December 2014

the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, INTERNET ADVERTISING, MARKETING AND INFORMATION SERVICES LAW AND POLICY

VENABLE SNAPSHOT

Received *Chambers USA* "Award of Excellence" for the top privacy practice in the United States

Named Two of the "Top 25 Privacy Experts" by *Computerworld*

"Winning particular plaudits" for "sophisticated enforcement work" – *Chambers and Partners*

Recognized by *Chambers Global* and the *Legal 500* as a top law firm for its outstanding data protection and privacy practice

ISSUE EDITORS:

Stuart P. Ingis
singis@Venable.com

Michael A. Signorelli
masignorelli@Venable.com

Ariel S. Wolf
awolf@Venable.com

ADDITIONAL CONTRIBUTORS:

Emilio W. Cividanes
ecividanes@Venable.com

David L. Strickland
dlstrickland@Venable.com

Julia Kernochan Tama
jktama@Venable.com

Kelly A. DeMarchis
kademarchis@Venable.com

Tara Sugiyama Potashnik
tspotashnik@Venable.com

Matt H. MacKenzie
mhmackenzie@Venable.com

Rob L. Hartwell
rhartwell@Venable.com

Emma R. W. Blaser
eblaser@Venable.com

Chan D. Lieu
cdlieu@Venable.com

Marissa L. Kibler

The November 2014 elections will bring change to Capitol Hill when the 114th Congress commences in January. In the House, Republicans increased their majority by twelve seats. The Republicans also gained control of the Senate, and will control both houses of Congress for the first time since 2006.

Change in control of the Senate will bring about change in the leadership of committees with jurisdiction over privacy and data security. In the Senate Commerce Committee, current Chairman Jay Rockefeller (D-WV) who is set to retire will be replaced by current Ranking Member John Thune (R-SD). In the Senate Judiciary Committee, Ranking Member Charles Grassley (R-IA) will replace current Chairman Patrick Leahy (D-VT), who will serve as ranking member. In the Senate Homeland Security and Governmental Affairs Committee, Ron Johnson (R-WI) will take over for Tom Carper (D-DE) as chairman.

Overall, when the 114th Congress begins in January, privacy and data security issues are expected to remain on the agenda for several key committees. In particular, House Energy and Commerce Committee Chairman Fred Upton (R-MI) recently announced that the committee will hold a series of hearings next year focusing on cyber threats. Other issues that will continue to receive attention in the 114th Congress include FTC oversight and reform, data security and breach notification, and cybersecurity. This issue of the download covers recent developments in auto privacy self-regulation, cybersecurity policymaking in Congress and the Executive Branch, and federal agency efforts related to drones and facial recognition technology, as well as other state and international developments.

In this Issue:

In the Marketplace

Automakers Commit to Protect Consumer Privacy through Self-Regulation

The two leading trade associations for automobile manufacturers—the Association of Global Automakers and the Alliance of Automobile Manufacturers, Inc.—released the Consumer Privacy Protection Principles for Vehicle Technologies and Services ("Principles") in November 2014.[1] The Principles were developed jointly by the two trade associations over the course of many months in recognition of the increasing ability of in-car technologies and services to collect and use information about the driving experience.

The Principles apply to "covered information," which is defined as any information collected, generated, recorded, or stored by a vehicle in electronic form, when retrieved from a vehicle by the manufacturer, that is linked or linkable to the vehicle from which the information is retrieved, or personal subscription information provided by individuals who register for vehicle technologies and services. When covered information includes biometric, driver behavior, and geolocation information, that information receives heightened protection under the Principles. In addition, the Principles require a warrant or court order for government access to geolocation information.

The Principles are meant to be a baseline framework that different manufacturers may implement as they see fit. Subscribing to the Principles is voluntary. At the time of release, nineteen auto manufacturers had made a public commitment to subscribe to the Principles. Participating companies must implement the Principles for new vehicles manufactured no later than Model Year 2017 and for vehicle technologies and services, subscriptions that are initiated or renewed on or after January 2, 2016.

