

RANDY L. DRYER (0924)
MICHAEL P. PETROGEORGE (8870)
Parsons Behle & Latimer
One Utah Center
201 South Main Street, Suite 1800
Salt Lake City, Utah 84111
Telephone: (801) 532-1234
Facsimile: (801) 536-6111

*Attorneys for Amici Curiae American Advertising
Federation, American Association of Advertising
Agencies, Association of National Advertisers, Inc.,
Email Sender and Provider Coalition, Electronic
Frontier Foundation, Center for Democracy &
Technology*

Of Counsel:

LEE TIEN
Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco, California 94103

Counsel for Electronic Frontier Foundation

JOHN MORRIS
Center for Democracy and Technology
1634 Eye Street, NW, Suite 1100
Washington D.C. 2006

*Counsel for Center for Democracy &
Technology*

**IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION**

FREE SPEECH COALITION,

Plaintiff,

vs.

MARK SHURTLEFF, *et al*,

Defendants.

Case No. 2:05-cv-00949 DAK

**BRIEF OF AMICI CURIAE IN SUPPORT
OF PLAINTIFF FREE SPEECH
COALITION'S MOTION FOR
PRELIMINARY INJUNCTION**

Judge Dale A. Kimball

The American Advertising Federation ("AAF"), the American Association of Advertising Agencies ("AAAA"), the Association of National Advertisers, Inc. ("ANA"), the Email Sender and Provider Coalition f/k/a Email Service Provider Coalition ("ESPC"), the Electronic Frontier Foundation ("EFF") and the Center for Democracy & Technology ("CDT") (collectively, the "Amici"), by and through undersigned counsel, submit this brief in support of plaintiff Free Speech Coalition's ("FSC") Motion for Preliminary Injunction.

TABLE OF CONTENTS

| | Page |
|---|----------|
| INTRODUCTION..... | 1 |
| RELEVANT FACTUAL INFORMATION UNDERLYING THE CONSTITUTIONAL INFIRMITIES OF THE CPR ACT | 4 |
| I. EMAIL MARKETING VIA THE INTERNET IS AN ALMOST BILLION DOLLAR INDUSTRY AND IS GROWING RAPIDLY | 4 |
| A. The Internet..... | 4 |
| B. Email | 6 |
| C. SPAM..... | 8 |
| II. THE CPR ACT EXPRESSLY REGULATES COMMERCIAL EMAIL COMMUNICATIONS AND DIRECTLY IMPACTS INTERSTATE COMMERCE..... | 9 |
| III. EMAIL IS AN INHERENTLY INTERSTATE FORM OF COMMUNICATION..... | 10 |
| IV. THE REGULATORY AND PENAL SCHEME OF THE CPR ACT IS PREDICATED ON UNWORKABLE DISTINCTIONS WHICH IGNORE THE REALITIES OF EMAIL COMMUNICATIONS | 12 |
| A. The Utah vs. Non-Utah Distinction | 13 |
| B. The Adult vs. Minor Distinction..... | 14 |
| V. THE CPR ACT WILL IMPOSE SIGNIFICANT BURDENS AND FINANCIAL COSTS ON LEGITIMATE EMAIL MARKETERS AND LEGITIMATE BUSINESSES FROM AROUND THE COUNTRY WHO ADVERTISE OTHERWISE LAWFUL PRODUCTS AND SERVICES TO ADULTS IN UTAH AND TO PERSONS IN OTHER STATES..... | 15 |
| VI. THE CPR ACT CONTAINS VAGUE AND UNDEFINED TERMS PREVENTING LEGITIMATE BUSINESSES FROM KNOWING WHAT IS PROHIBITED AND FROM EFFECTIVELY COMPLYING WITH ITS PROVISIONS | 19 |
| A. The CPR Act Fails to Define “Primary Purpose” | 21 |
| B. The CPR Act Fails to Define the Terms “Advertising” and “Promoting” | 21 |
| C. The CPR Act Fails to Define the Term “Minor” | 22 |
| D. The CPR Act Fails to Clearly Articulate What Activity a Minor is “Prohibited By Law From Purchasing” | 23 |
| E. The CPR Act Fails to Define What it Means For a Prohibited Communication to be “Sent” | 23 |

TABLE OF CONTENTS (continued)

| | Page |
|---|-------------|
| VII. THE CPR ACT REGULATES LAWFUL SPEECH BETWEEN ADULTS | 25 |
| VIII. THE CPR ACT WILL NOT ACCOMPLISH ITS PURPOSE OF PROTECTING UTAH’S MINORS | 27 |
| IX. THE FTC HAS EXTENSIVELY STUDIED CENTRALIZED REGISTRY SYSTEMS SUCH AS THAT CREATED BY THE UTAH CPR ACT AND HAS REJECTED THEM AS BEING AN UNWORKABLE MEANS OF PROTECTING MINORS FROM UNWANTED MATERIAL | 28 |
| X. THE CPR ACT IS LIKELY TO DO MORE HARM THAN GOOD | 30 |
| A. The Registry May Be the Target of Internal Subversion..... | 31 |
| B. The Registry System May Be Abused by Spammers to Acquire Valid Email Addresses, Particularly Those Belonging to or Accessible by Utah’s Minors | 32 |
| C. Unspam’s Security Measures Will be Largely Ineffective | 33 |
| D. The State of Utah Specifically Recognizes the Security Risks Inherent in the Registry System | 35 |
| XI. THERE ARE OTHER LESS RESTRICTIVE ALTERNATIVES TO PROTECT UTAH’S MINORS FROM UNWANTED EMAIL CONTENT..... | 36 |
| LEGAL ARGUMENT | 38 |
| I. THE CPR ACT IS PREEMPTED BY SECTION 7707(B) OF THE FEDERAL CAN-SPAM ACT | 38 |
| II. THE CPR ACT VIOLATES THE COMMERCE CLAUSE OF THE UNITED STATES CONSTITUTION..... | 41 |
| A. The CPR Act is Unconstitutional Per Se Because it Regulates Email, a Form of Interstate Communication and Commerce Demanding Cohesive National Treatment | 42 |
| B. The CPR Act Regulates Conduct Occurring Wholly Outside of Utah..... | 43 |
| C. The CPR Act Imposes Substantial Burdens on Interstate Commerce That are Clearly Excessive When Compared Against the Minimal Local Benefits | 46 |
| D. The CPR Act Discriminates Against Out-Of-State Businesses..... | 49 |
| III. THE CPR ACT IS IMPERMISSIBLY VAGUE AND THEREFORE VIOLATES THE DUE PROCESS CLAUSE OF THE FOURTEENTH AMENDMENT..... | 50 |
| IV. THE CPR ACT UNDULY CHILLS THE FIRST AMENDMENT RIGHTS OF LEGITIMATE EMAIL MARKETERS | 51 |

TABLE OF CONTENTS
(continued)

| | Page |
|---|-------------|
| A. The CPR Act Does Not Directly or Materially Advance the State’s Interest in Protecting Minors | 51 |
| B. The CPR Act is Not Sufficiently Tailored to Meet the State’s Interest in Protecting Minors..... | 53 |
| CONCLUSION | 55 |

TABLE OF AUTHORITIES

FEDERAL CASES

United States Supreme Court Cases

| | |
|---|-------|
| <i>Bolger v. Youngs Drug Products Corp.</i> , 463 U.S. 60 (1983) | 54 |
| <i>Central Hudson Gas & Electric Corp. v. Public Serv. Commission</i> , 447 U.S. 557 (1980) | 51 |
| <i>Cincinnati v. Discovery Network, Inc.</i> , 507 U.S. 410 (1993) | 53 |
| <i>Cipollone v. Liggett Group, Inc.</i> , 505 U.S. 504 (1992) | 38 |
| <i>Grayned v. City of Rockford</i> , 408 U.S. 104 (1972)..... | 50 |
| <i>Healy v. Beer Institute</i> , 491 U.S. 324 (1989)..... | 43 |
| <i>Hill v. Colorado</i> , 530 U.S. 703 | 50 |
| <i>Lorillard Tobacco Co. v. Reilly</i> , 533 U.S. 525 (2001)..... | 53 |
| <i>Reno v. ACLU</i> , 521 U.S. 844 (1997)..... | 5, 54 |
| <i>Silkwood v. Kerr-McGee Corp.</i> , 646 U.S. 238 (1984)..... | 38 |
| <i>Thompson v. Western States Medical Center</i> , 535 U.S. 357 (2002)..... | 54-55 |

Tenth Circuit Court of Appeals Cases

| | |
|---|---------------------|
| <i>ACLU v. Johnson</i> , 194 F.3d 1149 (10 th Cir. 1999) | 4, 10, 41-43, 45-49 |
| <i>Faustin v. City & County of Denver</i> , 423 F.3d 1192 (10 th Cir. 2005) | 50 |
| <i>Revo v. Disciplinary Board of the Superior Court for the State of New Mexico</i> , 106 F.3d 929, 932-33 (10 th Cir. 1993) | 51 |
| <i>Utah Licensed Beverage Association v. Leavitt</i> , 256 F.3d 1061 (10 th Cir. 2001)..... | 51, 53 |
| <i>U.S. West, Inc. v. F.C.C.</i> , 182 F.3d 1224 (10 th Cir. 1999) | 51, 55 |

Other Federal Cases

| | |
|---|-------|
| <i>American Booksellers Foundation v. Dean</i> , 342 F.3d 96 (2 nd Cir. 2003)..... | 5, 54 |
|---|-------|

| | |
|---|--------------|
| <i>Pioneer Military Lending, Inc. v. Manning</i> , 2 F.3d 280 (8 th Cir. 1993) | 48 |
| <i>American Library Association v. Pataki</i> , 969 F.Supp. 160 (S.D.N.Y. 1997) | 5, 10, 41-49 |

FEDERAL STATUTES

| | |
|--|---------------|
| Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7701 <i>et seq.</i> | 3 |
| 15 U.S.C. § 7701(11) | 18, 39 |
| 15 U.S.C. § 7707(b) | 18, 38-39, 41 |

STATE STATUTES

| | |
|--|-----------------------------|
| Utah’s Unsolicited Commercial and Sexually Explicit Email Act, Utah Code Ann. §§ 13-36-101 <i>et seq.</i> (repealed 2004) | 12 |
| Utah Child Protection Registry Act, Utah Code Ann. § 13-39-101 <i>et seq.</i> | 2 |
| Utah Code Ann. § 13-39-101 | 9 |
| Utah Code Ann. § 13-39-102 | 39 |
| Utah Code Ann. § 13-39-201 | 2, 9-10, 25, 31, 36 |
| Utah Code Ann. § 13-39-202 | 2, 9, 19-21, 23, 26, 39, 49 |
| Utah Code Ann. § 13-39-301 | 2, 32, 39 |
| Utah Code Ann. § 13-39-302 | 2, 12 |
| Utah Code Ann. § 15-2-1 | 22 |
| Utah Code Ann. § 76-6-703 | 40 |
| Utah Code Ann. § 76-6-703 | 40 |
| Utah Code Ann. § 76-7-321 | 22 |
| Utah Code Ann. § 76-10-104 | 22 |
| Utah Code Ann. § 76-10-1201 | 2 |

| | |
|-----------------------------------|----|
| Utah Code Ann. § 76-10-2201 | 22 |
|-----------------------------------|----|

INDEX OF EXHIBITS

| | |
|-----------|--|
| Exhibit A | February 27, 2004, Senate Floor Debate on HB 165 (Utah CPR Act) |
| Exhibit B | Joe Baird, <i>New laws on the books for Utah</i> , Salt Lake Tribune, May 1, 2006 |
| Exhibit C | Merchant Direct Information |
| Exhibit D | Company X Information |
| Exhibit E | Company Y Information |
| Exhibit F | Company Z Information |
| Exhibit G | The Brewers Association Information |
| Exhibit H | Food & Wine Classic Information |
| Exhibit I | LocalWineEvents.com Information |
| Exhibit J | Telluride Wine Festival Information |
| Exhibit K | Gastronomy Information |
| Exhibit L | Park City Jazz Foundation Information |
| Exhibit M | Sonoma Valley Film Society Information |
| Exhibit N | Napa Valley Mustard Festival Information |
| Exhibit O | Las Vegas CVA Information |
| Exhibit P | Brewvies Information |
| Exhibit Q | SLC Downtown Alliance Information |
| Exhibit R | Lake Tahoe Shakespearean Festival Information |
| Exhibit S | Excerpts from June 4, 2003, <i>Report for Congress: E-Commerce Statistics: Explanation and Sources</i> , full transcript available at: www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL31293_06042003.pdf |
| Exhibit T | Excerpts from May 11, 2005, U.S. Dept. of Comm, <i>E-Stats</i> , full transcript available at: www.census.gov/eos/www/papers/2003/2003finaltext.pdf |

| | |
|------------|--|
| Exhibit U | Excerpts from March 9, 2004, Federal Trade Commission, <i>Do Not E-Mail Registry Meeting</i> (1:00 p.m.), full transcript available at: www.ftc.gov/reports/dneregistry/xscripts/dne040309pm.pdf |
| Exhibit V | Excerpts from March 10, 2004, Federal Trade Commission, <i>Do Not E-Mail Registry Meeting</i> , full transcript available at: www.ftc.gov/reports/dneregistry/xscripts/dne040310am.pdf |
| Exhibit W | February 17, 2006, U.S. Dept. of Comm., <i>U.S. Census Bureau News, Quarterly Retail Commerce E-Sales, 4th Quarter 2005</i> , www.census.gov/mrts/www/data/05Q4.html |
| Exhibit X | Excerpts from July 27, 2005, Federal Trade Commission, <i>In the Matter of: CAN-SPAM Report to Congress</i> , full transcript available at: www.ftc.gov/reports/canspam05/50727PM.pdf |
| Exhibit Y | Excerpts from March 9, 2004, Federal Trade Commission, <i>Do Not E-Mail Registry Meeting</i> (11:00 a.m.), full transcript available at: www.ftc.gov/reports/dneregistry/xscripts/dne040309am.pdf |
| Exhibit Z | Excerpts from February 11, 2004, Federal Trade Commission, <i>In the Matter of: Report to Congress Pursuant to CAN-SPAM Act</i> , full transcript available at: www.ftc.gov/reports/dneregistry/xscripts/dne040211.pdf |
| Exhibit AA | Email Marketing Pledge, www.espccoalition.org/pledge/php |
| Exhibit BB | July 8, 2005, State of Utah Dept. of Comm., <i>Policy Statement Concerning Utah Code Ann. § 13-39-202(1)</i> |
| Exhibit CC | Utah Registry website, www.utahkidsregistry.com |
| Exhibit DD | Unspam Contract |
| Exhibit EE | Excerpts from March 15, 2004, Federal Trade Commission, <i>In the Matter of: Report to Congress Pursuant to CAN-SPAM Act</i> , full transcript available at www.ftc.gov/reports/dneregistry/xscripts/dne040315pm.pdf . |
| Exhibit FF | Michigan CPR Act, M.C.L.A. 752.1061 <i>et seq.</i> |

| | |
|------------|--|
| Exhibit GG | [Proposed] Illinois CPR Act, HB 0572 |
| Exhibit HH | May 10, 2004, Dr. Aviel D. Rubin, <i>A Report to the Federal Trade Commission on Responses to their Request for Information on Establishing a National Do Not E-mail Registry</i> |
| Exhibit II | Excerpts from June 2004, Federal Trade Commission, <i>National Do Not E-Mail Registry: A Report to Congress</i> , full report available at: www.ftc.gov/reports/dneregistry/report.pdf |
| Exhibit JJ | Excerpts from December 2005, Federal Trade Commission, <i>Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress</i> , full report available at: www.ftc.gov/reports/canspam05/051220canspamrpt.pdf |
| Exhibit KK | October 25, 2006, Letter from FTC Staff to The Honorable Angelo “Skip” Saviano, State Rep., 77 th Dist., Ill. House of Reps |
| Exhibit LL | Stephen Speckman, <i>FBI May Look into Hacker Case at U</i> , Deseret Morning News, Aug. 11, 2005, www.deseretnews.com/dn/view/0,1249,600154941.00.html |
| Exhibit MM | Leslie Miller, <i>Data-theft concerns flood VA</i> , Deseret Morning News, May 27, 2005, www.deseretnews.com/dn/view/0,1249,635210845,00.html |
| Exhibit NN | Excerpts from Matt Bishop, <i>Issues for a “Do Not E-mail” List</i> , full report available at: www.ftc.gov/reports/dneregistry/experttrpts/bishop.pdf |
| Exhibit OO | Excerpts from May 2, 2004, Edward W. Felten, <i>Report on the Proposed National Do Not E-Mail Registry</i> , full report available at: www.ftc.gov/reports/dneregistry/experttrpts/felten.pdf |
| Exhibit PP | List of annual beer, wine or spirit festivals in the United States, www.localwineevents.com/festivals/festival_list.php |
| Exhibit QQ | Sample Evite Invitation |

