institute 285
IDology inc. 286
iKeepSafe 288
The Progress & Freedom Foundation 290
Facebook 292
Linden Lab 293
Microsoft 295
MySpace.com 297
Institute for Policy Innovation 299
Sentinel 301
Symantec 302
Verizon 304
WiredSafety 306
WiredSaftey 306
Yahoo! 308

A Reader's Guide to Enhancing Child Safety

John Palfrey*
July, 2009

Digital environments are becoming the most important public spaces of the 21st century. These digital spaces are where many young people—and many older people—spend enormous amounts of time. These spaces are today akin to public parks and to schoolyards. These are environments where many social lives take place, where nearly all information can be found and republished, and where important functions like learning and participation in civic life occur. With every passing year, more and more of life is taking place in ways that are mediated by digital technologies—by people young and old.

Just as there are great things about life online, so, too, are there risks associated with it. But many young people do not distinguish between life online and life offline—it is just life. All of us—teachers, parents, law enforcement officers, politicians—need to heed this lesson that our children are teaching us. And as we seek to protect our kids in this hybrid world, we need to be sure not to violate Constitutional protections for speech and privacy. Nowhere in the world is this balance being struck well today; nowhere in the world do we yet see ample, balanced protection of safety and of civil liberties online. To protect our children's safety in this new, hybrid world while maintaining civil liberties and helping children to learn along the way is a noble and important goal.

---

* John Palfrey is Henry N. Ess Professor of Law and Vice Dean for Library and Information Resources at Harvard Law School. He is also a faculty director of the Berkman Center for Internet and Society at Harvard University. This overview draws upon the research for a co-authored book, *Born Digital: Understanding the First Generation of Digital Natives* (2008) with Urs Gasser, as well as many conversations with danah boyd, Dena Sacco, Internet Safety Technical Task Force Members, and others about Internet safety issues and children.

As we seek to understand emerging problems online—such as the myriad threats to the safety of our children—and to anticipate a future that seems to be arriving faster and faster, we have to understand our children and our grandchildren and how they are different. There are profound differences in terms of how many of them are leading their lives as compared to some of us who are their parents and grandparents. Take identity, for instance, which is one of the attributes of how young people often use technologies and relate to the world differently than those who came before. Young people shape their identities by what they wear and who their friends are, just as they always have. But they also shape their identities through profiles in online social networks, through the personalities that they develop through instant messaging and texting and Twittering, and through blogs and LiveJournals and their avatars in games and virtual worlds. Identity is shaped in this converged space of online and offline. And as they spend all this time online, so too do they run risks in online spaces, just as they do offline.

Young people interact with both friends and strangers online. Their understanding of the word "friend," in fact, is changing. They may consider someone they have never met, other than in an online chatroom, to be a close friend. They spend a great deal of time online with their friends—as they play games together, plan something that they might do later, share music and movies, or just chat—and chat, and chat (or: text, and text, and text). Sometimes friends do terrible things to one other. Sometimes, they are mean to one another in ways that they would not be in real space, when face to face; after all, it's much easier to leave a hard conversation online than it is offline. Other times, these are just the spaces where growing up takes place, with good and bad.

It's no surprise that there should be problems that arise online. These are places where kids are spending a great deal of time, where they are playing and learning and just hanging out. They leave a lot of information about themselves around these places. That information is sometimes accessible to those whom they do not know. And they are often experimenting with who they are and how they want to interact with other people.

It is against this backdrop that we undertook the work of the Internet Safety Technical Task Force. The Attorneys General who commissioned the work of this Task Force asked us to consider, in particular, whether technologies could help make kids safer online. They told us that their investigators are experiencing a disturbing trend: more and more, they were finding that a young person online, especially in social networks, was likely to encounter a sexual predator. Many parents have told us of their similar fears. As Task Force members, we have taken these concerns to heart.

The primary thing that joined each of the Task Force members to one another was our shared sense of purpose: as parents, teachers, and professionals, we care about making the world safer for all children. We came from a very broad range of perspectives, political and otherwise. Members represented 29 different organizations, drawn from some of the largest social networks from around the world, prominent technology companies, non-profit advocacy groups, and academia. We did not agree on every topic by any means, but we did share a sense of common purpose.

Readers of this book will not be surprised that there are complicated politics involved in this topic. The way that this report was compiled may enable the careful reader to understand some of these political tensions. The primary report was drafted by the team members from the Berkman Center for Internet & Society at Harvard University which chaired the Task Force. We as the Berkman Center team took seriously all comments that we received from Task Force members and the public. It was not possible to incorporate all these proposed changes, but we sought to describe as clearly as we could the areas of consensus.

