UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Policy Planning
Bureau of Consumer Protection
Bureau of Economics

March 31, 2006

The Honorable Carol Fukunaga
State Senator
Eleventh District
State Capitol
Honolulu, HI 96813

Re: HI SB 2200

Dear Senator Fukunaga:

The staff of the Federal Trade Commission's ("FTC" or "the Commission") Office of Policy Planning, Bureau of Consumer Protection, and Bureau of Economics[1] are pleased to respond to your letter of February 15, 2006, that asks for our views on Hawaii SB 2200 ("SB 2200" or "the bill"), a bill that appears to be designed to protect children from unwanted commercial messages that advertise products or services they are prohibited from purchasing or contain adult advertising or links to adult content. In particular, your letter solicited our expertise and opinion on whether SB 2200 would reduce the amount of unwanted emails and what impact the bill might have on Hawaii consumers and competition.

Hawaii SB 2200 would require the Hawaii Department of Commerce and Consumer Affairs ("the Department") to establish and operate a child protection registry and make it unlawful for a person to initiate any commercial message or communication to any registered contact point if the message or communication advertises products or services that a minor child is prohibited by law from purchasing, or if the message contains or advertises adult content or links to such content.

This letter briefly summarizes the Commission's interest and experience in consumer privacy and provides the staff's opinion regarding the possible impact of SB 2200 on consumers and competition. Based on our experience, our review of your letter, and SB 2200, the FTC staff have reached the following conclusions:

- Because existing computer security techniques are inadequate to prevent the abuse

[1] This letter expresses the views of the FTC's Office of Policy Planning, Bureau of Consumer Protection, and Bureau of Economics. The letter does not necessarily represent the views of the Commission or of any individual Commissioner. The Commission has, however, voted to authorize us to submit these comments.

of such a registry, SB 2200 may provide pedophiles and other dangerous persons with a list of contact points for Hawaii children.

- SB 2200 is unlikely to reduce the amount of email spam received by registered email addresses. Further, because such a registry cannot be effectively monitored for abuse, it may have the unintended consequence of providing spammers with a mechanism for verifying the validity of email addresses. This consequence may actually increase the amount of spam sent to registered children's addresses in general, including spam containing adult content.

- The proposed registry would likely impose substantial costs on legitimate email marketers. Combined with the prospect of substantial criminal and civil liability for individual violations, the extra burden that SB 2200 would place on Internet sellers may, therefore, hamper a particularly competitive segment of merchants in those industries covered by SB 2200, curtail the benefits of such competition to consumers, and cause consumers to no longer receive information that they value.

A brief summary of the Commission's history in consumer privacy and a detailed analysis in support of each of the FTC staff's conclusions is provided below.

I. Interest and Experience of the Federal Trade Commission

The FTC enforces Section 5 of the Federal Trade Commission Act, which broadly prohibits "unfair or deceptive acts or practices in or affecting commerce."[2] Protecting consumer privacy is a central element of the FTC's consumer protection mission.[3] In recent years, advances in computer technology have made it possible for detailed information about people to be compiled and shared more easily and cheaply than ever. These developments have produced many benefits for society as a whole and individual consumers.[4] At the same time, some consumers have expressed concerns about the compilation and sharing of their personal information and a desire to limit unwanted contacts from marketers that use such information. As personal information becomes more accessible, individuals and institutions have found it necessary to take precautions against the misuse of such information. In recent years the FTC has brought a number of cases to enforce promises in privacy statements, including promises

---

[2] 15 U.S.C. § 45.

[3] *See generally* FTC, PRIVACY INITIATIVES (2006), *at* http://ftc.gov/privacy/index.html.

[4] For example, it is easier for law enforcement to track down criminals, for banks to prevent fraud, and for consumers to obtain credit.

about the security of consumers' personal information.[5]

Under the Gramm-Leach-Bliley Act, the Commission has also implemented rules concerning financial privacy notices and the administrative, technical, and physical safeguarding of personal information and has enforced provisions against pretexting.[6] The Commission also protects consumer privacy under the Fair Credit Reporting Act[7] and the Children's Online Privacy Protection Act.[8] The FTC also educates consumers and businesses about the importance of personal information privacy and security.[9] In addition, the Commission provides Congress

---

[5] *See generally* FTC, ENFORCING PRIVACY PROMISES: SECTION 5 OF THE FTC ACT (2006), *at* http://ftc.gov/privacy/privacyinitiatives/promises.html. *See, e.g., Eli Lilly & Co.*, FTC Dkt. No. C-4047 (May 10, 2002) (settling charges relating to the unauthorized disclosure of sensitive personal information collected through the company's Prozac.com website), *available at* http://www.ftc.gov/os/2002/05/index.htm; *Microsoft Corp.*, FTC Dkt. No. C-4069 (Dec. 24, 2002) (settling charges relating to the privacy and security of personal information collected through the company's "Passport" web service), *available at* http://www.ftc.gov/os/2002/12/index.htm.

