Federal Trade Commission

Messaging Anti-Abuse Working Group Annual Meeting
Orlando, Florida

Consumer Protection Update
David C. Vladeck[1]
Director, FTC Bureau of Consumer Protection
February 23, 2011

Thank you for inviting me to speak with you today. While it is simple for someone to spoof an email address or hide behind a proxy service when registering a web site, I assure you that I really am David Vladeck.

But, what if instead of coming here and speaking to you in person, I phoned in my presentation. How would you know that it was really me speaking? What if I sent my presentation via email or text messaging?

MAAWG members know better than anyone else that the ease of lying about who you are makes online commerce and telemarketing very different than face-to-face commercial transactions. Scam artists thrive in markets where identity and reputation doesn't matter. If you are running a scam, why not bombard consumers' inboxes with spam? Why not unleash a barrage of text messages asking consumers to visit your website? Why not set your autodialer to

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

call thousands of residential phone numbers? When the consumer complaints begin to mount, why not just change your name and continue business as usual?

Messaging abuse threatens the vitality of online commerce and infringes on consumers' privacy. I applaud MAAWG's efforts to combat messaging abuse through industry collaboration and the advocacy of technological solutions.

At the FTC, we share MAAWG's concerns with messaging abuse. A significant portion of the FTC's consumer protection mission focuses on online abuses and privacy violations, some of which I'd like to highlight.

I. Protecting Consumers From Online Threats

The FTC is fighting online threats using all of the tools at its disposal – law enforcement, rule making, advocacy of technological solutions, research, and consumer and business education.

A. Enforcement

Law enforcement is the Commission's most visible and aggressive tool for fighting online threats. Whether the bad guys are using text messaging, email, or deceptive banners and popups, the Commission is working to protect consumers.

1. Text Messaging

Yesterday, the Commission filed its first law enforcement action against a sender of unsolicited text messages. The case charges Philip Flora, a California resident, with sending millions of unsolicited text messages to the mobile phones of US consumers.[2] We are still

---

[2] *See* Press Release, "FTC Asks Court to Shut Down Text Messaging Spammer" (Feb. 23, 2011), *available at* http://ftc.gov/opa/2011/02/loan.shtm.

determining the scope of Flora's text messaging scheme, but a 40 day snapshot into his actions reveals the breadth of his activities, and how much havoc just one person can wreck. Using 32 pre-paid cell phones, Flora blasted over 5 million text messages — almost a million a week --- typically advertising loan modification or debt relief services. To transmit this many messages, Flora needed to send, on average, 85 messages per minute around the clock.

Flora sent email spam to consumers, advertising his text message blasting services. In these emails, Flora offered to send 100,000 text messages for only $300.

Many consumers who received Flora's text messages had to pay a per-message fee each time they received a message. Many others found that Flora's text messages caused them to exceed the number of messages included in their mobile service plans. While the financial injury suffered by any consumer may be small, the aggregate injury is likely quite large. And, even for those consumers with unlimited messaging plans, Flora's unsolicited messages were harassing and annoying, coming at all hours of the day.

The Commission has charged Flora with engaging in the unfair practice of sending unsolicited text messages, violating the CAN-SPAM Act, and engaging in deception by advertising a loan modification service that was supposedly affiliated with the federal government. The Commission has asked the Court to order Flora to stop sending unsolicited text messages and to freeze Flora's assets so we can use them for consumer redress.

2. Email Spam

For years, the Commission has sued spammers, charging them with violating the CAN-SPAM Act. These cases help establish the rules of the road for legitimate marketers. But they are unlikely to deter the criminal gangs that use spam as a vector for malware.

In June 2009, however, members of the anti-spam community gave the Commission evidence about a rogue Internet Service Provider based in California, but controlled by overseas criminals. The ISP, 3FN, recruited and willingly hosted a massive amount of malicious electronic content, including child pornography, malware, phishing sites, and the servers that control botnets. In just two weeks, the FTC filed an enforcement action and obtained a TRO requiring the data centers where 3FN's servers were located to disconnect the servers from the Internet. According to statistics published by Google, the shutdown of 3FN resulted in a temporary 30% drop in worldwide spam levels. Ultimately, the Court issued a Default Judgment against the Defendant and ordered disgorgement in excess of $1 million.[3] This was the first time in FTC history that the Commission used its authority under Section 5 to shut down an ISP.

