AI AND THE EVOLUTION OF CLOUD COMPUTING: EVALUATING HOW FINANCIAL DATA IS STORED, PROTECTED, AND MAINTAINED BY CLOUD PROVIDERS

HEARING

BEFORE THE

TASK FORCE ON ARTIFICIAL INTELLIGENCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

OCTOBER 18, 2019

Printed for the use of the Committee on Financial Services

Serial No. 116–60

U.S. GOVERNMENT PUBLISHING OFFICE

42–363 PDF WASHINGTON : 2020

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
WM. LACY CLAY, Missouri
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
ED PERLMUTTER, Colorado
JIM A. HIMES, Connecticut
BILL FOSTER, Illinois
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CINDY AXNE, Iowa
SEAN CASTEN, Illinois
AYANNA PRESSLEY, Massachusetts
BEN MCADAMS, Utah
ALEXANDRIA OCASIO-CORTEZ, New York
JENNIFER WEXTON, Virginia
STEPHEN F. LYNCH, Massachusetts
TULSI GABBARD, Hawaii
ALMA ADAMS, North Carolina
MADELEINE DEAN, Pennsylvania
JESÚS "CHUY" GARCIA, Illinois
SYLVIA GARCIA, Texas
DEAN PHILLIPS, Minnesota

PATRICK MCHENRY, North Carolina, *Ranking Member*
ANN WAGNER, Missouri
PETER T. KING, New York
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
STEVE STIVERS, Ohio
ANDY BARR, Kentucky
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
TREY HOLLINGSWORTH, Indiana
ANTHONY GONZALEZ, Ohio
JOHN ROSE, Tennessee
BRYAN STEIL, Wisconsin
LANCE GOODEN, Texas
DENVER RIGGLEMAN, Virginia
WILLIAM TIMMONS, South Carolina

CHARLA OUERTATANI, *Staff Director*

TASK FORCE ON ARTIFICIAL INTELLIGENCE

BILL FOSTER, Illinois, *Chairman*

EMANUEL CLEAVER, Missouri
KATIE PORTER, California
SEAN CASTEN, Illinois
ALMA ADAMS, North Carolina
SYLVIA GARCIA, Texas
DEAN PHILLIPS, Minnesota

FRENCH HILL, Arkansas, *Ranking Member*
BARRY LOUDERMILK, Georgia,
TED BUDD, North Carolina
ANTHONY GONZALEZ, Ohio
DENVER RIGGLEMAN, Virginia
TREY HOLLINGSWORTH, Indiana

CONTENTS

WITNESSES

FRIDAY, OCTOBER 18, 2019

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

AI AND THE EVOLUTION OF CLOUD COMPUTING: EVALUATING HOW FINANCIAL DATA IS STORED, PROTECTED, AND MAINTAINED BY CLOUD PROVIDERS

Friday, October 18, 2019

U.S. HOUSE OF REPRESENTATIVES,
TASK FORCE ON ARTIFICIAL INTELLIGENCE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The task force met, pursuant to notice, at 9:33 a.m., in room 2128, Rayburn House Office Building, Hon. Bill Foster [chairman of the task force] presiding.

Members present: Representatives Foster, Cleaver, Porter, Casten, Garcia of Texas; Budd, Gonzalez of Ohio, Riggleman, and Hollingsworth.

Chairman FOSTER. The Task Force on Artificial Intelligence will now come to order. Without objection, the Chair is authorized to declare a recess of the task force at any time. Also, without objection, members of the full Financial Services Committee who are not members of the task force are allowed to participate in today's hearing, consistent with the committee's practice.

Today's hearing is entitled, "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers."

The Chair now recognizes himself for 5 minutes for an opening statement.

First off, thanks, everyone, for joining us today on what should be a very interesting hearing of the task force. Today, we are looking to explore the rise of cloud computing in the financial services sector, including the opportunities and risks of companies' migration to the cloud, as well as the regulatory framework for protecting sensitive financial information that is stored in the cloud.

And I should also mention that it seems possible that we are going to have votes called, Floor votes in the House called part way through the hearing, and in that case, we will have a game-time decision about which Members might be interested in reconvening. And if not, we can just convene for a private discussion among the Members, if that turns out to be what is feasible.

The transition to cloud computing is something that is a double-edged sword. I have faced that personally where, several years ago when I couldn't stand it anymore, what was happening in politics, and I went and downloaded TensorFlow to my laptop and worked

through the various—this is Google's open-source AI engine. And so the tradeoffs there were pretty obvious to me, that the data set I wanted to be working on fit on my laptop, but it just wasn't reasonable. The problems of having to reconfigure your system for the latest version of Python, everything like that, so that the advantages of going to a cloud-based system just for a small-scale user are enormous. Not to mention all of the defensive things that you get when you go to a competent cloud provider where the first lines of defense are actually provided by the cloud service.

But then, when you talk about the policy implications, we are always struggling with data privacy and the basic fact that AI works much better with large data sets, and that has huge policy implications with which we are struggling. If we are not careful, it is going to encourage the consolidation that is already a natural feature of any digital enterprise, which is essentially a natural monopoly, and this AI has a good chance of amplifying this. If you don't have access to the large data sets, it is hard for a startup to compete. And if they do have access, then there are huge potential—a privacy breach, for example, can cause economic damage massively in excess of the market capitalization of some little startup. And so, we have to be very careful that the AI policies that we apply to the cloud don't further force consolidation in an already consolidated industry.

The second thing is just the way that AI will be a continuing attack on privacy. Some of the most competent spear-phishing attacks now involve multifactor attacks where you are using an AI voice synthesizer in concert with a spear-phishing attack to make it very likely that an ordinary person will click on the enclosure. And so we are seeing, I think it was within the last year, that for the first time, an AI engine competed on a level playing field with teams of hackers in terms of finding software vulnerabilities.

We are talking about a future that is now, where both cyber offense and cyber defense are going to be best employed by AI. These sorts of efforts are out of the scale where a small person holding their own computer can actually hope to compete in this world, so you are going to be increasingly dependent on large cloud vendors and companies that deploy on the cloud for the defensive work that you will have to do. So, that is another huge issue.

I don't want to take up a lot of time here. I would like to get to the witnesses' testimony as much as possible, and I just want to thank you all for appearing, and I will turn it over to the acting ranking member, Mr. Riggleman.

Mr. RIGGLEMAN. Thank you, Mr. Chairman, for convening this hearing today, and generally, for pulling this task force together. If I had known a task force on artificial intelligence was a possibility, someone like myself might have run for Congress much sooner in life, so it is great to be here.

And to our witnesses, I look forward to hearing each of your testimonies, and I appreciate you being here.

Cloud services offer many benefits, both to financial institutions and consumers. And as been discussed by Ranking Member Hill and others, the work this committee is doing through both the FinTech and AI Task Forces is exploring ways to streamline compliance, lower regulatory costs, and also deliver an overall better,

more affordable experience for American consumers. By utilizing the cloud, companies can do just that, help the consumer.

Financial institutions are able to innovate and thrive in an environment that affords both scaleability and flexibility. There are, however, some risks when dealing with anything new, including technology and operations, which we look forward to discussing further in today's hearing.

In less than a century, computing has revolutionized the banking industry, along with the types and delivery of financial products and services that can be offered. Today, we all know that a majority of banking and personal finance is handled either on your phone or on a computer, but it hasn't always been that way.

Banks first started using computers in the 1950s, predominantly to process checks, and later, electronic funds transfers. Since banks first began to use computers, they have relied on the secure information technology infrastructure run by nonbank companies or third-party service providers (TSPs).

In the 1980s and 1990s, banks started to use personal computers for their employees. By the end of the 20th Century, a greater proportion of workers in finance used computers than in any other industry. Then came the internet and everything changed, especially in banking.

I say all of this to show that the financial industry has a long history of utilizing computers, and now they are outsourcing many of those responsibilities to the cloud, which is why I am glad we are having this hearing today. It is of the utmost importance to ensure that all of these operations supported by the cloud are safe, secure, and private for its customers.

We have all heard about the Capital One breach that happened this past summer, and that breach was connected to AWS, the bank's cloud service provider. Our job in Congress is to ensure that financial institutions of all sizes, their third-party service providers, and every other entity involved in the chain has legislative or regulatory certainty to do what is needed to protect consumers' data.

If you look at the Treasury's FinTech report last year on nonbanks and FinTechs, you will see a recommendation that Federal regulators ease the adoption of new technologies, such as cloud computing, with the aim of reducing barriers to the migration of activities to the cloud. I agree we need to ensure innovation is not stifled, because innovation is ultimately what protects consumers while also providing more options and more choices.

All that to say, I look forward to constructive dialogue today. I hope we can find solutions that promote innovation while also ensuring consumer safety. Today's hearing is the start of what I expect will be a longer conversation involving identity, privacy, and consumer safety. I look forward to ongoing discussions as our world only becomes more connected.

Thank you, and I yield back.

Chairman FOSTER. Thank you.

Today, we welcome the testimony of Meredith Broussard, associate professor at NYU, and affiliate faculty member at the NYU Center for Data Science; Alla Seiffert, director of cloud policy and counsel at the Internet Association; Steve Grobman, senior vice

president and chief technology officer at McAfee; Dr. Jordan Brandt, CEO and cofounder of Inpher; and Paul Benda, senior vice president for risk and cybersecurity policy at the American Bankers Association.

Witnesses are reminded that your oral testimony will be limited to 5 minutes, and without objection, your written statements will be made a part of the record.

Ms. Broussard, you are now recognized for 5 minutes.

STATEMENT OF MEREDITH BROUSSARD, ASSOCIATE PROFESSOR, NYU, AND AFFILIATE FACULTY MEMBER, NYU CENTER FOR DATA SCIENCE

Ms. BROUSSARD. Chairman Foster, Acting Ranking Member Riggleman, and members of the task force, thank you very much. It is an honor to be asked to testify today. I am a professor at NYU, a computer scientist turned journalist, and the author of a book called, "Artificial Unintelligence: How Computers Misunderstand the World."

I would like to speak today about the realities of AI and cloud computing as a way of thinking through the human-scale issues with running bank operations in the cloud.

Computer scientists like to say, the cloud is someone else's computer, and we know exactly where those computers are. Amazon Web Services controls 48 percent of the cloud computing market, and it has 4 major data centers, or server farms, in the United States. They are large, usually windowless buildings in Northern Virginia, Ohio, Oregon, and northern California.

Worldwide, 76 percent of the cloud market is controlled by a few big firms: Amazon; Google; Microsoft; and Alibaba. Inside their server farm buildings, these companies maintain thousands of physical computers that anyone can rent space on, including banks.

The U.S. Government is a cloud client. The AWS GovCloud is a secure set of servers that host data and programs for DHS, Treasury, DOD, cloud.gov, and other agencies. The computers that power the AWS GovCloud are physically located in Amazon's building in Virginia and backed up on the West Coast. Running bank operations in the cloud means moving bank operations to one of these buildings, which are vulnerable to a variety of physical or cybersecurity threats.

Again, the reality there is market dominance. We should ask, does it make sense to have all of the defense programs and all of the Citibank and Chase and SoftBank data stored in the same Amazon building in Northern Virginia?

Let's also think about the people in the banking and cloud computing ecosystem. It helps to hear from the IT professionals who manage local and cloud computers. A 2014 Ponemon Institute survey asked IT professionals to rate their organization's effectiveness in securing data and applications used in the cloud. Fifty-one percent rated their organizations as low in effectiveness. They said the likelihood of a data breach in the cloud has increased. Sixty-nine percent believe that their organizations failed to be proactive in assessing information that was too sensitive to be stored in the cloud.

If IT professionals have so little faith in their own organizations, and we know there is a high demand but low supply of IT profes-

sionals who are experts in cybersecurity, it seems that more regulation and oversight will help protect bank operations in the cloud.

I want to talk now about artificial intelligence (AI). Artificial intelligence is widely misunderstood. Hollywood images of AI like The Terminator or Commander Data from Star Trek are what most people think of when they think of AI. And these Hollywood images are delightful, but they are not real. AI is best understood as a branch of computer science, the same way that algebra is a branch of mathematics.

Inside AI, there are other branches, including: machine learning; expert systems; and natural language processing. These are just a few of them, but machine learning is the most popular kind of AI in business right now. And it is so popular that there has been linguistic confusion. When people say, "I am using AI for my business," usually what they mean is, "I am using machine learning for my business."

And "machine learning" is another misleading name. It sounds like the computer has sentience, or learning like a human being, and it does not. Machine learning is math. It is computational statistics on steroids.

Banks are using machine learning to help make business decisions about things like who qualifies for a mortgage. But one problem is that machine learning models discriminate by default. Let's say that I have a data set of people who have gotten mortgages in the past. The data will be tainted by the history of red-lining and residential segregation in the United States. If I build a machine-learning model based on this data, the model will discriminate against citizens.

We need to audit the AI algorithms and machine-learning models used by banks and other types of companies for fairness and to prevent discrimination. The issue here is not where these AI programs run or whether the data is stored on bank computers or on Amazon's computers. Instead, we should ask what the AI is used for, plus, how it is used, what kind of AI is used, what specific data is used to train a machine-learning model, and what specific data is used to make decisions after the model is trained.

One option is that these kinds of questions could be answered in plain language, and this information could be communicated as part of the regulatory examination.

The final thing I will mention is the cultural conflict between tech and finance. In the tech world, nobody talks about regulatory compliance or teaches it much in schools. The move-fast-and-break-things ethos is diametrically opposed to the mindset of compliance. It doesn't surprise me that in April 2019, when Federal examiners visited the AWS site in Virginia, they didn't notice the Capital One data breach. The Amazon—

Chairman FOSTER. Thank you. And at this point, we are on a tight time schedule.

Ms. BROUSSARD. Okay. Sorry.

Chairman FOSTER. The Members can read your full written testimony.

Ms. BROUSSARD. Thank you for the opportunity to contribute, and I look forward to answering your questions.

[The prepared statement of Ms. Broussard can be found on page 39 of the appendix.]

Chairman FOSTER. Thank you.

Ms. Seiffert, you are now recognized for 5 minutes.

STATEMENT OF ALLA SEIFFERT, DIRECTOR, CLOUD POLICY AND COUNSEL, INTERNET ASSOCIATION

Ms. SEIFFERT. Chairman Foster, Acting Ranking Member Riggleman, and distinguished members of the task force, thank you for the opportunity to appear before you today to discuss the use of the cloud in financial services. My name is Alla Seiffert, and I am the director of cloud policy and counsel at Internet Association.

Internet Association, or IA, represents over 40 of the world's leading internet companies. Our members are global leaders in the drive to develop lower-cost, more secure, scaleable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors. All of the major U.S.-based hyperscale cloud service providers are members of IA.

I would like to thank Chairman Foster, the task force leadership, and your staff for your continued commitment to exploring emerging areas around cloud computing and AI within financial services. I would like to start with a background on cloud computing.

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configureable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud service providers, or CSPs, make available to customers a wide range of services that function as IT building blocks that customers can use to build applications to meet their IT goals and be more secure, innovative, and responsive to their customers. The cloud is flexible enough to be used for everything, from storing national security data to managing my PayPal balance.