[6] 15 U.S.C. § 6801 *et seq.* (1999). *See generally* FTC, FINANCIAL PRIVACY: THE GRAMM-LEACH BLILEY ACT (2006), *at* http://ftc.gov/privacy/privacyinitiatives/glbact.html.

[7] 15 U.S.C. § 1681 *et seq.* (as amended 2003). *See generally* FTC, CREDIT REPORTING: THE FAIR CREDIT REPORTING ACT (2006), *at* http://ftc.gov/privacy/privacyinitiatives/credit.html.

[8] 15 U.S.C. § 6501 *et seq.* (1998). *See generally* FTC, CHILDREN'S PRIVACY: THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT (2006), *at* http://ftc.gov/privacy/privacyinitiatives/childrens.html. The Act requires operators of commercial web sites to: post a privacy policy on the web site's homepage and link to the policy on every page where personal information is collected; provide notice about the site's information collection practices to parents and obtain verifiable parental consent before collecting personal information from children; give parents a choice as to whether their child's personal information will be disclosed to third parties; provide parents access to their child's personal information and the opportunity to delete the child's personal information and opt-out of future collection or use of the information; not to condition a child's participation in a game, contest, or other activity on the child's disclosing more personal information than is reasonably necessary to participate in that activity; and maintain the confidentiality, security, and integrity of personal information collected from children.

[9] *See generally* FTC, ENFORCING PRIVACY PROMISES (2006), *at* http://www.ftc.gov/privacy/privacyinitiatives/promises.html; FTC, ID THEFT HOME (2006), *at* http://www.consumer.gov/idtheft/; FTC, FTC CONSUMER ALERT, SPYWARE (2006), *at* http://ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm.

with information and analysis regarding privacy issues.[10]

In recent years, the FTC's privacy agenda has included the Commission's "Do Not Call" Registry," which provides consumers with a simple, free, and effective means to limit unwanted telemarketing calls.[11] The Commission has also worked vigorously to combat mass email "spam," both before and after the enactment of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"),[12] through law enforcement against spammers, the education of consumers and businesses, and through continued study of the problem.[13] In addition, the Commission is in the process of completing rulemakings and reports required by CAN–SPAM.[14] The FTC has pursued a vigorous law enforcement program against deceptive spam and, to date, has brought 85 cases in which spam was an integral element of the alleged overall deceptive or unfair practice.

The Commission's recent report to Congress, *Subject Line Labeling As a Weapon Against Spam*, and the Division of Marketing Practices' recent report, *Email Address Harvesting and the Effectiveness of Anti-Spam Filters*, note that Internet Service Providers ("ISPs") have developed a number of technological options to sort, delete, or block unsolicited commercial email.[15] The Commission has also monitored the development of filtering technologies that consumers may use in their personal email accounts to sort, delete, or block unwanted commercial email that may contain age-inappropriate content, and has encouraged consumers to consider using such

---

[10] *See, e.g.*, Press Release, FTC, FTC Testifies on Data Security and Identity Theft (June 16, 2005), *available at* http://ftc.gov/opa/2005/06/datasectest.htm.

[11] *See generally* FTC, NATIONAL DO NOT CALL REGISTRY (2006), *at* http://ftc.gov/bcp/conline/edcams/donotcall/index.html.

[12] 15 U.S.C. § 7701 *et seq.* (2003).

[13] *See generally* FTC, SPAM, PRESS ROOM (2006), *at* http://www.ftc.gov/bcp/conline/edcams/spam/press.htm.

[14] *See generally id.*

[15] FTC, SUBJECT LINE LABELING AS A WEAPON AGAINST SPAM, A REPORT TO CONGRESS 10-12 (2005), *available at* http://www.ftc.gov/reports/canspam05/050616canspamrpt.pdf; FTC DIVISION OF MARKETING PRACTICES, EMAIL ADDRESS HARVESTING AND THE EFFECTIVENESS OF ANTI-SPAM FILTERS 5-6 (2005), *available at* http://www.ftc.gov/opa/2005/11/spamharvest.pdf. Examples include: customized filters that block out email messages containing words that occur more frequently in known spam; "blacklists" of Internet Protocols determined to be an open relay or proxy used by spammers; and "whitelists" of legitimate marketers that ensure legitimate, non-spam email is not blocked.

technologies.[16]

Notably, in one of the FTC's congressionally-mandated reports – a June 2004 report entitled *National Do Not Email Registry, a Report to Congress* ("Do Not Email Report")[17] – the Commission analyzed the issues identified in your February, 15, 2006, letter. In the Report, the Commission concluded that spammers would most likely use a registry as a mechanism for verifying the validity of email addresses and, without the ability to authenticate their identities, enforcement officials would be largely powerless to identify and pursue those responsible for misusing a registry. Thus, a registry would raise serious security, privacy, and enforcement difficulties, especially for children's email accounts.[18] A discussion of the Report's conclusions is provided below. FTC staff have also previously commented on another state proposal similar to SB 2200.[19]

II. Summary of SB 2200

Hawaii SB 2200[20] would require the Hawaii Department of Commerce and Consumer Affairs to "establish and operate, or contract with a qualified third party to establish and operate, the child protection registry."[21] Under the bill, "[t]he department or a third party administrator shall establish procedures, to the extent possible, to prevent the use or disclosure of protected

---

[16] *E.g.*, FTC, YOU'VE GOT SPAM: HOW TO "CAN" UNWANTED EMAIL 2 (2002), *available at* http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf.

