SELECTED DOCKET AND LEGISLATIVE SUMMARIES, 2011


On September 22, 2011, the Federal Communications Commission ("Commission" or "FCC") released a Notice of Proposed Rulemaking ("NPRM") seeking comment on the accelerated short-term and long-term deployment of Next Generation 9-1-1 ("NG911"), enabling the public to send emergency communications to 911 Public Safety Answering Points ("PSAPs") via text, photo, video, and data. NG911 will enhance the information available to PSAPs assessing and responding to emergencies and provide them with the tools needed to quickly process and analyze incoming information. Equally noteworthy, adding text and other media capabilities to the 911 system promises to bring significant benefits to persons with disabilities.

After summarizing and distinguishing different technical options for providing text-based and visual information to PSAPs, the FCC sought comment on implementing a short-term short message service ("SMS") solution and requested further comment on long-term deployment approaches.

I. FACILITATING THE SHORT-TERM DEPLOYMENT OF TEXT-TO-911

The Commission recognizes that SMS-to-911 has a number of technical limitations that affect its ability to act as a reliable emergency system. Specifically, the FCC notes that "SMS is essentially a store-and-forward messaging service that is not designed to provide immediate or reliable message delivery; does not support two-way real-time communication; does not provide the sender's location information; and does not support the delivery of other media such as photos, video, and data." As a result, it believes that these factors make SMS "inappropriate as a long-term text-to-911 solution and warrant caution in encouraging it as a short-term solution."

At the same time, however, SMS-to-911 offers certain potential benefits as an interim solution. For instance, it can be deployed relatively quickly, consumers have already embraced the technology, and the vast majority of wireless providers and mobile devices support SMS. Having balanced these considerations, the FCC notes that "PSAPs, providers, and vendors should have the option to implement SMS-to-911 as a short-term alternative."
Accordingly, the agency encourages SMS-to-911 trials “to develop improved information about the strengths and limitations of this approach.”

The Commission requests comment on the feasibility of overcoming or mitigating SMS technical limitations (e.g., inability to provide accurate location information to PSAPs) at a reasonable cost to providers. Furthermore, the Commission seeks comment on NG911 approaches based on software applications. Under this system, smartphone users could install 911-specific applications that would enable them to send text and other non-voice media to PSAPs. While the FCC believes that this system architecture “could be rolled out in a relatively short-period of time and would not require any major provider network upgrade,” it is particularly interested in the costs and timeframe for deploying such a system.

II. FACILITATING THE LONG-TERM DEPLOYMENT OF NEXT-GENERATION 911 TEXT AND MULTIMEDIA APPLICATIONS

The NPRM also seeks additional information on the benefits of long-term NG911 applications, particularly with respect to (1) improving 911 accessibility for persons with disabilities; (2) meeting consumer expectations; (3) providing PSAPs with valuable additional information; and (4) increasing reliability and resiliency.

To improve accessibility for persons with disabilities, the Commission requests information on the benefits and associated costs of facilitating advanced text-to-911 and multimedia systems, such as those using Session Initiation Protocol (“SIP”) and Real-Time-Text (“RTT”). The Commission asserts that these applications have “the potential to provide substantially improved accessibility to 911 services for people with disabilities, as well as to provide an alternative means for non-disabled people to access 911 when voice access is unavailable or could pose risks to the caller, for example in a silent call scenario.” In addition, multimedia applications could enhance accessibility for people with disabilities who rely on media other than text to communicate.

The Commission also seeks comment on whether promoting or requiring delivery of texts and multimedia communications accurately reflects current and evolving consumer expectations and the needs of PSAPs and first responders. Additionally, the agency requests comment on the benefits of providing additional information to PSAPs, enabling them and first responders to more accurately assess the nature and severity of an emergency and determine the appropriate response. For example, if vehicles in an accident have automatic collision notification systems, the PSAP would “receive additional information regarding the severity of the crash that could help determine the likely medical needs of accident victims and the appropriate
emergency medical response.” The Commission also believes that, in some cases, enhanced information could lead to quicker apprehension of criminal suspects or serve as a tool to screen fraudulent or malicious 911 calls. In sum, providing PSAPs with extra tools to assess and respond to an emergency event would allow for efficient allocation of resources and minimize unnecessary efforts.