3. Misuse of pop-ups and banner ads

Scammers have found numerous other ways to trick consumers into paying money. For instance, in December 2008, the FTC sued Innovative Marketing, Inc., the corporate centerpiece of a massive, deceptive advertising scheme that flooded the Internet with more than one billion deceptive ads, ensnared millions of domestic and foreign consumer victims, and caused more than $163 million in consumer injury.[4] For more than five years, the Defendants marketed a wide range of computer security products to consumers. To frighten and intimidate consumers into purchasing these products, the Defendants relied on deceptive advertising that featured convincing, but utterly bogus, system scans that purported to scan consumers' computers for

---

[3] *See* Press Release, "FTC Permanently Shuts Down Notorious Rogue Internet Service Provider" (May 19, 2010), *available at* http://www.ftc.gov/opa/2010/05/perm.shtm.

[4] *See* Press Release, "Court Halts Bogus Computer Scans" (Dec. 10, 2008), *available at* http://www.ftc.gov/opa/2008/12/winsoftware.shtm.

harmful and illegal files. Invariably, these scans falsely reported that consumers' computers were filled with viruses, spyware, or pornography and urged consumers to "fix" these fake threats for a fee.

Advertising networks received so many complaints about the Defendants' ads that they eventually banned them. Undeterred, the Defendants then masqueraded as Internet advertising agencies seeking to place ads on behalf of legitimate companies. Although the ads placed by Defendants appeared legitimate, they were in fact trojan horses that redirected consumers away from the web sites they were viewing and transported them to one of the Defendants' web sites. After hijacking consumers, Defendants displayed the same bogus system scans that purported to scan consumers' computers for harmful and illegal files.

At the FTC's request, the Court shut the company down and froze the Defendants' assets. The Commission has already obtained $8.3 million that, if at all possible, will be used to redress injured consumers.

B. Rule Making

Fraudulent marketers don't play by the rules. Legitimate marketers, however, sometimes need a gentle push from the FTC to change their ways. One example of this is the Commission's recent regulations regarding robocalls.

1. Pre-Recorded Messages- Robocall Regulations

The FTC has issued new regulations regarding robocalls – outbound telemarketing calls that deliver a prerecorded message. Why? Because we got the message: Consumers really dislike robocalls. Who doesn't? In August 2008, the Commission issued amendments to the Telemarketing Sales Rule (TSR) prohibiting telemarketing robocalls unless the seller has

obtained the call recipient's prior signed, written agreement to receive such calls from that seller.[5] An "established business relationship" does not provide a basis for placing a robocall.

The new rules restrict robocalls in other ways. For instance, the written agreement is required regardless of whether the number called is on the National Do Not Call Registry. It also does not matter whether the call delivering a prerecorded message is answered "live" by a person or by an answering machine or voicemail service.

And even if the telemarketers and sellers have written permission, the prerecorded message must provide recipients an automated mechanism to opt out of further calls.[6] The opt-out mechanism must be disclosed "immediately" after the disclosure of the name of the seller, the purpose of the call, and the nature of the goods or services being sold. If the recipient invokes the opt-out mechanism, that mechanism must automatically add the number to the seller's do not call list and then disconnect the call "immediately." Violators face penalties of up to $16,000 per call.

C. Advocating Technological Solutions and Staying Current with new Communication Methods

In the high-tech arena, the FTC's enforcement and regulatory programs are supplemented with advocacy of technological solutions and research.

1. Domain-level Email Authentication Efforts

Many of you are aware of the FTC's advocacy of domain level authentication. While the FTC maintains a vigorous anti-spam enforcement program, spam is a technological problem

---

[5] *See* 73 Fed. Reg. 51,163 (2008).