[17] FTC, NATIONAL DO NOT EMAIL REGISTRY, A REPORT TO CONGRESS (June 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf. Specifically, CAN-SPAM required that the FTC transmit to Congress a report that: "(1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-Email registry; (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and (3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts." 15 U.S.C. § 7708. *See also* FTC, EFFECTIVENESS AND ENFORCEMENT OF THE CAN-SPAM ACT, A REPORT TO CONGRESS (Dec. 2005) ("Effectiveness and Enforcement Report"), *available at* http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

[18] *See generally* Do Not Email Report, *supra* note 17, at i-ii.

[19] FTC Staff Comment to the Honorable Angelo "Skip" Saviano Concerning Illinois HB 0572 to Create a Child Protection Registry (2005), *available at* http://www.ftc.gov/os/2005/11/051101cmtbill0572.pdf.

[20] Hawaii S.B. 2200, 23rd Leg. (2006), *available at* http://www.capitol.hawaii.gov/sessioncurrent/bills/SB2200_SD1_.pdf.

[21] *Id*. at § B(a).

contact points. . . ."[22] These contact points would include: instant message identities; wireless communications device numbers; fax numbers; email addresses; or other electronic addresses subject to rules adopted by the Department.[23] A parent, guardian, individual, school, or other institution responsible for a contact point to which a minor may have access may register that contact point with the Department.[24] Such a registration would last for up to three years and expire upon a minor's eighteenth birthday.[25]

Under SB 2200, "[a] person shall not send, cause to be sent, or conspire with a third party to send a message to a contact point that has been registered for more than thirty calendar days with the department if the primary purpose of the message is, directly or indirectly, to advertise or otherwise link to a message that advertises a product or service that a minor is prohibited by law from purchasing, viewing, possessing, participating in, or otherwise receiving."[26] The sending of such a message "is prohibited only if it is otherwise prohibited for the minor to purchase, view, possess, participate in, or otherwise receive the product or service."[27] The consent of a minor or third party to receive the message is not a defense.[28]

The bill would require the Department to establish a procedure to allow senders to verify compliance with the registry.[29] A person desiring to send a message containing content inappropriate for minors would need to pay the Department for access to this mechanism at a rate set by the Department based on the number of contact points checked against the registry, not to exceed .03 cents per contact point.[30] SB 2200 would also prohibit a person from releasing to

---

[22] *Id.*

[23] *Id*. at § A.

[24] *Id*. at § B(b), (d).

[25] *Id*. at § B(c).

[26] *Id*. at § D(a).

[27] *Id*. at § D(e).

[28] *Id*. at § D(c). It is not a violation if a person is merely an intermediary between the sender and recipient of a prohibited electronic message or unknowingly provides transmission of such a message over a computer network or facility. *Id*. at § D(d)(1)-(2).

[29] *Id*. at § B(f). *See also id*. at § (H) ("The department shall adopt rules . . . necessary for the purposes of this part.").

[30] *Id*. at § B(g). Such collected fees would be credited to a children's protection registry fund administered by the Department and to the Hawaii Attorney General in order to administer and conduct investigations, enforcement, and defense of the registry. *Id*. at §§ B(h), C(a)-(c).

another person information contained on the registry, selling or using the registry for any reason other than to meet the requirements of the bill, or accessing or attempting to access the registry except as provided under the bill.[31]

SB 2200 would make "an intentional or knowing violation" of the bill a computer crime punishable as a class C felony, in addition to any penalties authorized by the state's computer crime statute.[32] A civil action based on such a computer crime could also be brought by an authorized individual or the registrant of the contact point on behalf of a minor who has received a prohibited message, a person through whose facilities such a message was transmitted, or the Attorney General against a person who has violated the bill.[33] A person bringing such an action could recover actual damages including reasonable attorney's fees or, in lieu of actual damages, the lesser of five-thousand dollars per each message received or transmitted or two-hundred fifty-thousand dollars for each day the violation occurs.[34] In addition, SB 2200 would give the Hawaii Attorney General the power to investigate the business transactions of a person reasonably believed to have violated the bill.[35]

III. Effect of SB 2200 on Registered Children

A. SB 2200 May Provide Pedophiles and Other Dangerous Persons With a List of Contact Points of Hawaii Children

The registry proposed by SB 2200 would create an extensive directory of children's contact points that currently does not exist. As explained below, such a list cannot be effectively monitored for abuse.[36] By compiling such a list that cannot be effectively monitored for abuse,

---

[31] *Id*. at § E(a)-(c).

[32] SB 2200 at § F. *See also* HAW. REV. STAT. § 78 Part IX (2004).

[33] SB 2200 at § G(a)(1)-(3).

[34] *Id*. at § G(c)(1)-(2).