INTRODUCTION

The Amici are trade associations and public interest organizations representing businesses, groups and individuals who rely on electronic mail ("email") as a means of transmitting constitutionally protected expression, including commercial speech regarding goods and services offered and sold in the stream of interstate commerce, to recipients both inside and outside the State of Utah.¹ A number of the Amici's individual members (a) advertise or assist others in using email to advertise products and services such as wine, beer, gambling, tobacco, firearms, tattooing, body piercing, car rentals, etc., that cannot be lawfully purchased or acquired by minors in the State of Utah, or (b) otherwise have an interest in a free and open Internet marketplace. The members of the Amici are not "spammers" as that term is commonly understood, nor are they purveyors of pornographic material. They are legitimate businesses who use the Internet in general, and email in particular, to cultivate business relationships, communicate with existing and prospective customers, receive and place customer orders, and otherwise engage in e-commerce, an ever growing segment of the United States economy. The

¹ As set forth in the Amici's application for leave to participate in this action, the AAF represents over 50,000 professionals in the advertising industry in Utah and throughout the United States, and consists of over 130 corporate members that include advertisers, agencies, and media companies comprising the nation's leading brands and corporations. The AAAA is the national trade association for advertising agencies, whose members represent nearly all the large, multi-national advertising agencies, as well as hundreds of mid-sized agencies located in 13,000 offices throughout the country. The ANA is the advertising industry's oldest trade association, representing companies offering more than 8,000 brands of goods and services. The ESPC is a cooperative group of industry leaders working to create solutions to the continued proliferation of spam, and the problems associated with the deliverability of email, and whose membership provides volume mail delivery services to an estimated 250,000 clients that represent the full breadth of the nation's marketplace. The ESPC's members account for 12% of the total email sent around the Internet today (25% if you remove spam from the equation). The CDT is a non-profit public interest and Internet policy organization representing the public's interest in an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy and individual liberty. The EFF is a donor-supported membership organization working to protect fundamental rights regardless of technology, to educate the press, policymakers, and the general public about civil liberties issues related to technology, and to act as a defender of those liberties. Among its various activities, EFF opposes what it considers to be misguided Internet legislation and regulation.

Amici and their members have a significant interest in any statute or regulation governing the use of email as a tool of commerce.

The Utah Child Protection Registry Act, U.C.A. § 13-39-101 *et seq.* (2006) (the “CPR Act”) is just such a statute, seeking to control the flow of certain advertisements and other information, particularly commercial information, via email. The CPR Act is a strict liability statute, providing criminal, administrative and civil penalties for even the most unintentional violations. *See id.* §§ 13-39-301, -302 & -303. The CPR Act creates a voluntary “Registry” of email addresses purportedly belonging to or accessible to Utah minors (*see* U.C.A. § 13-39-201 (2006)), and prohibits the sending of two types of email messages to any email address on the Registry: (a) messages which advertise a product or service that a minor cannot lawfully purchase, and (b) messages containing information deemed “harmful to minors” (i.e., pornography).² *See id.* § 13-39-202(1).

The Amici are principally concerned with the first provision of the CPR Act. Although perhaps well intended, the CPR Act has broad and sweeping implications which reach far beyond its literal language. First, it effectively prohibits and criminalizes email advertisements and newsletters which would otherwise be lawful, even as between adults, solely because they are sent in electronic form and might be accessed or viewed by a Utah minor. No other form of advertising is prohibited in this manner, and there is no rational basis to treat email advertising in a different manner from print ads, billboards, television commercials or other more traditional

² The CPR Act defines the term “harmful to minors” by reference to Utah Code Ann. § 76-10-1201. Section 76-10-1201 defines “harmful to minors” to mean “that quality of any description or representation, in whatsoever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse when it: (a) taken as a whole, appeals to the prurient interest in sex of minors; (b) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and (c) taken as a whole, does not have serious [literary, artistic, political or scientific] value for minors.”

forms of marketing, or from other forms of advertising on the Internet such as pop-up ads, banner ads or website hyperlinks. Second, the statute is an overly broad enactment that reaches far beyond the borders of Utah, and criminalizes a growing segment of the e-commerce industry. Third, the statute is vague and fails to clearly define its scope or identify for legitimate businesses the type of email communication that is and is not prohibited. Fourth, the burden and financial cost of complying with the CPR Act will be significant to mainstream businesses, and will have a significant adverse impact on commerce across the United States. Finally, the CPR Act is unlikely to accomplish its stated purpose, i.e., to protect Utah's children from pornographic and other sexually explicit content.³ While protecting children is certainly a laudable goal, the CPR Act may actually expose Utah's minors to more harmful and offensive content.

The Amici agree with the FSC that Congress has already preempted the CPR Act through the 2003 Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7701 *et seq.* ("CAN-SPAM"), that the CPR Act constitutes an unconstitutional restraint on interstate commerce, and that the statute violates the First Amendment. In addition, the Amici firmly believe that the vagueness of the CPR Act prevents legitimate businesses who increasingly rely on the Internet to conduct their business from knowing when they are running afoul of the law, requiring them to either significantly curtail their normal business practices, or face serious criminal or administrative penalties or costly litigation. For all of the reasons

³ See e.g., February 27, 2004, Senate Floor Debate on HB 165 (comments of Senator John Valentine), www.le.state.ut.us/asp/audio/index.asp?Sess=2004GS&Day=0&Bill=HB0165&House=S, Tr. attached hereto as Exhibit A (The CPR Act is an "attempt to try to protect against pedophiles making contact with children over the Internet."); Joe Baird, *New laws on the books for Utah*, Salt Lake Tribune, May 1, 2006 ("Baird Article"), attached hereto as Exhibit B ("The state, as of today . . . has . . . a child-protection registry to deter adult-oriented marketers from targeting Web-messaging usernames, and cell phone and fax numbers. . . . With the passage of HB417, state officials are also hailing what they call another layer of protection for Utah's children from pornographic content.").

outlined below, the Amici support the FSC's motion for preliminary injunction, and urge this Court to enter an order enjoining enforcement of the CPR Act, and striking down the statute as an unconstitutional enactment.

**RELEVANT FACTUAL INFORMATION UNDERLYING THE
CONSTITUTIONAL INFIRMITIES OF THE CPR ACT⁴**

This case requires the Court to apply well-developed principles of constitutional law to the unique and relatively new field of Internet commerce. The Amici's purpose is to assist this Court in understanding the significant practical effects the CPR Act will have on email marketing, a growing area of the United States economy, and how the CPR Act therefore runs afoul of the supremacy clause, the dormant commerce clause and the protections of the First and Fourteenth Amendments. This section, hereinafter referred to as "Statement of Facts" or "SOF," lays out the factual detail and background necessary to frame the legal analysis set forth below.

I. EMAIL MARKETING VIA THE INTERNET IS AN ALMOST BILLION DOLLAR INDUSTRY AND IS GROWING RAPIDLY

A. The Internet.

"The Internet is a decentralized, global medium of communication that links people, institutions, corporations and governments around the world." *ACLU v. Johnson*, 194 F.3d 1149, 1153 (10th Cir. 1999). "It is a giant computer network that interconnects innumerable smaller

⁴ Exhibits C thru R set forth detailed summaries of the information counsel for the Amici has obtained from a variety of sources, including corporate websites and personal interviews of corporate executives, regarding the potential impact the CPR Act will have on a variety of legitimate businesses who participate in e-commerce and rely on e-mail marketing as a means of communicating with consumers and advertising alcohol, tobacco, gambling and other prohibited or potentially prohibited products and services over the Internet, on behalf of themselves and/or their clients. A number of these companies fear prosecution by the State of Utah under the CPR Act, and have therefore provided such information on the condition of strict anonymity. These companies are referred to herein, and in the relevant exhibits, as "Company X," "Company Y," and "Company Z." Counsel for the Amici submits these exhibits, and all information contained therein, pursuant to their professional obligations of candor under Rule 11 of the Federal Rules of Civil Procedure and Rule 3.3 of the Utah Rules of Professional Conduct, and expressly represent and affirm that the information provided in the referenced exhibits is true and correct to the best of their knowledge and belief after a reasonable and good faith investigation.

groups of linked computer networks and individual computers,” and through which text, images and sounds are quickly, easily and inexpensively transported and displayed. *Id.* Although exact estimates are difficult due to its constant and rapid growth, the Internet is currently believed to connect billions of users worldwide.⁵ The Internet is a unique, rapidly evolving medium of human communication and commerce. *See Reno v. ACLU*, 521 U.S. 844, 850 (1997). By its very nature, the Internet does not have borders. *See American Booksellers Found. v. Dean*, 342 F.3d 96, 103 (2nd Cir. 2003). Thus, persons who speak or do business over the Internet are able to communicate to computer users throughout the country and around the world quickly, and at a relatively low cost.

The use of the Internet as a tool of national and international commerce has expanded significantly over the past few years, and e-commerce is now a multi-billion dollar industry.⁶ *Cf.* March 9, 2004, Federal Trade Commission (“FTC”), *Do Not E-Mail Registry Meeting* (1:00 pm.) (“Mar. 9 FTC Tr. Pt. II”) at 39 (comment of Ronald Plessner), excerpts attached hereto as Exhibit U (“[T]he whole idea of the Internet is to be able to communicate and to have [e]-commerce available.”). As of 2003, more than 100 million American consumers were believed to purchase products and services online. *See E-Commerce Report* at 10; March 10, 2004, FTC, *Do Not E-Mail Registry Meeting* (“Mar. 10 FTC Tr.”) at 33-36 (comments of Scott Silverman, Shop.org), excerpts attached hereto as Exhibit V. In that same year, e-commerce outperformed

⁵ *See, e.g., American Library Ass’n v. Pataki*, 969 F. Supp. 160, 164 (S.D.N.Y. 1997) (“The nature of the Internet makes it very difficult, if not impossible, to determine its size at any given moment.”); *Reno v. ACLU*, 521 U.S. 844, 850 (1997) (“[T]he growth of the Internet has been and continues to be phenomenal.”).

⁶ E-commerce refers to “business processes which shift transactions to the Internet (or some other nonproprietary, Web-based system),” and spans all four major economic sectors—manufacturing, merchant wholesale, retail and service. *See* June 4, 2003, *Report for Congress: E-Commerce Statistics: Explanation and Sources* (“E-Commerce Report”) at 1, excerpts attached hereto as Exhibit S; May 11, 2005, U.S. Dept. of Comm. E-Stats, www.census.gov/estats (“E-Stats”) at 1-4, excerpts attached hereto as Exhibit T.

total economic activity in all four major economic sectors.⁷ See E-Stats at 1. By 2005, e-commerce accounted for more than 80 billion dollars in retail sales, an increase of approximately 24% over 2004. See February 17, 2006, U.S. Dept. of Comm., U.S. Census Bureau News, *Quarterly Retail Commerce E-Sales 4th Quarter 2005*, www.census.gov/mrts/www/data/05Q4.html (“Census Bureau Report”) at 1, attached hereto as Exhibit W.⁸

B. Email.

In addition to operating websites that directly advertise a company’s goods and services, allow ordering on-line, and facilitate prompt customer service, legitimate businesses have turned to email as an increasingly effective tool of e-commerce. Email has now become an integral part of the marketing plan for a significant number of legitimate businesses who use email to generate new customers, communicate with and serve existing customers, announce new products and services, increase sales and attendance at client events, and otherwise provide information about their business. Businesses, particularly those in the retail sector, also use email to drive consumers to their physical locations. See Mar. 10 FTC Tr. at 34 (comments of Scott Silverman, Shop.org). Email marketing campaigns take a variety of forms, including regular or periodic e-newsletters, electronic catalogs, electronic postcards or traditional email text messages. In many industries, email has now surpassed direct mail, facsimile, telephone, print ads, and other forms of traditional marketing as the primary mode of communicating with customers.

⁷ In 2003, retail e-commerce sales were \$56 billion. See E-Stats at 4. This constituted an increase of approximately 25% over 2002, and “strongly outpaced total retail sales growth of 4 percent.” *Id.*

⁸ Total retail sales in 2005 increased by just 7.2%. See Census Bureau Report at 1-2.

Email is now considered to be one of the fastest, most effective, and least expensive ways of finding and building relationships with customers (*see* Mar. 10 FTC Tr. at 17 (comments of Beth Marshall, MBNA)),⁹ and email marketing now constitutes a significant aspect of overall e-commerce in the United States. *See* Mar. 10 FTC Tr. at 32-33 (comments of Elizabeth Treanor, Shop.org) (E-commerce has “really been driven by e-mail”). There are believed to be more than 300 million email addresses in use in the United States, and the number may well exceed one billion. *See* March 9, 2004, FTC, *Do Not E-Mail Registry Meeting* (11:00 a.m.) at 32-33 (comments of Peter Mesnick, IMN, Inc. f/k/a iMakeNews), attached hereto as Exhibit Y; February 11, 2004, FTC, *In the Matter of: Report to Congress Pursuant to CAN-SPAM Act* (“Feb. 11 FTC Tr.”) at 30-31 (comments of Jason Catlett, JunkBusters), excerpts attached hereto as Exhibit Z. In 2005 alone, legitimate businesses such as advertising agencies, email service providers, and others spent approximately 885 million dollars on email marketing efforts,¹⁰ and sent millions of email messages promoting a wide range of products, events and services. These email messages generated approximately 251 million dollars in revenue for legitimate businesses and their marketing partners nationwide.¹¹

Legitimate email marketers gather email addresses for use in email marketing campaigns in a variety of ways. Most legitimate businesses collect email addresses directly from their

⁹ *See also* Mar. 10 FTC Tr. at 33 (comments of Elizabeth Treanor, Shop.org) (“Eighty-seven percent of all e-retailers who do business online believe strongly that e-mail is their best way to get to their customers; it’s better than advertising, it’s much better than pop-up ads.”); *see also* Mar. 9 FTC Tr. Part II at 44-45 (comments of Jerry Cerasale, DMA) (“The Internet, the search engines now become advertising vehicles where you get—so even the web sites, there are so many of them, the Internet no longer is a way to try and [develop your business]—for a new company to try and—you have to try and drive traffic to your website one way or another, and e-mail allows that lower barrier of entry. You can’t get it [through other forms of e-commerce]. You can’t get that entrepreneur, job-creating engine that the Internet can be through e-mail.”).

