



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

Office of Policy Planning
Bureau of Consumer Protection
Bureau of Economics

October 25, 2005

The Honorable Angelo "Skip" Saviano
State Representative
77th District
House of Representatives
314 State House
Springfield, IL 62706

Re: Illinois HB 0572

Dear Representative Saviano:

The staff of the Federal Trade Commission's ("FTC" or "the Commission") Office of Policy Planning, Bureau of Consumer Protection, and Bureau of Economics¹ are pleased to respond to your letter of September 12, 2005, that asks for our views on Illinois HB 0572 ("HB 0572" 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 HB 0572 would reduce the amount of unwanted emails and what impact the bill might have on Illinois consumers and competition.

Illinois HB 0572 would require the Illinois Attorney General to establish 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. The bill would also impose liability on a person that promotes or allows the promotion of such a message through a third party.

This letter briefly summarizes the Commission's interest and experience in consumer privacy and provides the staff's opinion regarding the possible impact of HB 0572 on consumers and competition. Based on our experience, our review of your letter, and HB 0572, the FTC staff have reached the following conclusions:

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.

- Because existing computer security techniques are inadequate to prevent the abuse of such a registry, HB 0572 may provide pedophiles and other dangerous persons with a list of contact points for Illinois children.
- HB 0572 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 HB 0572 would place on Internet sellers may, therefore, hamper a particularly competitive segment of merchants in those industries covered by HB 0572, 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 (2005)*, 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 Act⁷ 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 (2005), 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 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 (2005), at <http://ftc.gov/privacy/glbact/index.html>.

⁷ 15 U.S.C. § 1681 *et seq.* (as amended 2003). See generally FTC, CREDIT REPORTING: THE FAIR CREDIT REPORTING ACT (2005), 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 (2005), 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 (2005), at http://ftc.gov/privacy/privacyinitiatives/promises_educ.html; FTC, ID THEFT HOME (2005), at <http://www.consumer.gov/idtheft/>; FTC, FTC CONSUMER ALERT, SPYWARE (2005), at <http://ftc.gov/bcp/online/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 79 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* noted 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 technologies.¹⁶

Notably, in one of the FTC's congressionally-mandated reports – a June 2004 report

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 (2005), 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 (2005), 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>. 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.

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>.

entitled *National Do Not Email Registry, a Report to Congress* (“Do Not Email Report”)¹⁷ – the Commission analyzed the issues identified in your September 12, 2005 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.

II. Summary of HB 0572

Illinois HB 0572¹⁹ would require the Office of the Illinois Attorney General to “establish a Child Protection Registry in which parents may register their children’s Contact Points as off limits from certain categories of commercial messages”²⁰ These contact points would include: electronic mail addresses; instant message identities; postal addresses; telephone numbers; and any additional points designated by the Illinois Attorney General “from time to time and as messaging technology develops.”²¹

Under the bill, “[e]xcept as otherwise authorized by the Attorney General in rules prescribed under this Act, it is unlawful for a person to initiate any commercial message or other communication to any registered contact point if the message or communication: (1) advertises products or services that a minor child is prohibited by law from purchasing; or (2) contains or advertises adult content or links to adult content.”²²

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.

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

¹⁹ HB 0572, 2005 Leg., 2005-06 Sess. (Il. Jan. 27, 2005), *available at* <http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=50&GA=94&DocTypeId=HB&DocNum=0572&GAID=8&LegID=14958&SpecSess=&Session=>.

²⁰ *Id.* at § 5(a).

²¹ *Id.* at § 5(c)-(d).

²² *Id.* at § 5(e)(1)-(2).

A person may also be liable where he or she promotes, or allows the promotion of, another's goods, products, or services through a third party where that person: (1) knows or should have known in the ordinary course of business that they were being promoted in such a message; (2) received or expected to receive an economic benefit from such promotion; and (3) took no reasonable action to prevent the transmission or to detect it and report it to the Illinois Attorney General.²³

Neither actual nor implied consent given by a minor creates a defense to liability.²⁴ But a person does not violate the Act if the contact point in question has been on the registry for less than thirty days or if a person "reasonably relies" on the registry, as provided by the Attorney General and "takes reasonable measures to comply with this Act."²⁵

The Illinois Attorney General is required to establish procedures to permit the reporting of violations of the Act.²⁶ HB 0572 also makes it an Illinois Class B criminal misdemeanor to violate the Act. Each separate message in violation of the Act constitutes a separate violation.²⁷ Each unauthorized use of the Registry constitutes a Class A misdemeanor, for which a fine of not more than \$500,000 may be imposed.²⁸ In addition, "[p]arents may recover actual damages, on behalf of their children" for messages sent to a contact point in violation of the Act.²⁹ In lieu of actual damages, a parent may recover \$1,000 per violation.³⁰

III. Effect of HB 0572 on Registered Children

A. HB 0572 May Provide Pedophiles and Other Dangerous Persons With a List of Contact Points of Illinois Children

The registry proposed by HB 0572 would create an extensive directory of childrens' contact points that currently does not exist. As explained below, such a list cannot be effectively

²³ *Id.* at § 5(f)(1)-(3).

²⁴ *Id.* at § 5(g).

²⁵ *Id.* at § 10.

²⁶ *Id.* at § 15(a).

²⁷ *Id.* at § 15(b).