Security is a top priority for CSPs, and they invest a tremendous amount to make their services secure. By using cloud services, customers such as financial institutions can focus on carrying out their core business functions and benefit from the security measures that CSPs have in place. In that way, the cloud is kind of like an office building landlord. It will rent you space and make sure you have doors that lock, but it is ultimately your responsibility to decide whom you let into your office for meetings. Consequently, financial institutions remain accountable for managing the risk of their IT environments, whether they are run in-house, through a third-party-managed service provider, or a CSP.

Today, financial institutions use the cloud for a wide range of applications, from storing publicly available data or running test environments, to creating digital channels, storing sensitive records, or running critical workloads. We have the following three major themes to discuss with the task force today.

First, cloud implementation is a shared responsibility between CSPs and customers. Financial institutions that use cloud computing operate in an environment where they manage certain aspects of their IT resources and are responsible for configuring those resources, but they rely on the CSP to manage the cloud itself. This

division of labor means that both the CSP and the customer bear responsibility for making sure services are run efficiently and securely. Because each party is responsible for securing the resources they control, security in the cloud is something we call a shared responsibility. Simply put, CSPs are responsible for security of the cloud, while the customer is responsible for security in the cloud. CSPs provide a broad range of information, tools, and assistance to help customers with these responsibilities.

Second, cloud adoption increases cybersecurity. This is because embracing cloud technology helps banks increase overall security by modernizing applications and gaining better visibility into their networks, traffic, and vulnerabilities. The opportunities offered by cloud computing enable enterprises to level out their IT security posture and implement best-in-class cybersecurity solutions.

Large cloud providers have the resources and expertise to invest in and maintain state-of-the-art and comprehensive IT security and deploy it on a global basis across all of their platforms. Financial institutions, particularly small and midsized firms, could find it economically infeasible to achieve similar levels of security on their own.

Third, the cloud increases the resilience of our nation's financial institutions. Specifically, it allows firms of all sizes to leverage a suite of best-in-class tools for backup, security, and continuity of operations. CSPs design their infrastructure to be resilient to outages and incidents, and customers can take advantage of this infrastructure to architect for enhanced operational resilience. Since CSPs can rapidly redistribute data across geographically diverse storage regions, cloud environments can enhance firms' strategies for business continuity and operational resilience.

In conclusion, I would like to reiterate IA's gratitude for being included in discussions with the Financial Services Committee's Task Force on Artificial Intelligence, and for the opportunity to testify today. IA, along with our member companies, stands ready to support the task force and the committee in helping financial services companies adopt the cloud in a secure way.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Seiffert can be found on page 58 of the appendix.]

Chairman FOSTER. Beautifully timed. Thank you.

Mr. Grobman, you are now recognized for 5 minutes.

STATEMENT OF STEVE GROBMAN, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MCAFEE

Mr. GROBMAN. Good morning, Chairman Foster, Acting Ranking Member Riggleman, and members of the task force. Thank you for the opportunity to testify about two important issues for the financial services sector: the cloud; and artificial intelligence. Both have advantages to the industry and raise security concerns.

Financial services organizations are migrating to the cloud to reduce complexity, cut costs, and focus their capabilities on delivering financial services to their customers. By using the cloud, both large and small institutions benefit from advanced technology that normally is available only to those who can invest significantly in highly technical workforce. Cloud providers also generally practice

strong cyber hygiene, enabling a quick response to vulnerabilities and issues.

Yet, there are also security challenges in moving to the cloud. As cloud providers service many clients, a breach can place multiple organizations' data at risk. An analogy I like to use is that traditional, on-premise computing is like an automobile, and cloud computing is a lot like an airplane. While an airplane is safer than an automobile, given its more advanced technology, when a failure does occur, the impact can be catastrophic.

Today, almost all organizations, including financial services, use multiple cloud providers, a trend that is leaving organizations with less visibility to their operations. To remediate the situation, organizations need solutions to manage visibility and monitor security between cloud service consumers and providers. Known as CASB, this function is a critical new class of application that is rapidly being adopted to manage and secure diverse cloud environments.

Another security issue is the use of unauthorized cloud applications by employees, what we call shadow IT. This creates risk for both the technology and the data. Like cloud, we must understand the capabilities, limitations, and risks of AI. Financial services organizations are using AI and machine learning to enable advanced analytics that allow them to better service and protect customers and better manage overall costs.

AI is also the new foundation of cyber defense, enabling us to better detect threats and find the so-called needle in a haystack of needles. AI-based automation is helping us alleviate the cybersecurity talent shortage, enabling us to free up human security professionals to focus on the most critical aspects of cyber defense.

But AI is actually quite fragile. In many industries that use AI, such as meteorology, where an adversary does not exist, the fragility is not an issue. In cybersecurity, adversaries are building techniques to confuse AI models and evade detection. To mitigate these risks, McAfee is investing in understanding the adversarial techniques and researching ways to make AI more resilient against attacks.

AI can also be used as a tool by the adversaries. Bad actors can use AI to identify the most vulnerable victims, automate phishing, and evade detection. AI improves their ability to execute attacks and enables content creation for use in social engineering and information warfare such as deepfake videos.

These and many other adversarial uses of AI can and will occur, putting our financial services sector, as well as our democracy and civil society, at increased risk. Most major financial institutions are prepared for major cyber attacks, in part due to the regulatory oversight of the Bank Service Company Act, and the Gramm-Leach-Bliley Act. Financial service organizations also actively engage in cyber sharing groups in collaboration with DHS, the OCC, and the Federal Reserve.

Likewise, overall, the largest third-party cloud providers also have strong cybersecurity records. They have solid plans in place to respond to cyber attacks, they are committed to aligning with the NIST cybersecurity framework, and they are active in public-private partnerships.

Cloud providers are less regulated than their counterparts in the financial services sector, as many policymakers know that overly prescriptive regulation would stifle innovation in technology companies and could quickly be outdated as technology advances. Yet, Federal regulators do have a legitimate interest in seeing that IT and cybersecurity services provided by cloud providers to financial institutions are robust.

To best secure cloud and AI technology in the financial services sector, we recommend voluntary collaboration and the use of industry-supported standards and best practices, such as the NIST cybersecurity framework. When appropriate, existing cybersecurity rules for highly regulated critical infrastructure industries should be updated to reflect the rapid speed of innovation.

Thank you for the opportunity to discuss these issues, and I look forward to answering your questions.

[The prepared statement of Mr. Grobman can be found on page 51 of the appendix.]

Chairman FOSTER. Thank you. Again, beautifully timed.

Dr. Brandt, you are now recognized for 5 minutes.

STATEMENT OF JORDAN BRANDT, CEO AND COFOUNDER, INPHER, INC.

Mr. BRANDT. Thank you, Chairman Foster, Acting Ranking Member Riggleman, and members of the task force. And, Chairman Foster, I have to say, it is impressive that you have experimented with TensorFlow. So, thank you for your efforts.

Cloud computing and AI are distinct and complementary technologies that offer tremendous economic and consumer benefits. The cloud reduces cost and democratizes access to computational resources which, in turn, powers AI to streamline business functions and provide new insights that improve consumer welfare.

The committee has correctly identified that these benefits must be harnessed with proper legislative and technological safeguards for both data security and privacy. Whereas cloud computing and AI pose distinct risks, a common theme applies to both: Don't put all of your eggs into one basket. The consolidation of sensitive personal information into any individual entity, to be mined by data-hungry AI algorithms, poses significant economic risks and an existential threat to the privacy of our citizens. Fortunately, the emergence of privacy enhancing technologies, or PETs, and specifically encryption in-use capabilities, can address the concerns of both cloud data security and privacy in AI.

As banks move more of their data and information processing to the cloud, they are effectively consolidating risk into a select few providers of cloud computing infrastructure. The magnitude of this risk was underscored by the recent Capital One hack. The breach could have been prevented by securely computing across distributed data in a multi-cloud architecture, in which data is processed without exposing the underlying personal information. This would have eliminated a single point of failure.

To illustrate how this works, it is important to firstly define the three pillars of encryption, which is the best mathematical safeguard of data. First, we have encryption in transit, which secures the transmission between the sender and the receiver. Second,

encryption at rest, which secures data storage while it is sitting on a hard disk. And third, we have encryption in use, such as homomorphic encryption and multiparty computation, which secures data in memory while it is being processed.

In-transit and at-rest encryption are already ubiquitous. Encryption in-use is rapidly evolving from academic research into practical applications today, as its computing performance for large data sets quantifiably improves.

For example, at Inpher, we have made multiple order-of-magnitude improvements in the performance of both homomorphic encryption and multiparty computation without compromising accuracy. We are currently deploying this technology to solve real-world privacy and security challenges in banking, defense, healthcare, and other industries.

Our platform keeps data private, secure, and resident, precluding the need to centralize information into a single repository. This proactive safeguard enables financial institutions to minimize risk and leverage the full benefits of AI without a privacy tradeoff. PETs thus internalize the letter and the spirit of U.S. and international data privacy regimes which jointly emphasize privacy by design.

Specifically, in the financial services sector, we are witnessing the application of PETs in fraud and anti-money-laundering, credit scoring, trade surveillance, and all forms of predictive modeling where compliant data sharing is critical. PETs safely overcome data silos and increase data utility.

Regulators and law enforcement also benefit from privacy-preserving computing, as they are able to run forensics and surveillance on encrypted data for pattern matching and event detection without compromising individual privacy or inviting potential liability. They can find the bad guys without compromising on its citizens. To this end, we have briefed many domestic and international regulators about these capabilities over the last year, and we are encouraged by their enthusiastic support.

To conclude, as a nation, we are in a technology arms race with countries like China that do not share our views on individual rights. We must not accept the false dichotomy between AI and our privacy. We can have both. Privacy-preserving computing not only champions and achieves this outcome, but also fosters new innovation and economic expansion that benefits our government, industry, and every American citizen.

We truly appreciate your interest and desire to learn more about this very complex topic, and we remain at your disposal for any further questions that you may have.

[The prepared statement of Dr. Brandt can be found on page 36 of the appendix.]

Chairman FOSTER. Thank you.

And, Mr. Benda, you are now recognized for 5 minutes.

STATEMENT OF PAUL BENDA, SENIOR VICE PRESIDENT, RISK AND CYBERSECURITY POLICY, AMERICAN BANKERS ASSOCIATION

Mr. BENDA. Thank you.

Good morning, Chairman Foster, Acting Ranking Member Riggleman, and distinguished members of the task force. I appreciate the opportunity to come before you today to discuss how financial data is stored, protected, and maintained by cloud providers. My name is Paul Benda, and I am a senior vice president for risk and cybersecurity policy at the American Bankers Association (ABA).

Prior to joining the ABA, I served in the government, both in the Air Force and as a civilian in the Departments of Defense and Homeland Security, where I focused on research and development of new technologies to protect against kinetic and cyber threats. After I transitioned to the private sector, I focused on assessing physical and cybersecurity practices of businesses and recommended improvements to make them more secure.

At the ABA, my portfolio is on physical and cybersecurity policy, helping our members understand emerging threats, new technologies, and the political and legislative environments surrounding their use. The ABA believes the flexibility, scaleability, and advanced technologies available in the cloud make it a valuable tool for financial institutions to consider using. We appreciate the opportunity to share our thoughts on how financial data is stored and protected in the cloud, and we would like to highlight four main points.

First, banks are responsible for their data. Title V of the Gramm-Leach-Bliley Act (GLBA) has long-established standards that require a bank to take meaningful steps designed to ensure the security and confidentiality of its customers' information. These requirements are in place regardless of whether that information is stored on premise, by a third party, or in the cloud. Regardless of the location, banks are responsible for ensuring that data is protected.

Second, the cloud offers benefits, but risks must be managed. It is clear that there are potential benefits as well as risks regarding use of the cloud. But the decision on its use should be left to each individual bank, as each bank is different and is most capable of performing an overall risk-benefit calculation for their environment. If done appropriately, use of the cloud is likely to have no adverse effect on the overall risk profile of a bank and would most likely improve their resiliency.

Third, all parties should collaborate to improve cloud security and efficiency. Banks inhabit a unique regulatory space. No other industry has the level of regulator guidance, oversight, or examination structure in place to ensure that financial data is protected. The baseline shared responsibility model of security used by CSPs attempts to shift all responsibility for information security to its customers, although many CSPs do offer to manage certain IT controls on behalf of their customers, which can blur the lines of responsibility.

We believe it would be helpful, especially for financial data deployments, that a transparent set of unified security controls be de-

veloped, that security control responsibilities are clearly delineated for each deployment, and that a process for CSPs to notify customers of potential security misconfigurations in their cloud deployments be instituted. This cooperative approach to security would increase overall security of the data and aid in the management of this critical data as it resides in the public cloud.

We would welcome a discussion between banks, cloud service providers, and regulators that will allow us to work in a collaborative manner to ensure that the right frameworks, processes, and programs are in place to allow adoption of these new technologies, while maintaining the safety and soundness of the financial institution.

Fourth, regulatory clarity is important. From a financial services perspective, the GLBA, the Bank Service Company Act, and banking agency guidance already provide a robust regulatory framework to oversee bank utilization of their cloud. But additional clarity would be helpful on the roles and responsibilities of regulators with respect to their direct oversight of cloud service providers. We believe that the oversight authorities in the Bank Service Company Act could be aligned and coordinated with the proposed set of unified security controls for financial data deployed in the cloud so that banks could clearly understand those areas where they could depend on regulators to provide oversight of the cloud service providers, and where banks must utilize private-sector methods to ensure that appropriate due diligence is done.

A clear delineation of roles and responsibilities that is arrived at in a collaborative manner would improve overall security as well as efficiency into the oversight process for banks of all sizes.

The challenges in the space are complex. We believe that every stakeholder wants to ensure that security of these critical systems is maintained, and at the same time, innovation is not hindered. A collaborative approach that merges the best of the safety and soundness culture of banks and regulators with the entrepreneurial spirit of cloud service providers is likely to achieve a lasting outcome that is acceptable to all parties.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Benda can be found on page 24 of the appendix.]

Chairman FOSTER. Thank you.

I will now recognize myself for 5 minutes for questions.

Our witnesses here seem to have identified four lines of defense here. The first line of defense that Ms. Seiffert mentioned was just that cloud service providers have multiple physical locations. And so, when you are talking about physical attacks, that is a pretty solid strategy.

The second one that, I guess, Mr. Grobman mentioned, is the use of multiple cloud providers. And I would be interested, I will be asking questions on whether that is—how realistic a possibility that is.

The third one is advanced encryption techniques as a way to be able to survive even a significant cyber breach.

And the fourth general thing is just the future of AI as the main tool that will be used for real-time cyber defense.

And so starting with the first point, Ms. Seiffert, to what extent is having multiple physical locations a real protection, and to what extent could it be illusory, if you have a shared hardware vulnerability? For example, if you lose your hardware root of trust, the key used to download software updates, for example, and if that gets corrupted or lost or the bad guys get their whole—you could be in a situation where, yes, we have multiple locations, but because of a shared hardware vulnerability or a silicon bug that is discovered.

Can you say little bit about that, whether that is going to prove illusory or not?