The Principles are as follows:

1. **Transparency**: Participating Members commit to providing Owners and Registered Users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of Covered Information.
2. **Choice:** Participating Members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information.
3. **Respect for Context**: Participating Members commit to using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.
4. **Data Minimization, De-Identification & Retention**: Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes.
5. **Data Security**: Participating Members commit to implementing reasonable measures to protect Covered Information against loss and unauthorized access or use.
6. **Integrity & Access**: Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to offering Owners and Registered Users reasonable means to review and correct Personal Subscription Information that they provide during the subscription or registration process for Vehicle Technologies and Services.
7. **Accountability**: Participating Members commit to taking reasonable steps to ensure that they and other entities that receive Covered Information adhere to the Principles.

Heard on the Hill

House Intelligence Committee Hearing on Cybersecurity Threats

On November 20, 2014, the House Permanent Select Committee on Intelligence ("Committee") held a hearing entitled "Cybersecurity Threats: The Way Forward." The witness before the Committee was Admiral Michael S. Rogers, Commander, U.S. Cyber Command and Director, National Security Agency. In his testimony, Adm. Rogers discussed the scope of the cybersecurity threat facing critical infrastructure.

[1] Ass'n of Global Automakers and the Alliance of Auto. Mfrs., *Privacy Principles For Vehicle Technologies and Services* (Nov. 2014), available at https://www.globalautomakers.org/media/papers-and-reports/privacy-principles-for-vehicle-technologies-and-services.

In response to questioning, Adm. Rogers stated that the Committee should assume that there are nation states that have the capability to infiltrate the United States' critical infrastructure. He further stated that nation states have already been able to gain access to industrial control systems and appeared to be gathering information about how these systems work. Adm. Rogers also noted that organized crime, which has traditionally focused its activities with respect to cyber attacks on stealing data that it can sell, has begun serving as a surrogate for nation states to obscure the source of an attack.

According to Adm. Rogers, responding to these threats will require greater information sharing between the government and the private sector. Specifically, he stated that the government needs to be able to inform the private sector about known threats that companies might encounter and measures they should take to respond to these threats. He also stated that the government needs to be able to receive information from private companies about attacks on their systems. To facilitate this type of information sharing, Adm. Rogers encouraged the Committee to publicly define the types of information that would be shared between the government and the private sector. He testified that clearly defining the types of information that will be shared will ease fears that the private sector will share personal information about their customers with the government, as the government does not need such information to better protect the private sector against cyber attacks.

President Signs Cybersecurity Bills

On December 18, President Obama signed into law five bills that address cybersecurity. The Cybersecurity Enhancement Act of 2014 (S. 1353), amends existing authorities of the National Institute of Standards and Technology ("NIST") to require the agency to work with the private sector to develop a voluntary, flexible cybersecurity framework for critical infrastructure. This follows the Administration's Cybersecurity Executive Order 13636 issued on February 12, 2013, that called for NIST to adopt a framework and NIST's subsequent issuance of the first version of the framework in February 2014, a year later. The bill also requires NIST to promote cybersecurity education and awareness programs as well as encourage cybersecurity research by the federal government.

President Obama also signed into law the following four cybersecurity bills applicable only to government agencies: National Cybersecurity Protection Act (S. 2519), Cybersecurity Workforce Assessment Act (H.R. 2952), Federal Information Security Modernization Act of 2014 (S. 2521), and Border Patrol Agent Pay Reform Act (S. 1691).

From the White

BuySecure Initiative

On October 17, 2014, President Obama issued an Executive Order ("EO") announcing a White House initiative called BuySecure.[2] The President announced his EO in an address given at the Consumer Protection Financial Bureau ("CPFB"), where he identified data breaches as a growing threat to American consumers and outlined a number of efforts designed to help shore up payment information security and other areas of cybersecurity policy in the United States.

