Engine

July 5, 2016

The Honorable Mitch McConnell Majority Leader U.S. Senate Washington, DC 20510	The Honorable Harry Reid Democratic Leader U.S. Senate Washington, DC 20510
The Honorable Paul Ryan Speaker U.S. House of Representatives Washington, DC 20515	The Honorable Nancy Pelosi Democratic Leader U.S. House of Representatives Washington, DC 20515

Dear Leader McConnell, Leader Reid, Speaker Ryan, and Leader Pelosi,

We are a group of startups, entrepreneurs, and innovators who believe that strong encryption is a necessary tool for digital security and critical to the functioning of the internet economy. We are concerned about the anti-encryption rhetoric that has increasingly come to dominate conversations in Washington D.C. We appreciate your efforts to explore this complex topic further in forums removed from a politically charged environment. We request that you consider the unique perspective of startups like ours when exploring proposals that would impact the future of encryption technologies and digital security.

While much of the dialogue on cybersecurity has focused on whether the government can and should enlist large technology companies to assist in decrypting information for law enforcement purposes, there has been little discussion of the impact that legislation relating to encryption would have on the startups that are responsible for all new net job growth in this country. Encryption is at the heart of many of our products and services. Without the security and confidence that encryption provides, it would be difficult or impossible for us to find customers and investors, and ultimately, grow our businesses. While some proposals put forth to date, such as Senators Richard Burr and Dianne Feinstein's draft "Compliance with Court Orders Act," would have a broad and devastating impact on the nation's economy and security, startups face unique challenges that make such anti-encryption proposals particularly dangerous.

Unlike larger technology companies, startups like ours lack the resources necessary to comply with the anti-encryption proposals some legislators have put forward. In its dispute with the FBI, Apple estimated that building a decrypted version of its operating system would require the company to devote six to ten engineers working full time for two to four weeks. Even for the subset of startups that have six engineers on staff, losing a month of those employees' time could bankrupt the company. Additionally, even if a startup could afford to design a "backdoor" for government access, it would be excessively difficult to adequately protect that "backdoor" from the innumerable cybercriminals and bad actors that would try to exploit it. To secure a single decrypted operating system, Apple estimated it would have to build one or two secure facilities that could cost $50 million. No startup has anywhere near that kind of free capital to devote to protecting government-mandated vulnerabilities. Consequently, imposing anti-encryption mandates on startups will inevitably result in massive security threats. It is not a question of whether criminals will get access to these backdoors, but when and how much damage they will cause.

The fallout of this increase in cybercrime will hit startups harder than larger, well-known companies. Startups do not have the name recognition or consumer trust that would allow us to weather the security breaches that will occur if we are forced to abandon encryption technologies and provide backdoor access into our systems. Many of us have already lost business from international clients over the perceived vulnerability of U.S. companies to government surveillance and data collection. If Congress mandates that we create backdoors or otherwise weaken encryption, even more customers will abandon our services for competitors in countries that still recognize the importance of encryption and security.

Our defense of encryption is meant to promote public safety, privacy, and security, not undermine them. We share the law enforcement community's interest in preventing crime, and we will continue to cooperate with the government to combat terrorism. However, because wrongdoers will always have access to encryption tools and services created overseas, weakening encryption in the U.S. will only make U.S. citizens and companies vulnerable to cyberattacks without any significant benefit to law enforcement.

As you continue to explore the policy landscape surrounding encryption, it is our hope that you will take the concerns of our community into account. Attached hereto is testimony from startups around the country highlighting their unique perspectives on encryption and why it is important to their companies. We look forward to continued engagement with you and your colleagues over the coming months and appreciate your consideration.

Sincerely,

Binary Formations
Mechanicsville, VA

Biometrica Systems
Las Vegas, NV

Bracket Computing
Mountain View, CA

Canary
New York, NY

Capitol Bells
Washington, DC

Inflection
Redwood City, CA

Keen IO
San Francisco, CA

Lean Team Tuning LLC
Plattsburgh, NY

LyteShot
Chicago, IL

Mapbox
Washington, DC

Chat ID
New York, NY

CitiQuants Corporation
Miami, FL

Convo
San Francisco, CA

Descartes Biometrics, Inc.
Blaine, WA

Devbright
Peoria, IL

Development Seed
Washington, DC

DevNetwork
San Francisco, CA

Dwolla
Des Moines, IA

Estate Map, LLC
Minneapolis, MN

FireboxGaming
Charleston, WV

Foursquare
New York, NY

Garmentory Inc.
Seattle, WA

GitHub
San Francisco, CA

Help Scout
Boston, MA

Infinit
New York, NY

Nourishwise
Nashville, TN

Optimizely
San Francisco, CA

Patient IO
Austin, TX

Pitch Data
New York, NY

Plickers
San Francisco, CA

SafeLogic
Palo Alto, CA

Sandberg Tech of North Dakota
Devils Lake, ND

Soha
Sunnyvale, CA

Sportzpeak
San Francisco, CA

Starry, Inc.
Boston, MA

The Community Company Inc.
Crystal City, VA

Vera
Palo Alto, CA

Virtru
Washington, DC

Waterfall International
San Francisco, CA

Aire
London

CitiQuants™

CitiQuants (http://www.citiquants.com/)
Miami, FL

Founded in 2014, CitiQuants is a cloud-based analytics platform that captures timely, reliable, and accurate data to facilitate decisionmaking around corporate expansion and site selection. If a company is looking to expand to a new city or region, it can utilize CitiQuants and our proprietary algorithm to compare the cost of various locations based on inputs like human capital, operating costs, real estate prices, and numerous other metrics. CitiQuants is a small startup with just 3 employees, but we serve over 50 global Fortune 500 companies through Zagada—our research analyst parent—which we are migrating to CitiQuants, and provide data on cities across the U.S., Latin America, Asia-Pacific, and Europe.