Ms. SEIFFERT. Thank you for your question. That is without a doubt a possibility, but nevertheless, the multiple availability zone architecture of cloud computing really does lead to significant increases in resiliency. There are a number of ways to configure cloud-native applications with respect to the failover mechanism. I think your point is incredibly valid, what if a vulnerability exists upon multiple availability zones, but it is my understanding that there is a way to architect applications such that in order to have backup and redundancy storage, and essentially seamless failover, in the event of issues in one location.

Chairman FOSTER. Let's see. The question of whether multiple cloud providers are also a realistic useful defense, that is something that Congress, for example, could mandate for too-big-to-fail banks, that they simply maintain a hot spare provider, in addition to the hot spares that are provided internal to each cloud service provider. And I was wondering if anyone, Mr. Grobman or Mr. Benda, might have a comment on that, where obviously that would impose costs.

Mr. GROBMAN. Sure.

Chairman FOSTER. And we struggle with this all the time in this committee, the tradeoff between short-term profitability and reducing tail risk.

Mr. GROBMAN. I think, in general, having diverse implementations can add some additional levels of security, but we also need to recognize that a lot of the issues here are not new. In your last question, you pointed out that a single technical vulnerability could impact multiple physical locations. That is true regardless of whether it is a cloud or a traditional on-premise implementation. I think similarly, if you look at multiple cloud providers, there are going to be some issues that are cloud provider-specific and some that would be at an application level or really not matter whether or not it had multiple providers. So, I think it is going to add some help but not be the silver bullet solution.

Chairman FOSTER. Yes, like the meltdown inspector bugs, for example, applied to multiple processor architectures, so that even having a separate set of processes your cloud is running on was not necessarily a defense.

Mr. GROBMAN. Correct. I do think that particular issue is illustrative of how effective the large cloud providers are at remediating vulnerabilities. All of the large cloud providers patched their hardware with new firmware literally within days, whereas we have seen private data centers usually take many weeks, if not months, to get those same patches.

Chairman FOSTER. Okay. Now, in terms of advanced encryption techniques, Dr. Brandt, you said that you had made big improvements in the speed, and I guess you probably have competitors in this. If you look at the overall trajectory of performance of privacy-preserving computing, is there a way to estimate the point at which it might be a pretty small overhead for things like training neural networks and so on?

Mr. BRANDT. Yes. Thank you for the question. Indeed, there have been drastic improvements over the last several years, orders-of-magnitude improvements that we have seen in the performance of encryption and use specifically. Again, keeping data encrypted while it is being processed, which can also help protect against these hardware vulnerabilities. If you focus on the data itself, even if the hardware is compromised, the data itself would be secure.

Of course, the tradeoff has been higher computational overhead to achieve this. With the current trajectory, we are seeing that large data sets to be used for training neural networks or training AI models in general is becoming quite practical. This is especially because that is an offline process. It doesn't need to be done necessarily in real time. Even if you are talking about an order of magnitude higher compute overhead than you would have in plain text, it still can be—

Chairman FOSTER. Okay. Now, unfortunately, I must bring the gavel down on myself and recognize my colleague, Mr. Riggleman, for 5 minutes.

Mr. RIGGLEMAN. Thank you, Mr. Chairman. And thank you again to the witnesses.

And I first want to thank Ms. Broussard for your definition on AI and ML. That is an argument I have had in the DOD, I think, for the past 5 years. So, I appreciate that before we get started.

We have had a few hearings here in Congress, and we have a lot of things here. I want to make sure we get to our colleagues. I have written down, you were talking about—the chairman was talking about the four issues that he saw here. I have some specific questions just based on my background in, not really cloud computing, but trying to do the governance and security, overseeing cloud computing in the DOD, specifically the challenges with competition amongst cloud computing and the fun that we have had there with security, but also the regulatory issues.

I want to start with Mr. Grobman, and then I want to go to Mr. Benda. We were talking about continuity of operations, I think, a little bit earlier is how I would look at it, and this is something that I am looking at as we are going forward. Do you think continuity of operations (COOP) would be less expensive with cloud applications, even based on scaleability—which I will go to Mr. Benda about—but do you think actually when you are looking at the cloud and where we are going right now, do you believe that would be less expensive for continuity of operations going forward rather than staying on premise?

Mr. GROBMAN. Yes. And the reason is, cloud operators are able to execute at scale and be able to have expertise in specific areas that would not be practical at the typical institutions that use them. So, for the financial services sector or the DOD to have the same level of competence in the low-level capabilities a CSP has

would not be practical. I think it does make things work a lot faster.

Mr. RIGGLEMAN. It is interesting because we talked about data stovepipes beforehand, before cloud computing became a thing, right? And my worry is creating funnel clouds of excellence also, which we called them. But talking about that, we talked about cost and scaleability, and talking about continuity of operations—and going to Mr. Benda—and sorry, I am off script right now, so we are having fun right now—so talking about scaleability, would you say maybe that it improves—and going on, Mr. Grobman, would you say it would improve our security posture based on the fact it could be less expensive, based on cloud computing, to have more continuity of operations as far as cost and scaleability?

Mr. BENDA. I think that the value of the cloud is certainly the pay-as-you-go model. You pay for what you use. The scaleability is there, in that the cloud has several server farms that you can access and provide you failover capabilities that are in there. I think the cost process or the cost model is that you are not—the way I have heard it described is that it is an operational expense versus capital expense. So, the clouds take on that capital expense. It should reduce costs overall and provide a better resilience capability because that scaleability is there on an instant and that is when you pay for it.

Mr. RIGGLEMAN. If we are becoming increasingly reliant on technologies, why do you think at this time anybody would wait to adopt them?

Mr. BENDA. I think if you look at it from a financial services perspective, there are multiple reasons. One, the cloud is new. You have to learn a whole new set of things on how to secure it. It can be more secure, or it can be less secure, depending on how well you know it.

The other thing is, I think there is a lack of regulatory clarity in how the cloud is treated and how it is examined. It is a real issue for banks, and I think the Treasury report that you referenced, sir, makes some really good recommendations.

Mr. RIGGLEMAN. Thank you very much.

Ms. Seiffert, the same question to you, do you think there is an ability for any scaleable pricing that targets smaller institutions? And this is what I get excited about a little bit, is that when we are looking at smaller institutions trying to enter into the cloud computing space, do you think that scaleable pricing is there based on the fact that we have a better way of doing business than on premise?

Ms. SEIFFERT. Thank you for the question. Small and midsized institution absolutely have the ability to really leverage the power of the cloud to save money, as well as really piggyback on a fair amount of cybersecurity know-how that the cloud service providers bring to the table. A small or midsized institution, a credit union in Texas, a small bank in Missouri, they are really not able to retain the level of staff or technical know-how to keep their systems as secure as the cloud service providers are able to keep their infrastructure.

And so, in that respect, the consumption-based pricing model really favors smaller institutions because their compute spend is

just going to be less. It is also going to be more predictable than needing to not only buy a data center, but also patch it to include with the vulnerabilities that were mentioned earlier.

Mr. RIGGLEMAN. This allows me to mention to everybody, so piggybacking off Dr. Brandt, and then going to Mr. Benda, when you are talking about technology, and advances that we had, and going to Mr. Benda and seeing everything that is happening, in the last 25 seconds here—yes, sir, I see the gavel ready—in the last 25 seconds, are we to a point where really it isn't about location anymore, it is about access, right? If we are to that point right now, should we be more aggressive in making sure that our regulatory structure supports that?

Mr. BENDA. I would agree, I think it is about access, but we have to make sure that those physical security controls are in place, and I think that is really where regulators can help.

Mr. RIGGLEMAN. Thank you, and I yield back. The witnesses were wonderful. Thank you.

Chairman FOSTER. Thank you.

The gentlewoman from Texas, Ms. Garcia, is now recognized for 5 minutes.

Ms. GARCIA OF TEXAS. Thank you, Mr. Chairman. And thank you to all the witnesses today.

First, let me say that I still don't have clarity. I think it is a little cloudy in my head as to exactly what the real challenges are here. And I am concerned more about the consumer, perhaps a consumer like myself, who still keeps a checkbook, who doesn't trust a lot of online banking or online shopping because I find a lot of mistakes, even in some of my credit card statements. The very idea that somewhere in never-never land, there is a cloud taking care of my financial information, has made me even more nervous today than I was before.

Ms. Seiffert, you said there was a shared responsibility, that security in the cloud was the responsibility of the customer financial institution, and security of the cloud was the CSP. What does that really mean?

Ms. SEIFFERT. Sure. Thank you very much for the question. What that means is there are a variety of services that are available for banks to configure—

Ms. GARCIA OF TEXAS. No, I know that, but can you give me an example of what you mean by the difference between "of" the cloud and "in" the cloud? So that a person like me who is watching this today can really understand.

Ms. SEIFFERT. Absolutely. When it comes to the software, so whereas you pull up your phone and you have your banking application there, when it is your time to log in, you enter your user name and your password, maybe there is a two-factor authentication. The security of the application as it communicates with the data that is possibly stored in the cloud, it is your bank's responsibility to make sure that application is secure.

So you as a consumer, you are seeing an application, that is all the financial services—

Ms. GARCIA OF TEXAS. So if I don't use my phone for banking, I don't have to worry about this cloud business?

Ms. SEIFFERT. Not quite.

Ms. GARCIA OF TEXAS. Okay.

Ms. SEIFFERT. It depends on what your—

Ms. GARCIA OF TEXAS. Again, remember you are talking to a consumer who doesn't do online banking.

Ms. SEIFFERT. So, let's say you are—

Ms. GARCIA OF TEXAS. But you have my data over there in West Virginia in the same place where the FBI has a data center, and that makes me nervous too.

Ms. SEIFFERT. It is a very secure data center.

But sort of the physical security of the data center, who is allowed to get in, you and I probably can't just walk into some data center and have a look around just because we would like to. And the physical security of data centers is a cloud service provider's responsibility. The specific application data that is stored there, let's say that you are accessing a loan through a bank. Let's say you go in person to a bank branch in order to apply for a loan. The security of the application, let's say they take down your data on a website or on some sort of document, and they e-mail it for processing. The security of that is the bank's responsibility.

Ms. GARCIA OF TEXAS. Okay. Well, it is a little cloudy, okay? But I will move on to Ms. Broussard.

Do you agree with this shared responsibility? Because I think you said that no one in tech thinks about regulatory issues, and instead, they want to move fast and break things. And so if my data as a consumer is stolen or misused, should the liability fall on the CSP or on the financial institution that is using the CSP?

Ms. BROUSSARD. Thank you for the question. The issue of liability is a really good one. We can think about shared responsibility and we can think about shared liability. For example, if you go to a hotel and you are injured at a hotel because of something that the hotel did, then the hotel bears some responsibility, right? The best way to think about cybersecurity issues and issues of liability in the computational world is to think about the equivalence in the real world and think through how things would proceed in that way.

And specifically in this case, we do have a communication issue, a really major communication issue around compliance and around tech, because AI issues are very difficult to understand, and bank regulatory issues are pretty hard to understand if you are not trained in it.

One of the things that I think we need is we need better training for cloud computing staff about bank regulatory issues. And we need better communication by both parties about what are the regulations and what is actually happening on the digital side and how is everybody staying protected.

Ms. GARCIA OF TEXAS. All right. Thank you.

Ms. BROUSSARD. Thank you.

Ms. GARCIA OF TEXAS. I yield back. Thank you, Mr. Chairman.

Chairman FOSTER. Thank you.

The gentleman from Ohio, Mr. Gonzalez, is recognized for 5 minutes.

Mr. GONZALEZ OF OHIO. Thank you, Mr. Chairman. And thank you, everybody, for being here today for this important task force hearing.

I want to start with some questions for Mr. Benda. You spoke about a collaborative approach between the CSPs, the regulators, and the banks to provide clarity and guidance on rules and responsibilities. I agree, that makes total sense. We need to have this sort of collaboration. Right now, there is sort of this finger-pointing thing going on, which I think everybody really loves.

Not to put you on the spot here, but as you think through that, from your perspective, what do you think the right roles and responsibilities for each of those three entities should be? It is a big question, I know.

Mr. BENDA. That is a big question.

Mr. GONZALEZ OF OHIO. Give me some broad brush strokes, if you could?

Mr. BENDA. The one thing I would say on that is that banks are comfortable and understand the requirements of GLBA and their responsibility to be, overall, the caretaker of that customer's data. We spend hundreds of millions of dollars every year to make sure that happens. We are not interested in offloading that responsibility.

When we look at the different roles, we think there is a a clash of culture between safety and soundness, regulatory compliance culture that banks have, versus move-fast-break-things on the tech side. We would love to see a more efficient examination process that allows banks to operate and utilize and take advantage of all the wonderful things that the cloud can provide.

But then the regulators have their role of, instead of having 5,000 banks go and hit Amazon for a certain thing, we rely on the regulators to look at the physical security access point. We look at them for those things where there is a multi-tenant cloud, the regulators have access that they need to ensure that the banks' due diligence for that third-party oversight is done and that the banks do their appropriate role.

I think working in a collaborative manner, we can make things better for everyone and make things more secure.

Mr. GONZALEZ OF OHIO. And then as a followup, what is the barrier to having that sort of collaboration, and how can we as Congress make sure that that actually occurs? Because it strikes me that would be a more effective means than what we are doing now.

Mr. BENDA. I think the Treasury report that Congressman Riggleman mentioned actually has this exact recommendation in it. I would just ask for an update from Treasury on where they stand on that, and we are happy to work together with the regulators to make that happen.

Mr. GONZALEZ OF OHIO. Great.

And then, Ms. Broussard, so your analogy of the hotel—and this could be for anybody—but the analogy of the hotel suggests that or implies that it is easy to make attribution, right? If something at the hotel was deficient, and I get hurt, that is on the hotel. If it is something that I am doing myself, that is probably on me. And that makes sense.

My question with respect to security in the cloud is, how easy is it to make those attributions and does that prevent any sort of barrier?

Ms. BROUSSARD. Thank you for the question. I used the analogy of the hotel because when you go into a hotel, you are renting space.

Mr. GONZALEZ OF OHIO. Right.

Ms. BROUSSARD. And in the cloud environment, you are also renting space from one of the cloud providers.

As far as how easy it is to figure out what went wrong, it really depends on the individual situation. Sometimes, it is quite obvious, for example, somebody forgot to patch a security hole, and a hacker got in through that security hole, and it is a well-understood breach. Other times, we have folks who are really, really creative about finding ways in, and so we have a new kind of breach, an unknown unknown, if you will—

Mr. GONZALEZ OF OHIO. Right.

Ms. BROUSSARD. —and we don't have ways to predict that because it hasn't happened yet. And AI is especially not helpful in that regard, because AI can help us protect against things that have already happened, that are known, but it can't be creative in the same way that humans are creative. That is one of the things that is hard about cybersecurity, is you always have to keep up.

Mr. GONZALEZ OF OHIO. Thank you.

Mr. Grobman?