Finally, the NPRM notes that IP-based messaging services “could contribute to improved reliability and resiliency of emergency response networks because they generally consume less bandwidth than voice calls and may use different spectrum resources or traffic channels.” This may enable individuals in disaster areas to send text messages to 911 even if they cannot place a voice call through their regular network systems. To explore this further, the FCC requests information on the impact of IP-based messaging solutions on PSAP operations and emergency response during large-scale disasters.

III. 911 PRIORITIZATION IN MAJOR DISASTERS AND EMERGENCIES

The NPRM also seeks comments on how to ensure the proper routing of 911 calls during times of high demand. Specifically, the Commission cites the August 23, 2011 earthquake and Hurricane Irene as examples of the “concentrated demands on the capacity of commercial communication networks during and immediately after emergencies,” which jeopardizes the ability of consumers to reach 911 and request aid. The Commission requests comments on how to address this concern in both legacy and emergency broadband networks and discusses different approaches to generate ideas.

First, the Commission suggests prioritizing 911 traffic over non-911 traffic. However, it seeks further information as to whether prioritization is feasible on current networks and what the costs of this deployment would be. Another suggestion to improve consumers’ ability to reach 911 is to encourage users to limit their use of the network so that calls to 911 are more likely to go through. The NPRM seeks comment on the possible best practices from service providers or others that might encourage consumers to mitigate congestion. Finally, the Commission is particularly interested whether the deployment of text-to-911 would reduce network congestion. As a result, it seeks comment on the potential for prioritization of 911 traffic in existing and future mobile broadband networks.

IV. THE COMMISSION’S ROLE IN EXPEDITING DEPLOYMENT OF TEXT-TO-911 AND OTHER NEXT GENERATION 911 APPLICATIONS

As a final matter, the Commission seeks comments on its role in expediting
the development and widespread deployment of both short- and long-term NG911 solutions. Specifically, the FCC asks whether it should impose an incentive-based approach or a full regulatory scheme to accelerate NG911 implementation. Additionally, it solicits comment on whether there are any regulatory or statutory changes that are needed to facilitate and oversee the deployment of NG911 networks.


The Federal Communications Commission ("FCC" or "Commission") adopted a Report and Order and Further Notice of Proposed Rulemaking ("Order") on October 27, 2011, creating the Connect America Fund ("CAF") and reforming the high-cost component of the Universal Service Fund ("USF"). In the Order, the FCC set five performance goals for the USF: (1) preserve and advance universal availability of voice service; (2) ensure universal availability of modern networks capable of providing voice and broadband service to homes, businesses, and community anchor institutions; (3) ensure universal availability of modern networks capable of providing advanced mobile voice and broadband service; (4) ensure that rates for broadband services and rates for voice services are reasonably comparable in all regions of the nation; and (5) minimize the universal service contribution burden on consumers and businesses. The Commission also set the annual funding target at no more than $4.5 billion over the next six years. Finally, the FCC mandated that eligible telecommunications carriers ("ETCs") offer broadband services in addition to their existing requirement to offer voice services.

The Commission foresees the CAF ultimately replacing all existing high-cost support mechanisms. The purpose of the CAF is to help make broadband available to homes, businesses, and communities that would not otherwise
have access to broadband services. The *Order* states that the CAF will rely on incentive-based, market-driven policies in order to distribute universal service funds efficiently. Moreover, the CAF will help facilitate the Commission’s intercarrier compensation (“ICC”) reforms.

In areas served by price cap carriers that lack access to residential fixed broadband at or above the Commission’s broadband speed benchmark, the CAF will introduce broadband support in two phases. Phase I, beginning in early 2012, will provide additional funding for price cap carriers to extend scalable broadband to hundreds of thousands of unserved Americans. To do this, all existing legacy high-cost support to price cap carriers will be frozen, making available an additional $300 million in CAF funding. In Phase II, the Commission will employ a combination of a forward-looking cost model and competitive bidding to support the deployment of networks providing voice and broadband service for five years. The FCC anticipates that the CAF will expand broadband availability to millions of Americans who are currently unserved.