Some of the most controversial aspects in this area are revealed in the pages of this book. After the main report had been finalized, we invited each Task Force member to contribute a one-page response to highlight support or areas of disagreement with the findings of the Task Force at large. These one-page responses offer a glimpse of where broader disagreement continues to divide those who work on these issues. The responses of some Attorneys General to the release of this report, in the mainstream press and through public statements, likewise reveal these fault lines.

The first area of disagreement is about the relative degree of risk of sexual predation as compared to other safety concerns. Academic researchers made plain their findings, more or less universally, that the risk of sexual predation is real and worrisome, but that the online environment has not made kids more at risk that they have been in the past. Others disagree vehemently with these findings, contending that the advent of social networks and other online services has given rise to new and severe risks to kids. No one disagrees that there is a risk of sexual predation online. The issue that is not settled is what the exact risk is, to whom it is most acute, and how to address it. The one-page submissions by AT&T, FOSI and Connect Safely, for instance, point to various aspects of how to approach this issue of research and its implications.

Another area of dispute centers on how to think about the growth of online bullying alongside the continuing risk of sexual predation. Researchers presented their findings that bullying online is a growing concern for kids, parents and teachers. Young people do more harm to one another—peer to peer—

than adults do to them. This is a very important point. We need to think in terms of how "friends" act toward one another just as much as we think about how strangers might reach our children. The problems that can occur are terrible here, too, and they are increasingly being reported as common. The psychological harm done to young people by their peers online can be devastating. But others disagree, arguing that an emphasis in the safety debate on bullying does not make sense. The biggest fear (and corresponding greatest harm), they argue, is predation, not bullying, and any shift in emphasis away from online predation is to be avoided.

The debate about youth and access to harmful online content, too, continues to rage, as it has since the advent of widespread use of the Internet. Young people can access much more content—information and imagery and just about any kind of media one can imagine—online than they ever could before. Sometimes, they are accessing information that helps them to learn about their world—to expand their horizons, to help them to think more critically, to give them a way into a public discourse where they can contribute their own voices, to find things that could never be housed in a single library. For some kids, learning on their own online is a big part of their growing up, and it's great. But it's also easy to access pornography and, with some effort, young people may access child pornography. This is not entirely new: of course, young people have sought out pornography in the past, or been presented with it by a friend or an older cousin or sibling. The difference today is its easy access online, from anywhere at any time. The debate between those who emphasize the importance of public morals and those who emphasize the right to free expression has not abated. Consider the one-page submission by Enough is Enough for consideration of these issues.

The question of how to respond to each of these threats to safety—predation, bullying, and access to harmful and unwanted content—gives rise to a further series of differences between perspectives. Some argue that the use of technologies, such as online identity authentication and age verification in particular, ought to be widespread, if not mandatory, and that young people will be much safer if we were to do so. A less-strong version of this argument draws upon the notion that the technologies are sufficiently malleable that they offer enormous promise for protecting kids from a range of risks. Others argue that, when faced with these problems, we too quickly turn to the idea that technology can solve these problems that technology has wrought—and that this is a mistake. The extensive use of strong authentication and age verification technologies will not solve the problem, they argue, and will bring with them negative externalities, including risks to innovation, free expression and privacy. For a sense of the different viewpoints on this topic, consider in particular the articulate submissions of Aristotle and IDology on the one hand

and those of the Center for Democracy and Technology, the Institute for Policy Innovation, and the Progress and Freedom Foundation on the other.

Finally, there is extensive debate about whether we ought to mandate any particular technology as a solution to child safety. Legislation has been filed at the state and federal levels in the United States and in other countries in recent years that would require the use of particular technologies in the interest of protecting children. The Task Force members all agreed that such a mandate does not make sense at this time. The AOL-Bebo submission, for instance, makes the case for this perspective. That said, this debate is far from settled; despite the clear statement of our Task Force, legislators continue to propose such legislation in a variety of contexts.

These problems of online life are neither easily nor quickly solved. All serious observers agree on this score. These problems are so complex, and changing so quickly, as to defy easy, one-off answers. We know that we cannot expect that a single, static technological approach will keep our kids from danger. We can't just "pass a law" against these things and imagine that we can enforce that law in the way we've always enforced the law and hope that all will be well. The problems don't lend themselves to such easy answers. Of course, we can and should pass laws against these crimes and enforce them. It is crucial that we have the laws, policies, and legal infrastructure sufficient to enable enforcement—including in these new environments.