¹⁰ *See* Email Labs, www.emaillabs.com/resources_statistics.html#spamfading.

¹¹ *See* Interactive Advertising Bureau, www.iab.net/news/pr_2006_04_20.asp.

existing customers, or from persons who have visited their stores or websites (or those of their marketing partners) and registered to receive offers or information about the company's products and services. Some of these businesses use their email lists internally to send out e-newsletters and email advertisements on their own behalf, while others contract with third party email service providers to send emails for them. These third party vendors typically serve hundreds of thousands of customers each month, and charge a fee based on the number of email messages sent on behalf of the client.

C. SPAM.

The email messages sent by legitimate businesses and their marketing partners (such as those represented by the Amici) comply with CAN-SPAM, and are typically sent only to those individuals who have "opted-in" to receive such messages. Legitimate businesses also comply with accepted industry standards for the use of email as a marketing tool. *See, e.g.,* Email Marketing Pledge, www.espcalition.org/pledge.php, attached hereto as Exhibit AA.¹² They do not send what is commonly referred to as "spam," or use email as a means of facilitating scams or defrauding the public. Spam is typically sent by unscrupulous persons, including off-shore operators and pedophiles. These "spammers" use a variety of technological techniques to operate anonymously and avoid detection, and often hijack the computer systems of others to give the appearance that the spam is coming from a legitimate source when it is not. Spammers typically make no effort to comply with CAN-SPAM or any other laws, and do not follow any accepted industry standards.

¹² According to the ESPC, more than 80 businesses have committed to the Email Marketing Pledge, agreeing to follow the guidelines and standards set forth therein.

II. THE CPR ACT EXPRESSLY REGULATES COMMERCIAL EMAIL COMMUNICATIONS AND DIRECTLY IMPACTS INTERSTATE COMMERCE

The CPR Act and its implementing regulations create a registry of “contact points” purportedly belonging to or accessible by Utah minors (the “Registry”),¹³ and makes it unlawful for any “person” to “send, cause to be sent, or conspire with a third party to send a communication to a contact point or domain that has been registered for more than 30 calendar days . . . if the communication: (a) has the primary purpose of advertising or promoting a product or service that a minor is prohibited by law from purchasing; or (b) contains or has the primary purpose of advertising or promoting material that is harmful to minors. . . .” U.C.A. §13-39-202(1) (2006). The statute expressly defines a “contact point” to include “an email address” (*id.* § 13-39-101(1)(a)), and was initially enacted to apply *only* to email communications. *See* U.C.A. §§ 13-39-101(1)(b) & -201(2)(b-c) (2004).¹⁴ As applied through its implementing regulations, the statute unavoidably requires any legitimate business (whether located in the State of Utah or not) which desires to send any potentially prohibited communication to any email address (whether the address is known to be owned or accessed by a Utah resident or not) to scrub its email list against the Registry every 30 days, and to remove from its mailing list any registered address.¹⁵ It cannot be reasonably disputed that the CPR Act therefore constitutes an

¹³ *See* U.C.A. § 13-39-201(1) (“The division shall (a) establish and operate a child protection registry to compile and secure a list of contact points the division has received pursuant to this section; or (b) contract with a third party to establish and secure the registry as described in Subsection 1(a)"); U.A.C. R152-39-1 (“Pursuant to Utah Code Section 13-39-203, these rules (R152-39) are intended to establish the procedures under which: (1) a person may register a contact point with the registry; and (2) a marketer may verify compliance with the registry.”).

¹⁴ Effective May 1, 2006, the CPR Act was amended to extend the Registry to other electronic “contact points,” including instant messaging IDs, mobile phone numbers and other telephone numbers. *See* U.C.A. §§ 13-39-101(b) & -201(2) (b-c) (2006).

¹⁵ *See* U.C.A. § 13-39-201(4) (“A person desiring to send a communication described in Subsection 13-39-202(1) to a contact point or domain shall (a) use a mechanism established by rule made by the division under Subsection 13-39-203(2); and (b) pay a fee for use of the mechanism [as] determined by the division. . . .”); U.A.C. R152-39-5

express regulation of commercial email, which will have a direct and unavoidable burden on e-commerce. As discussed further below, the CPR Act is therefore pre-empted by CAN-SPAM and violates the dormant commerce clause. *See infra* Legal Argument §§ I & II.

III. EMAIL IS AN INHERENTLY INTERSTATE FORM OF COMMUNICATION

Although the CPR Act purports to regulate conduct occurring within the State of Utah, its practical effects reach far beyond its borders. To begin with, the CPR Act regulates email communication via the Internet, an activity which is inherently interstate.¹⁶ Email messages, including those used by legitimate businesses in e-commerce, pass through multiple computer networks, and travel across multiple transmission lines, in multiple states, before reaching the intended recipient. This is true even where the sender and recipient reside in the same state. Accordingly, even an email message sent by one Utah resident to another Utah resident likely travels outside of the State of Utah, and impacts computer networks and transmission lines in multiple states.¹⁷

The CPR Act effectively regulates every legitimate business who happens to use email to advertise or assist others in advertising alcohol, tobacco, gambling, firearms, tattooing, body

(“(1) After a marketer has complied with R152-39-4 and paid the fee established by the Division under Section 13-39-201(4)(b), the marketer may submit the marketer’s email list to the provider according to the privacy and security measures implemented by the provider. (2) After the provider has complied with R152-39-5(1), the provider shall, according to the privacy and security measures implemented by the provider, inform the marketer of the email addresses from the marketer’s email list that are contained on the registry.”).

¹⁶ *See, e.g., Johnson*, 194 F.3d at 1160 (internal quotation omitted) (“The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states’ jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet.”); *Pataki*, 969 F. Supp. at 169 (“The internet, like . . . rail and highway traffic . . . , requires a cohesive scheme of regulation so that users are reasonably able to determine their obligations.”).

¹⁷ *See, e.g., Johnson*, 194 F.3d at 1161 (“Even if it is limited to one-to-one email communications . . . there is no guarantee that a message from one New Mexican to another New Mexican will not travel through other states *en route*.”); *Pataki*, 969 F. Supp. at 171 (“The Internet is . . . a redundant series of linked computers. Thus, an [email] message from an Internet user sitting at a computer in New York may travel via one or more other states before reaching a recipient who is also sitting at a terminal in New York.”).

piercing, credit cards, car rentals and other products and services that may not be lawfully sold to or purchased by Utah minors, or may be deemed “harmful to minors” under Utah law. *See e.g.*, Merchant Direct (Exhibit C); Company X (Exhibit D); Company Y (Exhibit E); Company Z (Exhibit F); Gastronomy (Exhibit K); LocalWineEvents.com (Exhibit I); Telluride Wine Festival (Exhibit J); Food & Wine Classic (Exhibit H); and The Brewers Association (Exhibit G). Many of these legitimate businesses are located outside of and do minimal (if any) business in the State of Utah. *See e.g.*, Merchant Direct (Exhibit C); Company X (Exhibit D); Company Y (Exhibit E); Company Z (Exhibit F). Because these legitimate businesses have no way of knowing from the email addresses alone whether an email address belongs to a Utah resident, or may be accessible by a Utah minor (*see infra* SOF § IV), they cannot unilaterally purge from their mailing lists those email addresses belonging to or potentially accessible by Utah minors. They will therefore be required to either refrain from sending any potentially prohibited email messages to any email address, or scrub their entire list against Utah’s Registry, pay the required fee for doing so, and conform their business practices to the requirements and standards of Utah law.

There is nothing in the CPR Act or its implementing regulations to prevent persons outside of Utah from registering their email address with the state. By way of non-exclusive example, a divorced father residing in Colorado might register his email address because it is accessible to his minor children—residents of Utah—on a periodic basis. A person from another state may affirmatively misrepresent his or her state of residency and register his or her email

address even though it may never be accessed by a Utah minor.¹⁸ The CPR Act also makes no accommodation for the fact that email messages sent to a “Utah” address may actually be received outside of the state, such as when a Utah resident opens his or her email messages while traveling. The CPR Act therefore reaches out far beyond the borders of Utah, regulating email communications and e-commerce entirely across state lines, and imposing an undue burden on interstate commerce. As discussed further below, the CPR Act therefore violates the dormant commerce clause. *See infra* Legal Argument § II.

IV. THE REGULATORY AND PENAL SCHEME OF THE CPR ACT IS PREDICATED ON UNWORKABLE DISTINCTIONS WHICH IGNORE THE REALITIES OF EMAIL COMMUNICATIONS

The CPR Act provides for criminal, civil and administrative liability, and allows for fines, penalties and/or civil damages ranging from \$1,000 to \$5,000 per violation against any person who sends a prohibited email message to any address on the Registry for more than thirty (30) days.¹⁹ In so doing, the CPR Act attempts to distinguish between (a) emails sent to Utah residents from emails sent to non-Utah residents, and (b) emails sent to minors from emails sent

¹⁸ Neither the CPR Act nor its implementing regulations provide any protection against such abuse. Although registrants are required to check a box on the registration page and affirm that they are a Utah resident and/or that they are the parent or legal guardian of a Utah minor with access to the account (*see* www.utahkidsregistry.com attached hereto as Exhibit CC), there are no penalties for misrepresenting such facts or requirement for verification. *See, e.g.*, Contract between Division and Unspam (“Unspam Contract”) at Statement of Work, ¶ (1)(g)(iv), attached hereto as Exhibit DD (“Unspam has no duty to verify that a minor has access to any registered contact point.”). The registrant is also not required to provide a name, address or other information that would allow them to be easily identified or tracked down by the State. Accordingly, anyone, in any jurisdiction, can register their out-of-state e-mail address under the CPR Act.

¹⁹ In addition to criminal fines, administrative penalties and civil damages, the CPR Act allows the prevailing party in any civil action to recover his or her “costs and reasonable attorneys fees.” U.C.A. § 13-39-302(2)(b) (2006). This provision imposes an additional layer of risk on legitimate businesses engaged in e-commerce. A similar provision in Utah’s Unsolicited Commercial and Sexually Explicit Email Act, Utah Code Ann. §§ 13-36-101 *et seq* (repealed as a result of CAN-SPAM)—which provided for civil damages of only \$10 per violation (as opposed to the \$1000 per violation allowed under the CPR Act)—resulted in one over-zealous plaintiff’s firm filing hundreds of lawsuits in an effort to obtain quick settlements from the alleged violators, including windfall attorneys’ fee payments. There is no reason to believe that similar lawsuits will not be filed under the CPR Act.

to adults. As set forth below, such distinctions are not easily made in the context of email communications. As a result, legitimate businesses nationwide will have no practical alternative but to scrub their email lists against the Utah Registry, highlighting the CPR Act's significant and undue burden on interstate commerce in violation of the dormant commerce clause. *See infra* Legal Argument § II.

A. The Utah vs. Non-Utah Distinction

An email address is made up of a series of characters typically created by the account holder or email service provider, followed by a domain identifier such as “aol.com,” “hotmail.com” or “yahoo.com,” separated by an “@” symbol, such as john.doe@aol.com, j.doe@yahoo.com or jdoe125@hotmail.com. An email address may be owned and accessed by only one person, or may be used by and accessible to an entire household (or anyone else in possession of the required password). By its very nature, an email address typically provides no information that would allow a sender to identify every individual who may “own” or access the email address, or the state in which such users may reside. *See* S. Rep. 108-102 at 21 (2003), (“In contrast to telephone numbers, e-mail addresses do not reveal the State where the holder is located. As a result, a sender of e-mail has no easy way to determine with which State law to comply.”). Although individual companies and email service providers frequently obtain geographical or other information about a registrant at the time an email address is obtained, this is not always the case. Moreover, there is no way for the sender to know with any degree of certainty whether such information is (or ever was) accurate, or whether there are other users of the email address. *See e.g.*, Merchant Direct (Exhibit C); Company X (Exhibit D); Company Y (Exhibit E); Company Z (Exhibit F); and The Brewers Association (Exhibit G).

By way of non-exclusive examples, a person may register his or her email address online and provide his or her physical mailing address in California, and then move to Utah a few months later while maintaining the same email address. A divorced parent (an adult) residing in Colorado may have an email address which is shared with and accessible by his minor children using their computer in Utah. A registrant might provide a false mailing address to avoid direct mail solicitation, but provide a real email address because he or she wants to obtain information on-line. Finally, modern technology allows email users to access their email accounts from any computer with Internet access, and thus Utah residents may actually receive and view their email messages in another state. As such, an email marketer cannot unilaterally purge from its list those email addresses potentially accessible by a Utah resident, and the only practical way for legitimate businesses to avoid sending potentially prohibited email to those on the Registry is to scrub their entire mailing list once every 30 days.

B. The Adult vs. Minor Distinction

An email marketer also cannot reasonably identify the age of a potential recipient based on the email address alone, and thus an email marketer cannot unilaterally purge from its list those email addresses potentially accessible by a minor. For example, a child could register his own email address under his parent's name and biographical information, including age, to obtain information via email that he or she might not otherwise be able to obtain. Since the consent of a minor is not a defense under the CPR Act, the only practical way for legitimate businesses to avoid sending potentially prohibited email to those on the Registry is to scrub their entire mailing list once every 30 days.²⁰

²⁰ As set forth below, the statute also contains no clear definition of the term "minor." See *infra*, SOF § VI(C).

V. **THE CPR ACT WILL IMPOSE SIGNIFICANT BURDENS AND FINANCIAL COSTS ON LEGITIMATE EMAIL MARKETERS AND LEGITIMATE BUSINESSES FROM AROUND THE COUNTRY WHO ADVERTISE OTHERWISE LAWFUL PRODUCTS AND SERVICES TO ADULTS IN UTAH AND TO PERSONS IN OTHER STATES**

To avoid strict liability under the CPR Act, and the burdens and expenses associated with the criminal, civil and/or administrative penalties imposed by the statute, legitimate email marketers and businesses around the country, including members of the Amici, will have no practical choice but to either refrain from sending *any* email message containing *any* potentially prohibited content to *any* email address, or bear the burden and expense of having their email lists scrubbed against the Registry at least once every 30 days.