²⁸ *Id.*

²⁹ *Id.* at § 15(c).

³⁰ *Id.*

monitored for abuse.³¹ By compiling such a list that cannot be effectively monitored for abuse, HB 0572 may provide pedophiles and other dangerous persons with a potential list of contact points of Illinois 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.”³²

Although difficult to quantify, the risk of a pedophile or other dangerous persons misusing the registry data to discover the contact point of an Illinois minor is certainly real. First, such a list could be misused by registry personnel.³³ Second, such a list is subject to direct hacking by technologically sophisticated persons. Third, the Illinois 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.

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

³¹ 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,” H.R. 165, 2004 General Session (2004). The Commission will continue to monitor these registries with regard to their effect on children’s privacy.

³² Do Not Email Report, *supra* note 17, at 33-34.

³³ 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/expetrtrpts/rubin.pdf>.

As mentioned above, HB 0572 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.³⁴ A registry of email addresses, such as the one proposed by HB 0572, 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.³⁵ 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").³⁶

Disturbingly, 47 percent of the children surveyed in the Symmantec study reported receiving spam with links to pornographic websites.³⁷ The Commission has found no data to suggest that spammers are currently targeting children to receive specific types of spam,

³⁴ Do Not Email Report, *supra* note 17, at 1-12.

³⁵ 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* note 17, at 33-34.

³⁶ 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.

³⁷ Symantec Survey, *supra* note 17. 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.*

however.³⁸ Rather, spammers appear to use indiscriminate marketing techniques, and, therefore, children generally receive the same types of spam that adults receive.³⁹ 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 HB 0572-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.

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

³⁸ 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/online/pubs/alerts/spamalrt.htm>. *See also* Do Not Email Report, *supra* note 17, at 34, n.187.

³⁹ 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>.

registered contact points.⁴⁰ 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.⁴¹

Although Illinois 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.⁴²

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

⁴⁰ 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).

⁴¹ *Id.* at 19-20.

⁴² 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 hashed form, such as 5519e3f2ba5aef2dead64f72cf31507e88d6eb23, and add it to the registry.

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.⁴³

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.⁴⁴ 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.

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").⁴⁵ To ensure that

⁴³ 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.

⁴⁴ 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.

⁴⁵ *Id.* at 22-23.

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.⁴⁶ 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.⁴⁷

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.⁴⁸ 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.

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

⁴⁶ 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.

⁴⁷ *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.

⁴⁸ *Id.* at 8-13 (explaining these techniques).

task.”⁴⁹ 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.”⁵⁰

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, HB 0572 would also likely have significant consequences for email marketers throughout the United States, not just those that conduct business in Illinois. 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 HB 0572 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, in a centrally-scrubbed registry, before sending any customers an email newsletter featuring a new crime novel, a bookseller would need to submit its entire email list to the registry for scrubbing because Illinois minors are prohibited from purchasing “any book, pamphlet, magazine, newspaper, story paper or other printed paper devoted to the publication, or principally made up of criminal news, police reports, or accounts of criminal deeds, or pictures and stories of deeds of bloodshed, lust or crime.”⁵¹ 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 HB 0572 by sending a message to a registered email address. Under HB 0572, such marketers would need to conduct such scrubbing every 30 days.

The cost of such scrubbing and monitoring can be substantial for legitimate marketers,⁵² who are generally unlikely to use email to target minors for products they are prohibited from

⁴⁹ *Id.* at 23-26. *See also id.* at 8-12.

⁵⁰ *Id.* at 23-26.

⁵¹ 720 ILL. COMP. STAT. 670/1 (1889).

⁵² Do Not Email Report, *supra* note 17, at 31, n.165.

purchasing.⁵³ 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).⁵⁴ 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 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 altogether.⁵⁵ 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 for all consumers, not just minors. Thus, HB

⁵³ See, e.g., BEER INSTITUTE, ADVERTISING AND MARKETING CODE 1 (2005), available at <http://www.beerinstitute.org/adcode.htm> (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 (2005), 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 (2005), 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).”).

⁵⁴ 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).

⁵⁵ *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.

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. 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.⁵⁶ The extra burden that HB 0572 would place on Internet sellers may, therefore, hamper a particularly competitive segment of merchants in those industries covered by HB 0572, curtailing the benefits of such competition to consumers.⁵⁷

Conclusion


Illinois HB 0572 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, HB 0572 may provide pedophiles and other dangerous persons with a list of contact points for Illinois children and may actually increase the amount of spam sent to those addresses, including adult content. The extra burden that HB 0572 would place on legitimate Internet sellers may also hamper a particularly competitive segment of

⁵⁶ 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>.

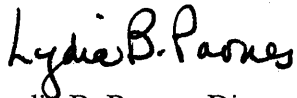
⁵⁷ For example, it is likely that some consumers would no longer receive information that they value and, in some cases, that they have specifically requested, such as a monthly email newsletter advertising current prices for covered goods or services. This is not to suggest, however, that the FTC is 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.

merchants in those industries covered by HB 0572, curtail the benefits of such competition to consumers, and cause consumers to no longer receive information that they value.

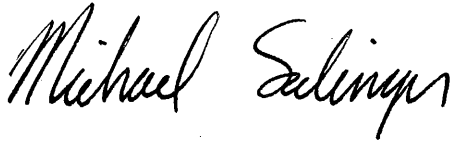
Sincerely,



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