No. 14-10275

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff–Appellee

v.

DAVID NOSAL,
Defendant–Appellant.

On Appeal from the United States District Court for the
Northern District of California, No. 08-cr-00237-EMC-1 (Chen, J.)

BRIEF OF *AMICUS CURIAE* BSA | THE SOFTWARE ALLIANCE IN SUPPORT OF NEITHER PARTY

Of Counsel
MARTIN HANSEN (application for admission forthcoming)
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-6000

SIMON J. FRANKEL
MATTHEW D. KELLOGG
COVINGTON & BURLING LLP
One Front Street, 35th Floor
San Francisco, CA 94111
Telephone: (415) 591-6000

Attorneys for *Amicus Curiae*
BSA | The Software Alliance

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, BSA | The Software Alliance states that it has no parent corporation, subsidiary, or affiliate that has issued shares to the public.

December 9, 2014

By: */s/ Simon J. Frankel*
Simon J. Frankel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICUS CURIAE* AND SOURCE OF AUTHORITY TO FILE

BSA | The Software Alliance ("BSA") is an association of the world's leading software and hardware technology companies. On behalf of its members, BSA promotes policies that foster innovation, growth, and a competitive marketplace for commercial information technology. As makers of the software and infrastructure that have powered the world's transition into the digital age, BSA's members have a keen understanding of the need for laws such as the Computer Fraud and Abuse Act that protect those technologies—and the businesses and consumers that use them—from wrongdoers. At the same time, BSA's members also have a strong interest in ensuring that these laws are not interpreted in ways that could impede the development of innovative technologies and services that benefit businesses and consumers alike.

BSA's members include Adobe, Apple, ANSYS, Autodesk, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rockwell Automation, Rosetta Stone, Siemens, PLM, Symantec, Tekla, and The Mathworks.[1]

---

[1] Counsel to the parties have consented to the filing of this brief. BSA affirms that no counsel for a party has authored this brief in whole or in part and that no person other than BSA and its counsel made a monetary contribution to the brief's preparation or submission. Fed. R. App. P. 29(c)(5).

INTRODUCTION AND SUMMARY OF ARGUMENT

The Computer Fraud and Abuse Act ("CFAA") makes it a crime to access a computer "without authorization," or in excess of authorization, and then to take one or more forbidden actions, most of which involve obtaining information from the computer. *See* 18 U.S.C. § 1030(a)(1)–(4). In the present case, Defendant–Appellant David Nosal was convicted of violating Section 1030(a)(4), which prohibits, in relevant part, anyone from "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value." *Id*. § 1030(a)(4).

The government's theory of liability centers on putative co-conspirators of Defendant who, after leaving their jobs at executive search firm Korn/Ferry, allegedly used the access credentials of an employee who had remained at the firm to access the firm's network.[2] *See* ER 1172–76 (Second Superseding Indictment) at ¶¶ 19(a), (f), (n), 20–21. Because the putative co-conspirators were not otherwise permitted to access the Korn/Ferry network, *see id*. at ¶ 19(a), (f), (n), the government contended that their access using the employee's credentials was

[2] The terms "access credentials" and "credentials" refer to user names, passwords, product activation keys, and similar tools that are used to access a computer or online service.

"without authorization" within the meaning of the CFAA, *see, e.g.*, Dkt. No. 280[3] (Government's Opposition to Defendant's Motion to Dismiss Remaining CFAA Counts) at 11:17–18; Dkt. No. 445 (Government's Opposition to Defendant's Motion for Acquittal Under Rule 29) at 11:21–28.[4]

Thus, a central question in this case is under what circumstances a third party's access to a protected computer using an authorized user's valid access credentials constitutes access "without authorization" within the meaning of the CFAA. The district court below issued two separate decisions that could be read to suggest that such access by a third party is *always* "without authorization" if the owner of the computer did not specifically authorize the third party to access the computer. *See* ER 163 (Order Denying Defendant's Motion to Dismiss); *see also* ER 35–36 (Order Denying Defendant's Motions (1) for a New Trial and (2) for Acquittal).

While the district court was correct that third-party access using an authorized user's credentials *often* constitutes access "without authorization," any interpretation of the CFAA that treated *all* such access as necessarily unauthorized

---

[3] "Dkt. No." citations refer to entries in the district-court docket below.

[4] As the government has explained, the CFAA's prohibitions against "exceeding" authorized access to a protected computer are "not at issue in this case." Dkt. No. 445 at 11:26.

would be overbroad and could lead to undesirable results. On the one hand, CFAA liability will often be appropriate where the credentials were stolen or otherwise misappropriated, or where the third party's access to the computer was undertaken for purposes of fraud or theft. In other instances, however, a third party might have legitimate reasons to access the computer using an authorized user's credentials with that user's consent and on that user's behalf. Access by a third party in these situations should not automatically result in a violation of the CFAA.