Those who elect to stop sending any potentially prohibited email message to any email address will forego a substantial source of revenue. By way of example, a company known as Merchant Direct uses email to market alcohol and tobacco products, including its “beer of the month,” “wine of the month” and “cigar of the month” clubs. *See* Merchant Direct (Exhibit C). These email messages are projected to result in revenues of approximately \$15 million in 2006 alone. *See id.* Company Y is an email service provider who sends email advertisements on behalf of approximately 500 customers in the alcohol beverage, tobacco, gambling and other industries whose products and services are likely prohibited under the CPR Act. *See* Company Y (Exhibit E). The email messages sent on behalf of these customers generate over \$200,000 in annual revenues for Company Y. *See id.* Company Z is another email service provider who sends approximately 750,000 email messages on behalf of customers in the alcohol beverage, gambling, tobacco and other industries whose products and services are likely prohibited under the CPR Act. *See* Company Z (Exhibit F). These customers constitute approximately 5% of

Company Z's total email marketing business, and the email messages sent on behalf of these customers generate over \$2 million in annual revenues for Company Z. *See id.*

Those who elect to scrub their lists against the Registry will be required to spend thousands (if not tens of thousands) of dollars every 30 days to engage in the process, and will be required to incur the additional personnel and technology costs associated with installing the necessary software, preparing their lists for scrubbing against the Registry, creating and maintaining a database of those email addresses identified as being on the Registry, and ensuring that potentially prohibited content is not transmitted to such addresses in the future. *See* Merchant Direct (Exhibit C) (scrubbing would cost at least \$5,000 per month (\$60,000 per year), not including the cost that would be passed on to Merchant Direct by its third party email services providers, or the personnel and technology costs associated with the scrubbing process); Company Y (Exhibit E) (scrubbing would cost approximately \$3,750 per month (\$45,000 per year)); Company Z (Exhibit F) (scrubbing would cost approximately \$25,000 per month (\$300,000 per year)).

The increased cost is particularly significant when compared against the current cost of sending email advertisements. Compared to other forms of marketing, including telemarketing, an email marketing campaign can be conducted at a relatively low cost, and thus *any* increase in cost is significant for the legitimate email marketer. *See, e.g.,* March 15, 2004, FTC, *In the Matter of: Report to Congress Pursuant to CAN-SPAM Act* ("Mar. 15 FTC Tr.") at 25-27 (comments of Joshua Goodman, Microsoft Research), excerpts attached hereto as Exhibit EE ("I don't know how much it costs to do a telemarketing effort per call, a one cent cost for you to check a Registry is cheap. If you're going to be sending e-mail, legitimate e-mail, and it costs

you one cent per message to check a Registry, that's obviously going to be a huge burden relative to the cost of sending e-mail normally.”). By way of specific example, scrubbing would increase Merchant Direct's internal email marketing costs by 600%, from \$1,000 per month (\$12,000 per year) to \$6,000 per month (\$72,000 per year). *See* Merchant Direct (Exhibit C). Scrubbing would increase the cost for Company Y's affected email marketing customers by at least 50% (*see* Company Y (Exhibit E)), and would increase the email transmission fees of Company Z's customers by approximately 17%. *See* Company Z (Exhibit F).

The cost of scrubbing is also significant when viewed in the context of how many email addresses may be registered as compared against the total number of emails that may actually be sent. By way of non-exclusive example, Merchant Direct sends out monthly emails to more than 1 million email addresses. *See* Merchant Direct (Exhibit C). Because Merchant Direct cannot legally ship its alcohol and tobacco products to Utah, it purges from its email lists those email addresses known (or believed) to be associated with Utah shipping addresses. *See id.* It is therefore highly unlikely that many of the 150,000 email addresses currently registered on the Registry²¹ will be on Merchant Direct's email list. Merchant Direct will nonetheless be required to pay thousands of dollars each month to scrub every name on its list (rather than just those names actually identified as being on the Registry). *See id.*

²¹ *See* Baird Article (Exhibit B). This 150,000 figure likely includes a significant number of email addresses that have been registered by schools or other institutions providing email service to minors. *See* U.C.A. § 13-39-2-1(3)(a)(2006) (allowing such institutions to register their entire domain with the Registry). This figure does *not* represent the actual number of Utah residents who have personally logged on to the Registry's website and asked to have their individual and/or household email addresses included on the Registry.

These already substantial costs and burdens will only increase as other states adopt statutes similar to the CPR Act.²² As additional states adopt and enforce child registry systems, legitimate email marketers will be required to, at the very least, (a) scrub their email lists against each state's registry, (b) maintain databases identifying which email addresses have been registered in which states, and (c) carefully review the content of their email messages to ensure that they do not send to any registered email address, in any state, any content that is potentially prohibited by that state. This process will become more time consuming, costly, difficult and complex as each state adopts its own scrubbing processes and requirement, and its own standards for what is prohibited and what is not. This is exactly what happened prior to 2003, when a variety of states, including Utah, passed anti-spam statutes requiring the nation's legitimate email marketers to comply with over thirty different laws, many of which imposed different obligations and requirements.²³ See 15 U.S.C. § 7701(11) (CAN-SPAM—Congressional Findings and Policy) (“Many states have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but then states impose different standards and requirements”). As a result of these significant costs, the CPR Act imposes an undue burden on interstate commerce, in violation of the dormant commerce clause. See *infra*, Legal Argument § II.

²² The State of Michigan has already adopted such a statute, and other states, including Illinois, have considered such statutes in recent legislative sessions. See M.C.L.A. 752.1061 *et seq.*, attached hereto as Exhibit FF; Illinois HB0752, attached hereto as Exhibit GG. The Amici believe that other states are awaiting the outcome of the pending legal challenge to the Utah CPR Act before acting on their own legislative initiatives.

²³ In 2003, Congress passed CAN-SPAM and pre-empted these individual state anti-spam statutes, creating one uniform system of regulation for email marketers. See 15 U.S.C. § 7707(b); see also July 27, 2005, FTC, *In the Matter of: CAN-SPAM Report to Congress* (“July 27 FTC Tr.”) at 75-77, excerpts attached hereto as Exhibit X (comments of Trevor Hughes, ESPC) (“One of the most important things that the CAN-SPAM Act did, and I think this can be a goal that can be identified and recognized and checked off as at least initially successful, was it created a common platform for legitimate businesses to understand what was onside and what was offside with regards to commercial Email. The CAN-SPAM Act ostensibly preempted some 37 state laws at the same time of its passage, and those state laws were creating a really crazy quilt of standards that legitimate email senders were really having a daunting challenge to respond to.”).

VI. THE CPR ACT CONTAINS VAGUE AND UNDEFINED TERMS PREVENTING LEGITIMATE BUSINESSES FROM KNOWING WHAT IS PROHIBITED AND FROM EFFECTIVELY COMPLYING WITH ITS PROVISIONS

As originally drafted, the CPR Act was extremely broad in scope, prohibiting *any* email communication that in any way referenced or incorporated references to any potentially prohibited product or service such as alcohol, tobacco, gambling, firearms, tattoos, body piercing, credit cards, car rentals, etc. *See* U.C.A. § 13-39-202(1)(a) (2004). In this regard, the Utah CPR Act threatened to criminalize email communications from those in a variety of industries, including those such as the travel, entertainment, dining and special event industries, where products and services are often inextricably intertwined with alcohol and other prohibited products and services.

By way of non-exclusive example, a hotel company might send an email advertisement offering a special weekend rate and, as part of that email communication, provide information advertising or promoting the hotel's bar, casino or weekly wine dinner. *See* Company Y (Exhibit E). *See also* Las Vegas CVA (Exhibit O). A local Utah restaurant group, Gastronomy, Inc., sends an email newsletter to its frequent-diners advertising a monthly wine dinner or offering advice on the type of wine that is best served with certain dishes. *See* Gastronomy (Exhibit K). Brewvies, a Salt Lake City movie theater, offers beer to its adult movie goers, and its patrons can register to receive periodic email newsletters which contain information not only about the movies shown, but promotes the theater's alcohol products. *See* Brewvies (Exhibit P). A number of food, art and music festivals, such as the Fidelity Park City Jazz Festival and the Sonoma Valley Film Festival, are sponsored by wine and beer companies, and often include the logos and/or website hyperlinks of these sponsors in their email communications. *See* Sonoma

Valley Film Festival (Exhibit M); Park City Jazz Foundation (Exhibit L). *See also* Napa Valley Mustard Festival (Exhibit N); Lake Tahoe Shakespearean Festival (Exhibit R); SLC Downtown Alliance (Exhibit Q); LocalWineEvents.com (Exhibit I); Food & Wine Classic (Exhibit H); and The Brewers Association (Exhibit G).

Recognizing the vagueness in the statute, the Division of Consumer Protection (“Division”), the agency charged with implementing and enforcing the statute—issued a policy statement which attempted to define key terms and limit the scope of the statute. *See generally* July 8, 2005, State of Utah Dept. of Comm., Policy Statement Concerning Utah Code Ann. § 13-39-202(1) (“Division Policy Statement”), attached hereto as Exhibit BB. First, the Division indicated its belief that an email advertisement “contains or advertises material” only if “the primary purpose of the communication, directly or indirectly, is to advertise or otherwise link to the material.” *See id.* at 2. Second, the Division stated its belief that the CPR Act did “not prohibit an advertisement of a product or service a minor may purchase only under some circumstances,” such as prescription drugs or body piercing. *See id.* at 1. Third, the Division opined that the CPR Act did not “preclude an advertisement for a contract that might be voidable because a party is a minor, or an advertisement of a product or service that might facilitate or enable illegal activity by a minor,” such as advertisements for credit cards, hotel rooms or car rentals. *See id.*²⁴

²⁴ To the extent these limitations and exemptions are not found anywhere in the CPR Act or the Division’s implementing regulations, they bind only the current administration and are subject to change at any time based on shifting political or policy considerations.. As recognized by the Division itself, the “policy statement is not legal advice or a legal opinion” Division Policy Statement at 1, and does not bind the Utah Attorney General, or the judges that will actually interpret and apply the law. More concerning, the statements will not deter the potentially innumerable civil plaintiffs (or their lawyers) who may bring lawsuits in an effort to recover statutory damages and attorneys’ fees. *See infra* note 21.

In its 2006 legislative session, the Utah Legislature adopted some (but not all) of the limitations recommended in the Division’s policy statement in an attempt to further narrow the scope of the CPR Act. In particular, the Division limited the CPR Act prohibitions to those email communications having “the *primary purpose* of advertising or promoting a product or service that a minor is prohibited by law from purchasing.” U.C.A. § 13-39-202(1)(a) (2006) (emphasis added). As set forth below, however, the 2006 amendments do not fully address the problem, and the revised CPR Act continues to contain vague and undefined terms.

A. The CPR Act Fails to Define “Primary Purpose”

The CPR Act fails to define the term “primary purpose.” For instance, how much of the email must be devoted to the prohibited product or service to render it unlawful? Is it 20%? 30? 50%? *See, e.g.*, Gastronomy (Exhibit K); Park City Jazz Festival (Exhibit L); Sonoma Valley Film Society (Exhibit M); Napa Valley Mustard Festival (Exhibit N); Brewvies (Exhibit P); SLC Downtown Alliance (Exhibit Q). What if the communication contains a hyperlink to a website whose primary purpose is to advertise or promote prohibited products and services? *See, e.g.*, Las Vegas CVA (Exhibit O); Lake Tahoe Shakespearean Festival (Exhibit R). Does the email communication itself then violate the statute? The Division thinks that it would,²⁵ but the statute is unclear.

B. The CPR Act Fails to Define the Terms “Advertising” and “Promoting”

The CPR Act likewise fails to define the terms “advertising” and “promoting.” For instance, does an email communication have to be sent for a purely commercial purpose to be prohibited? Must the communication contain a direct offer to sell the prohibited product or

²⁵ *See* Division Policy Statement at 2.

service? Does an e-newsletter or similar message sent primarily for “informational” or “educational” rather than “solicitation” purposes fall within the scope of the statute? *See, e.g.*, Gastronomy (Exhibit K); Las Vegas CVA (Exhibit O); SLC Downtown Alliance (Exhibit Q). Once again, the statute gives no guidance to legitimate businesses on these issues.

C. The CPR Act Fails to Define the Term “Minor”

The CPR Act also contains no definition of the term “minor.” Utah law generally defines a minor as anyone under 18 years of age, who is not emancipated, married or a member of the armed services. *See generally* U.C.A. § 15-2-1 (defining period of “minority” to extend to the age of 18, but stating that all minors reach the age of majority upon marriage); *id.* § 76-7-321(4) (defining a “minor” as any person under the age of 18 who is not otherwise emancipated, married or in the armed forces); *id.* § 76-10-2201(1)(c) (defining minor as anyone under 18 who is neither married nor “emancipated by a court of law”). However, it is unlawful for anyone under 21 to purchase or consume alcohol (*see id.* §§ 32A-1-105(30)), and for anyone to sell tobacco to any person under 19 years of age. *See id.* § 76-10-104. Does the CPR Act, which expressly uses the term “minor” and not “person,” incorporate the more commonly accepted definition of minority under Utah law and allow otherwise prohibited email messages to be sent to anyone who is over the age of 18, emancipated, married, or in the armed services, regardless of whether they can lawfully purchase the advertised product and service? Or does it apply a different definition of minority depending on the content of the particular email message? The statute provides legitimate businesses no clarity on these important issues.

D. The CPR Act Fails to Clearly Articulate What Activity a Minor is “Prohibited By Law From Purchasing”

The CPR Act fails to articulate the products or services a minor is “prohibited by law from purchasing.” For instance, does the statute apply only to products and services that can never lawfully be purchased by a minor, such as alcohol or tobacco, or does it include within its scope products and services which may be lawfully purchased with parental consent, such as firearms, tattoos and body piercing? Does it apply to offers for credit cards, rental cars, etc. for which minors do not have the legal capacity to contract for? Moreover, the CPR Act fails to distinguish between material that is “harmful” for an older minor (e.g., a 17 year old) as opposed to a younger minor (e.g., an 8 year old). It is therefore impossible for legitimate businesses to ascertain all of the potential messages that may be prohibited under the statute.

E. The CPR Act Fails to Define What it Means For a Prohibited Communication to be “Sent”

The CPR Act imposes criminal, civil and/or administrative liability against any person who “sends, cause[s] to be sent, or conspire[s] with a third party to send” a prohibited communication. U.C.A. § 13-39-202(1)(2006). Once again, these terms are not defined and the potential scope of liability is unclear. As demonstrated by the following examples, a private individual may “send” or forward potentially prohibited information via email even though they have no commercial purpose in doing so:

- Anyone who receives an email advertising or promoting a potentially prohibited product or service could forward that email message to any friend or relative in their personal address book.
- A person can host a private cocktail party and send out an email invitation using “Evite” or some similar web based program. Under the broad definitions of the CPR Act and its implementing regulations, the email invitation technically advertises or

promotes, at least in part, the consumption of alcohol. *See, e.g.,* Sample Evite Invitation (Exhibit QQ).

- Anyone visiting websites such as www.winecountry.com or www.localwineevents.com can forward the websites, and their wine related content and advertisements, to any friend or relative simply by entering their email addresses and clicking a button. *See* Company X (Exhibit D); LocalWineEvents.com (Exhibit I). *See also* Las Vegas CVA (Exhibit O).

It is impossible to know from the language of the CPR Act alone whether the private sender of such messages would be subject to liability if the recipient's email address happens to be on the Registry for more than 30 days. Modern technology also allows any email user to send to any email address a hyperlink to any website, and thereby convert Internet information not itself subject to the CPR Act into a prohibited communication simply because it is sent via email. It is unclear from the vague language of the CPR Act whether such conduct would expose the sender (or the website owner) to liability if the recipient's email address happens to be on the Registry for more than 30 days.

The continued vagueness of the CPR Act makes it impossible for legitimate businesses to understand what is prohibited, and invites disparate interpretations and applications by state and local law enforcement as well as the state judges who will be asked to interpret its provisions in criminal and civil proceedings. It is therefore highly probable that a significant number of otherwise lawful and innocuous email communications will be swept into the broad scope of the CPR Act's provisions. As discussed below, all of this renders the statute unconstitutionally vague in violation of the due process clause of the Fourteenth Amendment. *See infra* Legal Argument § IV.