The *Order* directs the Wireline Competition Bureau to undertake public processes to determine the design and operation of the Phase II cost model and encourages stakeholders to participate in the process. The model will be used to determine the efficient amount of support that is required to extend and sustain “robust, scalable broadband in high-cost areas.” In each state, the CAF will provide support only to areas where a federal subsidy is necessary to ensure the operation of broadband networks. The CAF will not provide any support to an area where unsubsidized competitors are providing broadband services that already meet the FCC’s requirements.

The CAF requires that in each state the incumbent price cap carrier undertake a state-level commitment to provide affordable broadband to all high-cost locations within its service territory in that state. In places where the incumbent carrier declines this commitment, the Commission will use competitive bidding to distribute support. The Commission hopes that Phase II of the CAF will distribute a total of up to $1.8 billion annually in support for areas with no unsubsidized broadband competitor. The Commission expects the model and competitive bidding mechanism to be adopted by December 2012, with disbursements ramping up in 2013 and continuing through 2017.

The *Order* also reforms the Commission’s rules for rate-of-return companies, stating that those receiving legacy universal service support will be required to offer broadband service meeting initial CAF requirements upon a customer’s reasonable request. In addition to broadband service rules, the Commission adopted seven reforms, including limiting reimbursements for operation expenses and capping per-line support at $250 per month.

Furthermore, the Commission creates the CAF Mobility Fund to provide
support to mobile broadband carriers who are implementing CAF. There are
two phases for the CAF Mobility Fund. During Phase I, the Commission will
provide up to $300 million in one-time support, in order to immediately
accelerate the deployment of networks for mobile voice and broadband
services. Support in Phase I will be awarded through a nationwide reverse
auction, to occur during third quarter 2012. Phase I also includes the
establishment of a complementary, one-time Tribal Mobility Fund, which will
award up to $50 million in additional universal service funding to Tribal lands.

In Phase II, expected to be implemented in 2013, the CAF Mobility Fund
will provide up to $500 million per year in ongoing support to mobile
broadband services. This will include ongoing support for Tribal areas of up to
$100 million per year as part of the $500 million budget. Additionally, the
Commission will allocate at least $100 million per year to ensure that
Americans living in the most remote areas can obtain affordable access
through alternate technology, including satellite and unlicensed wireless
services.

The Commission also uses the Order to establish a national framework for
certification and reporting requirements, in order to ensure that the public
interest obligations of all universal service recipients are met. The Commission
is clear that it is not disturbing the existing role of states in designating ETCs
or in monitoring that ETCs are using universal service support for its intended
purpose. Finally, the Commission includes in the Order its plan for ICC
reform, which includes both immediate reforms in order to “curtail wasteful
arbitrage” and a multi-year transition plan.

Summarized by Maria Perrone

In re Implementation of Sections 716 and 717 of the Communications
Act of 1934, as Enacted by the Twenty-First Century Communications
and Video Accessibility Act of 2010; Amendments to the Commission’s
Rules Implementing Sections 255 and 251(a)(2) of the Communications
Act of 1934, as Enacted by the Telecommunications Act of 1996; In the
Matter of Accessible Mobile Phone Options for People who are Blind,
Deaf-Blind, or Have Low Vision, Report and Order and Further Notice of

On October 7, 2011, the Federal Communications Commission (“FCC” or
“Commission”) adopted a Report and Order and Further Notice of Proposed
Rulemaking (“Order”) implementing provisions of Section 104 of the Twenty-
First Century Communications and Video Accessibility Act (“CVAA”).
Specifically, Section 104 amends Title VII of the Communications Act of 1934 ("the Act") by adding Sections 716, 717, and 718.

Section 716 requires manufacturers and providers of advanced communications services, such as interconnected VoIP, electronic messaging services, and interoperable video conferencing service, to make their products and services accessible and usable to individuals with disabilities, unless doing so is not achievable. This imposes a higher standard than Section 255's "readily achievable" standard, which existed prior to CVAA.