The need for lawful third-party access is particularly pressing in the context of cloud computing. In the traditional model of computing, it was typical for only one person to control access to a particular computer, as the person accessing the computer was typically also its owner (or the owner's employee, student, agent, or designee). Today, however, computing services are increasingly provided by service providers over the Internet via remote servers, often referred to as "in the cloud" because such services are not tied to a specific physical location or device.

Where cloud services are involved, it is increasingly important that the business or individual who subscribes to a cloud service (the "cloud customer") be able to exert at least some control over who can and cannot access the data, software, and other materials that the customer chooses to host on computers owned and operated by the company providing such services (the "cloud provider"). This may include allowing *one* cloud provider to access the cloud

customer's account on *another* cloud provider's computers, for example, in order to assess security risks, provide advanced search services, or perform similar functions.

Accordingly, although BSA takes no position on the outcome of this case, BSA urges the Court to reject a bright-line, *per se* rule that would impose CFAA liability in any case in which a third party accesses a computer using an authorized user's credentials with the authorized user's permission. Nothing in the CFAA's text compels automatic (potentially criminal) liability for all instances of such access, nor do this Court's holdings in cases such as *LVRC Holdings LLC v. Brekka* require such a result.

Instead, this Court should adopt a more pragmatic standard that recognizes the range of scenarios in which an authorized user (such as a cloud customer) may legitimately wish to enable a third party to access a protected computer owned by someone else (such as the servers hosting the cloud customer's account) on the authorized user's behalf and for that user's benefit. This approach might take into account, for example: (1) whether the authorized user had a legitimate basis for granting access to the third party (*e.g.*, because the user created or otherwise has an interest in the data stored on the computer); (2) whether the authorized user in fact permitted the access in question; (3) whether the access was for the benefit of either the owner of the computer or an authorized user; and (4) whether the access

was within the scope of authorization granted by the computer owner to the authorized user, such that the access would have been authorized if undertaken by the authorized user and not the third party.

ARGUMENT

I. Cloud Computing Is a Critical Emerging Technology with Significant Long-Term Benefits for Businesses, Individual Users, and the Economy—and an Attendant Need for One Cloud Service to Access Another Cloud Service Using a Customer's Access Credentials.

The emergence of cloud computing has been one of the most important technological developments of the twenty-first century. Cloud computing differs from traditional computing in that computing resources (that is, data storage and processing, applications, and services) are made available from an off-site data center operated by a cloud provider rather than maintained "locally" by a business or individual, such as on a personal computer ("PC") or mainframe computer. *See* Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud?*, 50 Am. Bus. L.J. 413, 418–20 (2013); *see also* Nat'l Inst. of Standards & Tech. ("NIST"), U.S. Dep't of Commerce, *The NIST Definition of Cloud Computing* 2 (Sept. 2011) (hereinafter *NIST Definition*), *available at* http://tiny.cc/148kix.

Cloud providers generally offer one or more of several different types of cloud services, three of the most prominent of which are:

- Software as a Service ("SaaS"), which enables customers to access software applications such as email and word processing;

- Platform as a Service ("PaaS"), which enables customers to create and deploy their own software applications using a cloud provider's resources, which serve as a "platform" for the customers' applications; and

- Infrastructure as a Service ("IaaS"), which enables customers to use a cloud provider's hardware (such as the provider's servers, storage, and networking hardware) and basic infrastructure software to run customers' software, including both platform software and applications.

NIST Definition at 2–3. Each of these models shares the defining characteristic of cloud computing: computing resources that were once local (or "on premises") have moved to "the cloud," where they are provided over the Internet by a third party.

A. The Growth of Cloud Computing Offers Enormous Benefits to Both Businesses and Individual Users.

As explained below, cloud computing can help reduce IT costs, support innovation and competition in the marketplace, provide enhanced data security, and increase convenience and productivity. These attributes are expected to make cloud computing a key contributor to economic growth and job creation.

1. Cloud computing helps reduce IT costs.

Cloud computing helps reduce costs by providing businesses access to world-class information technology ("IT") without requiring large capital investments in infrastructure, software, or other resources. Under the traditional model of computing, IT-dependent businesses often invested large amounts of capital in buying and maintaining IT hardware and infrastructure, software, staff,

and other IT resources. *See, e.g.*, Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law*, 16 J. Tech. L. & Pol'y 229, 233 (2011) ("License fees, maintenance fees and professional service fees come at a premium for those wishing to house their IT services solely in-house. In addition, physical, on-site data centers come with high operating costs.").

Through cloud computing, businesses and individuals now can access software applications (such as word processing, communications, or other productivity applications), data storage, and a huge range of IT services "on demand" from leading IT providers over the Internet. In most cases, users pay for only those services and IT resources that they need at any given time, resulting in substantial cost savings. *See* King & Raja, 50 Am. Bus. L.J. at 418–20. And because cloud providers typically are able to distribute their costs across many customers, they usually can offer on-demand resources at a price much lower than the cost that a single business would incur if it were to purchase and maintain those IT resources on its own. *See, e.g.*, Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761, 1822 (2011).