A component of the BuySecure initiative encourages the adoption of Chip-and-PIN technology into American point-of-sale transactions. The EO requires that the federal government incorporate Chip-and-PIN technology into all federal government credit cards and update federal government credit-card terminals to accept the technology. In his address at the CFPB, the President also noted that several of the nation's largest retailers will be updating their point-of-sale terminals to accept the new technology early in 2015.

As the President explained in his address at the CFPB, the BuySecure initiative will also augment the resources available to those fighting and responding to identity theft. The Administration will support the Federal Trade Commission in expanding IdentityTheft.gov, an online portal for identity theft victims, and will also seek to increase information sharing between the government and the private sector to limit the scope and reach of data breaches. The President also expressed support for the private sector to make credit-score information more easily accessible.

The President also announced a forthcoming "Cybersecurity and Consumer Protection Summit," which will take place in early 2015. In his address, the President explained that the Summit will assemble stakeholders from the financial sector to

[2] Exec. Order No. 13681, 79 Fed. Reg. 63,489 (Oct. 17, 2014), *available* at https://www.federalregister.gov/articles/2014/10/23/2014-25439/improving-the-security-of-consumer-financial-transactions.

collaborate and share best practices, promote stronger security standards, and discuss the future of technologies that help protect consumers from financial harm. The President reiterated his desire for Congress to pass comprehensive data breach legislation and comprehensive cybersecurity legislation as key components of the Nation's strategy to address these growing threats in the future.

Around the Agencies

NTIA Facial Recognition Technology Multistakeholder Process

On November 6, 2014, the National Telecommunications and Information Administration ("NTIA") held its tenth Privacy Multistakeholder Meeting on drafting a voluntary framework for facial recognition technology or "FRT," focusing on potential practices associated with the collection, storage, and transmission of facial recognition data. Participants discussed potential issues to address in a Code of Conduct, including encryption of facial recognition data, secure storage, access limitations, and authentication. Participants also discussed whether entities that use FRT for certain purposes, such as crime prevention, should be allowed to decline requests from individuals seeking to withdraw their facial recognition data from a database.

An eleventh meeting took place on December 15, 2014, continuing the group's discussions on storage, transmission, and withdrawal. The group weighed in on draft code provisions prepared by separate groups of volunteering participants. Participants considered a proposed requirement that would direct entities collecting facial recognition data to adopt "appropriate" retention and disposal practices and to disclose how long facial recognition data will be retained and any other retention and disposal practices. The group also discussed whether the code should reference specific cryptographic standards. There was additional consideration on whether the code should include a provision that would require an entity to establish a procedure to allow consumers to request the removal of their facial templates.

The next meeting is expected to take place in early 2015 and will focus on refining draft code language and consider potential issues regarding audit trails, access, and correction.

Vehicle Privacy: FTC Weighs in on V2V Technology and Sen. Schumer Introduces GPS Legislation

As a sign of the Federal Trade Commission's ("FTC" or "Commission") continuing interest in the "Internet of Things," the Commission filed a comment in the National Highway Traffic Safety Administration's ("NHTSA") advance notice of proposed rulemaking ("ANPRM") related to vehicle-to-vehicle or "V2V" communications. [3] The FTC's comments focused largely on privacy and security concerns implicated by V2V technologies.

NHTSA launched the ANPRM in late summer along with a supporting comprehensive research report on V2V communications technology. The ANPRM is intended to help NHTSA and the Department of Transportation gather input from the public and stakeholders in advance of a notice of proposed rulemaking, scheduled to be delivered in 2016 by the agency. V2V communications systems allow nearby vehicles to engage in a dynamic wireless exchange of anonymous data. The technology offers the potential for significant safety improvements by allowing vehicles to sense imminent threats arising from the relative positions of other vehicles and road hazards and then issue driver advisories or take preemptive action to avoid and mitigate crashes. The technology is also a building block for "driverless" vehicles.