Accessibility can be achieved by building accessibility features into the equipment or relying on third-party applications, so long as these applications are available at a nominal cost. Manufacturers or providers who claim accessibility is not achievable have the burden of proving such a defense. The CVAA requires the Commission to consider four factors in determining whether or not accessibility of a product or service is achievable: (1) the nature and cost of the steps needed to achieve the requirements; (2) the technical and economic impact on the operation of not only the manufacturer or provider, but also the specific equipment or service in question; (3) the type of operations of the manufacturer or provider; and (4) the extent to which the provider or manufacturer offers accessible services or equipment containing varying degrees of functionality and features at differing price points. The achievability requirements established by Section 716 become effective October 8, 2013.

The Order contains specific waivers and exemptions to the new accessibility requirements. Section 716 makes manufacturers and providers of customized equipment or services, services or equipment designed primarily for purposes other than using advanced communications services ("ACS"), public safety ACS, and certain other classes of ACS eligible for a waiver from its requirements. These entities must file a Request for Waiver with the Consumer and Governmental Affairs Bureau ("CGB"). CGB subsequently issues a Public Notice regarding the waiver request and must make a determination within 180 of such notice.

The Commission also must implement new recordkeeping and enforcement requirements. Section 717 requires manufacturers and providers to maintain records of the "efforts taken" to comply with Sections 255, 716, and 718, all of which govern accessibility. Although the Commission does not mandate a specific method of recordkeeping, manufacturers and providers must be prepared to produce sufficient records demonstrating non-achievability or showing that a third party application is accessible and available at nominal cost, keep three sets of records, and annually certify to the Commission that they are complying with recordkeeping requirements. The FCC also requires that records be preserved for a period of two years from the date the covered entity ceases to offer or distribute the product or service to the public. Section
717 recordkeeping requirements are effective October 8, 2012.

The new enforcement rules under Section 717 consolidate current provisions under Section 255 with new complaint procedures covering all services subject to Section 255 and Section 716. Under the new rules, consumers must file a Request for Dispute Assistance ("Request") with CGB prior to filing a complaint. The purpose of this Request is to offer the covered entity and the consumer an opportunity to reach a settlement on their own. If CGB discovers that an entity is exempt from Section 716 obligations, CGB will inform the consumer why the entity has no responsibility and the dispute will terminate. If the entity and consumer have not reached a settlement after thirty days, the consumer may file an informal complaint.

The informal complaint process is designed to mitigate burdens consumers might face with formal complaints. An informal complaint must include a statement of facts explaining the violation, the date the consumer acquired the product or service in question, and certification that the consumer previously filed a Request. Next, the Commission serves a copy of the complaint to the entity and gives the entity twenty days from the date of service to respond. The entity’s answer must include the steps taken to achieve accessibility or its "not achievable" standard, any defenses, a signed declaration, and any proposed alternative relief. The Commission then applies the four achievability factors to determine whether the accessibility of the entity’s product or service is “not achievable.” This determination must be made within 180 days of the complaint’s filing.

If the consumer chooses to forgo the informal complaint process, Section 717 permits the filing of a formal complaint. The Commission requires both the complainant and defendant to: (1) show a good faith attempt to settle before filing of complaint, and (2) submit detailed factual and legal support with affidavits and documentation for their position. Section 717 likewise places strict limits on the availability of discovery and subsequent pleadings, in order to make the process less burdensome for the complainant.

In addition to implementing new achievability, recordkeeping, and enforcement standards, the Commission also seeks further comment on several additional topics in a Further Notice of Proposed Rulemaking. Specifically, the Commission asks for comment and clarification on: (1) exemptions for small businesses, (2) Section 718 implementation (mobile browsers), (3) the meaning of “interoperable video conferencing,” (4) accessibility of information content, (5) electronically mediated services, (6) performance objectives, (7) safe harbor provisions, and (8) recordkeeping and enforcement for Section 718.

*Summarized by Lauren King*

The Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, requires operators of websites or online services directed at children under the age of 13, or those with actual knowledge they are collecting personal information from children under 13, to obtain verifiable consent from parents before collecting, using, or disclosing such information from children. The Children's Online Privacy Protection Rule ("COPPA Rule" or "Rule"), 16 C.F.R. § 312, which implemented the COPPA statute, became effective on April 21, 2000. The Rule gives parents control over what personal information websites may collect from children under 13.