Mr. GROBMAN. Representative, I really think it is very similar to in the physical world, that in order to have safe use of technology, it is a combination of the technology and the use. For example, in order to safely drive a car, having safety features in the car is a critical component, but as a driver, you also need to apply the rules of the road. So if you are in a auto accident, it could be either because of a failure of the automobile or because you did something improper as a driver.

And it is very much the same in the world of the cloud, in that we do need to recognize that the underlying technology can have vulnerabilities, but also, the users of that technology can have misconfigurations or make other mistakes that would lead to issues.

Mr. GONZALEZ OF OHIO. Yes, and I agree. I guess the point I am trying to drive home is, so we get the clear rules of the road, we get the guidelines, we make sure that everything is right, I still think we have this attribution question that I am not sure that we have a great answer for right now.

With that, I yield back.

Chairman FOSTER. Thank you.

The gentleman from Illinois, Mr. Casten, is now recognized for 5 minutes.

Mr. CASTEN. Thank you, Mr. Chairman. And thank you all so much.

It strikes me that the thing that makes cloud computing so awesome is that its strength is its weakness, right? You have all of this organized data that you can access remotely, which means that if I am going to wear a black hat and find a place to target, that is a lot more attractive than getting onto my little laptop. The issues, and as Congresswoman Garcia raised, is this gap between who bears the liability for that, and then there is separately, who bears

the cost, which is not always the same, and sometimes don't tie out.

My first question for Mr. Benda is, let's say you are a major U.S. bank. You have customer data from all 50 States within your system. Jurisdictionally, how many different jurisdictions constrain how you regulate the data? Is it 51? Is there one overarching jurisdiction that sets what kind of constraints you have to impose or liabilities you have to manage to?

Mr. BENDA. There can be. A national bank like that is chartered by the OCC. That is the primary regulator. They would have the overarching control or regulation of that. What we would like to see is a harmonization of those regulations. We would like to see that we don't have to answer to 51 different masters, that we harmonize those regulations through a Federal regulator.

Mr. CASTEN. Are the obligations substantively different between the State and the Federal, and between the States?

Mr. BENDA. They can be, sir.

Mr. CASTEN. What if you have international clients, or one of your clients has a London account in addition to your U.S. account that is managed in your same system?

Mr. BENDA. Large banks have a lot of regulatory oversight and a lot of different challenges they have to face. Those are real issues that we work through every day, and we do our best to address them as best we can.

Mr. CASTEN. Given different liabilities for those different jurisdictions, to what degree do the banks segment the data? In other words, if I have data that is only subject to my London account, is that on the same network and the same accessible server as the one that is my Arkansas account?

Mr. BENDA. That is a great question, sir. I would have to get back to you on that. I don't know a specific implementation on how they would handle that.

Mr. CASTEN. Is it even possible to do that segmentation if your customer in Arkansas also has a London account?

Mr. BENDA. Per customer, that is a great question, sir. I don't know the ins and outs of that. I would have to get back to you on that.

Mr. CASTEN. Ms. Broussard, you seem like a nice person, but I am going to pretend you have on a black hat now.

Ms. BROUSSARD. Okay.

Mr. CASTEN. If you have all of these different regulations and you have a gap between the liability and the cost of—who bears liability and who bears cost between the cloud provider and the bank and the customer whose data is stored, and different international and State and Federal rules, where are the regulatory gaps? If you are going to hack into that system and say, where would I exploit the vulnerabilities? Because, given your brain power, if you can say with a black hat and then we can think about where we ought to be, where we ought to be bolstering the defenses, I am going to put you on the spot, but I would love your thoughts.

Ms. BROUSSARD. Sure. I actually think about this a lot. As a data journalist, one of the things you do is you look for where can things go wrong and you look for the things that go wrong, so thank you for the question.

I would say that cybersecurity is very important to consider holistically. We need to consider the attack surfaces in the real world as well as the virtual world. As far as who bears the responsibility, this is such a complicated question, and I have talked about it with a lot of lawyers, and it is hard to find a consensus. I would go back to your earlier question about how easy is it to write code against all of these different regulations.

One of the problems with making banking technology is that, as a programmer, you want to write once and run anywhere, but if we have 50 different States with different rules individually, and the computer is considered to be in cyberspace, well, I could just shrug and say, oh, well, it is in cyberspace, it doesn't matter. Or I could say, I need the rules to adhere to the rules of the real world. These are individual decisions, and I think that is one of the cultural differences between computer scientists and regulators.

Mr. CASTEN. Thank you. I yield back.

Chairman FOSTER. Thank you.

And Members are advised that votes have been called. The time is currently at 6 minutes and 25 seconds.

The gentleman from Missouri, Mr. Cleaver, who is also the Chair of our Subcommittee on National Security, International Development and Monetary Policy, is recognized for 5 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman. I am going to try to roll three questions into one because of the votes.

My favorite time of the year is October because of Halloween and all of the movies, the horror movies that come on. I know probably all of you are watching them at night with me. And I am on the Committee on Homeland Security as well, and I chair the Subcommittee on National Security. So I don't know if I am being troglodytic in my thinking, but a lot of this scares me more than Dracula does, and Dracula is real. I just want to make sure you know that.

But, we have this plan, this financial plan to create a financial ecosystem by Facebook. They are calling it stablecoin. I call it scary. At Homeland Security, we are always looking at what you said, Ms. Broussard, what can go wrong? What can happen? I am thinking power lines, water treatment facilities, and then on top of that, human error.

We have a situation that is quite threatening, and we know for a fact that the Chinese, the Iranians, and the Russians are all daily, daily messing with us, and you probably know about some of them, and a lot of them you don't know about. Tell me it is going to be okay or tell me it is not.

Mr. BRANDT. I think all of these discussions and some of the lack of clarity around liability, if we just focused on what is the precious asset here, it is the data. And if we look at the poll of what the banks are worried about, it is the data privacy, the data security. And regardless of what happens, if there is a breach, if there is a vulnerability in the hardware or the physical location, if the data itself is protected, then we are good. There are other bad things that can happen, of course, interruption of service, but at least people's data and their privacy are secured in that.

If we just focus on the life cycle of the data security itself, then it helps to, I think, simplify a lot of these questions that we are having.

Mr. GROBMAN. Representative, I agree with your point that the threat landscape is extremely broad. But one of the things that we have to recognize is we can't put a priority on the most important thing to worry about is energy or water or our financial system, because if any one of those systems had a major cyber breach, it would be catastrophic, which is why we need to really have a comprehensive cyber defense approach across all of our critical systems.

Mr. CLEAVER. But we are not even close to that, are we?

Mr. GROBMAN. No, we are not.

Mr. CLEAVER. I yield back, Mr. Chairman.

Chairman FOSTER. Thank you.

I would like to thank our witnesses for their testimony today.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

Thank you, and this task force hearing is adjourned.

[Whereupon, at 10:35 a.m., the hearing was adjourned.]

A P P E N D I X

October 18, 2019

October 18, 2019

Testimony of

Paul Benda

On Behalf of the

American Bankers Association

before the

Task Force on Artificial Intelligence

of the

House Financial Services Committee

Testimony of

Paul Benda

On behalf of the

American Bankers Association

before the

Task Force on Artificial Technology

of the

House Financial Services Committee

October 18, 2019

The American Bankers Association ("ABA") appreciates the opportunity to provide testimony regarding "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers." The ABA is the voice of the nation's $17.9 trillion banking industry, which is comprised of small, midsized, regional and large financial institutions. Together, these institutions employ more than 2 million people, safeguard $14 trillion in deposits and extend more than $10 trillion in loans. Our members have a substantial interest in technology, including AI and cloud computing, and we look forward to working with you and the Members of the Taskforce on this very important issue.

Introduction

The rise of cloud computing has led to a digital transformation of many industries, from the entertainment sector where streaming music and movies is now the standard, to email and office applications accessed through a web browser. The rise of a ubiquitous internet connection allows users to download data on demand, access advanced applications and have the computing power needed to run these applications from a mobile phone – essentially the "clouds" that the internet runs on today. There are many reasons that the cloud benefits American businesses. For instance, it allows the outsourcing of expensive computing infrastructure to specialists who can reach critical mass and attain significant economies of scale. The cloud's "pay as you go" model

reduces a company's overhead by allowing it to only pay for the infrastructure that it needs, when it is needed. It also allows a rapid ramp-up in capacity when needed, and enhances operational resilience because cloud operators have more assets and a better ability to provide back-up capabilities. Finally, as cloud capabilities advance, cloud service providers (CSPs) have begun to offer advanced analytic and artificial intelligence tools to their customers to allow them to better understand their data in ways they could never achieve in a cost-efficient manner on their own.

With these benefits, it is no surprise that businesses and governments are looking for a way to migrate certain computing functions to the cloud. While some sectors have fully embraced the cloud, others in highly regulated fields, such as financial services and healthcare, have been more cautious in their approach to adopting the use of the cloud. There are a variety of reasons for this more measured approach, including the fact that in the early days of the development of the cloud there was a lack of confidence by many in the financial industry that CSPs could effectively support the rigorous regulatory requirements and oversight that financial institutions and their vendors must operate within. As the CSPs have matured, financial institutions have begun to explore the cloud. For example, a recent Gartner survey of senior finance executives found that by 2020 about 36 percent of enterprises could be using the cloud to support more than half of their transactions[1]. Today, for many financial institutions the benefits of moving to the cloud are becoming more attractive as CSPs and the financial institutions themselves mature in their ability to mitigate and reduce these risks.

The American Bankers Association (ABA) appreciates the opportunity to share our thoughts on how financial data is stored and protected in the cloud. In particular, we highlight the following four points that we believe are relevant to this discussion:

- **Financial institutions are Responsible for Protecting Their Data**. Title V of the Gramm Leach Bliley Act (GLBA) has long-established standards that requires a financial institution to take meaningful steps designed to ensure the security and confidentiality of its customer's information, regardless of

[1] Gartner survey of senior finance executives from January through March 2017 to explore their technology perspective, influence of IT, needs and priorities in technology investment. https://www.gartner.com/en/newsroom/press-releases/2017-09-13-gartner-says-finance-is-moving-to-the-cloudmuch-faster-than-expected

whether that information is stored or handled by a financial institution or its vendor on the financial institution's own system or in a third-party cloud.

- **The Cloud Offers Benefits, But Risks Must be Managed.** The cloud can provide significant benefits, but risks must be managed consistently and effectively. Use of the cloud should remain an option for all financial institutions, but each financial institution must make a determination as to whether it is the right fit for its organization based on its business model, risk analysis and mitigation strategy and consistent with regulatory requirements.

- **All Parties Should Collaborate to Improve Cloud Security and Efficiency.** Financial Institutions inhabit a unique regulatory space and represent a critical aspect of the American economy. Financial institutions, CSPs and regulators, including core providers that provide products and services to smaller banks, should work in a collaborative manner to ensure that the right frameworks, processes and programs are in place to allow adoption of these new technologies while maintaining the safety and soundness of our financial system.

- **Regulatory Clarity is Important.** From a financial services perspective, the GLBA, Bank Services Company Act (BSCA) and banking agency guidance already provide a robust regulatory framework to oversee bank utilization of the cloud, but additional clarity would be helpful on the roles and responsibilities of regulators with respect to their direct oversight of CSPs.

I. Financial institutions are Responsible for Protecting Their Data

The financial sector believes strongly in protecting sensitive personal and financial information. For hundreds of years, customers have relied on banks to protect their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to federal data protection laws and oversight. The GLBA required the federal

regulatory agencies to establish standards for safeguarding customer information. These standards require financial institutions to take meaningful steps that are designed to ensure the security and confidentiality of customer information, protect against anticipated threats to such information, and protect against unauthorized access to, or use of, this information that could result in substantial harm or inconvenience to any customer. Moreover, these standards apply equally regardless of whether that information is stored or handled by a financial institution or its vendor on the financial institution's own system or in a third-party cloud. These standards also require that financial institutions have in place incident response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Compliance by banks with GLBA is regularly examined by the federal banking agencies. Unlike other sectors, where violations of statutory and regulatory restrictions must occur before regulatory oversight is likely to occur, financial institutions are subject to strict regulatory oversight and regular exams regarding their compliance with privacy and data protection laws.

The federal banking agencies have formal procedures that govern bank examinations, particularly surrounding security. For example, this oversight includes the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook, which is an extensive document containing multiple booklets with over 1,000 pages of IT guidance and examination instructions. The Handbook not only provides meaningful guidance to financial institutions regarding the regulatory expectations for, among other things, information security, outsourced technology services and business continuity, but also is used by the regulators to examine banks and assess their compliance.

In 2012, the FFIEC issued cloud guidance, "Outsourced Cloud Computing." The guidance identifies critical areas that financial institutions must consider and assess when using the cloud, including due diligence, vendor management, audit, information security, legal, regulatory and reputational considerations and business continuity planning. Of particular note, the cloud guidance stresses that "[a] financial institution's use of third parties to achieve its strategic plan does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations."[2] Financial institutions have long been required to maintain

[2] FFIEC "Outsourced Cloud Computing" July 10, 2012 page 2

oversight of their vendors, and the use of CSPs is no different, a point reinforced by the FFIEC guidance.

If a bank fails to comply with the GLBA, including in the context of the cloud, the federal banking agencies can bring enforcement actions to recover significant penalties. Specifically, compliance with Section 501(b) of the GLBA, is enforced by the federal banking agencies under Section 8 of the Federal Deposit Insurance Act ("FDIA"). The federal banking agencies can bring an enforcement action alleging that a failure to comply with the Guidance is an unsafe or unsound practice. In this regard, Section 8 of the FDIA includes various penalties and remedies for an unsafe or unsound practice, including:

- a cease-and-desist order;
- an order requiring that the financial institution correct or remedy any conditions resulting from the unsafe or unsound practice;
- Removal or suspension of financial institution parties from office;
- a civil penalty of $5,000 for each day in which the financial institution violates a cease-and-desist order or order requiring the correction of an unsafe or unsound practice;
- a civil penalty of $25,000 for each day in which the financial institution recklessly engages in an unsafe or unsound practice; and
- up to $1,000,000 or 1 percent of assets for knowingly engaging in an unsafe or unsound practice.

The GLBA mandates that financial institutions protect their customer data. While typical cloud implementations follow a shared responsibility model for data security in which the CSPs have certain responsibilities related to the security of, for example, the physical infrastructure of the relevant cloud, the utilization, deployment, security and administration of such resources

made available by the CSP, however, are ultimately the responsibility of the financial institution using the cloud.

II. The Cloud Offers Benefits but Risks Must be Managed.

The economies of scale, cost reductions, flexibility, scalability, improved load balancing and access to advanced technologies all provide a meaningful business case for financial institutions to consider moving at least some aspects of their operations to the cloud, even if only on a small or limited scale. Additionally, large CSPs have data centers spread over wide geographic regions with resilient data architectures and redundancies in place to provide a high degree of operational resilience that is nearly impossible to match except for the largest financial institutions. Although there are compelling business and operational resilience reasons for financial institutions to consider the use of the cloud, it is critical that financial institutions first put in place strong and effective risk mitigation strategies to address the risks that are unique to the cloud.