VII. THE CPR ACT REGULATES LAWFUL SPEECH BETWEEN ADULTS

The CPR Act regulates email communications not only to Utah minors, but also to adults. To begin with, the CPR Act allows an adult (or, really, anyone) to register every email address used “in a household in which a minor is present” (U.C.A. § 13-39-201(3)(a)(iii)(2006)), even those addresses which are not typically used or accessed by minors. For instance, a father could register the private email address of his twenty-one year old son despite the fact that the email account does not belong to and is rarely (if ever) accessed by his younger siblings. The CPR Act likewise allows one adult in the household to register an email addresses without the express knowledge or consent of another adult user (*i.e.*, when a wife registers the email address of her husband).

The CPR Act also fails to *effectively* exempt from its scope those otherwise prohibited email messages that are sent to adults who have expressly opted-in or otherwise requested to receive the information. For instance, a husband may sign onto www.localwineevents.com and sign-up to receive email notice of local wine events, or any number of the wine related e-newsletters offered by the site. *See* Local Wine Events.com (Exhibit I). His wife later registers all of the family email addresses under the CPR Act. To avoid violating the CPR Act, the operator of www.localwineevents.com (or one of its marketing partner) must scrub its entire email list against Utah’s Registry and remove the registered email address from all future mailings. The husband, an adult, is therefore denied information via email that he affirmatively elected and is lawfully entitled to receive.

The Utah Legislature attempted to resolve this problem in the 2006 Legislative Session, amending the CPR Act to allow a person to “send a communication to a contact point if, before

sending the communication, the person sending the communication receives consent from an adult who controls the contact point.” U.C.A. § 13-39-202(4)(a)(2006). To take advantage of this exemption, however, the email sender must, among other things, (i) “verify the age of the adult who controls the contact point by inspecting the adult’s government-issued identification card *in a face-to-face transaction*,” and (ii) “obtain a written record indicating the adult’s consent that is *signed by the adult*.” *Id.* § 13-39-202(4)(b) (emphasis added). Consistent with standard industry procedure and protocols, the vast majority of those registering to “opt-in” and receive email communications do so electronically, over the Internet. Such registrations do not typically involve a face-to-face transaction. This is particularly true for out of state businesses. Accordingly, the requirements of the CPR Act effectively nullify the exception and legitimate businesses, particularly those operating out of state, are required to scrub their entire list against the Registry and purge from their list any email address on the Registry for more than 30 days.

There is also no mechanism for removing a registered email address once all minors in the household have reached the age of majority. By way of example, a mother registers the email address of her seventeen year old son. A few months later her son turns eighteen and is now considered an adult for most purposes under Utah law. His address nonetheless remains on the Registry, and email marketers are unable to send him prohibited content without violating the CPR Act.

Finally, as noted above, there will be those email marketers who, for a variety of reasons, elect to comply with the CPR Act by not sending any potentially prohibited content to any email address. A number of third party email service providers already have made that decision, informing Merchant Direct that they will no longer send email messages advertising or

promoting its alcohol or tobacco products on its behalf. *See* Merchant Direct (Exhibit C). *See also* Park City Jazz Foundation (Exhibit L). When such decisions are made, adults on the marketer's email list, both in Utah *and* in other states, are deprived of email communications they would otherwise be entitled to receive. The prominence of such decisions will only increase as more states adopt statutes similar to the CPR Act, and the cost and burden of compliance with a patchwork set of laws becomes greater. As discussed further below, the CPR Act therefore constitutes an undue restraint on commercial speech. *See infra* Legal Argument § III.

VIII. THE CPR ACT WILL NOT ACCOMPLISH ITS PURPOSE OF PROTECTING UTAH'S MINORS

The primary intent and purpose of the CPR Act is to protect Utah's minors from email messages that contain pornographic and other offensive and potentially harmful content. *See supra* note 3. The CPR Act will be largely ineffective in the fight against such messages, however, and, as discussed in Section X below, may actually increase the risk of exposure for those who register their email address.

The vast majority of pornographic and other potentially harmful email content comes not from the legitimate businesses who will make an effort to comply with the CPR Act, but from spammers, including offshore emailers and pedophiles, who have become particularly skilled at avoiding the law. *See* May 10, 2004, Dr. Aviel D. Rubin, *A Report to the Federal Trade Commission on Responses to their Request for Information on Establishing a National Do Not E-mail Registry* ("Rubin Rep.") at 13, attached hereto as Exhibit HH.²⁶ There is no reason to believe that these spammers will comply with the provisions of the CPR Act any more readily

²⁶ *See also* Mar.15 FTC Tr. at 11-12 (comments of Jerry Popek, United Online) ("Today's spammers are adept at violating rules, laws and legitimate efforts to block their e-mail and are highly motivated. We would expect that culture will continue.").

than they have complied with other email and Internet regulations, such as CAN-SPAM.²⁷ Accordingly, a significant portion of the email content the CPR Act aims to restrict will still find its way into the email in-boxes of Utah's minors (including those with addresses on the Registry). This further demonstrates why the CPR Act imposes an undue burden on interstate commerce and unduly restricts commercial speech. *See infra* Legal Argument §§ II & III.

IX. THE FTC HAS EXTENSIVELY STUDIED CENTRALIZED REGISTRY SYSTEMS SUCH AS THAT CREATED BY THE UTAH CPR ACT AND HAS REJECTED THEM AS BEING AN UNWORKABLE MEANS OF PROTECTING MINORS FROM UNWANTED MATERIAL

At the direction of the United States Congress, and pursuant to Section 7708 of CAN-SPAM, the FTC conducted an extensive study on the feasibility of a national "Do Not Email" registry similar to that created under the CPR Act. The FTC concluded in 2004 that any such registry will be largely ineffective in the fight against unwanted email, and will likely do more harm than good:

This Report concludes that a National Do Not Email Registry, without a system in place to authenticate the origin of email messages, *would fail to reduce the burden of spam and may even increase the amount of spam received by consumers.* . . .

[T]he Commission has determined that *spammers would most*

²⁷ *See, e.g.*, Mar. 10 FTC Tr. at 46 (comments of Steve Richter, E-mail Marketing Association) ("[W]hat I'm seeing since the inception of the CAN-SPAM Act, is that the legitimate e-mailers are more legitimate now. They have gone out of their way to make sure that every single item in that CAN-SPAM Act is complied with, and vigorously. . . . And there's never been more spam before. There's more spam, now, since the CAN-SPAM Act than there was before. It's worse. It seems bolder, as far as what [the spammers are] selling and passing the point of obscenity."); *id.* at 47 (comments of Elizabeth Treanor, Shop.org) ("The legitimate folks are going to come and they're going to run their lists. They're not going to e-mail those folks on the list. But its not going to block spammers from sending e-mail. So, if they get a hold of the list or they continue to harvest and do whatever they do, they're still going to be able to send their e-mail."); July 27 FTC Tr. at 21-23 (comments of Josh Baer, Skylist and UnsubCentral) ("[T]he really bad people don't follow the laws and aren't going to comply with authentication and other things like that. . . ."); Mar. 9 FTC Tr. Pt. II at 5 (comments of Joseph Rubin, Executive Director, Technology and E-Commerce, U.S. Chamber of Commerce) ("[W]e see the vast majority of spammers just don't follow the law now, and wouldn't use a Registry. And we think that hurdle, in and of itself, creates a huge burden [] to a Do Not E-mail List.").

likely use a Registry as a mechanism for verifying the validity of email addresses and, without authentication, the Commission would be largely powerless to identify those responsible for misusing the Registry. *Moreover, a Registry-type solution to spam would raise serious security, privacy, and enforcement difficulties. The Commission's concerns with the security, privacy, and enforcement challenges surrounding a Registry reach a zenith with respect to children's email accounts. A Registry that identifies accounts used by children, for example, could assist legitimate marketers to avoid sending inappropriate messages to children. At the same time, however, the Internet's most dangerous users, including pedophiles, also could use this information to target children.*

June 2004, FTC, National Do Not E-Mail Registry: A Report to Congress ("2004 FTC Report").

2004 FTC Report at i, excerpts attached hereto as Exhibit II. (emphasis added).²⁸

The FTC reaffirmed these conclusions in December 2005, cautioning against the creation of state-based child protection registries:

The Commission generally supports initiatives that protect children from inappropriate content, but *state registries that maintain sensitive information belonging to children raise troubling issues*. The Commission has serious concerns about the security and privacy risks inherent in any type of do-not-email registry . . . *Although difficult to quantify, the risk of pedophiles or other dangerous persons misusing the registry data to discover the email address of a minor is certainly real. . . .* Several sources with whom the Commission consulted on this Report raised similar security and privacy concerns. . . .

. . . [T]he Commission would caution against legislative action on the state level to adopt registry-style laws in the hope that they may effectuate improved protections for children in the online

²⁸ The FTC solicited and obtained "input from dozens of individuals and organizations" and used "a number of information-gathering techniques, including: a Request for Information ("RFI") that resulted in responses from some of the nation's largest Internet, computer, and database management firms; interviews with over 80 individuals representing 56 organizations, including consumer groups, email marketers, Internet Service Providers ("ISPs"), and technologists; requiring the seven ISPs that collectively control over 50 percent of the market for consumer email accounts to provide detailed information about their experiences with spam; soliciting public comments through an Advance Notice of Proposed Rulemaking ("ANPR") concerning the CAN-SPAM Act rules; and retaining the services of three of the nation's preeminent computer scientists." 2004 FTC Report at i.

environment. The Commission believes that grave security and privacy concerns argue decisively against such measures.

December 2005, FTC, *Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress* at 40-41, excerpts attached hereto as Exhibit JJ (emphasis added).²⁹ These facts are relevant not only to the issue of preemption under the CAN-SPAM Act (*see infra* Legal Argument § I), but further demonstrate why the CPR Act imposes an undue burden on interstate commerce and an undue restriction on commercial speech. *See infra* Legal Argument §§ II & III.

X. THE CPR ACT IS LIKELY TO DO MORE HARM THAN GOOD

The Registry creates a readily available list of valid email addresses, particularly those which belong to and/or are accessible by Utah minors. Such a list would be an extremely valuable commodity. *See, e.g.*, 2004 FTC Report at 16-17 (“[A] list of valid email addresses is extremely valuable—far more valuable than a list of working telephone numbers. . . . [T]here seems to be a consensus that while a list of unconfirmed email addresses is valuable to spammers, a list of *live* email addresses would be a gold mine.”).³⁰ If such a list were to get into the hands of unscrupulous spammers the addresses on the Registry would be inundated with the very spam messages they seek to avoid. There are a number of different ways in which the

²⁹ *See also* 2004 FTC Report at 34 (“[W]e conclude that any Do Not Email Registry that earmarked particular email addresses as belonging to children would raise very grave concerns . . . The possibility that such a list could fall into the hands of the Internet’s most dangerous users, including pedophiles, is truly chilling.”); October 25, 2005, Letter from FTC Staff to The Honorable Angelo “Skip” Saviano, State Rep., 77th Dist., Ill. House of Reps. (“Saviano Letter”), attached hereto as Exhibit KK (providing the FTC’s views on Illinois’ proposed child protection registry statute, noting that “[s]pammers are unlikely to honor any such registry of prohibited contacts and may, in fact, misuse such a list to spam the children on it,” and cautioning that the creation of a child protection registry “may provide pedophiles and other dangerous persons with a potential list of contact points for Illinois children, and may actually increase the amount of spam sent to those addresses, including adult content.”).

³⁰ *See also* Mar. 10 FTC Tr. at 6-8 (comments of Elizabeth Treanor, National Retail Federation, and Scott Richards, MBNA); *id.* at 30-31 (comments of Steve Richter, E-mail Marketing Association); *id.* at 44-45 (comments of John Collingwood, MBNA); Saviano Letter at 7-8 (Exhibit KK).

Registry could be exposed, and those within the industry agree that spammers will stop at nothing to obtain and misuse the list.³¹ See 2004 FTC Report at 18; Saviano Letter at 7-9 (Exhibit KK).

A. The Registry May Be The Target of Internal Subversion

One way the Registry may be misappropriated is through internal theft. See Rubin Rep. at 6-7 & 10; see also Matt Bishop, *Issues for a "Do Not Email" List* ("Bishop Rep.") at 2-3, excerpts attached hereto as Exhibit NN. As a practical matter, the entire Registry will have to be maintained on defendant Unspam Registry Services, Inc.'s ("Unspam") computer network, and will be accessible to at least some of its personnel.³² Similarly, each of the legitimate email marketers who actually comply with the statute and scrub their internal lists against the Registry will need to maintain an internal list of those email addresses known to be on the Registry, and these sub-sets of the Registry will be accessible to at least some personnel of each legitimate

³¹ Breaches in the security of government maintained data are not uncommon. In 2004, a hacker accessed the personal information of 7,000 Weber State University students. See Stephen Speckman, *FBI May Look Into Hacker Case at U*, Deseret Morning News, Aug. 11, 2005, www.deseretnews.com/dn/view/0,1249,600154941,00.html. In August 2005, the University of Utah investigated the possible download of 100,000 social security numbers belonging to its former employees. See *id.* Just last month, the laptop of an employee from the Department of Veterans Affairs was stolen, compromising the names, birth dates and social security numbers of 26.5 million veterans. See Leslie Miller, *Data-theft concerns flood VA*, Deseret Morning News, May 27, 2006, www.deseretnews.com/dn/view/0,1249,635210845,00.html.

³² Unspam is the entity that has been contracted by the Division, pursuant to Utah Code Ann. § 13-39-201(1)(b), to implement and maintain the Registry. Through its co-founder and Chief Executive Officer, Matthew B. Prince, and with the assistance of Utah counsel, Unspam was one of the chief lobbyists for passage of the Utah CPR Act in the 2004 legislative session. Unspam has also been instrumental in the passage of a similar child protection registry statute in Michigan, and has entered into a contract with the others states, including Michigan, to provide database creation, database maintenance, and registry scrubbing services similar to that which it has contracted to provide the Division under the CPR Act. Unspam has developed its own proprietary software which it is using to create and maintain the Registry, and to perform the service of "scrubbing" email lists against the Registry. According to Unspam, one of the unique features of its proprietary software is the ability to take the registered email addresses and encrypt them through a process called "one-way hashing." Unspam's software is relatively new, however, and will be put to real time use for the first time in connection with the Utah Registry. There is no way to know for certain whether Unspam's software is truly secure, or whether the addresses maintained on the Registry may be compromised. To the best of the Amici's knowledge, the contract between Unspam and the Division does not require Unspam to conduct background checks of its employees, and Unspam does not otherwise guarantee against security breaches. See generally Unspam Contract.

email marketer. *See* Bishop Rep. at 3. Each of these persons becomes an attractive target for spammers and others seeking to purchase lists of knowingly valid email addresses, including those belonging to and/or accessible by minors, and there is no technological or other viable means of preventing this type of internal subversion. *See* Rubin Rep. at 6-7 & 10; Bishop Rep. at 3.³³

B. The Registry System May Be Abused by Spammers to Acquire Valid Email Addresses, Particularly Those Belonging To or Accessible By Utah's Minors

Cunning spammers could also obtain the list directly. To begin with, a spammer could hack into the computer network of Unspam, and obtain the entire Registry, or into the computer network of complying email marketers, and obtain a list of those email addresses previously identified as being on the Registry. Spammers could also use commonly available computer software to create a “directory” list³⁴ of hundreds of thousands of possible email address, pose as a legitimate email marketer, run its directory list against the Registry, and discover which of the potential email addresses are “live.”³⁵ *See* May 2, 2004, Edward W. Felten, *Report on the Proposed National Do-Not-Email Registry* (“Felten Rep.”) at 3-4, excerpts attached hereto as Exhibit OO; Bishop Rep. at 4; Saviano Letter at 9-10 (Exhibit KK).