The Federal Trade Commission ("FTC" or "Commission") previously reviewed the COPPA Rule in 2005 and made no changes. In 2010, considering evolving technologies and changes in children’s use and access of the Internet, the FTC began another review of the Rule. On April 5, 2010, the Commission sought public comment on all aspects of the COPPA Rule. Additionally, the FTC held a public roundtable and reviewed 70 suggestions from industry, advocacy groups, academics, technologists, and members of the public. The Commission now proposes amendments to ensure that the Rule continues to protect children’s privacy in five areas: definitions, parental notice, parental consent mechanisms, confidentiality and security, and the role of self-regulatory “safe harbor” programs.

Definitions: The COPPA Rule provides that required operators get parental consent before collecting personal information from children. The FTC proposes modifying the definitions of "collects or collection;" "online contact information;" "personal information;" "support for the internal operations of the Web site or online service;" and "Web site or online service directed to children." For example, "personal information" would now include geo-location information and some types of persistent identifiers used for purposes other than the website’s internal operations, for example, tracking cookies used for behavioral advertising. Additionally, the FTC proposes loosening the definition of "collection," as it pertains to the collection of children’s personal information. Doing so would allow operators to permit children to join interactive communities without parental consent, so long as the operators use reasonable measures to delete all or virtually all children’s personal information before making it public.

Parental Notice: The FTC proposes changes to existing rules that require website operators and online service providers to format parental notice information. The proposed amendments suggest that parents be given upfront,
succinct notice of key information. In other words, operators may not bury such within a privacy policy on their website.

*Parental Consent Mechanisms:* Many commentators suggested simplifying and modernizing the Rule’s mechanisms for gaining parental consent. The FTC proposes additional methods of getting verified parental consent, such as electronic scans of signed parental consent forms, video-conferencing, and use of government-issued identification confirmed against a database, as long as the parent’s ID is deleted promptly after verification is complete. These options would be in addition to the nonexclusive list of methods currently set forth in the Rule. The FTC also encourages the development of new consent methods by creating a voluntary 180-day notice and comment process whereby parties may request FTC approval of a specific consent mechanism. Additionally, the FTC proposes allowing operators partaking in a FTC approved safe-harbor program to use a method authorized by that program.

The Commission proposes elimination of the method of parental consent, known as “e-mail plus”, because it was found to be less reliable. This method allows operators that use collected information for internal purposes only to obtain consent through an email to the parent.

*Confidentiality and Security Requirements:* The FTC proposes stronger confidentiality and security requirements in the Rule to improve the protection and integrity of children’s personal information. Website operators would make certain that any service providers or third-parties to whom they disclose a child’s personal information use reasonable procedures to protect it; that operators retain the information for only a reasonably necessary amount of time; and that they use reasonable measures to correctly delete the information to protect against unauthorized access or use during its disposal.

*Safe Harbor:* The COPPA statute includes a “safe harbor” provision for participants in FTC-approved COPPA self-regulatory programs, intending to encourage industry members and other groups to develop their own COPPA oversight programs. The Rule currently provides that operators fully complying with an approved safe harbor program will be “deemed to be in compliance” with the Rule for enforcement purposes. Instead of formal enforcement actions, such operators are instead subject first to the safe harbor program’s own review and disciplinary process. The Commission proposes stronger oversight of self-regulatory “safe harbor programs” by requiring audits of their members, either annually or more frequently, and periodic reporting of the audit results to the FTC.

*Summarized by Rebecca Borges*

On October 26, 2011, Representative Lamar Smith (R-TX) introduced H.R. 3261, the Stop Online Piracy Act ("SOPA"). SOPA is the House of Representatives' version of Senate Bill S. 968, the PROTECT IP Act, introduced May 12, 2011 by Senator Patrick Leahy (D-VT). Title I of SOPA aims to provide the government and intellectual property holders with additional tools to prevent access to foreign sites that violate United States intellectual property law. Title II provides increased penalties for willfully infringing copyrights, economic espionage, and trafficking in illegal medicines and counterfeiting goods or services intended for the military, law enforcement, or critical infrastructure applications.