The robust regulatory regime in place for financial institutions provides a strong framework for financial institutions to make a balanced risk assessment on whether migrating applications to the cloud makes sense for their computing environment and business model. Utilizing the cloud does not necessarily increase the risks a financial institution may face, but simply changes the nature of the risk. A financial institution is in the business of storing sensitive financial data. This data must be protected regardless of where it may be stored, whether hosted on premise or in a public or private cloud. But while data is stored in physical infrastructure that is managed by a third party, such as the cloud, access and other controls must be tailored to the specific cloud implementation. For institutions that conduct appropriate due diligence on their CSP and take a deliberate approach to securing their cloud environment, there may be no difference in risk from an on premise environment and a cloud-based environment. In many ways, in a cloud environment, overall risks may be reduced due to the operational resilience capabilities and scalable architecture that a CSP can provide in the event of some type of capability failure.

Another advantage that the cloud can provide, especially to smaller institutions, is access to advanced analytic and artificial intelligence tools. These tools can help with security as well as

data analytics. For example, Security Information and Event Management (SIEM) monitoring is necessary to monitor your environment and detect, respond and mitigate security events. The challenge is that the amount of log and other data that is generated can hide unusual or nefarious events in the general noise of operations. Advanced tools exist that are designed to help ensure that high-value alerts are not lost in the noise, but these tools can be prohibitively expensive or difficult to deploy for smaller organizations. One thing that some CSPs provide is access to these types of tools as part of their environment, providing a capability that a smaller institution could not afford or replicate on its own.

It is clear that there are potential benefits and risks of the use of the cloud, but that decision should be left to each individual institution to weigh the risks and benefits of such a migration. If done appropriately, the use of the cloud may have little to no adverse effect on the overall risk profile of a financial institution and would most likely improve the resiliency of the financial institution.

III. All Parties Should Collaborate to Improve Cloud Security and Efficiency

There is strong competition among CSPs to obtain and maintain customers. This competition drives investments in new technologies and helps ensure that marginal costs are minimized. However, we also recognize that financial institutions are entering this dynamic space with regulatory oversight requirements that exceed anything applied to most other cloud customers. This can create challenges and barriers to entry. Larger financial institutions may have a better ability to bargain for contracts and products to meet their regulatory challenges, but it can be especially difficult for smaller financial institutions, that simply do not have enough market share, to work effectively with large CPSs to make changes to, for example, standardized contracts or product offerings. In addition, smaller financial institutions may have difficulty gaining access to the oversight data their regulators require them to obtain for any critical third party.

In many ways, this situation is similar to the issue small institutions face when dealing with the large core banking system providers who provide them the back-end systems that process their daily banking transactions. The smaller institutions have to have access to these services, but have little market leverage individually to pressure adoption of new technologies, or

obtain improved portability of data and services to avoid vendor "lock-in," and little capability to customize contracts. Just as the core providers are necessary to do business, the cloud and the tools available may become increasingly essential to a financial institution's competitiveness. As a result, it is critical that there is further collaboration to ensure that financial institutions of all sizes have the option of utilizing cloud products and services in a way that is consistent with regulatory requirements and expectations.

In the United States, there are some self-generated efforts by financial institutions to aid in improving oversight of third parties, including establishment of companies that work to make shared assessments available. While the companies in this space have different approaches, fundamentally the goal is to create efficiencies by performing a single assessment of a third party provider that is used by multiple financial institutions. One of these companies recently issued a press release touting its risk assessment of Microsoft Cloud Services that meets "the rigorous requirements of financial services customers" and covers the major cloud services that Microsoft provides including Azure and Office365. These types of services have the potential of providing significant help, especially to smaller institutions, to access the data necessary to satisfy the regulatory oversight requirements of critical third party providers and other CSPs should be encouraged to participate in these types of programs.

The progress on gaining access to necessary audit and internal control information is important, but several issues still remain. Importantly, this includes the shared responsibility model that is employed by most CSPs. The baseline shared responsibility model places the responsibility for the cybersecurity of a customer's implementation of a cloud offering entirely upon the customer. This approach may be understandable, but from the ABA's perspective it is our hope that the CSPs work more closely with financial institutions to find ways CSPs could be more proactive in helping secure financial institution cloud deployments. In particular, security controls should be standard and should not be subject to an "opt-in" by the customer. In addition, default security settings should be restrictive versus open and coordination among CSPs in the development of a unified security controls baseline for financial institutions would help ensure appropriate controls are used at the start of any deployment. The use of unified controls would also help financial institutions manage their third parties that utilize the cloud by ensuring that baseline controls are in place for their data and mitigating the risk of security control misconfiguration. CSPs understand their environment better than any single customer

and should have in place mechanisms to notify them of potential misconfigurations or security settings that pose a significant risk to the security of stored data.

Along with improved collaboration on security and notification procedures, we believe there is potential for financial institutions, CSPs and regulators to collaborate on a best practices model to provide standardized terms and conditions that provide financial institutions access to required audit and control data. While many CSPs currently publish attestations to the audits their services have undergone, for financial institutions increased transparency into the business continuity, security incident and breach response, and testing programs would help them comply with their regulatory requirements. Additionally, in the shared services model there are some CSPs that provide different options to customers regarding who manages some security controls. Additional transparency into these options and how the control environment is executed would help financial institutions manage both their risk and those of their third parties who utilize the cloud.

As part of a financial institution's cloud deployment, financial institution regulators have significant authority under the Bank Company Services Act to examine CSPs. Examination of a CSP would be a daunting task and would be exacerbated by the fact that a single CSP could service hundreds, potentially thousands of financial institutions. A potentially more efficient approach would be to establish some standardized parameters that financial institutions, CSPs and regulators could follow to ensure the appropriate contractual terms are in place for financial institutions to perform their due diligence and provide an expedited review process for regulators. This harmonization could provide increased transparency and provide the baseline for engagement with international regulators as CSPs and financial institutions cross multiple jurisdictions worldwide.

The challenges in this space are complex, and we believe that every stakeholder wants to ensure that the security of these critical systems is maintained and at the same time innovation is not hindered. A collaborative approach that merges the best of the safety and soundness culture of financial institutions and regulators with the entrepreneurial spirit of the CSPs is most likely to achieve a lasting outcome that is acceptable to all parties.

IV. Regulatory Clarity is Important

The GLBA and other standards provide an existing robust regulatory framework for financial data that resides in the cloud. Financial institutions are required to ensure any data provided to a third party provider is protected regardless of whether that entity itself is regulated. Whether CSPs should be regulated directly is a reasonable question to ask. But that question should be addressed in a broader context than just financial services. Regardless of potential regulation of CSPs, financial institutions will continue to be responsible for the security of their data, even when that data is handled or stored by vendors. Careful consideration, however, should be taken to ensure that any proposed path forward not impinge upon the ability of CSPs to innovate and offer new tools, nor single out financial services deployments and potentially increase costs or limit access to new or advanced capabilities.

One area worthy of consideration is the applicability of the Bank Services Company Act in the cloud context. Under the BSCA, "a depository institution that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises— (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the depository institution itself on its own premises." The services authorized include, "check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, or similar functions." We believe that cloud services would be considered services to assist in, for example, bookkeeping and similar functions. As regulators contemplate their role and responsibilities with respect to CSPs, in our view a collaborative approach would benefit all. For instance, it would be helpful to convene discussions with all stakeholders to help maintain the transparency of the financial regulatory oversight process and produce the most efficient outcome for all involved parties. At a minimum, regulators should update their July 2012 guidance on Cloud Computing to more specifically speak to any expectations they have for risk management of CSPs whether already in guidance or more unique to the cloud. In addition, it would be appropriate for the agencies to evaluate the BCSA to determine when CSPs should be included in their oversight and at what level.

Conclusion

The cloud is an exciting innovation that provides many benefits for financial institutions and their customers. At the same time, the unique regulatory environment faced by the financial sector presents certain challenges to CSPs that we believe can be addressed through greater collaboration with CSPs and the financial regulators. As the AI Task Force continues its exploration of these issues, we hope that you will consider the four points we have addressed in this testimony: financial institutions are required to ensure the security and confidentiality of their customer's information, regardless of whether that information is stored on a financial institution system or in a third party cloud; the cloud offers significant benefits but risks must be managed consistently and effectively; financial institutions must determine whether use of the cloud makes sense based on their business model, risk analysis and mitigation strategy and consistent with regulatory requirements; all parties, including core providers, should collaborate to improve cloud security and efficiency; and additional clarity on the roles and responsibilities of regulators with respect to their oversight of CSPs would be helpful.

Thank you for inviting me to testify today and I look forward to your questions.

"AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers"

Task Force on Artificial Intelligence
U.S. House Committee on Financial Services

October 18, 2019, 9:30AM
Room 2128 - House Rayburn Office Building

Testimony of Dr. Jordan Brandt, CEO and Cofounder of Inpher

I. Introduction

Cloud computing and AI are distinct and complementary technologies that offer tremendous economic and consumer benefits. The cloud reduces cost and democratizes access to computational resources, which in turn powers AI to streamline business functions and provide new insights that improve consumer welfare.

II. Issue Statement and Roadmap

The committee has correctly identified that these benefits must be harnessed with proper legislative and technological safeguards for data security and privacy. Whereas cloud computing and AI pose distinct risks, a common theme applies to both; don't put all of your eggs in one basket. The consolidation of sensitive personal information into any individual entity, to be mined by data-hungry AI algorithms, poses significant economic risks[1] and an existential threat to the privacy of our citizens. Fortunately, the emergence of Privacy Enhancing Technologies (PETs), and specifically encryption in-use capabilities, can address the concerns of both cloud data security and privacy in AI.

III. Preventing Data Centralization Risks

As banks move more of their data and information processing to the cloud, they are effectively consolidating risk into a select few providers of cloud computing infrastructure. The magnitude of this risk was underscored by the recent Capital One cloud hack.[2] The breach could have been

[1] IBM, *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years* (Jul. 23, 2019), https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

[2] Christian Berthelsen, Matt Day, and William Turton, *Capital One Says Breach Hit 100 Million Individuals in U.S.*, Bloomberg (Jul. 29, 2019), https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

prevented by securely computing across distributed data in a multi-cloud architecture, in which data is processed without exposing the underlying personal information. This would have eliminated a single point of failure.

IV. Application of Encryption in Use

To illustrate how this works, it is important to firstly define the three pillars of encryption, which is the best mathematical safeguard of data:

1. Encryption in-transit (https:)- Secures the transmission between sender and receiver.
2. Encryption at-rest (AES)- Secures data storage while on a hard disk.
3. Encryption in-use (Homomorphic Encryption, Multiparty Computation)- Secures data in memory while being processed.

In-transit and at-rest encryption are already ubiquitous. Encryption in-use is rapidly evolving from academic research into practical applications today, as its computing performance for large datasets quantifiably improves.

V. Privacy-Enhancing Technologies: Use Cases and Value

For example, at Inpher, we have made multiple order-of-magnitude improvements in the performance of both Homomorphic Encryption and Multiparty Computation without compromising accuracy. We are currently deploying this technology to solve real-world privacy and security challenges in banking, defense, healthcare, and other industries.[3]

Our platform keeps data private, secure, and resident-- precluding the need to centralize information into a single repository. This proactive safeguard enables financial institutions to minimize risk and leverage the full benefits of AI without a privacy tradeoff. PETs thus internalize the letter and the spirit of U.S. and international data privacy regimes which jointly emphasize privacy-by-design.[4]

Specifically, in the financial services sector, we are witnessing the application of PETs in: fraud and anti-money laundering, credit scoring, trade surveillance, and all forms of predictive modeling where compliant data sharing is critical.

---

[3] Inpher, *Case Studies*, https://www.inpher.io/case-studies-1#case-studies

[4] Notable international bodies including the United Nations ("UN"), Organization for Economic Co-operation and Development ("OECD"), European Data Protection Board ("EDPB"), and European Union Agency for Cybersecurity ("ENISA") have all promoted the implementation of PETs to minimize risks to privacy and data protection.

PETs safely overcome data silos and increase data utility. Regulators and law enforcement also benefit from privacy-preserving computing, as they are able to run forensics and surveillance on encrypted data for pattern matching and event detection without compromising individual privacy, or inviting potential liability. They can find the bad guys without compromising honest citizens. To this end we have briefed many domestic and international regulators about these capabilities over the last year and we are encouraged by their enthusiastic support.[5]

VI. Conclusion

To conclude, as a nation, we are in a technology arms race with countries like China that do not share our views on individual rights. We must not accept the false dichotomy between AI and our privacy; we can have both. Privacy-preserving computing not only champions and achieves this outcome, but also fosters new innovation and economic expansion that benefits our government, industry, and every American citizen.

We truly appreciate your interest and desire to learn more about these complex topics, and we remain at your disposal for any further questions you may have.

[5] Inpher, *Inpher Wins People's Choice Award at FCA TechSprint* (Aug. 9, 2019), https://www.inpher.io/news/2019/8/9/inpher-wins-peoples-choice-award-at-financial-conduct-authoritys-2019-tech-sprint.

Statement by

Meredith Broussard

Associate Professor, New York University

Affiliate Faculty, NYU Center for Data Science

before the

Task Force on Artificial Intelligence

of the

Committee on Financial Services

U.S. House of Representatives

October 18, 2019

Congressman Foster, Ranking Member Hill, thank you. It is an honor to be asked to testify today regarding "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers."

I'd like to speak about cybersecurity and the cloud in general, and then offer an opinion on strategies to improve cybersecurity in financial technology. I am an associate professor at the Arthur L. Carter Journalism Institute of New York University and an affiliate of the NYU Center for Data Science. I started my career as a computer scientist, working at AT&T Bell Labs. I later worked on Wall Street at Prudential Securities, and at a tech startup that did secure document management for complex financial transactions. I then switched to journalism, where now I teach data journalism. Data journalism can be described as the practice of finding stories in numbers, and using numbers to tell stories. I do a specific kind of data journalism called algorithmic accountability reporting. Increasingly, algorithms are being used to make decisions on behalf of citizens; algorithmic accountability reporters hold algorithms accountable, as well as the people who make algorithms. My academic research focuses on artificial intelligence for investigative reporting. In other words, I build AI tools in order to do accountability reporting in the digital world. I am also the author of a book called *Artificial Unintelligence: How Computers Misunderstand the World,* which explores the inner workings and outer limits of technology.[1] Understanding the outer limits of tech is essential for making decisions about cloud computing.

A great deal of cybersecurity discourse focuses on defense from attacks. In understanding regulation like the Strengthening Cybersecurity for the Financial Sector Act, I would argue that it is important to think through the interplay between humans and technical systems in addition to

[1] Broussard, *Artificial Unintelligence*.

considering the usual attack vectors. Effective regulation depends on effective communication as well as technical competence.

I was asked to address several points:

(1) The types of cloud deployments and services and how they are used within financial services;

(2) How AI could help automate the various components within a cloud infrastructure;

(3) Best practices for regulatory examiners when engaging cloud service providers and other related third-parties utilized by their regulated entities;

(4) Ways to combat systemic risks, strengthen consumer privacy, and decrease the risks associated with data breaches;

(5) Regulatory and legislative proposals to strengthen federal oversight of cloud infrastructures utilized by financial institutions.

I will address each of these points in turn.