[35] *Id*. at § G(d).

[36] Recently, two states have established similar children's registries, the "Michigan Children's Protection Registry Act," MICH. COMP. LAWS § 752.1061 *et seq*. (2004) and the "Utah Child Protection Registry Act," UTAH CODE ANN. § 13-39-101 *et seq*. (2004). The Commission staff will continue to monitor these registries with regard to their effect on children's privacy. In its December, 2005, report to Congress, *Effectiveness and Enforcement of the CAN-SPAM Act*, the Commission reiterated that it "generally supports initiatives that protect children from inappropriate content, but state registries that maintain sensitive information belonging to children raise troubling issues." Effectiveness and Enforcement Report, *supra* note 17, at 39-41. Thus, the Commission continues to "caution against legislative action on the state

SB 2200 may provide pedophiles and other dangerous persons with a potential list of contact points of Hawaii children. As the Do Not Email Report concluded, "[t]he possibility that such a list could fall into the hands of the Internet's most dangerous users, including pedophiles, is truly chilling."[37]

Although difficult to quantify, the risk of a pedophile or other dangerous persons misusing the registry data to discover the contact point of a Hawaii minor is certainly real. First, such a list could be misused by registry personnel.[38] Second, such a list is subject to direct hacking by technologically sophisticated persons. Third, the Hawaii Attorney General's office is unlikely to be able to screen every single individual who might seek, or to whom it might provide, registry access. For example, it is unlikely that the state would be able to perform background checks on every employee of all marketing firms that may potentially misuse their access to such a registry. In sum, a central registry of children's contact points may provide pedophiles and other dangerous persons with a means of contacting those children.[39]

---

level to adopt registry-style laws in the hope they may effectuate improved protections for children in the online environment. The Commission believes that grave security and privacy concerns argue decisively against such measures." *Id*. Because Michigan and Utah have only recently established such registries, which became effective last summer, it may be useful for you to continue to evaluate their experiences once they have been in effect for several years.

[37] Do Not Email Report, *supra* note 17, at 33-34.

[38] As a computer security expert retained by the FTC explained:

> In the Computer Security field, it is well known that insider attacks account for the most loss in terms of proprietary data. While we have well-developed techniques for thwarting external attackers, for example, firewalls, intrusion detection systems, and virtual private networks, the state of the art at protecting against malicious insiders is currently dismal. Proprietary algorithms, code, and designs leak all the time. Industrial espionage is rampant, and theft of data by people with legitimate access is the most common form of loss known to today's corporations. This is why the hashed list of email addresses, which is such a valuable target, is almost certain to be compromised at some point if a Do Not Email registry is deployed. The technology does not exist to protect it against insiders.

AVIEL D. RUBIN, A REPORT TO THE FTC ON RESPONSES TO THEIR REQUEST FOR INFORMATION ON ESTABLISHING A NATIONAL DO NOT E-MAIL REGISTRY 11 (May 2004), *available at* http://www.ftc.gov/reports/dneregistry/expertrpts/rubin.pdf.

[39] Since the Commission's Do Not Email Report, there have been no technological advances that would alleviate the risk that pedophiles and spammers would misuse registry data. Effectiveness and Enforcement Report, *supra* note 17, at 40 n.164 (citing expert report of Mathew Bishop, Ph.D., Professor of Computer Science at the University of California ("UC") Davis and Co-Director of the UC Davis Computer Security Laboratory).

B. Email Addresses on the Proposed Registry are Unlikely to Receive Less Spam and May Actually Receive More Spam, Including Adult Content

1. A Registry Could Provide Spammers With a List of Valid Children's Email Addresses For Spam Marketing

As mentioned above, SB 2200 would create an extensive directory of active children's email addresses. As technology stands today, it is impossible to know whether any particular stated email address is actively used by an actual user, until it is tested to verify that it is valid.[40] A registry of email addresses, such as the one proposed by SB 2200, would eliminate that technological hurdle, one of the few remaining barriers that can slow spammers down.

Spammers would have significant incentives to attempt to obtain a copy of such a registry or portions thereof for two main reasons. First, spam marketers of products and services used by children (e.g., CDs, ringtones, clothing, video games) could use such a list to focus their spam marketing campaigns. According to a 2003 study conducted by Symantec Corp., 76 percent of children who use the Internet have one or more email accounts.[41] Such email accounts are attractive contact points for spam marketers, and marketers of products used by children would likely be willing to pay a premium to obtain a list of children's email addresses. Second, even spam marketers that do not specifically target children would find such a list valuable simply because the email addresses on it would have been verified as being valid and could, therefore, help a spammer to evade an anti-spam filter put in place by an Internet Service Provider ("ISP").[42]

Disturbingly, 47 percent of the children surveyed in the Symmantec study reported

---

[40] Do Not Email Report, *supra* note 17, at 1-12.