More important than any law or any technology, though, is our commitment to a robust public dialogue about child safety. No one single person has all the answers. This Task Force report is meant as a contribution to this ongoing public dialogue. The Obama Administration is leading a similar effort through the National Telecommunications and Information Administration in 2009, established by the "Protecting Children in the 21st Century Act," which will push work and discussion on this topic further forward. Many of the members of our Task Force are serving on this NTIA working group.

It is imperative that we listen to a range of credible perspectives on this politicized topic. We need to commit ourselves to basing our decision-making on the facts, not on mere intuition, political beliefs, or narrow financial interests. In turn, we need broad public education about the best practices—for young people, for parents, for teachers, for law enforcement, and for technology companies—about how to keep kids safe. We need to devote ourselves to getting skills and tools into the right hands—especially in the hands of our kids and their friends. And we have no choice but to cooperate in meeting these challenges together, rather than letting our different views separate us. The stakes are simply too high to do otherwise.

Acknowledgments

The co-editors wish to acknowledge all those who were involved in the Internet Safety Technical Task Force process for their contributions to this volume. The 49 Attorneys General who entered into the joint statement with MySpace and Facebook deserve thanks for kicking off this process. Each of the members of the Task Force, and the companies and organizations that supported them, deserve special thanks. The members of the Technical Advisory Board, ably chaired by Laura DeBonis, and the Research Advisory Board, equally well-chaired by danah boyd and ably supported by Andrew Schrock, have earned our lasting gratitude. We also thank the Berkman Center Cyberlaw Clinic and its students, especially its director, Professor Phil Malone. The Berkman Center staff has been extraordinary: Jessica Tatlock, the Task Force coordinator; Seth Young, communications director; Lexie Koss, communications assistant; Colin Maclay, managing director; Catherine Bracy, administrative director; Urs Gasser, the new executive director; and all those who pitched in throughout the process. We thank Dana Gershengorn, who gave the Task Force great insight based on her experience prosecuting child exploitation cases. We thank, too, the members of the public who participated in myriad ways throughout this process in such a constructive spirit.

Task Force Members

AOL
Aristotle
AT&T
Bebo
Berkman Center for Internet & Society at Harvard University (Directors)
Center for Democracy & Technology
Comcast
Community Connect Inc.

ConnectSafely.org
Enough Is Enough
Facebook
Family Online Safety Institute
Google Inc.
IAC
ikeepsafe
IDology, Inc.
Institute for Policy Innovation
Linden Lab
Loopt
Microsoft Corp.
MTV Networks/Viacom
MySpace and Fox Interactive Media
National Center for Missing & Exploited Children
The Progress & Freedom Foundation
Sentinel Tech Holding Corp.Symantec
Verizon Communications, Inc.
Xanga
Yahoo!, Inc.
Wiredsafety.org

Technical Advisory Board

TAB Members
Ben Adida, Harvard Medical School, Harvard University
Scott Bradner, Harvard University
Laura DeBonis, Berkman Center, Harvard University
Hany Farid, Dartmouth
Lee Hollaar, University of Utah
Todd Inskeep, Bank of America
Brian Levine, University of Massachusetts Amherst
Adi Mcabian, Twistbox
RL Morgan, University of Washington
Lam Nguyen, Stroz Friedberg, LLC
Jeff Schiller, MIT
Danny Weitzner, MIT

TAB Observers
Rachna Dhamija, Usable Security Systems
Evie Kintzer, WGBH
Al Marcella, Webster University
John Morris, Center for Democracy and Technology
Teresa Piliouras, Polytechnic University
Greg Rattray, Delta-Risk
Jeff Schmidt, Consultant
John Shehan, National Center for Missing and Exploited Children

Research Advisory Board

RAB Members
danah boyd (Chair), University of California-Berkeley
David Finkelhor, University of New Hampshire Crimes Against Children Research Center
Sameer Hinduja, Florida Atlantic University
Amanda Lenhart, Pew Internet and American Life Project
Kimberly Mitchell, University of New Hampshire Crimes Against Children Research Center
Justin Patchin, University of Wisconsin-Eau Claire
Larry Rosen, California State University at Dominguez Hills
Janis Wolak, University of New Hampshire Crimes Against Children Research Center
Michele Ybarra, Internet Solutions for Kids

Additional Research Presenter
Sam McQuade, Rochester Institute of Technology

Berkman Center Cyberlaw Clinic Students

Merritt Baer, Harvard Law School
Jim Ernstmeyer, Boston University Law School
Meagan Rasch-Chabot, Harvard Law School
Kelly Tallon, Harvard Law School