TITLE I: COMBATING ONLINE PIRACY

Section 102 of SOPA authorizes the Attorney General ("AG") to seek a court order issuing a preliminary injunction, injunction, or restraining order against a foreign infringing site. A site is designated a "foreign infringing site" if (1) the site or portion thereof is directed towards users in the United States and is actually used in the United States, (2) the site would be subject to seizure in the United States if it were a domestic site, and (3) the owner or operator of the site is committing or facilitating the commission of online piracy. The court order would require the owner, operator, or domain name registrant, or the site of the domain name registrant if such person cannot be found, to cease and desist all infringing activity.

Additionally, Section 102 authorizes the AG, with court approval, to serve a copy of the court order on Internet service providers, Internet search engines, payment network providers, and Internet advertising services. The court order requires these entities to "take technically feasible and reasonable" preventative measures against the foreign infringing site within five days of being served. Internet service providers are required to prevent access to the sites, including taking measures to prevent the transfer of the infringing site's domain name to the domain name's Internet Protocol (IP) address. Internet search engines must prevent the foreign infringing site from being served as a direct hyperlink. Payment network providers are required to prevent payment transactions involving customers located within the United States or individuals subject to United States jurisdiction. Internet advertising services that contract with the foreign infringing site must stop providing advertisements to the site, cease making advertisements for the site, and cease providing or receiving any compensation relating to the site. If any provider listed in Section 102 "knowingly and willfully fails to comply" or if any entity
"knowingly and willfully provides or offers to provide" a product or service to circumvent the requirements of Section 102, the AG may bring an action for injunctive relief against them.

Section 103 provides a "market-based system" for an intellectual property right holder ("plaintiff") harmed by the foreign infringing site to serve payment network providers and Internet advertising services a written notice of the identified site. The notice requires the payment service providers and Internet advertising services to suspend business with the site. The owner, operator, or domain name registrant of the identified foreign infringing site may serve a counter notification to the payment service providers and Internet advertising services if it (1) provides a name, address, email address, and telephone number, (2) states it has a good faith belief that it is not engaged in online piracy, and (3) consents to jurisdiction to the United States courts. If an effective counter notification is made, or if the Internet advertising service or payment network provider fails to comply, the plaintiff may file suit for a temporary restraining order, a preliminary injunction, or an injunction against the owner, domain name registrant of the identified foreign infringing site as under Section 102.

Section 104 provides immunity from liability to service providers that take action in accordance with Sections 102 and 103 or if the service provider takes voluntary action against a site that it has reasonable belief is a foreign infringing site. Section 105 provides immunity for entities that stop providing services to an Internet site that the entity believes in "good faith" and based on "credible evidence" is offering, selling, dispensing, or distributing (1) prescription medication without a valid prescription or (2) prescription medication that is adulterated or misbranded. Section 106 requires the AG to conduct a study on the enforcement and effectiveness of the Act and to amend the Act to adapt to emerging technologies.

TITLE II: ADDITIONAL ENHANCEMENTS TO COMBAT INTELLECTUAL PROPERTY

Section 201 proposes amending 17 U.S.C. § 506(a) to expand criminal copyright infringement to include (1) the distribution of copyrighted work through digital transmission for financial gain and (2) the distribution or public performance of a "work being prepared for commercial dissemination" by making the work available on a computer network. The Act defines "work prepared for commercial dissemination" to include a computer program, a
musical work, a motion picture or other audiovisual work, or a sound recording, if the (1) copyright owner expects to distribute the work commercially and the work has not been commercially distributed in the United States with the copyright owner's authorization, or (2) the copyright owner does not intend to offer copies of the work through commercial distribution but reasonably expects other forms of commercial dissemination. Additionally, the definition includes a motion picture that (1) has been made available for viewing in theaters but has not been made available for copies of sale or (2) had not been commercially disseminated.

Section 202 amends 18 U.S.C. § 2320 by expanding the criminal offenses of trafficking in inherently dangerous goods or services to include (1) the importation, exportation, or trafficking in counterfeit drugs or (2) intentionally participating or knowingly aiding in such trafficking. Section 202 also would expand 18 U.S.C § 2320 to include trafficking in goods and services falsely identified as meeting military standards or good and services intended for use in a national security, law enforcement, or critical infrastructure application.

Section 203 alters the penalties for economic espionage of trade secrets by (1) increasing the penalties for individuals from a maximum of $500,000 to "not less than $1,000,000 and not more than $5,000,000", and (2) increasing the fines for organizations that violate trade secret laws from a maximum of $10,000,000 to "not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization".