[41] The study, conducted by Symantec Corp. in June 2003, surveyed 1,000 children between the ages of seven and eighteen. *See* Press Release, Symantec, Symantec Survey Reveals More Than 80 Percent of Children Using Email Receive Inappropriate Spam Daily ("Symantec Survey") (June 9, 2003), *available at* http://www.symantec.com/press/2003/n030609a.html. The findings of the study are discussed in the Do Not Email Report, *supra* note17, at 33-34.

[42] As spammers send more messages, they necessarily increase the number of undeliverable messages coming from their Internet Protocol ("IP") addresses. ISPs, however, filter out all messages from an IP address from which a high number of undeliverable messages are sent. This filtering increases the probability that *all* of a spammer's messages from that IP address will not be delivered, including those messages that would have been delivered but for the undeliverable messages that were sent with them. By including in a marketing campaign a large number of known valid email addresses with email addresses of unknown validity, the spammer increases the odds that the ISP will deliver messages to the addresses of unknown validity. Do Not Email Report, *supra* note 17, at 18-19 n.93.

receiving spam with links to pornographic websites.[43] The Commission has found no data to suggest that spammers are currently targeting children to receive specific types of spam, however.[44] Rather, spammers appear to use indiscriminate marketing techniques, and, therefore, children generally receive the same types of spam that adults receive.[45] This fact is not surprising because spammers and others currently have no way of knowing that particular email addresses belong to children, unless the children have divulged their ages and email addresses, or otherwise indicated their minor status by signing up with an SB 2200-type registry. Thus, because such a registry cannot be effectively monitored for abuse, it may have the unintended consequence of providing spammers with a mechanism for verifying the validity of email addresses. This may actually increase the amount of spam sent to registered children's addresses in general, including spam containing adult content. To the extent that the registry may be misused to verify the validity of email addresses, such verified email addresses could then be re-sold to spam marketers in general, including spam marketers of adult content.

2. Existing Computer Security Techniques are Inadequate to Prevent the Abuse of Such a List

In its Do Not Email Report to Congress, the Commission analyzed three computer security techniques that registry proponents had claimed could significantly reduce the security and privacy risks associated with a registry of individual email addresses: (1) the centralized scrubbing of marketers' distribution lists; (2) the conversion of addresses to one-way hashes; and (3) the seeding of the registry with "canary" email addresses. As explained below, although each of these three techniques may reduce certain types of computer security threats, none of them can completely prevent the misuse of registry data.

---

[43] Symantec Survey, *supra* note 41. Notably, over 20 percent of children with email accounts open and read spam messages. *Id.* Even when children feel uncomfortable, offended, or curious after seeing inappropriate spam, 38 percent of them do not tell their parents. *Id.*

[44] When Commission investigators "seeded" 175 different locations on the Internet with 250 undercover email addresses, they found that the content of the resulting spam was unrelated to the location on the Internet from which the address was harvested. Consumer Alert, FTC, Email Address Harvesting: How Spammers Reap What You Sow (Nov. 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm. *See also* Do Not Email Report, *supra* note 17, at 34 n.187.

[45] According to one ISP, about thirty percent of all spam delivered to its subscribers' inboxes in January and February 2004 contained sexually explicit material or references. Do Not Email Report, *supra* note 17, at 32 n.174. The Commission found that 17 percent of pornographic offers in the spam it analyzed contained "adult imagery." FTC, FALSE CLAIMS IN SPAM, A REPORT BY THE FTC'S DIVISION OF MARKETING PRACTICES 13 (Apr. 30, 2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf.

a. Centralized Scrubbing Would Not Prevent Registry Misuse

Rather than distributing to email marketers copies of a registry that could then fall into the hands of pedophiles or other dangerous persons, some have proposed that a registry could instead require email marketers to submit their distribution lists to the registry to be scrubbed of registered contact points.[46] The state could then return a list purged of registered email addresses. But such centralized scrubbing would not prevent spammers from using the registry to obtain valid email addresses. Although central scrubbing by the registry might prevent spammers from obtaining a full copy of the registry, spammers would simply have to compare their pre-scrubbed and post-scrubbed lists for differences between them, and identify email addresses removed by the scrubbing. Thus, list scrubbing has a fatal flaw that, ironically, could allow spammers to verify addresses on their mailing lists. By repeatedly submitting lists of email addresses to a registry for scrubbing, spammers could potentially reconstruct a substantial portion of the registry.[47]

Although Hawaii could attempt to track the identities of marketers submitting their lists for scrubbing, in many cases the state would have no practical means of knowing whether persons making such submissions were misusing the registry data. Generally, a law-abiding marketer who purchased an email list and then submitted it to the registry for scrubbing would be indistinguishable from a malicious spammer who purchased the same list and then submitted it in order to validate addresses for future spamming. If a marketer who misused the registry for spamming purposes included its identity in the resulting violative spam the state could of course discipline such a marketer. This type of scenario is unlikely in the current context of technologically sophisticated and elusive spammers. Similarly, the state would generally have no practical way of preventing or detecting such a spammer from selling a validated email list to other spammers.

b. One-Way Hashing Would Not Prevent Registry Misuse

One-way hashing involves using cryptographic algorithms to transform a string of text into character strings called "hashes." In a hashed registry, a consumer could enter an email address on the registry using a web-based form. The state would then send a confirmation email to the consumer's email address. To activate the registration, the consumer would return to the registry's web site and enter a code appearing in the confirmation email. Upon activation of the registration, the state would convert the email address to a one-way hash using a publicly-known hashing algorithm. The entire registry would be stored as one-way hashes.[48]

---

[46] *See, e.g.*, Do Not Email Report, *supra* note 17, at 19 (noting that when the Commission solicited input for the Do Not Email Report, it received ten Request for Information ("RFI") responses proposing registries that use a centralized scrubbing mechanism).