³³ *See also* Feb. 11 FTC Tr. at 9-13 (comments of Cindy Cohn, EFF).

³⁴ A “directory” list is generated by commonly available computer software programs which use commonly known domain names, such as those belonging to major ISPs, major corporations, universities, etc., and generates a list of every possible email address on those domains. The program would start with last names, then first names followed by the last name, then first names followed by a dot and then the last name, and then the first letter of the first name followed by the last name, and so on and so forth until a large and comprehensive list of potential email addresses is generated. *See* Rubin Rep. at 9-10.

³⁵ Although the CPR Act prohibits the unlawful use and acquisition of the Registry (*see* U.C.A. § 13-39-301(2)(2006)), these provisions are not likely to deter the most unscrupulous spammers, and will be difficult to enforce.

Finally, spammers could use a variety of “phishing”³⁶ techniques to steal the address before it ever makes its way onto the Registry. By way of example, a phisher could develop a bogus website that looks and feels like the official Registry site. *See* Rubin Rep. at 13. The phisher could re-direct those seeking to register away from the official site, and collect live email addresses directly on its own dummy site. *See id.* A sophisticated phisher might even act as a middle man, completing the registration so that Unspam would not notice a precipitous drop in registrations and thereby detect the scheme. *See id.* Although careful logging and monitoring by Unspam may ultimately detect that a number of registrations are coming from a single registration point, a number of live email addresses will have already been compromised. *See id.*

C. Unspam’s Security Measures Will Be Largely Ineffective

Unspam claims that it uses a number of technological tools to protect against disclosure, including one-way, cryptographic hashing and canary email addresses. Neither of these methods are fool proof, however, nor will they prevent misappropriation via the methods discussed above. *See* Saviano Letter at 10-12 (Exhibit KK). Unspam implicitly acknowledges as much in its contract with the Division. *See* Unspam Contract, Scope of Work, ¶ (3)(b) (“If Unspam becomes aware that the privacy or security of the registry has been compromised, Unspam shall inform the [D]ivision within 24 hours after Unspam becomes aware of the privacy or security

³⁶ “‘Phishers’ are Internet outlaws who collect personal information from consumers by masquerading as companies with whom the consumers have a business relationship.” 2004 FTC Report at 16, n. 76. “Phishing” is a term used to describe the situation where an attacker uses an email message and/or bogus website that looks and feels like a particular site and draws web traffic to the bogus website. *See* Rubin Rep. at 13. Such techniques are frequently used to obtain financial information from the customers of unsuspecting banking and other financial institutions, but have also been used to trick consumers into providing personal information by posing as the website of a legitimate business or governmental entity. *See* 2004 FTC Report at 16, n. 76. There has already been at least one known instance where a phisher used a website or email message and claimed to be the non-existent National Do Not Email Registry in an effort to obtain live email addresses. *See* Mar. 10 FTC Tr. at 14-16 (comments of Scott Silverman, Shop.org, and Steve Richter, E-mail Marketing Association).

compromise. . . . Unspam shall cooperate fully with the Division to inform the public about any privacy or security compromise.”).³⁷

Cryptographic hashing³⁸ is basically a method for “anonymizing” an address, so that “the original address cannot be recovered from the anonymized version.” Felten Rep. at 3-4, n. 2. Even a hashed Registry, however, would be extremely valuable to a spammer. *See* Rubin Rep. at 8-10. Once the hashed email list is obtained using any of the previously discussed methods, all the spammer has to do is hash its own list of candidate email addresses and compare the candidate list against the Registry to determine which of the spammer’s candidate emails are “live” email addresses. *See* Rubin Rep. at 8; *see also* Mar. 15 FTC Tr. at 13 (comments of Jerry Popek, United Online). Using a standard 1 Ghz Pentium computer, the spammer could hash millions of candidate email addresses in a matter of seconds, and thereby quickly and inexpensively determine which ones are “live.” *See* Rubin Rep. at 8. This is a relatively unsophisticated process for those with a basic understanding of computer programming, including many spammers. *See id.* at 3-4, n. 2.

³⁷ The Unspam Contract contains general indemnification and warranty provisions whereby Unspam “warrant[s] and assume[s] responsibility for all products,” including software, and agrees “to indemnify, save harmless, and release the State of Utah, and all of its officers, agents, volunteers, and employees from and against any and all loss, damages, injury, liability, suits, and proceedings arising out of the performance of the contract which are caused in whole or in part by the negligence of [Unspam’s] officers, agents, volunteers, or employees.” Unspam Contract at ¶¶ 7 & 15. The incorporated Scope of Work specifically states, however, that “Unspam has no duty to ensure that” those comparing their email list against the registry “will not misappropriate the data received.” *See id.*, Statement of Work, ¶ (1)(g)(iii).

³⁸ Hashing refers to the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. *See* www.whatisit.techtarget.com. Hashing is used both for accessing data and for security. *See* www.webopedia.com. Using an algorithmic formula, each registered email address is given a “hash value” (also called a “message digest”) which is essentially a number generated from the string of text and characters that makes up the email address. *See id.* The hash value is generated in such a way that it is extremely unlikely that another email address will produce the same hash value, and difficult to recreate the original text. *See id.*

A spammer could also use publicly available software to create a directory list of potential email addresses and compare a hashed version of that list against the stolen, hashed Registry list to identify valid addresses. *See id.* at 9. A program running on a 1 Ghz Pentium computer could generate hundreds of millions of directory addresses, hash them, and compare them to the Registry in a matter of minutes. *See id.* at 10. Such a program could be left to run indefinitely, recording every time it generates a live email address. *See id.*

Canary addresses are invalid, random looking email addresses which are not distributed or used for any purpose. *Id.* at 12. Sometimes called *decoys* or *honeytokens*, canary addresses are placed on the Registry and monitored on a regular basis. *Id.* If a canary address begins to receive spam messages, it is a good indication that security has been breached, and that the Registry has been compromised. *See id.* By the time detection occurs, however, those who have registered are already being inundated with the very spam the CPR Act is designed to avoid. *See id.* Canary addresses therefore do nothing to improve the ultimate security of the Registry, and will not prevent spam from being sent to compromised addresses once a leak has occurred. *See id.*

D. The State of Utah Specifically Recognizes The Security Risks Inherent in the Registry System

The Utah Legislature specifically acknowledged these potential security risks and concerns, expressly requiring them to be disclosed to potential registrants:

The division shall provide a disclosure to a person who registers a contact point under this section that reads: ***“No solution is completely secure. The most effective way to protect children on the Internet is to supervise use and review all email messages and other correspondence. . . . While every attempt will be made to secure the Child Protection Registry, registrants and their guardians should be aware that their contact points may be at a***

greater risk of being misappropriated by marketers who choose to disobey the law.”

U.C.A. § 13-29-201(3)(c) (emphasis added).³⁹

The considerable security risks inherent in the Registry Act undermine the fundamental purpose of the statute, and further demonstrate why the statute imposes an undue burden on interstate commerce and unduly restricts commercial speech. *See infra* Legal Argument §§ II & III.

XI. THERE ARE OTHER LESS RESTRICTIVE ALTERNATIVES TO PROTECT UTAH’S MINORS FROM UNWANTED EMAIL CONTENT

There are a number of alternative means by which a minor’s access to potentially harmful and offensive email content may be restricted that do not impose undue burdens on interstate commerce or unduly restrict free speech and expression. First, parents can monitor their children’s computer and Internet activities, and screen email messages to identify and delete any potentially offensive material. The State of Utah could implement education policies and programs focused specifically on the harm of spam to children to help parents exercise these controls.⁴⁰

Second, major commercial Internet Service Providers (“ISPs”) such as Microsoft, America Online, Earthlink, etc., already provide features that subscribers may use to block unwanted email messages based on content, and thereby prevent children (and others) from receiving unwanted information. Computer owners and private network operators can also acquire private software applications commonly referred to as “filters” or “spam-blockers” to

³⁹ The Division has posted a similar warning and disclaimer on the Registry’s website. *See* www.utahkidsregistry.com, attached hereto as Exhibit CC.

⁴⁰ According to the FTC, consumer education is one of the most effective tools against spam. *See* 2005 FTC Report at iii.

effectively block unwanted messages and control the content of messages being delivered to the in-boxes on their systems.⁴¹ Parents could be encouraged to implement such tools on their home computers, and public institutions that provide email access to children could be required by law to implement such tools to block spam deemed harmful or inappropriate for minors. The state could also fund research or provide tax and other economic incentives for private companies to develop more advanced filtering technologies aimed specifically at pornography and other materials deemed harmful or inappropriate for minors. Each of these alternatives, while not perfect, constitutes a far less restrictive and considerably more reasonable alternative means of protecting Utah's children than the far-reaching and equally imperfect restrictions of the CPR Act, and do not impose the added security risks inherent in any centralized registry system. The existence of such viable alternatives establishes the CPR Act as an unconstitutional abridgment of commercial speech. *See infra* Legal Argument § III.

⁴¹ These tools have improved dramatically since the passage of CAN-SPAM in 2003, and have become a highly effective tool in blocking unwanted spam. *See* 2005 FTC Report at 13 (“The Commission staff’s independent research confirms that recipients’ ISPs can now effectively block or filter the vast majority of spam messages.”); *id.* at iii (“Tools available from ISPs and commercially available software, combined with the protections inherent in [CAN-SPAM], can significantly reduce the chance that consumers, especially children, will be assaulted by pornography distributed via spam.”); *see also* July 27 FTC Tr. at 11-13 (comments of Jerry Ceresale, DMA) (“[W]e understand from some of the big ISPs that they now have new and better techniques at filtering . . . I also think the technology, the filtering technology has improved dramatically since the CAN-SPAM Act was passed.”); *id.* at 23-24 (comments of Quinn Jalli, Digital Impact) (“I think filtering on the ISP level has become much more intelligent. . . . I think we’re seeing a move towards a much more intelligent and Bayesian approach to filtering that is working in the favor[] of legitimate Email marketers and forces I believe the [il]legal players to either get out of the market because the cost of playing has risen or forces them to take actions that are less efficient.”).

LEGAL ARGUMENT

I. THE CPR ACT IS PREEMPTED BY SECTION 7707(B) OF THE FEDERAL CAN-SPAM ACT

The Amici agree with the FSC that the CPR Act is preempted by Section 7707(b) of CAN-SPAM. *See* FSC Mem. at 10-17. The Supremacy Clause of the United States Constitution invalidates and preempts not only those state laws that conflict directly with the Constitution or laws of the United States, but also those (a) that attempt to regulate a field over which Congress has manifested an intent, express or implied, to occupy at the exclusion of the individual states, and (b) which serve to frustrate the fundamental purposes of a federal statutory scheme. *See, e.g., Cipollone v. Liggett Grp., Inc.*, 505 U.S. 504, 516 (1992); *Silkwood v. Kerr-McGee Corp.*, 646 U.S. 238, 248 (1984). The purpose of Congress in enacting the federal regulation is the “ultimate touchstone” in determining whether a state statute is preempted. *Cipollone*, 505 U.S. at 516.

Congress passed CAN-SPAM in direct response to the varied efforts of numerous individual states to regulate and control commercial email messages. Recognizing that email transcends state and even national boundaries, and that various state enactments led to a surge of different and often conflicting standards, Congress determined that a uniform, national system of regulation was required. *See* S. Rep. No. 108-102 at 21-22 (stating that “one national standard . . . is essential to resolving the significant harms from spam,” that the interstate nature of email makes it difficult to determine which individual state statutes to comply with, and that CAN-SPAM therefore “supercede[s] state and local statutes . . . that expressly regulate the use of

email.”).⁴² Congress therefore manifested a clear and unequivocal intent to control the regulation of email on a national level, and to preempt *any* state statute that attempts to control the sending of commercial email messages: “This chapter supersedes *any statute, regulation, or rule of a State . . . that expressly regulates the use of electronic mail to send commercial messages. . . .*” See 15 U.S.C. § 7707(b) (emphasis added).

There can be no serious dispute that the main focus of the CPR Act is the regulation of commercial email (*see* U.C.A. § 13-39-202(1)), and that the statute constitutes an attempt to expressly regulate the very type of email activity Congress sought to control *exclusively* on a national basis. *See infra* SOF, §§ II and III. The fact that the CPR Act now extends beyond email is wholly irrelevant,⁴³ and does not remove the CPR Act’s email provisions from the preemptive scope of CAN-SPAM.

Section 7707(b)(2)(B) exempts from preemption those state or local laws that “relate to acts of fraud or computer crime.” 15 U.S.C. § 7707(b)(2)(B). The Utah Legislature cannot invoke this exemption by simply labeling a violation of the CPR Act a “computer crime.” *See* U.C.A. § 13-39-301(1). The obvious purpose of CAN-SPAM’s computer crime exemption was to remove from preemption those state statutes that focus on and legislate against the

⁴² *See also* 15 U.S.C. § 7701(11) (“Many states have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but then states impose different standards and requirements. As a result they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.”); S. Rep. No. 108-102 at 13 (2003) (Congress has a “substantial government interest in regulating commercial e-mail on a Federal basis.”).

⁴³ As noted above, the CPR Act was recently amended, expanding the Registry to include other electronic “contact points” such as instant messaging IDs, cellular phone numbers, and other telephone numbers. *See* U.C.A. § 13-39-102(1)(b-c)(2006). The inclusion of these additional contact points does not change the fact that the CPR Act constitutes a direct regulation of email, however, and does not impact the constitutionality of the statute insofar as it applies to email.

growing use of computer technology to engage in otherwise criminal activity, and to protect computer users from would-be criminals who have chosen to use computer technology as a means of committing their crimes. The proper focus is therefore not on the labels used by a state in any given statute, but on the actual conduct which the state seeks to regulate and control. *Cf.* S. Rep. 108-102 at 22 (emphasis added) (“Section 8(b)(2) of the legislation clarifies that there would be no preemption of State laws that do not *expressly* regulate e-mail, *such as* common law, general anti-fraud law, and *computer crime law*.”).

The Utah Legislature enacted the Utah Computer Crimes Act in 1997. That statute, (which the Amici acknowledge to be exempt from the preemptive scope of CAN-SPAM), makes it unlawful for any person, “without authorization,” to “gain[] or attempt to gain access” to another person’s computer, and to then “alter[], damage[], destroy[], disclose[] or modify” that computer.⁴⁴ U.C.A. § 76-6-703(1). The definition of “computer crime” is specifically and narrowly targeted to protect the privacy and property rights of individual computer users from those using computer technology to interfere with, steal or otherwise alter their computer data and/or equipment, and is designed to, among other things, prevent identity theft, prevent hackers from pirating another person’s computer for their own use, etc. In sending a commercial email message to an address on the Registry, a legitimate email marketer neither “gains access” to nor “alters, destroys, damages, discloses or modifies” the recipient’s computer or any information

⁴⁴ “Computer crime” has been commonly defined as: (i) “deliberate actions to steal, damage, or destroy computer data without authorization, as well as accessing a computer system and/or account without authorization,” www.cyg.net/njblack.mo/dig.lib/glos; (ii) “[c]riminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored on-line data, or sabotage of equipment or data,” www.answers.com/topic/computercrime; and (iii) “the name given to any type of electronic fraud.” www.ballyclarehigh.co.uk/garden91/Glossary_FinalRW. The mere sending of a prohibited email to a registered address in violation of the CPR Act does not fit within these commonly accepted definitions.

stored thereon.⁴⁵ Accordingly, the mere sending of a prohibited email message under the CPR Act does *not* fit within the definition of a “computer crime” under Utah law.