1. **Types of cloud deployments**

There is a lot of confusion about what the cloud is. The most common expression among computer scientists is, "The cloud is someone else's computer." A program that *runs in the cloud* means that the program is running on someone else's computer. Data *stored in the cloud* means data stored on someone else's computer. The cloud is a wonderful metaphor, but practically speaking, the cloud just means "a different computer, probably located with thousands of other computers in a large warehouse in the tristate area." We can even pinpoint exactly where those computers are. Amazon Web Services, which controls 48% of the cloud computing market, has

four major data centers in the United States.[2] These are located in Northern Virginia, Ohio, Oregon, and Northern California. These data centers are also called server farms.

Amazon, Google, Microsoft, and Alibaba together control 76% of the worldwide market for cloud computing. These companies own or lease server farms, and inside the server farm buildings they maintain thousands of physical computers. Some of those computers are dedicated to a single purpose or client; some of those computers are shared by multiple clients. The hearing memo outlines four different types of clouds: public clouds, private clouds, community clouds, and hybrid clouds.

One example of a private cloud is the AWS GovCloud, the secure set of servers that hosts data and programs for DHS, Treasury, DoD, Cloud.gov, and other agencies. The computers that power the AWS GovCloud are physically located in buildings on the East Coast (in Virginia) and the West Coast. Those locations are powered by electricity. If the power goes out or those locations flood or are affected by extreme weather, the network will be compromised. All of the GovCloud servers are connected by underground wires to the global network we refer to as the Internet. These wires are also subject to physical constraints. They may be dug up, they may wear out, they may flood, they may be affected by earthquakes, or they may be vulnerable to any other physical threat. It is useful to understand the physical reality of the cloud in order to think about security for cloud computers. Cybersecurity threats arise from the natural world as well as from the humans who seek to penetrate secure systems.

Despite analysts' predictions, it is unlikely that *all* bank operations will eventually move to the cloud. It is more likely that the current trend will continue. Some operations will be most

[2] https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

efficient if done locally on one person's computer; other operations will be most efficient if done remotely on a more powerful cloud computer. Effective tech policy requires using the right tool for the task.

This gets us to the people part of the system. To get a good picture of how effective companies are at using cloud computing, it helps to hear from the IT professionals who manage local and cloud computers. A 2014 Ponemon Institute survey asked IT professionals to rate their organizations' effectiveness in securing data and applications used in the cloud.[3] Most (51%) rated their organizations as low in effectiveness. Based on their lack of confidence, these IT professionals also said the likelihood of a data breach in the cloud is increased.

Most banks currently do an effective mix of using the cloud for less-confidential services like email and HR, and keep their most secure information (consumer accounts, commercial accounts, customer data) in data centers that they manage themselves. Moving sensitive data to the cloud would require thoroughly vetting the cloud provider beforehand. In the same Ponemon survey, 62% of respondents did not agree or were unsure that cloud services were thoroughly vetted before deployment. Sixty-nine percent believed that their organizations failed to be proactive in assessing information that was too sensitive to be stored in the cloud.

If IT professionals have so little faith in their own organizations, and we know there is a high demand but low supply of IT professionals who are experts in cybersecurity, it seems that more regulation and oversight will help protect bank operations in the cloud.

2. How AI could help automate components of the cloud

[3] http://go.netskope.com/rs/netskope/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf

Artificial intelligence, like cloud computing, is widely misunderstood. Hollywood images of AI, like the Terminator or Commander Data from Star Trek, are what most people think of when they think of AI. These Hollywood images are delightful, but they are not real. AI is best understood as a branch of computer science, the same way that algebra is a branch of mathematics. Inside AI, there are other branches: machine learning, expert systems, and natural language processing are just a few of them. However, machine learning is the most popular kind of AI in business right now. It is so popular that there has been linguistic confusion. When people say "I am using AI for my business," what they usually mean is, "I am using machine learning for my business." Machine learning is another misleading name; it sounds like the computer has sentience or agency. It does not. Machine learning is math. It's computational statistics on steroids.

Banks are using machine learning to help make decisions about things like who qualifies for a mortgage. When we use machine learning, the first thing we do is take some data and construct a machine learning model to predict a certain value in the data. I describe the process in my book *Artificial Unintelligence:*

> There are three general types of machine learning: supervised learning, unsupervised learning, and reinforcement learning. Here are definitions of each from a widely used textbook called *Artificial Intelligence: A Modern Approach* by UC Berkeley professor Stuart Russell and Google's director of research, Peter Norvig:[4]
>
> > **Supervised learning:** The computer is presented with example inputs and their desired outputs, given by a "teacher," and the goal is to learn a general rule that maps inputs to outputs.
> > **Unsupervised learning:** No labels are given to the learning algorithm, leaving it on its own to find structure in its input. Unsupervised learning can be a goal in itself (discovering hidden patterns in data) or a means toward an end (feature learning).
> > **Reinforcement learning:** A computer program interacts with a dynamic environment in which it must perform a certain goal (such as driving a vehicle or

[4] Russell and Norvig, *Artificial Intelligence.*

> playing a game against an opponent). The program is provided feedback in terms of rewards and punishments as it navigates its problem space.
>
> Supervised learning is the most straightforward. The machine is provided with the training data and labeled outputs. We essentially tell the machine what we want to find, then fine-tune the model until we get the machine to predict what we know to be true.
>
> All three kinds of machine learning depend on *training data,* known datasets for practicing and tuning the machine-learning model. Let's say that my training data is a dataset of one hundred thousand credit card company customers. The dataset contains the data you would expect a credit card company to have for a person: name, age, address, credit score, interest rate, account balance, name(s) of any joint signers on the account, a list of charges, and a record of payment amounts and dates. Let's say that we want the ML model to predict who is likely to pay their bill late. We want to find these people because every time someone pays a bill late, the interest rate on the account increases, which means the credit card company makes more money on interest charges. The training data has a column that indicates who in this group of one hundred thousand has paid their bills late.
>
> We split the training data into two groups of fifty thousand names each: the training set and the test data. Then, we run a machine-learning algorithm against the training set to construct a model, a black box, that predicts what we already know. We can then apply the model to the test data and see the model's prediction for which customers are likely to pay late. Finally, we compare the model's prediction to what we know is true—the customers in the test data who actually paid late. This gives us a score that measures the model's precision and recall. If we as model makers decide that the model's precision/recall score is high enough, we can deploy the model on real customers.

It seems very attractive to create a model based on data, and then use the model to make decisions. It might also seem like it would be cheaper to use a machine learning model than to use a human staffer for making decisions. The problem is, almost every dataset is biased. Machine learning models discriminate by default.[5] If I have a dataset of people who have gotten mortgages, the data will be tainted by the history of redlining and residential segregation in the United States. Facial recognition systems are trained on datasets of faces; the bias is baked in

[5] Benjamin, *Race after Technology.*

based on who is in the dataset. In their groundbreaking "Gender Shades" project, Joy Buolamwini and Timnit Gebru showed that the most commonly used facial recognition systems are good at recognizing people with light skin, but fail to recognize darker skinned people.[6] In part, this is because the people who made the facial recognition technology (who are probably men with light skin, based on the dominant demographics of the tech industry) either failed to notice or failed to care that the tech failed for people with darker skin.

Good suggestions have been made by Cathy O'Neil, Jack Balkin, and others[7] about how to audit algorithms and machine learning models. If banks run machine learning models on sensitive data on-premises, it makes it easier to audit them, as will certainly be required in the near future. If the models run in the cloud, it makes it slightly more difficult to audit them because of the different levels of visibility available in cloud environments.

The issue here is not whether banks should use AI in the cloud or on-premises. When a bank uses AI, we should ask what the AI is used for, plus how it is used, what kind of AI is used, what specific data is used to train the model, and what specific data is used to make decisions after the model is trained. These questions need to be answered in addition to the basic questions of where the AI program and its associated data will run and be stored. One option: the questions above could be answered in plain language, and this information could be communicated as part of the regulatory examination.

3. Best practices for regulatory examiners

[6] Buolamwini and Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification."
[7] O'Neil, *Weapons of Math Destruction*; Balkin, "Information Fiduciaries and the First Amendment."

Every modern organization uses a combination of in-house (on-prem) and cloud (remote) resources. When a bank contracts with a Cloud Service Provider (CSP) like Amazon Web Services, they are required to do their due diligence just as they would with any outside vendor.

Regulators have been overseeing banks for hundreds of years, but cloud computing oversight is relatively new. Additional guidance is appropriate. There should be abundant oversight of CSPs, including regular on-site visits and more documentation of physical and virtual security practices. More regulators are likely needed to staff the regulatory positions. Cybersecurity is so complex that it is impossible for a single person to be an expert in both physical and virtual security. A team approach is necessary.

Another important thing to be aware of is the cultural conflict between tech and finance. In the tech world, which is the world that trains cybersecurity people and cloud computing people and IT people and AI people, nobody talks about regulatory compliance. The ACM, the membership organization that provides guidelines for computer science education globally, only developed ethical guidelines in the past two years. Regulatory compliance is not part of core computer science education. "Compliance" is a word most software developers don't hear unless they work in finance. The "move fast and break things" ethos is diametrically opposed to the mindset of compliance. It thus doesn't surprise me that in April 2019, when federal examiners visited the AWS site in Virginia, they did not notice the Capital One data breach in which 100 million customers' data was stolen.[8] "The examiners were greeted warily at the Amazon offices," the *Wall Street Journal* wrote of the visit. "Chaperoned by an Amazon employee, they were allowed to review certain documents on Amazon laptops, but not allowed to take anything

[8] https://www.wsj.com/articles/fed-examined-amazons-cloud-in-new-scrutiny-for-tech-11564693812

with them, some of the people said." The Amazon IT workers were behaving in a way that is culturally appropriate for their workplace: trying to keep data and procedures secret to protect what they perceive as Amazon's assets. Amazon's IT staff is not necessarily trained in financial industry compliance the way a bank's IT staff would be. One option is to require cloud providers' staff to be trained in financial regulatory requirements, just as staff who administer clinical trials must be trained in HIPAA security and procedures. The legislation could require training, then the specific training could be implemented at the level of, say, an industry association so the training could keep up with the pace of change in the technology world.

4. **Ways to combat systemic risks, including data breaches**

Liability in cyberspace should mirror liability in the physical world. A server farm is a bit like a hotel in that each bank is renting secure space (a hotel room in this analogy) from the server farm. If you suffer injury at a hotel, because of the hotel's negligence or an accident, the hotel is liable. In its FAQ about the 2019 data breach, Capital One writes: "Like many companies, we have a Responsible Disclosure Program which provides an avenue for ethical security researchers to report vulnerabilities directly to us."[9] It is ethical for a bank to constantly monitor its systems for vulnerabilities, just as it is for CSPs.

5. **Regulatory and legislative proposals to strengthen federal oversight of cloud infrastructures utilized by financial institutions**

[9] https://www.capitalone.com/facts2019/2/

This testimony has been prepared for a hearing entitled "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers." I am under the impression that the Committee is considering the proposed Strengthening Cybersecurity Act. The act proposes to extend existing regulation. Already, bank regulators have the power to oversee and examine third-party vendors for banks. This act proposes to extend this regulatory authority to the NCUA and FHFA so that credit unions, Fannie Mae, Freddie Mac, and FHLBs are similarly protected.

I would argue in favor of this or a similar act because additional protections and constant oversight are needed to protect Americans' financial information in the digital sphere, just as protections and oversight are needed in physical banks. We should approach the safety of our financial data with at least the same level of care that we devote to food safety in restaurants. Thinking about the physical reality of AI and cloud computing is important so that we don't make the mistake of thinking that tech is something different or special that demands exceptional treatment.

Citizens' rights and human rights must be protected online as they are offline. Effective regulation of financial technology in the cloud will allow us to foster innovation and competition while protecting consumers. CSP staff should be trained in regulatory compliance in order to serve bank customers, and more plain language explanations of complex AI technology should be made available by banks and CSPs so that regulators can adequately monitor the health of financial technology systems.

Thank you for the opportunity to contribute to this hearing. I look forward to answering your questions.

References

Balkin, Jack M. "Information Fiduciaries and the First Amendment." *UC Davis Law Review, Vol. 49, No. 4, 2016* 49, no. 4 (February 3, 2016). https://ssrn.com/abstract=2675270.

Benjamin, Ruha. *Race after Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity, 2019.

Broussard, Meredith. *Artificial Unintelligence: How Computers Misunderstand the World*. MIT Press, 2018.

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." In *Proceedings of Machine Learning Research*, 81:1–15, 2018.

O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. First edition. New York: Crown, 2016.

Russell, Stuart J, and Peter Norvig. *Artificial Intelligence: A Modern Approach*, 2015.

STATEMENT FOR THE RECORD

STEVE GROBMAN, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MCAFEE, LLC

BEFORE THE U.S. HOUSE OF REPRESENTATIVES TASKFORCE ON ARTIFICIAL INTELLIGENCE, FINANCIAL SERVICES COMMITTEE

ARTIFICIAL INTELLIGENCE AND THE EVOLUTION OF CLOUD COMPUTING: EVALUATING HOW FINANCIAL DATA IS STORED, PROTECTED AND MAINTAINED BY CLOUD PROVIDERS

OCTOBER 18, 2019, 9:30 AM | 2128 RAYBURN HOUSE OFFICE BUILDING

Chairman Foster and Ranking Member Hill, it is an honor to take part in this hearing on the evolution of cloud computing and its implications for securing the financial services sector from cyberattacks. Along with governments, telecommunications, and energy and water resources, the financial services sector is critical to the daily functioning of our economy and our overall security. Thank you for investigating ways to better protect this vital segment of our digital economy as such innovations as cloud computing and artificial intelligence change the way the financial services sector manages its information technology systems.

As McAfee's Senior Vice President and Chief Technology Officer, I set the technical strategy and direction to create technologies that protect smart, connected computing devices and infrastructure worldwide. I lead McAfee's development of next-generation cyber defense and data science technologies, threat and vulnerability research, and internal CISO and IT organizations. Prior to joining McAfee, I dedicated more than two decades to senior technical leadership positions related to cybersecurity at Intel Corporation, where I was an Intel Fellow. Participating in the public policy debate on how the public and private sectors can work together to protect our nation's critical infrastructures has and continues to be a professional and personal passion of mine.

MCAFEE'S COMMITMENT TO CYBERSECURITY

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates enterprise and consumer solutions that make our world a safer place for the benefit of all. Our holistic, automated, open security platform and cloud-first approach to building security solutions allow all security products to coexist, communicate, and share threat intelligence with each other anywhere in the digital landscape. Our customers range from government agencies to all sizes of businesses and millions of home users.

We are committed to solving the most challenging cybersecurity challenges in our industry, particularly the interoperability challenge. For too long, organizations have not been able to reap the full value of the cybersecurity tools they have purchased from vendors because of the lack of interoperability, the expense of integration, and the potentially valuable data locked

away from sight in proprietary silos. According to the industry analyst firm Enterprise Strategy Group, organizations use, on average, 25 to 49 different security tools from up to 10 vendors, each of which generates siloed data. Today, integrating security products into an established operational environment can be extremely resource-intensive, time-consuming and costly, all at the expense of hours that could be better spent hunting and responding to threats. What's needed is for cybersecurity companies to share "the plumbing" – the foundation, or common platform, upon which cybersecurity tools are built.