[47] *Id*. at 19-20.

[48] For example, a consumer might register an email address, such as abc@ftc.gov. Then, using a securing hashing algorithm standard, the registry would convert the address into a

A marketer authorized to use an email registry would convert registered email addresses on its distribution list into hashes using the same hashing algorithm used by the registry. The marketer would also create a database identifying each original email address and its associated hash. The marketer would then submit its hashed distribution list to the state for scrubbing. The registry would compare the marketer's hashed distribution list to the hashed registry and return to the marketer a hashed distribution list purged of those hashes appearing on the registry. A legitimate marketer would then send messages only to those addresses that corresponded to hashes on the list returned by the state. An illegitimate spammer, however, could determine which of the addresses on its original distribution list were on the registry (and, therefore, are valid addresses) by comparing the hashed list submitted to the state with the scrubbed list of hashes returned by the state and determining the email addresses that corresponded to the purged hashes.[49]

It is virtually impossible using current computing and software technology to determine an original un-hashed text by analyzing the resulting hash. Thus, if someone obtained the registry of hashed email addresses, it is unlikely that the database could be un-hashed and turned back into a list of readable email addresses. Hashing may protect a registry from outside hackers by maintaining data in an encrypted form. But, although a hashed registry would provide some measure of security against a hacker, it would not protect against the likely threat of a spammer using the registry as a tool for validating email addresses.[50] In sum, whether un-hashed or hashed, centrally-scrubbed or distributed, the legitimate bulk emailer needs to know which addresses on its distribution list are on the registry. The inevitable corollary is that the illegitimate spammer can use the registry to deduce valid email addresses through comparison.

---

hashed form, such as 5519e3f2ba5aef2dead64f72cf31507e88d6eb23, and add it to the registry.

[49] A spammer with little technical sophistication could easily convert millions of email addresses to hashes in seconds using a standard desktop computer. Do Not Email Report, *supra* note 17, at 21-22 n.105.

[50] As a computer security expert retained by the Commission explained:

> Cryptographic hashing can be thought of as a method for "anonymizing" an address . . . that helps to protect the original list from becoming a source of new addresses for spammers. However, due to the mathematical properties of cryptographic hashes, it is still possible for a person who knows an email address to tell whether that address is on the anonymized list. So a system based on cryptographic hashes is roughly equivalent . . . to one that allows emailers to query a centralized database to check whether particular addresses are on the list.

Id. at 22. Another computer security expert retained by the Commission explained that "hashing provides absolutely no security against a marketer who obtains a scrubbed list and uses [it] to sell the addresses that were scrubbed by the Registry." *Id*. at n.106.

c. Seeding the Registry Would Not Prevent Misuse

The Do Not Email Report also analyzed the utility of seeding a registry with secret, registry-controlled addresses designed to detect spammers ("canary addresses").[51] To ensure that emails received by canary addresses would be true indicators of registry misuse, each canary address would have to be extremely unlikely to receive spam, absent a registry violation. In other words, the canary addresses could not already be circulating on email lists on the Internet and would need to include characters unlikely to be generated by a computerized dictionary attack program.[52] For instance, using a random character generation program, the Commission could establish the email address "25ce12a4@federaltcommiss.com." The address would be monitored constantly. Any email sent to the canary address would indicate a misuse of the registry.

Seeding a registry with canary addresses may aid the detection of the outright hacking of an un-hashed registry, if such an address obtained through hacking then receives spam. But it is unlikely that seeding could prevent spammers from misusing a registry through the submit-and-compare technique. A canary address would not be circulating on a spammer's pre-scrub email lists outside the registry, absent a direct hack, and would include character strings unlikely to be created by a dictionary attack program. Therefore, with a hashed registry, a canary address would never receive a spam message, preventing the detection of a misuse of the registry.[53]

Moreover, although the receipt of email by a canary address may make it possible to detect the misuse of a registry it could not prevent such abuse, as such detection would necessarily occur only after the registry had already been compromised. Detection would likely be too little help too late. The widespread use of false headers, open relays, open proxies, and zombie drones by sophisticated spammers would make it exceedingly difficult or impossible to trace a message from the seeded address back to its source.[54] The result would be the same even if a centralized registry were to distribute un-hashed copies of the registry, including canary addresses, to marketers.

---

[51] *Id*. at 22-23.