Section 204 requires the Unites States Sentencing Commission to review Federal Sentencing Guidelines for intellectual property crimes, and if appropriate, grants them the authority to make amendments. Finally, Section 205 requires the Secretary of State and Secretary of Commerce to appoint at least one intellectual property attaché to United States embassies in each geographic region covered by the regional bureau of the Department of State, with the purpose of advancing intellectual property policy of the United States Government.

*Summarized by John Billings*


On July 20, 2011, the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade approved the proposed Secure and Fortify Electronic (SAFE) Data Act. The SAFE Data Act has two focuses: first, to establish national uniform standards for personal data security, and second, to notify consumers in the event of a data breach. The bill
The Act defines “personal information” as encompassing “an individual’s first name or initial and last name, or address, or phone number,” combined with one or more of that individual’s Social Security number, Driver’s license number, passport number, military identification number, financial account number, credit card number, or debit card number (as well as any required security code necessary for financial account access. Personal information under the Act does not contain any public record information. The Act is silent on the disclosure of email addresses.

II. REQUIREMENTS FOR INFORMATION SECURITY

The Act first requires the Federal Trade Commission ("FTC") to promulgate regulations requiring any person engaged in interstate commerce that maintains personal information data to “establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information.” Under Section 2 of the Act, these entities must establish a security policy for the safe handling of this information and institute processes that take preventative and corrective action to mitigate possible security breaches. Possessors of such information also must evaluate the personal data they maintain and retain only the personal information necessary to effectuate a legitimate business purposes. Entities subject to the Gramm-Leach-Bliley Act are exempt from this requirement.

The FTC is required within one year of enactment to issue rules and guidance to identify methodologies or technologies that would render data in its electronic form “unusable, unreadable, or indecipherable” in the event of a breach. These guidelines may not mandate the deployment of any specific technology, product, or software.

III. NOTIFICATION REQUIREMENTS IN THE EVENT OF A SECURITY BREACH

Section III establishes the notification requirements in the event of a breach of security that may compromise an individual’s personal information. Within 48 hours of determining that a breach has occurred, entities must notify appropriate law enforcement and the FTC, as well as begin to notify individuals whose information was compromised as a result of the breach. After receiving such notice the FTC may place notice of the breach on its website.

Notice may be provided by written communication or email and must
contain a description of the personal information that was acquired or accessed
by an unauthorized person. If the breach involves the disclosure of information
of over 5,000 individuals, the entity also must notify all the major credit
reporting agencies. The entity that possessed the information may be required
to provide two years of credit monitoring services at no cost to the endangered
party, depending on the nature of the information exposed. These notice
requirements may be substituted for other measures if the costs to provide
notice would be excessive or the entity lacks sufficient contact information to
notify the parties. Parties may be exempt if they determine that the breach in
question provides no reasonable risk of identity theft, fraud or unlawful
conduct.

IV. APPLICATION AND ENFORCEMENT

The requirements of the Act are enforceable against any information broker
or person engaged in interstate commerce that owns or possesses data
containing personal information related to that commercial activity. The FTC
can prosecute individuals for noncompliance with the Act as an unfair
deceptive act or practice under section 18(a)(1)(B) of the Federal Trade
Commission Act.

The Act permits State Attorneys General to bring suit in United States
District Court on behalf of its residents to enjoin further violations, compel
compliance, and obtain civil penalties as related to the disclosure of personal
info. Penalties are determined by an amount not to exceed $11,000 multiplied
by the number of days of noncompliance, with a maximum total liability of
$5,000,000 for a single breach event. Each failure to send notification of a
security breach as required under Section III of the Act also may be assessed a
fine not to exceed $11,000 per failure.

The FTC also may initiate its own actions and has a right to intervene in
state actions. Further, if the Commission has instituted a civil action for a
violation, no State Attorney General or state official may bring an action under
the Act. Importantly, Section VI supersedes any state statutes or regulations
that expressly mandate information security practices as related to the
treatment of personal information. However, such preemption does not
foreclose states from enforcing other consumer protection laws.

*Summarized by Sam Thomas*