CitiQuants relies on encryption in two main ways. The first is to guarantee secure platform access. If, for example, a company's Chief Financial Officer is doing a comparative analysis for a potential expansion, it is critical that only a specific set of individuals within that company have access to the report. Most of our comparative analyses include sensitive, private business information that must be protected from hackers on the platform, in the cloud, and in transit. We maintain or delegate permissioning and controls around who can access these analyses and the sensitive information they include, and encryption is integral to this process. Encryption also protects the data that clients host on our platform.

The second way we rely on encryption is for licensing access and distribution purposes. As a growing digital publisher, our success depends on having control over our revenue stream. Digital rights management schemes can play some role in this, but encryption has proved to be even more valuable for our company. We use a third-party for informational rights management and content protection when sharing data and analyses with clients. Encryption is an essential piece of the security protections they provide. Say, for example, we produce a report for a company and they pay a certain fee for five people on their operations team to access. It is critical that we make certain that the report is not distributed beyond those five individuals, either within the company or to other entities that have not paid for access. Encryption ensures that shared content is only readable by the sender (us) and the intended reader (paying customers).

Efforts by policymakers to weaken encryption would have an irreversibly negative impact on our bottom line. Our customers demand strong protections when utilizing our platform, and our ability to effectively operate depends on having strong safeguards to protect our revenue stream. As the scale and use of our platform increases, strong encryption will become even more critical to our success.

CONVO

Convo (www.convo.com)
San Francisco, CA

Convo is a SaaS platform for collaboration within and among businesses. Over Convo, our users communicate and share information about mission-critical business needs such as product design, healthcare, emergency care, and editorial content creation. Launched in 2013, Convo has signed up more than 15,000 enterprise customers including major news networks, research centers, and hospitals.

Some of Convo's flagship features include the ability to point to specific parts in an image or in a presentation or a PDF file. A research director at Gartner explained, what's cool about Convo is that you can annotate on a particular paragraph of that document or area in a photograph. Although as simple as text messaging, these features are more powerful than screen sharing and greatly reduce the need for in-person meetings in geographically distributed teams. Most of Convo's customers report a reduction in email usage for internal communication by more than 70 percent.

In addition to these product features, strong, robust encryption also differentiates our service from others. Our customer's data is increasingly sensitive and valuable, therefore we encrypt data both in transit—as it travels between a server and a user's machine—and at rest. We go beyond other vendors in our category by encrypting all data on the server at all times so that in case of an attack, a hacker would find only gibberish.

As a result of the revelations around American surveillance practices, we have seen international customers looking for vendors that host data outside the U.S. In this climate, technology companies like ours have to work especially hard to convince our business customers that their data is safe, even if we are based and host their data in the US. For some customers, our assurance is not enough, though. We have recently lost customers because they were unwilling to host business data on U.S. soil.

Encryption should be considered a basic right for all business users. Any legal mandate that outlaws or weakens encryption would make our customers' data vulnerable to attack and furthermore, make our services less attractive or unusable to customers that demand high levels of security. Requirements to make our product less secure would have very little benefit to the government, but would come at an extremely high cost for Convo, in terms of both the resources required to comply and the potential resulting loss of business.

Development Seed (https://www.developmentseed.org/)
Washington, DC

Development Seed helps governments and civic groups better serve citizens with technology and data. We are a small team of 19 people, but we do big work. Founded in 2003, we build mapping and modelling tools to better plan electricity grids in Africa, track service disruptions in refugee camps in Lebanon, provide live election data to the Washington Post's website readers, and we built the only part of Healthcare.gov with 100 percent uptime.

Interacting with government and taking political action can involve incredibly sensitive transactions, whether that is signing up for personal healthcare from your work computer, signing a petition on LGBT rights in Uganda, or reporting criminal activity on the US-Mexico border. To responsibly provide services like this we must use the best encryption available. To ask our partners to put trust in the tools we build we have to be open about any limitations and vulnerabilities and we often open our software for public scrutiny.

It is unlikely that tools we build would be used for communication that would be of interest to U.S. law enforcement. However, any legal requirement to build tools that include capabilities to decrypt and make data available to U.S. law enforcement would seriously undermine our business. The majority of our work involves international clients who simply would not accept such software. We would be forced to stop building tools for U.S. markets and to consider relocating significant parts of our operations to partner firms outside of the U.S.