[52] If the registry were seeded with FTC-controlled email addresses that were likely to be targeted by dictionary attack programs (e.g., "john@ftc.gov"), the receipt of a message at this address would not necessarily indicate that the Registry had been misused to search for valid addresses. A spammer with a dictionary attack program may have sent the message. *Id*. at 22 n.110.

[53] *Id*. at 22-23 n.112. As one computer security expert concluded, "canaries are useless when dealing with a hashed registry." Do Not Email Report, *supra* note 17, at 22-23 n.111.

[54] *Id*. at 8-13 (explaining these techniques).

3. Senders of Offensive Spam Will Be Difficult to Locate and Prosecute

The FTC's experience in its spam cases shows that the primary law enforcement challenge is identifying and locating the targeted spammer. As the Do Not Email Report explains, the ability of spammers to hide their identities by using false headers, open relays, open proxies, zombie drones, and foreign servers makes tracing an email's path "an often fruitless task."[55] Thus, "[t]racing an email almost always leads to a dead end because spammers rarely send messages from their own email accounts. ISPs which, like the Commission, have considerable experience dealing with spam, have been similarly stymied by spammers' use of zombie drones and other camouflage tactics."[56]

Unable to identify a spammer based on the email trail, law enforcement and ISPs must locate spammers by tracing the flow of funds from victim to spammer. The experiences of law enforcement and ISPs belie claims that spammers can be caught easily. First, numerous spam messages, such as those that are purely malicious vehicles for viruses and Trojans, do not typically request money. Second, spammers that request funds often use novel payment methods, offshore banks, stolen credit card accounts, and other techniques that make tracing the flow of money a painstaking, and often futile, endeavor.

IV. Impact on Consumers and Competition

In addition to the risks to children discussed above, SB 2200 would also likely have significant consequences for email marketers throughout the United States, not just those that conduct business in Hawaii. Because an email address does not indicate the geographic residence of its user, a marketer cannot easily separate out residents of certain locations from a marketing list. Any sender of email marketing goods, products, or services covered by SB 2200 would, as a practical matter, therefore, need to scrub each registered address from its list in order to ensure that it did not violate the registry and subject itself to substantial criminal and civil penalties.

For example, with a centrally-scrubbed registry, before sending any customers an email newsletter featuring a laser pointing device, a merchant would need to submit its entire email list to the registry for scrubbing because Hawaii minors are prohibited from purchasing such devices.[57] Similarly, a winery would need to scrub its entire email list before embarking on an email marketing campaign to promote its wines to avoid inadvertently violating SB 2200 by sending a message to a registered email address. Under SB 2200, such marketers would need to conduct such scrubbing every 30 days.

---

[55] *Id*. at 23-26. *See also id*. at 8-12.

[56] *Id*. at 23-26.

[57] HAW. REV. STAT § 136-3 (1999) ("It shall be unlawful to sell or furnish a laser pointing device to any minor.").

The cost of such scrubbing and monitoring can be substantial for legitimate marketers,[58] who are generally unlikely to use email to target minors for products they are prohibited from purchasing.[59] Marketers of certain types of products, such as sexually explicit content, are already subject to substantial legal penalties if they do not comply with laws that protect minors (and adults who do not wish to view such content).[60] Spammers are unlikely to honor any such registry of prohibited contacts and may, in fact, misuse such a list to spam the children on it. The costs of complying with SB 2200, in addition to the potential for substantial criminal and civil liability for individual violations, may cause some legitimate marketers to consider ending mass

---

[58] Do Not Email Report, *supra* note 17, at 31 n.165.

[59] *See, e.g.*, BEER INSTITUTE, ADVERTISING AND MARKETING CODE 1 (2006), *available at* http://www.beerinstitute.org/BeerInstitute/files/ccLibraryFiles/Filename/000000000384/2006ADCODE.pdf (stating that brewers should not market to underage persons, and that "[t]hese guidelines apply to all brewer marketing materials, including Internet and other cyberspace media."); DISTILLED SPIRITS COUNCIL OF THE UNITED STATES, CODE OF RESPONSIBLE PRACTICES FOR BEVERAGE ALCOHOL ADVERTISING AND MARKETING (2006), *available at* http://www.discus.org/industry/code/code.htm (stating that alcoholic beverages should not be marketed to underage persons, and that "[t]he provisions of the Code apply to every type of print and electronic media, including the Internet and any other on-line communications, used to advertise or market beverage alcohol."); and FREE THE GRAPES!, WINE INDUSTRY CODE FOR DIRECT SHIPPING (2006), *available at* http://www.freethegrapes.org/wineries.html#code (specifying that wineries may direct ship wine to adults only in states where it is legal to do so; must request the birth date of the purchaser to verify he/she is over 21 years of age before completing any transaction; and must conspicuously label shipments with a minimum notification "signature of person age 21 or older required for delivery"). *See also* FTC, CIGARETTE REPORT FOR 2003 8-9 (2005), *available at* http://www.ftc.gov/reports/cigarette05/050809cigrpt.pdf (noting that in 2003, besides creating a company website, cigarette "companies reported no expenditures on any other Internet advertising (*e.g.*, banner ads on third party sites and direct mail advertising using -email).").