The Commission's comments highlighted its previous work on connected vehicles at its Internet of Things workshop held in November 2013, which, in part, examined privacy and security issues relating to connected car technologies. The workshop highlighted three key concerns that arise out of increased vehicle connectivity: (1) concerns over the ability of connected car technology to track consumers' precise geolocation over time; (2) concerns over information about driving habits being used to price insurance premiums or set prices for other auto-related products without drivers' knowledge or consent; and (3) concerns regarding the security of connected cars. The FTC's comments support NHTSA's efforts to take privacy and security concerns into account as it continues its development of V2V policy.

---

[3] Fed. Trade Comm'n, Comment Before the National Highway Traffic Safety Administration Regarding the NHTSA Proposed Rule Entitled "Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications (Oct. 2014), *available* at http://www.ftc.gov/policy/policy-actions/advocacy-filings/2014/10/federal-trade-commission-comment-national-highway.

In a related development, Congress is also looking at vehicle privacy issues. Senator Chuck Schumer (D-NY) introduced legislation (S. 2933) that would prohibit the placement of a GPS tracking device on a vehicle without the vehicle owner's consent. Following his announcement in October that he was drafting the bill, Senator Schumer introduced the final version on November 17, 2014. The stated purpose of the bill is to prevent the stalking of individuals through the use of GPS devices – particularly domestic violence victims and "other vulnerable populations." The bill grants certain exceptions to the prohibited use of GPS devices on another individual's vehicle, including for the purpose of protecting the safety of the vehicle owner. The bill was referred to the Senate Judiciary Committee.

FFIEC Issues Cybersecurity Observations

On November 3, 2014, the Federal Financial Institutions Examination Council ("FFIEC") issued a document titled "FFIEC Cybersecurity Assessment General Observations" ("Observations"), which the FFIEC gleaned from its recent cybersecurity assessments of regulated financial agencies.[4] The Observations included a recommendation for financial institutions to join the Financial Services Information Sharing and Analysis Center ("FS-ISAC"). The assessment was a pilot of the FFIEC's cybersecurity assessment program, and included over 500 community financial institutions. The Observations are not formal guidance from the FFIEC.

The FFIEC found that cyber risks faced by institutions varied significantly between entities. The FFIEC explained that the level of cyber risk is based on an institution's activities and connections to the Internet, balanced against any implemented safeguards. The Observations called for greater engagement from senior management and board members in cybersecurity preparedness. The FFIEC offered examples of what elements an institution should review, such as the connection types (e.g., wireless networking and bring-your-own-device policies), the products and services offered, and what technology is used to deliver those services. As well as assessing cyber risk, the FFIEC also suggests that institutions should consider their preparedness for a cybersecurity event, and should review risk management protocols, threat intelligence, cybersecurity controls, and vendor management.

The FFIEC concluded its observations by reissuing its call for greater cybersecurity awareness and engagement by boards of directors and senior management. Additionally, the Observations called for greater integration and information sharing between financial institutions. One way the FFIEC recommends financial institutions to share information is through the FS-ISAC. In a separate release, the FFIEC explained that the FS-ISAC information sharing is important to mitigating cybersecurity risk and gaining insight into specific vulnerabilities.[5]

FCC Clarifies Opt-Out Rules for Fax Advertisements

On October 30, 2014, the Federal Communications Commission ("FCC") issued an order requiring opt-out information on all fax advertisements, even when the recipient has previously consented to receiving the ads. A footnote in the 2006 Junk Fax Order referenced "unsolicited" faxes, which led some companies to believe that the Order did not apply to faxes sent to persons that have given prior express permission. In its recent Order, the FCC stated that consumers need an easy and cost-free way to opt out if they should ever change their minds about receiving faxes, and therefore requires all fax ads – including those sent to persons who previously consented – to meet the opt-out notice requirements of the original 2006 Order. These requirements include: (1) a clear and conspicuous notice of opt-out on first page of ad; (2) a cost-free opt-out; and (3) a 30-day window to comply with an opt-out request.