Allowing state legislatures to twist the intent and purpose of the computer crime exception, and immunize a direct regulation on commercial email from the preemptive reach of CAN-SPAM merely by classifying a violation as a “computer crime,” would create a loop-hole which would swallow the rule, and effectively eviscerate the preemptive effect of Section 7707(b). The Utah Legislature should not be allowed to circumvent CAN-SPAM through such creative drafting, and enforcement of the CPR Act should be enjoined as an unconstitutional intrusion on federal regulation of commercial email.

II. THE CPR ACT VIOLATES THE COMMERCE CLAUSE OF THE UNITED STATES CONSTITUTION

The Amici also agree with the FSC that the CPR Act violates the Commerce Clause. *See* FSC Mem. at 17-20. Under the dormant commerce clause, a state law is unconstitutional *per se* where it regulates an area of interstate commerce that, by its unique nature, demands cohesive national treatment. *See Pataki*, 969 F. Supp. at 169; *Johnson*, 194 F.3d at 1160. State regulation of commerce is also unconstitutional if the state (a) seeks to regulate conduct occurring wholly outside of the state, (b) imposes burdens on interstate commerce which are clearly excessive when compared against the putative local benefits, or (c) discriminates against out of state businesses. *See Johnson*, 194 F.3d at 1160-61; *Pataki*, 969 F. Supp. at 169. Each of these constitutionally fatal conditions are implicated by the Utah CPR Act.

⁴⁵ Insofar as some unscrupulous spammer might use an email message as a conduit for a virus or other similar tool to accomplish such a task, his activity would be subject to separate prosecution under the existing Utah Computer Crimes Act. `

A. The CPR Act is Unconstitutional *Per Se* Because It Regulates Email, a Form of Interstate Communication and Commerce Demanding Cohesive National Treatment

The Internet undeniably represents an instrument of interstate communication, and is one of those unique areas of interstate commerce that requires consistent, uniform regulation at a national level. *See Pataki*, 969 F. Supp. at 173.⁴⁶ Uniformity is required not only for the regulation of web content, but also the regulation of one-to-one email communications which by their very nature cannot be confined within the boundaries of any one state. *See Johnson*, 194 F.3d at 1161 (quoting *Pataki*, 969 F. Supp. at 171) (“A state regulation ‘cannot effectively be limited to purely intrastate communications over the Internet because no such communications exist.’”). There can be no real dispute that insofar as the CPR Act applies to email it seeks to regulate and control communications over the Internet. *See* SOF §§ I-III. Accordingly, the CPR Act seeks to regulate a quintessential mode of interstate (and international) communication and commerce that required cohesive, uniform regulation at a national level.⁴⁷ *Id.* §§ II-III. The CPR Act therefore constitutes a *per se* violation of the commerce clause. To conclude otherwise would subject emailers to the vagaries, inconsistencies and outright conflicting provisions of multiple state regulatory schemes.

⁴⁶ *See also Pataki*, 969 F. Supp. at 169 (“The Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze the development of the Internet altogether. . . . The Commerce Clause ordains that only Congress can legislate in this area. . . .”); *id.* at 182 (“The Internet, like . . . rail and highway traffic . . . , requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. Regulation on a local level, by contrast, will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities.”); *American Book Sellers*, 342 F.3d at 103 (internal quotations omitted) (“Because the internet does not recognize geographic boundaries, it is difficult, if not impossible, for a state to regulate internet activities without projecting its legislation into other states. . . .”).

⁴⁷ States can no more feasibly regulate email on the Internet than they can regulate the sending of letters through our national postal system.

B. The CPR Act Regulates Conduct Occurring Wholly Outside of Utah

The CPR Act is also unconstitutional because it regulates conduct occurring wholly outside of the State of Utah. The critical inquiry in determining whether a statute has an extraterritorial effect is whether its “practical effect” is to control conduct wholly beyond its borders. *See Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989). In conducting this analysis, the court may consider how the statute interacts with the “legitimate regulatory schemes of other States and what effect would arise if not one but many or every state adopted similar legislation.” *Id.*; *see also Pataki*, 969 F. Supp. at 176 (inherent in the dormant commerce clause is a “need to contain individual state overreaching”; the need “arises not from any disrespect for the plenary authority of each state . . . but out of recognition that true protection of each state’s respective authority is only possible when such limits are observed by all states.”).

Johnson and *Pataki* are particularly instructive. In *Johnson*, the Tenth Circuit struck down a New Mexico statute attempting to prohibit the dissemination of communications via the Internet deemed harmful to minors. 194 F.3d at 1152. The court rejected the argument that the statute was only intended to apply intrastate. *Id.* at 1161. The court noted that Internet communications by their very nature “cannot effectively be limited to purely intrastate” activity, and that New Mexico’s statute therefore “represent[ed] an attempt to regulate interstate conduct occurring outside” of New Mexico. *Id.* *Pataki* involved a New York statute regulating the content of websites accessible by minors, particularly pornographic content. The statute was held unconstitutional because it had the “undeniable and impermissible” effect of projecting New York’s standards of decency on Internet users in other states. *Id.* at 177. Since New York could not limit Internet access to regulated websites by users in New York, even if those promoting

prohibited websites never intended those sites to be accessed in New York, the statute had the practical effect of regulating conduct wholly outside of New York's borders, despite the fact that it also had some effects within the state. *Id.*

As noted above, while the CPR Act purports to regulate only those unsolicited email messages that are sent to email addresses registered as belonging to or accessible by a Utah minor, the practical effects reach much farther. *See infra* SOF §§ III-V. Email messages, even those between residents of the same state, travel across various transmission lines and various computer networks in a variety of states before reaching the intended recipients. *Id.* §§ II and III. Email messages can also be received in any location, at any time, and a Utah resident may receive an email message while traveling in another state (or even country). *Id.*; *see also* Pataki, 969 F. Supp. at 171.

By their very nature, email addresses have *no* geographic designation, and email communications have *no* boundaries. *See infra* SOF §§ II-IV. Even where geographical information is collected by email marketers at the time of registration, there is no way for the sender to know, with any degree of reasonable certainty, that the information is valid or reflects the recipient's actual location at the time the message is sent and received. *Id.* §§ IV. Legitimate email marketers therefore have no choice but to either refrain from sending any potentially prohibited email message to any email address, in any state (as some email marketers have already elected to do), or bear the burden and expense of scrubbing their entire email list—including addresses belonging to non-Utah residents—at least once every 30 days.⁴⁸ *Id.* Under

⁴⁸ Although the amended CPR Act contains a consent defense, that defense requires “face-to-face” verification of the registrant's age. *See supra* note 24. Because the vast majority of registrations are submitted on-line, however

either scenario, the CPR Act projects its requirements on those conducting business outside of the state, and has an undeniable extraterritorial effect.

Many of the legitimate businesses which would run afoul of the CPR Act (e.g., online beer and wine sellers, wineries, casinos, alcohol related festivals,⁴⁹ etc.) are based wholly outside of the State of Utah, are not registered to do business in the State of Utah, and have no connection whatsoever to the State of Utah other than the fact that a few Utah residents may browse their websites or visit their locations while traveling. *See, e.g.,* Merchant Direct (Exhibit C); *see also* SOF §§ IV and V. The email address of a Utah resident may nonetheless find its way onto the email lists of these legitimate businesses, through online registration with the company itself, or with one of their various marketing partners. As such, even these largely out of state businesses will be required to scrub their lists against the Utah Registry at least once every 30 days, and to conform their email marketing practices to the requirements of Utah law.

The extraterritorial effect of the CPR Act will only be exacerbated as other states (like Michigan and Illinois) adopt and enforce similar registry systems. *See* SOF §§ V. Each of these states will apply their own restrictions on the types of commercial email messages that can be sent to minors, import their own definitions of the phrase “harmful to minors” (a definition which, by its very nature, requires an interpretation of local community standards), and mandate their own mechanisms and impose their own costs for scrubbing email lists against their

most legitimate businesses will be practically prevented from relying on this defense. *See id.*; *see also infra* Legal Argument § II(D).

⁴⁹ There are over 125 annual beer, wine or spirit festivals in the United States. *See, e.g.,* www.localwineevents.com/festivals/festival_list.php, attached hereto as Exhibit PP. Most of these festivals maintain websites that allow a visitor to register his or her email address (or that of a friend or relative) to receive future email communications about the event. *See, e.g.,* The Brewers Association (Exhibit G); Food & Wine Classic (Exhibit H); Sonoma Valley Film Festival (Exhibit M); and Napa Valley Mustard Festival (Exhibit N).

registries.⁵⁰ All of this will subject legitimate email marketers not only to inconsistent and potentially conflicting regulation, but to the draconian choice of either (a) paying the exorbitant cost to have their email lists scrubbed in as many as 50 different states, at least once per month, in perpetuity, or (b) having to self-censor all of their email messages and send only those that meet the standards of the most restrictive state. This would impose a burden on interstate commerce that is not only substantial, but wholly untenable.⁵¹

C. The CPR Act Imposes Substantial Burdens on Interstate Commerce That Are Clearly Excessive When Compared Against the Minimal Local Benefits

The CPR Act is unconstitutional because the burdens on interstate commerce are clearly excessive when compared to the putative local benefits. *Pike, Pataki and Johnson* are particularly instructive in the application of the balancing test utilized in a commerce clause challenge.

Pike involved an Arizona statute requiring that all cantaloupes grown in Arizona be systematically packed in the state before shipment or sale to any other state. *Id.* at 138. Bruce

⁵⁰ Cf. *Pataki*, 969 F. Supp. at 182 (“Courts have long recognized . . . that there is no single ‘prevailing community standard’ in the United States. Thus, even were all 50 states to enact laws that were verbatim copies of the New York Act, Internet users would still be subject to discordant responsibilities.”).

⁵¹ The FTC recently considered the effects of a child protection registry on interstate commerce and concluded that such statutes would unduly chill e-commerce throughout the United States:

The costs of complying with [Illinois] HB 0572, in addition to the potential for substantial criminal and civil liability for individual violations, may cause some legitimate marketers to consider ending mass email campaigns all together. The aggregate effect of HB 0572 might be to close off the legitimate email marketing of those products and services that it would cover, throughout the United States, not just for Illinois residents, and to all consumers, not just minors. Thus [Illinois] HB 0572 would likely have a greater effect on sellers that rely on email contact points in lieu of a physical presence in order to conduct business, such as a stand-alone Internet company. . . . The extra burden that [Illinois] HB 0572 would place on Internet sellers may, therefore, hamper a particularly competitive segment of merchants in those industries covered by [Illinois] HB 0572, curtailing the benefits of such competition to consumers.

Saviano Letter at 14-15 (Exhibit KK). These conclusions are persuasive and counsel in favor of a ruling that the CPR Act constitutes an unconstitutional intrusion on interstate commerce.

Church, Inc., in contravention of the Arizona statute, harvested cantaloupes in Arizona and shipped them 31 miles to its packing facility in California. *Id.* An Arizona official issued an order prohibiting the company from shipping its Arizona cantaloupes to California before they were packed. *Id.* Without available facilities in Arizona, the company faced imminent loss of its \$700,000 crop. *Id.* at 137. The district court enjoined enforcement of the order as an unlawful burden on interstate commerce. *Id.* The United States Supreme Court affirmed, recognizing that Arizona had a legitimate interest in protecting and promoting the quality and reputation of its melon produce, but holding that it would impose an undue burden on interstate commerce to require Bruce Church to build a \$200,000 packing facility in Arizona rather than ship its melons the short distance to its existing facility in California. *Id.*

In *Pataki*, the district court concluded that while New York's efforts to regulate the flow of pornographic information to minors over the Internet were laudable, the local benefits were not "overwhelming." *Id.* at 178. The court noted that the law had no effect on Internet content emanating from outside the United States, which constituted nearly half of the offensive content. *Id.* It further stated that even if New York could exercise criminal jurisdiction over parties whose only connection with the state was posting content on the Internet that might be viewed within the state, prosecution was "beset with practical difficulties." *Id.* at 178. The court therefore concluded that the New York statute "casts its net worldwide" and resulted in a "severe" and "extreme burden on interstate commerce" balanced against "attenuated" and "limited local benefits." *Id.* at 178, 181.

In *Johnson*, the Tenth Circuit held that the burden of a New Mexico statute criminalizing the computer dissemination of material deemed "harmful to minors" imposed burdens on

interstate commerce that outweighed any local benefits. *Johnson*, 194 F.3d at 1149, 1161-62. In so holding, the Tenth Circuit specifically adopted the rationale of *Pataki*. It also considered the cost of compliance, concluding that those costs imposed an undue burden on, and created “an invalid indirect regulation of interstate commerce.” *Id.* at 1162.

Few would disagree that Utah has a legitimate interest in protecting minors from exposure to harmful content (i.e., pornography). As discussed above, however, the burdens of the CPR Act also weigh heavily on legitimate interstate commerce. *See* SOF §§ V. To comply with the CPR Act, legitimate email marketers must either refrain from sending any potentially prohibited content to any email recipient, in any state, or bear the burden and expense of scrubbing their email lists against the Registry at least once every 30 days, *in perpetuity*. *Id.* §§ IV and V. Those who choose not to send any prohibited email messages will be forced to give up a lucrative source of revenue. *Id.* § V. For others, the cost of scrubbing against the Registry will be in the tens of thousands of dollars every year, *forever*, and will substantially increase the cost of their email marketing campaigns.⁵² *Id.* § V. These burdens are substantially greater than the significant but one time investment rejected by the United States Supreme Court in *Pike*, and comparable to those at issue in *Johnson* and *Pataki*. *Cf. also Pioneer Military Lending, Inc. v. Manning*, 2 F.3d 280, 284 (8th Cir. 1993) (one time cost of \$80,000, and annual costs of \$123,000, imposed a sufficient burden on interstate commerce to invalidate state regulations).

⁵² The only other way for legitimate businesses to forego the cost of scrubbing and still send their email messages is to invoke the newly created consent defense. *See supra* SOF § VII. This defense requires “face-to-face” verification of the registrant’s age, however, and because most registrations are obtained online, the defense itself imposes significant burdens on legitimate businesses. *See id.*; *see also supra* Legal Argument § II(D).

Contrasted against these significant burdens on interstate commerce, the local benefits of the CPR Act are minimal *at best*. *Id.* §§ VIII-X. As in *Johnson* and *Pataki*, a significant amount of the prohibited content comes not from legitimate email marketers who have an incentive and desire to comply with the law, but from spammers, including off-shore operators and pedophiles, who have become particularly adept at evading it. *Id.* § VIII. Nothing in the CPR Act enables the State of Utah to more effectively track down these less scrupulous spammers, or actually prevents their unwanted messages from being sent to Utah minors. As in *Pataki*, even if Utah could exercise jurisdiction over those out-of-state emailers who violate the law, prosecution would be difficult. Moreover, there are significant security concerns inherent in Utah's Registry that could expose the addresses on the Registry, and the Utah minors it is designed to protect, to even more unwanted and offensive content. *Id.* §§ IX and X. The minimal benefits of the CPR Act are significantly outweighed by the burdens in interstate commerce, rendering the statute unconstitutional under the dormant commerce clause.