[6] *See* 71 Fed. Reg. 58,715, 58,718 (2006) and 69 Fed. Reg. 67,287, 67,288-89 (2004).

requiring a technological solution. The protocol for email allows for the spoofing of the "from" line, making it exceedingly difficult for receiving ISPs to determine whether a message is truly from the purported sender.

The FTC first advised Congress that domain level authentication showed promise as an anti-spam technology in 2004. Seven years have now passed since the Commission first called for the wide scale deployment of domain level authentication. I know that MAAWG has been helping lead this charge. It's time to make this happen. All outbound email needs to be authenticated. And receiving ISPs need to start rejecting unauthenticated messages or filtering them more aggressively. Only when there is a truly functioning authentication system in place can other anti-spam technologies (such as reputation services) function effectively.

2. Mobile Lab

The FTC's advocacy, enforcement, and rule making depend on the agency investing in new technologies and providing its investigators with necessary tools. For several years, the FTC has investigated online frauds using its Internet Lab, a facility jammed with computers with IP addresses that are not assigned to the government and with evidence capturing software.

We are now broadening our ability to investigate mobile devices. The statistics tell the story. Cell phone ownership has risen dramatically in the U.S. over the past decade and now 82% of American adults own a cell phone, Blackberry, iPhone or other device that is also a cellphone. More and more mobile subscribers are using smartphones (rather than feature phones) that allow users to access the web and email on the go and run a host of applications and smartphones will soon overtake feature phones in the U.S. market.

Corporations are using the mobile medium to reach consumers, whether it is to provide services or content, or to market their products. Just this month, one company predicted that

U.S. mobile advertising spending will reach 5 billion dollars by 2015.[7] Consumers can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase. Consumers can search mobile web sites to get detailed information about products, or compare prices on products they are about to purchase while standing in the check-out line. Consumers can download mobile applications that perform a range of consumer services such as locating the nearest retail stores, managing shopping lists, tracking family budgets, or calculating tips or debts. They can also play interactive games containing targeted advertising. This market is exploding with new options for consumers and businesses.

New technology can bring tremendous benefits to consumers, but it also can bring new concerns and provide a platform for old frauds to resurface. The mobile marketplace is no different. The FTC Act applies whether a company is marketing via the traditional telephone, the television, the desktop computer, or a mobile device. The important principle to remember, however, is that the same rules of the road apply. Marketing must not be deceptive or unfair. Marketers should not mislead consumers about what they are downloading on their mobile devices or treat them unfairly. Consumers should have clear information so they can make informed choices.

The FTC is ensuring that it has the tools necessary to respond to the growth of mobile commerce and conduct mobile-related investigations. Last year the FTC's Bureau of

---

[7] Leena Rao, "Smaato: U.S. Will Spend $5 Billion On Mobile Advertising In 2015," TechCrunch (Nov. 2, 2010), *available at* http://techcrunch.com/2010/11/02/smaato-u-s-will-spend-5-billion-on-mobile-advertising-in-2015/.

Consumer Protection created a Mobile Lab – a gadget-lover's dream-house stocked with mobile devices on various platforms and carriers and evidence-capturing equipment and software. With these additions, FTC staff has improved its ability to conduct research and investigations into a wide range of issues in the mobile space. I have also assembled a team to stay abreast of the new developments in mobile technology and watch for unfair and deceptive practices. This group is conducting research, looking at apps, and following the latest reports on these technologies. We have some potential targets and I expect we will have some law enforcement actions in the pipeline.

The FTC has already brought a case applying FTC advertising law principles to the mobile application marketplace. In August, the Commission settled allegations that Reverb, a marketing company, deceptively endorsed gaming applications in the iTunes store.[8] The company posted positive reviews using account names that gave readers the impression the reviews had been submitted by disinterested consumers. The company agreed to an order prohibiting it from making such representations unless it discloses a material connection, when one exists, between the company and the product.

D. Consumer and Business Education

The FTC also has an extensive program to educate people about how to be safe and secure online, and to help businesses protect consumer information in their care. Today, I'm going to tell you a bit about two of our education projects: OnGuardOnline.gov and the BCP Business Center.