At McAfee, we're leading the drive toward interoperability and data sharing across the cybersecurity landscape. Together with IBM Security, McAfee recently launched the Open Cybersecurity Alliance (OCA) to bring together a large number of like-minded global cybersecurity vendors, end users, thought leaders, and individuals interested in fostering an open cybersecurity ecosystem, where products from all vendors and software publishers can freely exchange information, insights, analytics, and orchestrated response. OCA's purpose is to develop and promote sets of open source common content, code, tooling, patterns, and practices for interoperability and sharing data among cybersecurity tools. This partnership will enhance the ability of both the public and private sectors to keep up with and overtake cyber hackers, who are also leveraging such innovations as cloud computing and artificial intelligence to improve their own capabilities.

To solve the industry's most challenging issues and achieve interoperability across the cybersecurity landscape, we also must employ the best and the brightest in the field. This means developing and retaining a diverse and inclusive workforce.

MCAFEE'S COMMITMENT TO DIVERSITY AND INCLUSION

While we recognize there is still more to do, we're proud to describe the strides we're making at McAfee to promote diversity and inclusion. We believe we have a responsibility to our employees, customers, and communities to ensure our workplace reflects the world in which we live, and we're implementing programs to increase diversity and inclusion among our ranks. This business model is essential to the cybersecurity industry's success. Studies show time and again that diverse perspectives and human experiences lead to more creative approaches to solving challenges, and we know that inclusive teams deliver the best results.

Our most recent accomplishment was to audit our global employee base to examine pay parity. In April 2019, we achieved pay parity, making McAfee the first pureplay cybersecurity company to do so. It required an investment of $4 million to make salary adjustments on April 1. We'll continue to adjust the pay gap and uphold pay parity with annual analysis.

In 2018, our first year as an independent company, we released our first Inclusion and Diversity Report, which demonstrated our commitment to building a better workplace and community. In 2018, 27.1% of all global hires were women, and 13% of all U.S. hires were underrepresented minorities. In June 2018, we launched our "Return to Workplace" program for men and women who have paused their career to raise children, care for loved ones, or serve their country. This

12-week program offers the opportunity to reenter the tech space with the support and resources needed to successfully relaunch careers. As a result, 80% of program participants were offered a full-time position at McAfee.

Now, I'd like to address the Committee's central concerns: the effects of cloud computing and artificial intelligence (AI) on the security and integrity of the financial services sector.

THE FINANCIAL SERVICES SECTOR'S MIGRATION TO THE CLOUD

Financial services organizations are migrating to the cloud to reduce complexity, cut costs, and focus their capabilities on delivering financial services to their customers. According to the research firm MarketsandMarkets, the finance cloud market will grow at a compound annual growth rate (CAGR) of 24.4% to $29.47 billion by 2021.

Cloud adoption is ultimately about delegating certain functions to allow enterprises to focus on their core competencies. This includes:

- Infrastructure as a service (IaaS), delegating capabilities that would traditionally be run in a private datacenter
- Platform as a service (PaaS), delegating the technology building blocks and services that can be used to build solutions, and
- Software as a service (SaaS), delegating a complete application stack

With these "as-a-service" offerings, cloud providers usually take on the implementation of the service, which provides unique advantages, including:

- Faster innovation cycles
- The ability to optimize cost structure by having the opportunity to evolve and optimize an implementation of technology, as long as customer interfaces remain consistent
- Enhanced supportability of sophisticated solutions, as implementation and operational complexity is assumed and abstracted by their cloud providers

The technology at scale delivered to customers by cloud providers allows for very specific expertise that would not "scale down" to smaller organizations. This allows smaller organizations, including small businesses and organizations outside the technology industry, to access advanced technology that traditionally would be available only to large organizations or organizations that invest heavily in a highly technical employee base.

Cloud providers generally practice strong cyber hygiene, as they are executing at scale. For instance, all public cloud providers patched for the Spectre Meltdown vulnerability within days, while private datacenters had significant variability and, in many cases, did not have patches applied months after the vulnerability was disclosed. For example, AWS quickly disabled CPU microcode for the vulnerability.

Despite the benefits to organizations of moving to the cloud, there are also challenges. Organizations that transfer their IT capabilities to cloud providers have less visibility into their architecture and operations, given the delegation of "trust" to the provider. Any cyber vulnerabilities can impact multiple tenants. For example, a breach in a cloud provider's architecture can place multiple organizations' data at risk. An analogy I like to use is that traditional, on-premise computing is a lot like an automobile, and cloud computing is a lot like an airplane. While an airplane is safer than an automobile given its more advanced technology, when a failure does occur, the impact can be catastrophic.

Today, almost all organizations use multiple cloud providers. This trend is becoming the norm in the financial services industry, as it is in virtually all industries. Because of this, organizations need scalable monitoring and management solutions that allow common policies and operational capabilities to be applied to their multiple providers. In order to facilitate this, it is critical that programmatic interfaces are made available from the cloud provider or service to monitor solutions that can enable abstraction of monitoring, vulnerability detection, and management. This functionality is known as a Cloud Access Security Broker (CASB) and is a critical new class of application that is rapidly being adopted as a means to manage and secure diverse cloud environments.

Even with the addition of these types of advanced cloud cybersecurity tools, there are other cybersecurity issues related to the cloud, such as when an organization moves traditional computing to IaaS. Cloud environments add new complexity that a new workforce will need to understand in order to secure. As these public clouds are often accessible via public or private networks, organizations need to ensure that access is not accidentally granted to unauthorized entities via misconfigurations. Additionally, the control and configuration paradigms in cloud environments differ from traditional computing, and this could require the retraining of the existing IT workforce.

Another security issue with cloud is the use of unauthorized cloud applications, or Shadow IT, which often results when employees or small teams within a business attempt to work more efficiently by using IT resources outside of those sanctioned by the IT department. They run capabilities in a public cloud without IT controls, creating severe security risks and leading to exposure of an organization's technology and data. Shadow IT includes execution of rogue virtual machines in public IaaS as well as unsanctioned use of SaaS applications such as Microsoft 365, Gmail, GitHub and Source Forge (the top 4 according to McAfee's cloud team analysis). Given that a typical organization will access on average 120 such services, it is critical to understand and control legitimate, or sanctioned, applications from the unsanctioned applications. One of the challenges is that not all SaaS applications, including storage or collaboration services, are created equally, and without guidance from the chief information officer (CIO) or IT team, employees might opt for an application that has comparatively lax security controls, claims ownership of users' data, or is hosted in a country that tolerates, or even encourages, cyber-crime directed toward Western allied companies, particularly those in the financial services sector.

In sum, the financial services sector's use of cloud can provide many advantages – as long as security concerns continue to be top of mind, as they have been all along for this sector.

THE FINANCIAL SERVICES SECTOR'S USE OF ARTIFICIAL INTELLIGENCE

Financial services firms are using AI and machine learning to enable advanced analytics to better serve and protect customers. According to a study by Autonomous in an 84-page report on AI in the financial industry, the industry's slice of this massive AI pie represents upwards of $1 trillion in projected cost savings. By 2030, traditional financial institutions can save 22% in overall costs with AI: $490 billion in front office (retail functions), $350 billion in middle office (risk management and profit/loss calculations), and $200 billion in back office (settlements, regulatory compliance, and accounting).

For cybersecurity, artificial intelligence is without doubt the new foundation for cyber defense. The entire industry is tapping into the tremendous power this field offers to better defend our environments. AI enables better detection of threats beyond what we've seen in the past. It helps us out-innovate our cyber adversaries. The powerful ability of AI-based automation is key to addressing our talent shortage. AI means we can now delegate many tasks to free up our human security professionals to focus on the most critical and complex aspects of defending our organizations. AI enables us to evaluate data "at scale," and it enables us to find the so-called "needle in a haystack of needles" that has challenged our field for the last decade.

Yet it's important to understand that the cybersecurity industry is very different from other sectors that use AI and machine learning. To start, in many other industries, there isn't an adversary trying to confuse the models. AI is extremely fragile; therefore, one focus area at McAfee is Adversarial Machine Learning, where we're working to better understand how attackers could try to evade or poison machine learning models. We are developing models that are more resilient to attacks using AI techniques. As an industry, we need to be realistic about the immense power of AI-based technology. While it solves a host of problems for us – including making our defenses stronger – AI also intensifies the capabilities of our adversaries.

Bad actors can use AI to identify the most vulnerable victims, automate phishing, and evade detection. AI improves their ability to execute their attack and enables the creation of content to be used in social engineering and information warfare, as occurred in the 2016 election. One of the most troubling evolutions of AI-based information warfare technology is deep fake video generation, which can create realistic video of events that did not occur. These and many other adversarial uses of the technology can and will occur, putting our democracy and civil society at increased risk.

FINANCIAL SERVICES AND CLOUD PROVIDER CYBERSECURITY PREPAREDNESS

Our financial services and cloud provider customers and partners tell us the three biggest challenges they have are 1) dealing with conflicting regulations, 2) a constantly changing and

evolving technology landscape, and 3) the growing sophistication of cyber attackers. They also have to deal with cybersecurity tools that often don't work well with each other. The lack of interoperability among cybersecurity solutions limits their ability to exchange threat data on a rapid basis and creates seams of access for hackers.

The National Institute of Science and Technology's (NIST) Cybersecurity Framework provides a valuable roadmap for organizations of all sizes to evaluate their risk, see where their vulnerabilities are, and improve their cybersecurity capabilities. We commend the U.S. government for enabling this partnership that has improved the security posture of many critical infrastructure industries, including financial services and cloud providers. Likewise, compliance with Europe's General Data Protection Regulation (GDPR) is having a real impact on improving both the security and privacy practices of those U.S. companies that collect data from European Economic Area residents. GDPR protects personal data in both administrative and technical manners, requiring anyone handling the data to record their uses and make sure that they are securing the data.

Most major financial institutions are prepared for major cyberattacks with the potential to produce system-wide failure, in part due to the regulatory oversight of both the Bank Service Company Act (BSCA) and Gramm-Leach-Bliley Act (GLBA). Financial services companies have plans in place and are engaging actively in cyber sharing groups, in collaboration with the Department of Homeland Security (DHS), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve. They know what they'll do first to identify and respond to a nation-state attack against economic critical infrastructure.

Overall, third-party cloud providers also have a strong cybersecurity track record, due to their technical expertise and financial resources. These companies have solid plans in place to respond to cyberattacks, as evidenced by their commitment to aligning to the NIST Cybersecurity Framework. Cloud providers are also active in several public-private partnerships, such as the DHS Information Technology Sector Coordinating Council (ITSCC) and the National Telecommunications Advisory Committee (NSTAC), which further buttress their cybersecurity capabilities.

Cloud providers are less regulated than their counterparts in the financial services sector, given the general consensus among policymakers that overly prescriptive cybersecurity regulations would stifle the ability of internet companies to maintain their rapid rates of innovation. However, if service providers perform services for a bank, the BSCA gives federal regulators the ability to examine and regulate third-party vendors, including cloud providers. GLBA enables federal agencies to establish appropriate standards for financial institutions to ensure the security and confidentiality of customer information. Federal regulators have a legitimate interest in seeing that IT and cybersecurity services provided by cloud providers to financial institutions are well done to ensure confidence in our nation's financial services infrastructure.

Due to the increasing role cloud providers are playing in managing the IT capabilities of critical infrastructure companies (financial services, energy, telecommunications), policymakers should be exploring ways they can enhance the cybersecurity readiness of these companies.

CONCLUSION

The largest and most sophisticated companies in the financial services and cloud sectors are at the top of their game in cybersecurity, particularly in comparison to smaller companies and other industry sectors that have lagged in investing in the strategies, processes, people and technology needed to keep up with new threats and attackers. While innovations in both cloud and artificial intelligence are and will continue to enhance the cybersecurity of these sectors, these same innovations will progressively enable cyber hackers.

It is appropriate for policymakers to review the security capabilities of both financial services and third-party cloud providers, as both play vital roles in maintaining the safety and integrity of our nation's economy. However, policymakers should be wary of imposing additional cybersecurity mandates and regulations on the private sector, given the strong possibility that out-of-date, check-the-box compliance rules could be the result. Policymakers should first support voluntary collaboration and the use of industry-supported standards and best practices such as the NIST Cybersecurity Framework. When appropriate, existing cybersecurity rules for highly regulated critical infrastructure industries should be updated to reflect the rapid speed of innovation.

Thank you for the opportunity to discuss these issues with the Committee. I look forward to answering your questions.

Written Testimony of Alla Goldman Seiffert
Director of Cloud Policy and Counsel
Internet Association

Before the House of Representatives Committee on Financial Services
Task Force on Artificial Intelligence hearing:
"AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers"
October 18, 2019

Internet Association (IA) represents over 40 of the world's leading internet companies. We support policies that promote and enable internet innovation and are dedicated to advancing public policy solutions that strengthen and protect internet freedom, foster innovation and economic growth, and empower users.

Our companies are also global leaders in the drive to develop lower cost, more secure, scalable, elastic, efficient, resilient, and innovative cloud services to customers in both the private and public sectors. The major U.S.-based hyperscale cloud providers are all members of Internet Association.

To begin, I would like to give a brief overview of cloud computing. NIST defines cloud computing as a model for "enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] Typically, cloud service providers (CSPs) make available to customers a wide range of services that function as information technology building blocks that customers can use to build applications to meet their IT goals and be more secure, innovative, and responsive to their customers. These services are standardized and made available to all customers, including financial institutions.

A key benefit of the cloud is that CSPs are responsible for managing and securing certain aspects of the IT infrastructure supporting the services that customers use. Security is a top priority for CSPs and they invest a tremendous amount to make all of their services secure. By using these services, customers such as financial institutions can focus on carrying out core business functions and benefit from the security measures that CSPs have in place, as well as use security services that CSPs have developed to further protect their environments. In particular, IA member CSPs invest billions in cybersecurity and deploy resources and people in ways that simply cannot be matched by any single institution alone.

[1] Special Publication 800-145, National Institute of Standards and Technology, U.S. Department of Commerce, *NIST Definition of Cloud Computing: Recommendations of the NIST,* Peter Mell, Timothy Grace, September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

It is important to note that customers are responsible for determining the type of data that they store in the cloud and the types of applications they choose to run in the cloud. Indeed, financial institutions remain accountable for managing the risk of their IT environments, whether run in-house, through a third party (e.g., a managed service provider), or with a CSP. Financial institutions use the cloud for a wide range of applications, from storing publicly available data or running test environments to create new digital channels, storing more sensitive records, and running more critical workloads. In each case, customers' implementation of cloud services begin with the default security configuration that CSPs put in place, and each can take further steps to design, reconfigure, and manage their IT risks within their risk tolerance. While cloud computing use in the financial services industry is still nascent, cloud's security, scalability, and resilience features allow firms of all sizes to better manage risk.