Acknowledging possible confusion about the requirements for ads sent to previously consenting persons, the FCC issued retroactive waivers to some fax advertisers for a lack of opt-out information on previous transmittals. These advertisers now have six months to come into compliance with the regulations. In the meantime, other "similarly situated parties" may seek waivers to cover past noncompliance.

Decision Confirms FAA has Authority to Regulate Civilian Drones

On November 18, 2014, the National Transportation Safety Board ("NTSB") released a decision holding that the Federal Aviation Administration ("FAA") has the authority to regulate civilian drones.[6] This decision overturns a March 6, 2014 ruling by an administrative law judge ("ALJ"), which held that the FAA had no authority to regulate in this area.[7] Both decisions

[4] Fed. Fin. Insts. Examination Council, FFIEC Cybersecurity Assessement General Observations (2014), *available* at https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf.

[5] Fed. Fin. Insts. Examination Council, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement* (2014), *available* at https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf.

[6] Administrator v. Pirker, NTSB Order No. EA-5730 (2014), *available* at http://www.ntsb.gov/legal/pirker/5730.pdf.

[7] *Id.* at 3.

rested on the interpretation of the word "aircraft." The ALJ held that a drone being used to film a promotional video for the University of Virginia did not fit within the meaning of "aircraft," and therefore FAA rules did not apply. Instead, the ALJ found the drone to be within the definition of a model aircraft, a category he said was exempted from FAA rules on aircrafts. The NTSB overruled that interpretation, stating in its decision that the language in the regulations was clear on its face that an aircraft is "a device that is used or intended to be used for flight in the air" and "includes any aircraft, manned or unmanned, large or small." The NTSB noted that there is no formal exception for model aircraft, although some regulations made by the FAA may not practically apply.

In other above-related views, on December 19, 2014, retiring Senate Commerce Committee Chairman Jay Rockefeller (D-WV) introduced legislation entitled "the Unmanned Aircraft Systems ("UAS") Privacy Act of 2014" to address potential privacy issues regarding the commercial use of drones. The bill would require commercial drone operators to adopt privacy policies on data collected and used from drone surveillance.

In the States

California Eraser Button Law

Beginning on January 1, 2015, operators of Internet websites, online services, online applications, and mobile applications (together, "Service") in California will be required to provide a mechanism allowing minors registered with a Service to remove content and information from the operators' Service that they posted themselves. This so-called "Eraser Button" law (S.B. 568), which was signed into law by the Governor of California on September 23, 2013, covers Service that is directed to minors or operated with actual knowledge that minors are using the sites, services, or apps. The new law requires operators to provide a removal mechanism only to minors registered with the site, service, or app.

Under the new law, operators must (1) notify the registered minor of the existence of the mechanism; (2) provide clear instructions on how to remove or request removal of content; (3) provide a means for the minor to remove or anonymize the content that the minor has posted or request that the operator remove or anonymize it; and (4) provide a disclaimer notice that the removal process does not ensure complete or comprehensive removal.

The law provides for other exceptions, including for content required to be maintained by federal or state law, and content posted by a minor who was paid to post it.

The law also contains advertising and marketing restrictions for operators of Service directed to minors or operated with actual knowledge that minors are using the sites, services, or apps. Specifically, the law prohibits operators from advertising or marketing certain products and services that minors are not permitted to purchase by law, such as firearms, tobacco products, and ultraviolet tanning services. Operators of services directed to minors may comply with the law if the operator notifies its advertising service that it is a site directed to minors. Operators with actual knowledge that a minor is using the Service are in compliance with the law if the operator takes "reasonable actions in good faith designed to avoid" marketing and advertising to the minor.