FOURSQUARE

Foursquare (https://foursquare.com)
New York, NY

Foursquare is a technology company that enriches consumer experiences and informs business decisions through a deep understanding of location intelligence. The company's mobile apps, Foursquare and Swarm, are used monthly by more than 50 million people who have left more than 87 million tips and checked in more than 9 billion times. Foursquare business solutions include targeted advertising (Pinpoint), media measurement (Attribution), data analytics (Place Insights), and the developer tools (which includes the Places database that powers location data for Apple, Uber, Twitter, Microsoft, Pinterest, Waze, Garmin and 100,000 other companies and apps). Foursquare has 200 employees in headquarters in New York and offices in San Francisco, Chicago, Atlanta, Los Angeles, Detroit, London, and Singapore.

Foursquare utilizes encryption technologies and protocols to protect our user data, including from interception or alteration, and from eavesdropping, tracking, or the modification of received data. Our company also uses hashing technology to store and protect our users' passwords.

Policies that would require our company to weaken these protections or forego future protections are problematic for a number of reasons. First, any requirement to write reversible algorithms or build a backdoor into our existing encryption would completely defeat the purpose of those protections and put millions of our users at risk. Additionally, our company may in the future choose to expand our utilization of encryption in the event the market demands more robust protections. Legislation that weakens encryption would prevent our company from effectively meeting users' demands, which could result in a loss of users. Finally, an unrestrained requirement that we aid in efforts to subvert our own security would be very costly and difficult to comply with, as we have a small team with limited resources. Even if the government is able to reimburse for employee salaries, there would be a large opportunity cost, since resources would be diverted away from other mission-critical projects.

Inflection

Inflection (www.inflection.com)
Redwood City, CA

By the time you’ve finished reading this statement, 2.3 new background checks will have been delivered through our employment background screening platform GoodHire, and five potential fraud alerts will have been sent by our identity protection platform IdentitySmart.

Inflection is a Silicon Valley-based tech company committed to building trust through advanced identity and screening solutions. Since 2006, we’ve filtered and analyzed hundreds of millions of public records to support trusted connections between people in personal and professional interactions through our background screening, identity verification, and people search products.

Our customers rely on us to manage personally identifiable information for use in HR-critical business processes, in verifying identities online, and for alerting them to potential identity theft. Strong encryption is baked into virtually every layer of our platform, from TLS-encrypted communications to AES-encrypted storage. It’s a key mechanism for protecting the information that our customers entrust to us.

Weak or backdoored encryption technologies would have a catastrophic impact on our ability to secure sensitive customer data against cybercriminals and hackers. Since our inception in 2006, we’ve invested a significant amount of time and money in cybersecurity because we understand that it’s critical to the trust we’re committed to building with our customers and that we help them build with theirs. As a small company, (about 150 employees,) it would be extremely challenging to allocate additional resources to replacing all the security controls that would be undermined by backdoored encryption protocols.

Strong encryption is vital for maintaining our trusted brand, reputation, and economic viability. That’s why we’re joining with Engine and other startups to urge you to consider the consequences to the security of people’s personal information as well as the economic impact to companies like ours as you consider any anti-encryption or encryption-backdoor legislation.

NourishWise (https://nourishwise.com)
Nashville, TN

NourishWise is an online nutrition startup based in Nashville, TN. Founded in 2015, we connect local restaurants and their nutrition data to our passionate and healthy minded eaters. In so doing, we drive increased and repeat business for our restaurant partners while removing the guesswork and guilt from our eaters. Restaurants provide us with their recipe books and our team of registered dietitians cull through that data and analyze the nutritional value of various dishes. We then share that nutrition information with our eaters, who can make healthier choices when ordering.

Our brand is built on trust, and our current and future operations depend on being able to offer restaurants and users the strongest security protections available. Recipe information is highly sensitive and our partner restaurants understandably demand robust safeguards for their data. A data breach that resulted in the recipe book of one of our partner restaurants getting into the wrong hands would irreversibly damage our brand. On the user side, we are responsible for protecting payment information and we may begin collecting health data in the future. Adequately safeguarding private financial and health data from criminal hackers is not only essential to maintaining our users' trust, but it is also required by federal statute.

While NourishWise does not currently utilize encryption, we will almost certainly have to use encryption technologies to scale the company. As we collect data that is increasingly sensitive and valuable, using strong encryption to protect that data will become even more critical. That is why NourishWise is concerned with legislative proposals that would mandate anti-encryption "backdoors." Building strong encryption or outsourcing it to a third party is already a costly endeavor for any small startup. But building strong encryption and *then* being required to develop a government-only backdoor and protect it from cyber criminals would be virtually impossible for a company like ours.

A "backdoor" mandate is a mandate for insecurity. And while it is unlikely that law enforcement would ever need access to an encrypted recipe from one of our partner restaurants or the data of one of our users, hackers may. It is indisputable that "backdoors," no matter how well-protected they are, weaken data protections and create vulnerabilities that criminals could exploit to illegally access our partners' and users' trade secrets and financial, health, and other personal data. Ultimately, the perception that our data is insecure will drive businesses and users away from our platform, crippling our ability to expand into the thriving, sustainable technology business we hope to one day become.