D. The CPR Act Discriminates Against Out-Of-State Businesses

The CPR Act, as amended, exempts from liability those messages sent with consent to an adult user of a registered address. *See* U.C.A. § 13-39-202(4)(b) (2006). To take advantage of this exemption, however, the sender must, among other things, obtain written consent from the adult user in a "face-to-face transaction." *Id.* As discussed above, while local businesses may be able to meet these requirements, out of state businesses can not. *See infra* SOF § VIII. The CPR Act therefore imposes significant burdens on out-of-state businesses which are not equally imposed on local businesses, and discriminates against interstate commerce in violation of the dormant commerce clause.

III. THE CPR ACT IS IMPERMISSIBLY VAGUE AND THEREFORE VIOLATES THE DUE PROCESS CLAUSE OF THE FOURTEENTH AMENDMENT

The Fourteenth Amendment provides that “[n]o state shall . . . deprive any person of life, liberty, or property, without due process of law.” “It is a basic principle of due process that an enactment is void for vagueness if its provisions are not clearly defined.” *Faustin v. City & County of Denver*, 423 F.3d 1192, 1201 (10th Cir. 2005) (quoting *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972)). A statute is impermissibly vague if it (1) “fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits;” or (2) “it authorizes or even encourages arbitrary and discriminatory enforcement.” *Hill v. Colorado*, 530 U.S. 703, 730 (2000).

As discussed in detail above, the CPR Act fails to define a number of key terms, preventing persons of ordinary intelligence from ascertaining the full scope of its prohibitions, and understanding exactly what email communications are prohibited. *See* SOF § VI. The lack of clarity is evidenced not only on the face of the language, but by the potentially disparate interpretations provided by the Division. *Id.* The inherent vagueness invites disparate interpretations by the various state and local agencies that will be charged with enforcing its provisions, including the Attorney General’s office, the Division, and local district attorneys and law enforcement agencies, not to mention the innumerable state court judges who may be asked to interpret its provisions by plaintiffs’ lawyers seeking a quick settlement and/or award of attorneys fees. *Id.* The CPR Act is therefore unconstitutionally vague, as a matter of law, in violation of the due process clause of the Fourteenth Amendment.

IV. THE CPR ACT UNDULY CHILLS THE FIRST AMENDMENT RIGHTS OF LEGITIMATE EMAIL MARKETERS

The CPR Act restricts commercial speech based solely on content. Such restrictions “are subject to at least an ‘intermediate’ level of scrutiny.” *Utah Licensed Bev. Ass’n v. Leavitt*, 256 F.3d 1061, 1066 (10th Cir. 2001) (quoting *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm’n*, 447 U.S. 557 (1980)). The government must therefore establish that “(1) it has a substantial state interest in regulating the speech, (2) the regulation directly and materially advances that interest, and (3) the regulation is no more extensive than necessary to serve the interest.” *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224, 1233 (10th Cir. 1999) (quoting *Revo v. Disciplinary Bd. of the Supr. Ct. for the State of N.M.*, 106 F.3d 929, 932-33 (10th Cir. 1993).

No one disputes that the State of Utah has a substantial interest in preserving the sensibilities of minors, and protecting them against certain email messages that may unwittingly encourage them to engage in unlawful activity or otherwise be “harmful to minors.” The CPR Act nonetheless violates the First Amendment because it does not directly or materially advance these interests, regulates more speech than is necessary, and imposes an undue burden on legitimate email marketers.

A. The CPR Act Does Not Directly or Materially Advance the State’s Interest in Protecting Minors

The government bears the burden of demonstrating “that the harms it recites are real and that its restriction will in fact alleviate them to a material degree.” *Utah Licensed Bev. Ass’n*, 256 F.3d at 1071 (quoting *Edenfield v. Fane*, 507 U.S. 761, 768 (1993)). “This burden ‘is not satisfied by mere speculation or conjecture,’” *id.* (quoting *Edenfield*, 507 U.S. at 768), and “[a] speech regulation ‘may not be sustained if it provides only ineffective or remote support for

the government's purpose.'" *Id.* at 1071 (quoting *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 188 (1999)).

The State of Utah cannot meet its burden. First, the CPR Act will prevent email messages only from legitimate email marketers. As recognized by the FTC and the industry professionals who have explored the problem, centralized registries will be wholly ineffective at prohibiting spammers and other less scrupulous persons, including off-shore emailers and pedophiles, from continuing to send prohibited messages to registered addresses. *See* SOF § VIII. Because these email users are likely to send the most disturbing and damaging email messages, the CPR Act will do little to protect Utah's minors from the most harmful email content, and will have a minimal impact on the problem the state seeks to solve. *Id.*

Second, the CPR Act draws an irrational distinction between email and other types of commercial speech, prohibiting email advertisements, but doing nothing to protect Utah's minors from the same content in the mainstream media or on the World Wide Web. Nothing in Utah law prohibits television, radio, newspaper and billboard advertisers from marketing, gambling and other products and services which cannot be lawfully purchased by minors. Indeed, Utah's minors are bombarded by billboards all along Interstate-15 that advertise everything from beer to gambling, daily radio advertisements for local private clubs and the Nevada and Idaho casinos just across the Utah border, and television commercials promoting, among other things, alcohol and gambling. Many of these advertisements contain sexual content and innuendo. The World Wide Web (which studies show a majority of Utah's teenagers access almost daily) is likewise filled with pop-up ads, banner ads and hyperlinks advertising and promoting the very same products or services prohibited by the Utah CPR Act when they come to the minor via email.

The CPR Act makes an irrational and unsupported distinction between email and these other forms of advertising, and constitutes a minimal and ineffective first step at protecting Utah’s minors. *See Utah Licensed Bev. Ass’n*, 256 F.3d at 1071-72 (striking down a Utah statute prohibiting the advertisement of certain liquors in part because the “ban on the advertising of only certain kinds of alcohol beverages is irrational, and consequently, unconstitutional”).

Third, and most troubling, there are a number of security and privacy threats inherent in any centralized registry system which actually increase the likelihood that Utah minors will be exposed to harmful and inappropriate email content. *Id.* §§ IX and X. These security risks substantially dilute the already minimal benefit the CPR Act may have in protecting Utah minors.

B. The CPR Act is Not Sufficiently Tailored to Meet the State’s Interest in Protecting Minors

The State bears the burden of establishing that its regulation is sufficiently tailored to its desired objectives, and “a regulation of [commercial] speech cannot be sustained unless there is evidence that the state “‘carefully calculated the costs and benefits associated with the burden on speech imposed” by the regulations.’” *Utah Licensed Bev. Ass’n*, 256 F.3d at 1075 (quoting *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525 (2001) (quoting *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993))). There must be “a fit” between the restriction and the desired objectives—“a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is in proportion to the interest served.” *Id.* (quoting *Bd. of Trs. v. Fox*, 492 U.S. 469, 480 (1989)). While “the government need not employ the least restrictive means to accomplish its goal,” *id.*, “[t]he availability of less burdensome alternatives . . . signals that the fit between the legislature’s ends and the means chosen to

accomplish those ends may be too imprecise to withstand First Amendment scrutiny.” *Id.* (quoting *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 539 (1996)). A regulation on commercial speech “must be a last—not first—resort.” *Thompson v. Western States Med. Ctr.*, 535 U.S. 357, 373 (2002).

As discussed above, the CPR Act is overbroad and unduly regulates commercial speech because it prohibits speech between adults, including adult users of the registered email addresses who are entitled to and/or specifically request the content.⁵³ *See* SOF § VII. The CPR Act also imposes a significant burden and expense on legitimate email marketers. *Id.* § VI. The cost of compliance, and its potentially significant impact on First Amendment rights, are not justified by the minimal protection the CPR Act affords to Utah’s minors. *Id.* § VIII-X. This evidences a total failure by the State of Utah to make a “careful calculation” of the costs associated with its restrictions on free speech, rendering the CPR Act unconstitutional as a matter of law.

Finally, there are a number of available alternative means by which a minor’s access to offensive email material may be controlled—including but not limited to filtering technology and parental education, supervision and control—that do not involve the government imposed burdens on free expression inherent in the CPR Act.⁵⁴ *Id.* § XI. There is no evidence that the Utah Legislature even considered these other available alternatives prior to enacting the CPR

⁵³ *Cf. also Reno*, 521 U.S. at 875 (quoting *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 74-75 (1983) (“[W]e have repeatedly recognized the governmental interest in protecting children from harmful materials. . . . But that interest does not justify an unnecessarily broad suppression of speech addressed to adults. . . . Regardless of the strength of the government’s interest in protecting children, ‘the level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox.’”); *American Booksellers*, 342 F.3d at 96 (“Restrictions aimed at minors may not limit non-obscene expression among adults.”)).

⁵⁴ *See also American Booksellers*, 342 F.3d at 102 (citing *Reno*, 521 U.S. at 877) (recognizing filtering technology as a viable alternative to regulation of Internet content).

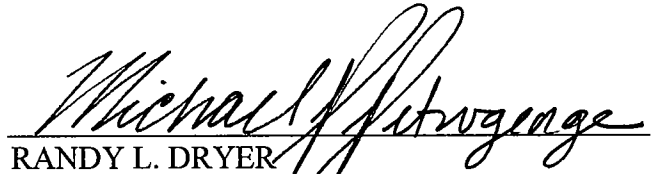
Act, strongly indicating that there is not a rational “fit” between the CPR Act and the State’s desire to protect minors. *See U.S. West*, 182 F.3d at 1238-39 (a state’s “failure to adequately consider an obvious and substantially less restrictive alternative . . . indicates that it did not narrowly tailor the [regulation]” to meet its goal); *see also Thompson*, 535 U.S. at 373 (regulation must be “last—not first—resort”). The fit is even more attenuated given the significant security and privacy risks inherent in any centralized registry system, and the risk that the CPR Act will actually result in more unwanted and offensive email content being sent to the registered addresses. *See* SOF §§ VIII-X. All of this supports the conclusion that the CPR Act is not sufficiently tailored to the purposes it purports to achieve, rendering it unconstitutional as a matter of law under the First Amendment.

CONCLUSION

The CPR Act imposes significant burdens on legitimate email marketers and other legitimate businesses across the country and will be largely ineffective in protecting Utah’s minors from unwanted, offensive and harmful email content. The practical effect of the statute will be to significantly increase the costs of engaging in e-commerce on a nationwide basis and/or chill the commercial speech of legitimate email marketers nationwide. The CPR Act will not result in any significant reduction in the amount of offensive or harmful email content that is actually sent to and received by Utah’s minors, and may in fact increase the prominence of such messages in the in-boxes of the registered accounts. The CPR Act constitutes a significant and unjustified intrusion on Congress’ authority both under CAN-SPAM and the Commerce Clause of the United States Constitution, violates the due process protections of the Fourteenth Amendment, and significantly infringes on the First Amendment rights of those legitimate

businesses who engage in e-commerce on a national (if not international) basis. This Court should therefore grant FSC's motion for preliminary injunction, and enter an order enjoining enforcement of the CPR Act, and striking it down as an unconstitutional enactment.

DATED this 16th day of June, 2006.

A handwritten signature in black ink, reading "Michael P. PetroGeorge", is written over a horizontal line.

RANDY L. DRYER

MICHAEL P. PETROGEORGE

PARSONS BEHLE & LATIMER

Attorneys for Amici Curiae American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, Inc., Email Service Provider Coalition, Electronic Frontier Foundation, Center for Democracy & Technology

CERTIFICATE OF SERVICE

I hereby certify that on this 16th day of June, 2006, I caused to be served, via U.S. Mail, postage prepaid, a true and correct copy of the foregoing **BRIEF OF AMICI CURIAE IN SUPPORT OF PLAINTIFF FREE SPEECH COALITION'S MOTION FOR PRELIMINARY INJUNCTION, *with exhibits***, to:

Jerome H. Mooney
JEROME H. MOONEY LAW
50 W. Broadway #100
Salt Lake City, Utah 84101

Attorneys for plaintiff Free Speech Coalition

Thomas D. Roberts
Assistant Utah Attorney General
160 East 300 South #500
P.O. Box 140857
Salt Lake City, Utah 84111

Attorneys for defendants Mark Shurtleff and Thad Levar

Brent O. Hatch
T. Parker Douglas
HATCH JAMES & DODGE
10 West Broadway #400
Salt Lake City, Utah

Attorneys for defendant Unspam

David L. Peterson
6195 Dry Creek Circle
Highland, Utah 84003-3008

Attorney for amici curiae the American Center for Law & Justice, the Utah Parent Teacher Association, Utah Senators Gregory Bell, D. Chris Buttars, Mike Dmitrich, Scott Jenkins, Mark Madsen, Ed Mayne, Howard Stephenson and John Valentine, and Utah Representatives J. Stuart Adams, Jeff Alexander, Sheryl Allen, Roger Barrus, Ron Bigelow, Bud Bowman, David Clark, David Cox, Greg Curtis, Margaret Dayton, Brad Dee, Lorie Fowlke, Kerry Gibson, Kory Holdaway, Fred Hunsaker, Bradley Johnson, Brad King, Bradley Last, M. Susan Lawrence, John Mathis, Karen Morgan, Michael Morley, Michael Noel, Curtis Oda, Patrick Painter, Ross I. Romero, David Ure, Mark Walker and Larry Wiley

And that I also caused to be sent, via e-mail, a true and correct copy of the foregoing document, *without exhibits*, to:

Jerome H. Mooney
JEROME H. MOONEY LAW

Stephen F. Rohde
ROHDE & VICTOROFF
steve@rohde-victoroff.com

David L. Peterson
david.l.peterson@us.army.mil

Attorney for amici curiae the American Center for Law & Justice, the Utah Parent Teacher Association, Utah Senators Gregory Bell, D. Chris Buttars, Mike

Attorneys for plaintiff Free Speech Coalition

Thomas D. Roberts
Assistant Utah Attorney General
ThomRoberts@utah.gov

Attorneys for defendants Mark Shurtleff and Thad Levar

Brent O. Hatch
bhatch@hjdllaw.com
T. Parker Douglas
pdouglas@hjdllaw.com
HATCH JAMES & DODGE

Attorneys for defendant Unspam

Dmitrich, Scott Jenkins, Mark Madsen, Ed Mayne, Howard Stephenson and John Valentine, and Utah Representatives J. Stuart Adams, Jeff Alexander, Sheryl Allen, Roger Barrus, Ron Bigelow, Bud Bowman, David Clark, David Cox, Greg Curtis, Margaret Dayton, Brad Dee, Lorie Fowlke, Kerry Gibson, Kory Holdaway, Fred Hunsaker, Bradley Johnson, Brad King, Bradley Last, M. Susan Lawrence, John Mathis, Karen Morgan, Michael Morley, Michael Noel, Curtis Oda, Patrick Painter, Ross I. Romero, David Ure, Mark Walker and Larry Wiley

A handwritten signature in black ink, appearing to read "Michael Petrov", with a horizontal line drawn through the middle of the signature.