One of the key questions for entities looking to comply with the law will be whether a site, service, or app is "directed to minors." The law defines "directed to minors" as "created for the purpose of reaching an audience that is predominately comprised of minors, and is not intended for a more general audience comprised of adults."[8] No service is deemed "directed to minors" solely because it refers or links to another online service directed to minors using information location tools, including a directory, index, reference, pointer, or hypertext link.[9]

Michigan Introduces Proposed Legislation Regarding "Data Brokers"

On November 12, 2014, Michigan State Representative Sean McCann (D-60) introduced H.B. 5923, a bill to amend Michigan's Identity Theft Protection Act with new requirements for entities that own or license data that is included in a database. Specifically, the bill would prohibit the following actions if taken by an entity that owns or licenses data in a database:

- fail to permit a consumer the ability to review personal identifying information in the database;

[8] Cal. Bus. & Prof. Code § 22580(e)

[9] *Id.*

- fail to display an opt-out notice on the entity's webpage (as required by the bill); or
- accept payment from a consumer who demands to review or remove personal identifying information from a database.

For purposes of the bill, personal identifying information means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts. This includes, but is not limited to:

- a person's name, address, telephone number, driver license or state personal identification card number, or social security number;
- place of employment, employee identification number, employer or taxpayer identification number, government passport number, or health insurance identification number;
- mother's maiden name;
- demand deposit account number, savings account number, financial transaction device account number, or the person's account password;
- any other account password in combination with sufficient information to identify and access the account;
- automated electronic signature or biometrics;
- stock or other security certificate or account number, credit card number; or
- vital record, or medical records or information.

The bill would require that the opt-out notice be conspicuously posted on an entity's website. This notice would need to provide "specific and easily understood instructions" for how a consumer may make an opt-out election on the entity's website that would stop that consumer's personal identifying information from being shared with, or sold to, a third party. The bill would exempt federally regulated financial institutions and entities covered by the Health Insurance Portability and Accountability Act ("HIPAA"). Violation of the bill would be punishable by fines ranging from $1,000 to $3,000.

International
EU Cookie Sweep Update

Between September 15 and September 19, the Article 29 Working Party ("WP29") conducted an audit of major European websites to verify their compliance with Directive 2002/58/EC ("Directive"). The Directive requires that website operators obtain prior informed consent from individuals before placing a cookie on the individual's web browser or accessing information stored on a cookie. The Directive exempts some types of cookies such as user-input cookies, authentication cookies, user-centric security cookies, and others.

Any European Data Protection Authority ("DPA") could participate in the audit, which only targeted websites that are directed at European consumers. The WP29 has not identified the number of websites that were audited; however, on September 22, 2014, the French DPA announced that it audited 100 websites. The French DPA has further announced that it reviewed websites' practice pertaining to:

- the number and type of cookies stored on a user's computer;
- the way the information on a website's practices with respect to cookies is conveyed to users;
- the visibility and quality of the information provided to users;
- the process of obtaining a user's consent; and
- the consequences for a user who refuses cookies.

The DPAs will share the results of their audits with the WP29, which will likely release a public statement about the results of the cookie sweep day in the future.

[10] 45 C.F.R. §§ 160 et seq. (2014).

About Venable's Privacy and Data Security Team

Venable's privacy and data security attorneys, pioneers in the field, provide an integrated approach to legal and business solutions in e-commerce, Internet advertising, financial services, homeland security and government surveillance, telemarketing and medical privacy. Our attorneys are well-versed in the evolving U.S., Canadian, European and Asian regulations governing our clients' businesses, and assist with drafting statutes and regulations. Our clients represent a variety of industries and are supported by Venable's renowned Legislative and Government Affairs, Advertising, IP and Communications Practices. Venable's Privacy and Data Security Practice is recognized in Chambers Global and the U.S. Legal 500 and has won the Chambers USA Award for Excellence.

About Venable

An *American Lawyer* Global 100 law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

Venable's Privacy and Data Security Team serves clients from these office locations:

WASHINGTON, DC
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
25TH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

SAN FRANCISCO, CA
SPEAR TOWER, 40TH FLOOR
1 MARKET STREET
SAN FRANCISCO, CA 94105
t 415.653.3750
f 415.653.3755

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949