Today, my testimony will identify several benefits and opportunities that cloud adoption creates for financial services firms, and I will focus on three central themes:

A. First, **cloud implementation is a shared responsibility between CSPs and customers.**
B. Second, **cloud adoption increases cybersecurity.**
C. Third, **cloud increases the resilience of our nation's financial institutions.**

Cloud security is a shared responsibility

As financial services firms look to achieve greater operational efficiency and modernize existing systems, they are increasingly turning to CSPs to manage their infrastructure and computing needs. Financial institutions that use cloud computing operate in an environment where they manage certain aspects of their IT resources and are responsible for configuring their use of cloud resources, but they rely on the CSP to manage other portions of their IT resources. This division of labor means that both the CSP and the customer bear responsibility for making sure the services are run efficiently and securely. Because each party is responsible for securing the resources they control, security in the cloud is what we call a "shared responsibility."

In general, the shared responsibility model means that CSPs are responsible for making sure the services they offer are secure and reliable, and CSPs give customers the ability to configure those services to achieve their business outcomes, including configuring the security settings of the services that they utilize. Certain cloud capabilities like application management, network configuration, and encryption settings are also the responsibility of the customer.

Simply put, CSPs are responsible for the security **of** the cloud, while the customer is responsible for security of the resources they store and process **in** the cloud. CSPs provide a broad range of information, tools, and assistance to help customers understand and properly administer their responsibilities.

In practice, this means CSPs protect the underlying infrastructure of their cloud and data centers from vulnerabilities, intrusions, fraud, and abuse.[2] While the specifics of this can be rather technical, these details are essential to understanding the shared responsibility model. In order to provide secure cloud infrastructure, CSPs manage and control the host Operating System (OS), the virtualization layer, and the physical security of its facilities. Customers are responsible for securely configuring the environments and applications that they deploy in a cloud environment, and CSPs also provide their customers with necessary security capabilities that can be configured to meet customers' unique security needs.

To ensure security within a given cloud environment, the customer configures and manages the security controls for the guest OS and other applications (including updates and security patches), as well as for the security group firewall. Customers also have the ability to configure cryptographic protection for certain services, which can be important based on the type of data and usage of workloads in the cloud environment. In some cases, CSPs may encrypt all customer information by default.

There are different service models for cloud computing, and customers may have more, or fewer, security responsibilities, depending on the types of services they use.

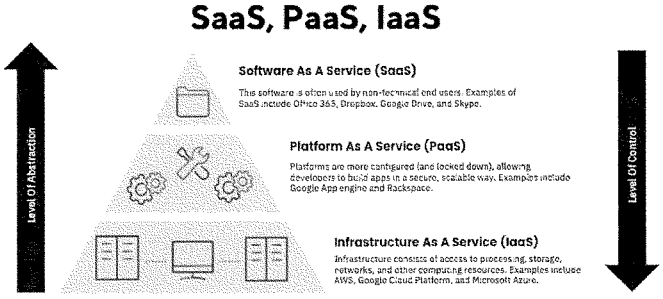

Figure 1: Diagram of IaaS, Paas, and SaaS as they relate to abstraction and level of end-user control.

It is important for financial institutions to have a clear understanding of the resources they are using when running in the cloud, and how the shared responsibility model applies to their applications. There exist domains of IT security controls that financial institutions should keep

[2] Panetta, Kasey. "Is the Cloud Secure?" Gartner. Gartner, Inc, October 10, 2019. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/.

in mind when using the cloud. CSPs manage those controls associated with their physical infrastructure and certain other aspects of their environment that may previously have been managed by the customer.

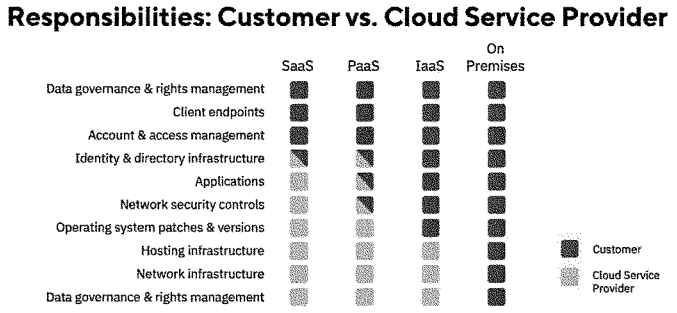

Figure 2: compared responsibilities between SaaS, PaaS, IaaS, and on-premises cloud models

In the financial services context, customers' security requirements will be informed by their own internal standards, as well as regulatory requirements and expectations.[3] The cloud model allows firms to implement best-in-class security controls and tailor them to the specific systems and workloads that each firm is running. Each customer is responsible for determining their security requirements and the cloud enables customers to meet those requirements. In addition, certain CSPs may offer tools, dashboards, and other real-time information and documentation to provide customers with information about configuration management, including how to configure services to meet appropriate requirements, such as implementation of multi-factor authentication or methods to enhance resiliency of services through data redundancy based on how the application is configured.

Even though CSPs are responsible for securing certain aspects of the cloud environment, customers are able and encouraged to evaluate the effectiveness of CSPs' security controls. CSPs provide assurance about the security of their environments through many mechanisms, including certifications from independent third-party auditors against industry standards. These audits speak to the design and implementation of CSPs' control environments. Customers then can use CSPs' control and compliance documentation available to them to perform their control evaluation and verification procedures as required by their internal

[3] II.C.20(a) Outsourced Cloud Computing, Federal Financial Institutions Examination Council (FFIEC), *IT Examination Handbook Infobase.* https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers/iic20(a)-outsourced-cloud-computing.aspx

compliance standards. Financial institutions typically incorporate the use of cloud into their risk management frameworks. Customers can use the assurance mechanisms that CSPs make available to ensure that they are adopting cloud in a manner consistent with their risk frameworks.

Cloud Increases Security Across Financial Services Firms

Cloud adoption helps banks increase overall security by modernizing applications and gaining better visibility into their networks, traffic, and vulnerabilities. The opportunities offered by cloud computing enable enterprises to significantly strengthen their IT security posture and implement best-in-class cybersecurity solutions.

Cloud application and infrastructure architects are presented with the opportunity to develop solutions that provide a business function while also designing systems securely. Financial institutions can leverage the security solutions implemented by CSPs to meet compliance and regulatory requirements to operate in a secure manner.

Financial services institutions are subject to regulatory and compliance requirements to ensure that their IT infrastructure is secure, to protect their and their customers' data, and ensure privacy. Financial services institutions are ultimately responsible for understanding these requirements and defining how they apply to their applications. This may include, for example, conducting due diligence and monitoring to ensure the security and resiliency of their CSPs' environments and taking steps to ensure that they architect their cloud environments in a secure, resilient, and compliant manner.

The cloud enables financial institutions to meet these security requirements and benefit from the operational efficiencies and other business opportunities that scalable technology has to offer.

The Department of the Treasury published a *Fintech Report* and put it thusly:

> The ongoing digital transformation of the financial services system is being driven not only by developments in computing power, the expanding ubiquity and interconnection of computers and mobile devices, and the exponential growth in digitized financial data, but also by technologies that can benefit from advances in data and computing capacity at greater scale and with greater efficiency. **Scalable technologies such as cloud computing enable financial services companies to store and process vast amounts of data and to quickly add new computing capacity to meet changing needs.** At the same time, advances in big data analytics, machine learning, and artificial intelligence

are expanding the frontiers of financial services firms' abilities to glean new and valuable business insights from vast datasets.[4]

Large cloud service providers typically have the resources and expertise to invest in and maintain state-of-the-art and comprehensive IT security and deploy it on a global basis across their platforms. Financial institutions, especially small and mid-sized firms, could find it economically infeasible to achieve similar levels of security on their own. Moreover, because customers can rapidly redistribute data across a CSP's geographically diverse storage and processing centers, cloud environments can enhance firms' strategies for business continuity.

Increased Resilience

Another key benefit of using cloud computing is that the use of cloud services enables financial services firms to design applications to be more resilient. Cloud allows firms of all sizes to leverage a suite of best-in-class tools for backup, continuity of operations, and redundancy.

CSPs design their infrastructure to be resilient to outages and incidents, and customers can take advantage of this infrastructure to establish enhanced operational resilience. CSPs arhitect their global infrastructure to protect against physical disruptions and to make available redundant IT components to customers. For example, major CSPs' infrastructure consists of multiple data centers in locations all over the world. Within a single metropolitan region, some CSPs organize groups of data centers into an "Availability Zone" (AZ). AZs are physically separated and independent from each other and are built with highly redundant networking to withstand local disruption.

Customers are able to design applications so that they utilize multiple AZs within a single region. By implementing this type of design pattern, customers increase the resiliency of their applications. In the unlikely event an AZ fails, this architecture allows applications to continue running seamlessly using resources in the other AZs. This protects customers, while allowing core business functions to continue uninterrupted. Customers are also able to keep redundant copies of data in both multiple AZs and multiple regions to ensure broader availability and durability.

Customers are further able to apply this design pattern to achieve even greater operational resilience by architecting applications to make use of more than one region. Cloud-specific features, such as regional autonomy, allow systems to operate freely in a region without dependencies on other regions. Cloud adoption can also facilitate system transparency and insights necessary to make automated decisions.

---

[4] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation,* Steven T. Mnuchin, July 2018. https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities--Nonbank-Financials-Fintech-and-Innovation_0.pdf

Financial services institutions are responsible for identifying their resiliency requirements, but the cloud enables them to build particularly resilient applications in line with broader risk management goals. For instance, by embracing key features of cloud technology, firms can deploy Enterprise Business Continuity Management (EBCM) across their entire technology stack. This is a risk and continuity of operations framework that enables companies of all sizes to think through (and plan) for a variety of scenarios that may befall the business. Cloud services play an integral role in provisioning extensible, flexible solutions that companies can configure to take advantage of seamless backup and restore services.

Conclusion

In conclusion, I would like to reiterate IA's gratitude for being included in discussions with the Committee Task Force on Artificial Intelligence and for the opportunity to testify here today. The IT postures of financial services firms have evolved a great deal over the years, and the internet industry is looking forward to supporting their continued growth and maturity.

Cloud computing has the power to meaningfully help financial services firms increase cybersecurity and resilience while also allowing firms to implement a shared responsibility model in managing their networks and data. IA – along with our members – stands ready to support the Task Force and Committee in helping financial services companies adopt cloud in a responsible way.

Thank you.

December 6, 2019

Chairman Bill Foster
House Committee on Financial Services
Task Force on Artificial Intelligence
2366 Rayburn House Office Building
Washington, DC 20515

Hearing: AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers

Questions for the Record from U.S. Representative Ted Budd (R-NC.)

Witness: Ms. Alla Seiffert, Director of Cloud Policy and Counsel at Internet Association

1. Ms. Seiffert, in today's digital world, data security is more critical than ever. Can you elaborate a bit more on how cloud computing services can lead to enhanced security, thus adding another layer of protection to both public and private sector data?

   Answer:
   Cloud adoption by financial services firms enables increased security for both new and old applications. Commercial cloud technology allows companies to minimize threat vectors for existing systems while also leveraging cloud-native security tools for data analysis and protection. The cloud empowers businesses of all sizes to get visibility into their networks, traffic, and vulnerabilities using commercially-available tools to protect customer and enterprise data.

   As financial services firms have grown and evolved, legacy software applications across data centers and mainframe computers have continued to increase in size and complexity. Enterprise cloud technology presents an opportunity for companies to re-engineer and re-architect their complex, legacy systems using modern software languages and security frameworks. Decommissioning antiquated software increases overall security by removing legacy code and eliminating vulnerabilities.

   An important feature of distributed computing and storage resources is that changes to software code can be pushed into production environments almost instantaneously and at very little cost. This allows firms, including those in the financial services industry, to patch software vulnerabilities early and often, leading to increased cybersecurity.

   Furthermore, cloud technology offers financial institutions the opportunity to use a new generation of cloud-native security tools such as logging, code testing, data analysis, fraud detection, and firewalls on their networks. Taken together, these capabilities increase overall firm security while also helping businesses meet compliance and regulatory requirements.

2. Ms. Seiffert, it is no secret that the federal government maintains a poor posture with regard to information technology. In your testimony, you highlight how the cloud facilitates agility and innovation for all customers – in particular financial services customers? Can you please expand on your thoughts in this area?

   Answer:
   Cloud adoption allows banks to focus on their core business functions while outsourcing data center management to third party providers whose sole business is information technology. The Department of Treasury's 2018 FinTech report notes: "scalable technologies such as cloud computing enable financial services companies to store and process vast amounts of data and to quickly add new computing capacity to meet changing needs."[1] This becomes a competitive advantage to firms who have adopted cloud, and is one of the main reasons that the technology's proliferation across the industry is increasing.

   Cloud further enables enterprises to adopt a best-in-class practice known as DevSecOps - or the combined business process that applies agile methodologies and cross-functional communication to the development, security, and operations functions in software development. This methodology leads to increased organization-wide cybersecurity by integrating security practitioners into every part of the application building and monitoring process. Firms that adopt DevSecOps bring in security teams at the outset of initiatives, which allows them to create both information security governance and automation practices in a way that is not possible with on-premises or legacy data center environments.

   Cloud's scalability also has the added benefit of lowering barriers to adopting good IT practices across the industry. The technology "creates a more level playing field between financial institutions of different sizes, by giving small- and medium-sized institutions access to computing resources that were previously only available to larger institutions with the ability to devote significant resources to technology infrastructure."[2]

3. Ms. Seiffert, innovation in the FinTech sector is continuing to occur at a rapid pace. In particular, new startups are continuing to emerge and could serve as one of the biggest beneficiaries of the solutions that cloud computing provides. How do FinTech startups benefit from cloud computing?

   Answer:
   New FinTech companies uniquely benefit from cloud adoption because they can leverage from

[1] Steven T. Mnuchin and Craig S. Phillips, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation – Report to President Donald J. Trump, Executive Order 13772 on Core Principles for Regulating the United States Financial System* (U.S. Treasury Report, U.S. Department of the Treasury, 48-49, 2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

[2] Hal S. Scott, John Gulliver, and Hillel Nadler, *Cloud Computing in the Financial Sector: A Global Perspective* (SSRN: Program on International Financial Systems, July 26, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427220

cutting-edge technology without the baggage of decades-old legacy enterprise architecture decisions. Specifically, start-up companies in the financial services space can use the full suite of services provided by hyperscale cloud service providers to achieve the following business benefits:

- Scale software to reach consumers across the world white remaining secure, audit-ready, and compliant. Cloud offers multiple available zones and data centers around the world to reach both customers and employees on desktop and mobile devices.
- Implement agile application development to patch vulnerabilities faster and gain competitive advantages in delivering customer features.
- Launch Artificial Intelligence (AI) and machine learning (ML) solutions with little friction. Cloud-based AL/ML frameworks can help start-ups do everything from creating more personalized customer experiences to improving transaction monitoring and tracking fraud.
- Ensure high service uptime, and contribute to continuity of operations by architecting resilient applications that make full use of cloud's features and monitoring tools.
- Remove barriers to customer acquisition due to lower costs and scalable solutions. This can lead to expanding financial access and serving more diverse customer segments, particularly those in developing or underserved markets.[3]

[3] Ibid.