---

[8] *See* Press Release, "Public Relations Firm to Settle FTC Charges That It Advertised Clients' Gaming Apps through Misleading Online Endorsements" (August 26 2010), *available at* http://www.ftc.gov/opa/2010/08/reverb.shtm.

OnGuardOnline.gov, which we manage, is a partnership of fourteen federal agencies, including all the heavy hitters in the realm of cybersecurity. The site – which gets more than two million unique visits each year – has materials you can use for your company's education programs, including advice on avoiding phishing attacks, scams and malware. Feel free to copy and distribute any of the OnGuard Online articles, videos and games for your clients and staff.

In 2008, Congress asked us to expand the OnGuardOnline.gov project to cover online safety for kids. In response, we developed a guide for parents, *Net Cetera: Chatting with Kids About Being Online*. Since October 2009, the FTC has distributed over seven million copies of the guide. Seven million!

Last year, we released the *Net Cetera Community Outreach Toolkit*. Each toolkit includes:

1. our guide for parents – *Chatting with Kids About Being Online*
2. a booklet for kids called *Heads Up*, with advice on dealing with cyberbullies, texting, file sharing, and using mobile phones
3. and videos, presentation slides and discussion guides to help you share this important information with your friends, family, coworkers and clients.

The other site I encourage you to bookmark is business.ftc.gov, the BCP Business Center. There you'll find practical compliance guidance on online advertising, privacy, data security, and other need-to-know topics for business people.

Many of the most popular pages on the Business Center deal with topics of interest to MAAWG members. Our CAN-SPAM Act compliance guide is the most viewed page on the site. And if you're responsible for data security, you'll want to check out our short video about Peer to Peer File Sharing. The resources on the BCP Business Center are yours to share.

So bookmark OnGuardOnline.gov and business.ftc.gov, and stop by often to find out what we're up to. Use the Business Center Blog to tell us what's on your mind. If you're interested in what we're doing, sign up to get an update whenever we have a new blog post, or subscribe to our monthly email newsletter, Penn Corner.

II. Protecting Consumers' Privacy

A. Enforcement Cases – Privacy and Data Security

I'm eager to also talk about the work we've been doing to safeguard consumer privacy and to think broadly about privacy protection going forward. Let me begin by talking about our enforcement efforts, including a privacy case we announced in December against Echometrix and a trio of recent data security cases.

EchoMetrix sells software — called Sentry — that enables parents to monitor their children's online activities.[9] EchoMetrix also advertised a web-based market research software program that allows marketers to see "unbiased, unfiltered, anonymous" content from social media websites, blogs, forums, chats and message boards. We alleged that one source of this content was the online activity of children recorded by the parental monitoring software.

We also alleged that EchoMetrix failed to adequately disclose to parents that it would share the information it gathered from their children with third-party marketers. EchoMetrix made only a vague disclosure about information sharing and buried it about 30 paragraphs into a multi-page end user license agreement. Burying an ambiguous statement in the EULA just

---

[9] *See* Press Release, "FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers" (Nov. 30, 2010), *available at* http://www.ftc.gov/opa/2010/11/echometrix.shtm.

doesn't cut it. That's especially true when personal information about children is being collected and shared.

The order requires EchoMetrix not to use or share the information it obtained through its Sentry parental monitoring program — or any similar program — for any purpose other than use by a registered user. The order also requires the company to destroy the information it had transferred from Sentry to its marketing database.

The FTC has also aggressively enforced data security laws. We've now brought 32 data security cases, ranging from cases against retailers, software providers, mortgage companies, data brokers, and others. These cases send a strong message that companies have to take reasonable measures to safeguard consumer data: Companies are stewards of the consumer information they maintain, and they've got to be responsible stewards.