[60] For example, under the FTC's recent "Label for E-mail Messages Containing Sexually Oriented Material" Final Rule, adopted pursuant to the CAN-SPAM Act, commercial email messages containing sexually oriented materials must "[e]xclude sexually oriented materials from the subject heading for the electronic mail message and include in the subject heading the phrase 'SEXUALLY-EXPLICIT:' in capital letters," and include the electronic equivalent of a "brown paper wrapper" in the body of the message. 16 C.F.R. § 316.4. Thus, the Rule protects minors (and adults who do not wish to inadvertently view sexually explicit content) by requiring that the sender prevent recipients from viewing such material without a recipient's affirmative decision to do so. Courts can award up to $11,000 in penalties per violation of the CAN-SPAM Act, including a violation of the Rule. 15 U.S.C. § 7706(a); 15 U.S.C. § 7(a)(1)(B); 15 U.S.C. § 45(m)(1)(A), as modified by 28 U.S.C. § 2461, as amended and implemented by 16 C.F.R. § 1.98(d).

email campaigns altogether.[61] The aggregate effect of SB 2200 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 Hawaii residents, and for all consumers, not just minors.[62] Thus, SB 2200 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. As noted in the FTC staff report, *Possible Anticompetitive Barriers to E-Commerce: Wine*, Internet merchants often provide consumers with lower prices, more choices, and better quality products and services.[63] The extra burden that SB 2200 would place on Internet sellers may, therefore, hamper a particularly competitive segment of merchants in those industries covered by SB 2200, curtailing the benefits of such competition to consumers.[64]

---

[61] *Id. See also* Jon Swartz, *Anti-Porn Spam Laws to Shield Kids Backfire*, USA TODAY, Aug. 21, 2005 at B1, *available at* http://www.usatoday.com/tech/news/computersecurity/2005-08-21-email-children_x.htm.

[62] If email marketers do illegally sell products to underage persons, they are still subject to state criminal statutes. Thus, email marketers must structure their activities so that they do not violate state laws already in place.

[63] *See* FTC STAFF, POSSIBLE ANTICOMPETITIVE BARRIERS TO E-COMMERCE: WINE 1 (July 2003), *available at* http://www.ftc.gov/os/2003/07/winereport2.pdf. *Id*. at 1, 3, 14-26. For example, "[t]he staff . . . concludes that online wine sales give consumers the opportunity to save money and to choose from a much greater variety of wines." *Id*. at 14. *See also* FTC STAFF, POSSIBLE ANTICOMPETITIVE BARRIERS TO E-COMMERCE: CONTACT LENSES (Mar. 2004), *available at* http://www.ftc.gov/os/2004/03/040329clreportfinal.pdf.

[64] For example, it is likely that some consumers would no longer receive information that they value and, in some cases, that they have specifically requested, such as a monthly email newsletter advertising current prices for covered goods or services. This is not to suggest, however, that the FTC is unconcerned about the marketing of age-inappropriate products and materials to minors, such as entertainment having violent content. *See* FTC, MARKETING VIOLENT ENTERTAINMENT TO CHILDREN: A REVIEW OF SELF-REGULATION AND INDUSTRY PRACTICES IN THE MOTION PICTURE, MUSIC RECORDING & ELECTRONIC GAME INDUSTRIES (2000), *available at* http://www.ftc.gov/reports/violence/vioreport.pdf (recommending that the motion picture, music recording, and electronic game industries continue to improve compliance with existing ad placement guidelines and rating information practices, avoid advertising venues with under-17 audiences, and enhance efforts to prevent minors from purchasing age-inappropriate content). The Commission also has a toll-free consumer complaint line and Internet complaint form available for consumer complaints about the marketing of media violence to children. FTC, FTC ACCEPTING COMPLAINTS ABOUT VIOLENT ENTERTAINMENT MARKETED TO KIDS (2004), *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/mediavioalrt.htm. In addition, as noted above, the FTC has also urged consumers to consider using filtering technologies in their personal email accounts that allow users to sort, delete, or block unwanted commercial email that may contain age-inappropriate content. *See supra* note 16.

Conclusion

Hawaii SB 2200 appears to be designed to protect children from unwanted commercial messages that advertise products or services they are prohibited from purchasing or contain adult advertising or links to adult content. By compiling a list of children's contact points that cannot be effectively monitored for abuse, however, SB 2200 may provide pedophiles and other dangerous persons with a list of contact points for Hawaii children and may actually increase the amount of spam sent to those addresses, including adult content. The extra burden that SB 2200 would place on legitimate Internet sellers may also hamper a particularly competitive segment of merchants in those industries covered by SB 2200, curtail the benefits of such competition to consumers, and cause consumers to no longer receive information that they value.

Sincerely,

Maureen K. Ohlhausen, Director
Christopher M. Grengs, Attorney Advisor
Office of Policy Planning

Lydia B. Parnes, Director
Daniel R. Salsburg, Attorney
Bureau of Consumer Protection

Michael A. Salinger, Director
Louis Silversin, Economist
Bureau of Economics