Several weeks ago we announced three cases against companies reselling consumers' credit reports. According to the FTC's complaints, the resellers buy credit reports from the big-three nationwide consumer reporting agencies — Equifax, Experian, and TransUnion — and combine them into special reports they sell to mortgage brokers and others to determine consumers' eligibility for credit. The companies allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access their reports. As a result, hackers accessed more than 1,800 credit reports without authorization through their clients' computer networks. Even after becoming aware of the data breaches, the companies did not make reasonable efforts to protect against future breaches.[10]

---

[10] The resellers are SettlementOne Credit Corporation and its parent company, Sackett National Holdings Inc.; ACRAnet Inc.; Fajilan and Associates Inc., doing business as Statewide Credit Services; and Robert Fajilan. *See* Press Release, "Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal

B. Non-Enforcement Initiatives

In addition to our enforcement efforts, the agency is also engaged in broader privacy initiatives. First, we're reviewing our Children's Online Privacy Protection Act rule to see if it has withstood the test of time. We are examining a number of questions: Does it provides adequate protection in light of significant changes in the marketplace affecting kids, such as the explosive growth in the use of social networking and smartphones and the development of technologies such as interactive TVs? Does COPPA's coverage of websites located on the Internet and online services reach the kinds of electronic media children use today? How should we address the collection of mobile geolocation data or information collected in connection with online behavioral advertising under the Rule? What about online gaming sites? Should they be covered? Are the methods for verifying parental consent, such as using a print-and-send form, obsolete? We hope to have some preliminary answers this summer.

More broadly, over the last year the FTC hosted three major roundtables – and reviewed many public comments – to get public input as part of a reexamination of the FTC's policy approach to privacy. Based on these efforts, we released a draft report that sets forth a framework for privacy that makes sense today.

The report is available at ftc.gov but let me give you some of the big-picture issues discussed in the Report.

First, we need to reduce the burden on consumers, and one way to do that is to build privacy into products and services at the outset — that is, privacy by design. There's tremendous value in building privacy and security into companies' procedures, systems, and

---

Information" (Feb. 3, 2011), *available at* http://www.ftc.gov/opa/2011/02/settlement.shtm.

technologies by design. That means thinking about ways to practice good data hygiene from the very beginning, such as providing reasonable security for consumer data, limiting collection and retention to the least amount necessary, and implementing reasonable procedures to promote data accuracy. The more companies do to establish good practices by default, on the front end, the less burden on consumers to expend lots of effort to salvage some privacy on the back end.

Another way to reduce the burden on consumers is to greatly simplify consumer choice. The way to make privacy choices meaningful to consumers is to present them in a short, concise manner at the point when the consumer is providing the data, so they're top of mind and easy to access when needed. We're also thinking about whether it would be helpful to have more consistent privacy policies, so consumers can compare competitors' privacy practices at a glance, which may lead to more competition around privacy practices. And strong protections for sensitive information such as health, financial, children's, and geolocation data should be a given.

To simplify choice even further, we are considering the elimination of the disclosure of extraneous information – commonly accepted business practices such as giving your address to a shipper – then it will be easier for consumers to pay attention to what really matters and will ease the burdens on business as well.

We also need to increase transparency. The Report discusses ways to increase transparency about commercial data practices. Despite the many issues raised with existing privacy policies, getting rid of privacy policies is not the answer – privacy notices help promote accountability for companies, for one thing. What we need is better privacy notices, perhaps in more consistent, shorter, more easily comparable formats.

We're also looking at ways to address concerns raised at the roundtables about the roles of data brokers, most of which have no direct interaction with consumers but collect and compile storehouses of data about consumers from myriad sources. Some panelists at the roundtables suggested that consumers should get access to their data as a means of improving transparency, while others discussed the costs of providing access and recommended that any access should vary with the sensitivity of the data and its intended use. Access is an important ingredient in accountability. The Report addresses this issue as well.

The Report also addresses the viability of some kind of universal mechanism, a one-stop-shop where consumers can register a preference not to be tracked, or not be targeted for online ads, and where marketers would have to respect such preferences. There have already been efforts to allow — by browsers and companies — to give consumers tools to indicate that they don't want to be tracked, or to adjust or tweak how they're tracked. These efforts are laudable. It is hard to say, though, how consumers will respond if many different associations, companies, and groups offer different options in different formats. A Do Not Track option against can simplify consumer choice.