Moreover, by working with a wide array of customers, cloud providers have the resources to invest and develop expertise in data processing, security, and other key IT functions that are beyond the capabilities of most businesses. *See id.* With lower IT costs and higher performance, businesses have more time and greater

resources to devote to their core missions. *See* Adrienne Hall, *Cloud Security, Privacy and Reliability Trends Study: A Silver Lining in Services Adoption*, Microsoft Trustworthy Computing Blog (June 11, 2013), http://tiny.cc/838kix (noting that 70 percent of small and midsize businesses responding to survey reported having reinvested money saved through cloud computing into product development, innovation, and expansion into new markets).

2. Cloud computing promotes innovation and competition.

By offering nearly instantaneous and more affordable access to exceedingly powerful IT resources and services, cloud computing levels the playing field among businesses and thereby promotes competition and innovation. The on-demand nature of cloud computing has been particularly important for small businesses and startups, allowing them to bring innovative products to the marketplace more easily and rapidly than in the past and with lower upfront capital investments. Harshbarger, 16 J. Tech. L. & Pol'y at 234–35 ("The cloud model is even more attractive to small businesses that often lack the required capital to implement an IT department or even implement the necessary IT infrastructure to do business."); Werbach, 60 Duke L.J. at 1812 ("[A] startup such as Smugmug, which hosts photos for over 150,000 paying customers, can move from its own server array to Amazon.com's cloud infrastructure, saving $500,000 in storage costs and providing flexible capacity for growth.").

Similarly important for these businesses is the "scalability" of cloud computing—that is, the ability to increase or decrease demand for computing resources rapidly in accordance with a business's changing needs. *See* Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 325 (2013). In the traditional model of computing, businesses needed to purchase and maintain IT resources such as infrastructure, software, and skilled IT staff themselves, regardless of how much those resources were used; when additional resources were required, additional capital investment was necessary. *See* BSA, *Cloud Computing and the Software Industry* 2 (Dec. 2009), http://tiny.cc/f38kix. In contrast, cloud computing's on-demand model enables businesses to pay for only the infrastructure and services they need when they need them. This means that even the smallest organizations can access extremely powerful computing hardware and state-of-the-art applications on demand and at a reasonable cost.

3. Cloud computing can provide strong security for electronic data.

Cloud computing also can help businesses more effectively protect the security of their electronic data, which has become a top priority in light of growing cyber threats. *See* Corporate Board Member & FTI Consulting, *Law in the Boardroom* 21 (2013), http://tiny.cc/jhwejx ("[D]ata security and IT risk is one of the most significant issues for directors and general counsel."); *see also*

TechAmerica, *CIO/CISO Insights: Achieving Results and Confronting Obstacles* 1 (2014), http://tiny.cc/u18kix ("Top priorities for CIOs [of federal agencies] include . . . improving cyber security.").

Cloud providers are well positioned to offer the enhanced security that businesses need. Because of its centralized model, whereby cloud providers deliver services and provide infrastructure from centralized data centers to multiple, geographically dispersed customers, cloud computing promotes more efficient and effective security practices. For example, under the traditional computing model, a software provider would have to send security updates to each customer individually and wait for the customers to install the updates on their own systems. Today, cloud providers can install security updates and address other security issues centrally, at their own data centers, and thereby provide strong security immediately and automatically to all customers using the service. Werbach, 60 Duke L.J. at 1821–22 ("Backup, business continuity, security, and other utility functions are significantly more efficient if deployed across a large virtualized cloud of computers.").

Research confirms that cloud computing provides enhanced security, particularly for small businesses. A 2013 study conducted by Microsoft found that 94 percent of small and midsize businesses reported experiencing new security benefits—such as an enhanced ability to maintain up-to-date security patches and

anti-virus software and to manage spam email—after switching from traditional on-premises technology to cloud-based solutions. *See* Hall, *Cloud Security, Privacy and Reliability Trends Study*, http://tiny.cc/838kix.

4. Cloud computing increases convenience and promotes productivity.

Cloud computing also offers significant benefits in terms of productivity and convenience. *See* Andrews & Newman, 73 Md. L. Rev. at 326 n.66; Werbach, 60 Duke L.J. at 1816. "Thanks to cloud computing, users no longer have to worry about storage capacity, memory, endless hardware purchases and upgrades, lengthy software downloads, or constant updates . . . because applications all run directly from the cloud, not from the user's [device]." Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 Nw. J. Tech. & Intell. Prop. 29, 29–30 (2010). Even the most basic computing tasks, such as word processing, are significantly enhanced by cloud computing. For example, a SaaS word-processing application allows users to create a document on one device, edit it on another, and enable colleagues around the world to access and edit the same document from their own devices.

5. Cloud computing promotes economic growth and job creation.

Given these benefits to businesses and individuals, it should come as no surprise that cloud computing is projected to fuel significant economic growth and created jobs. In 2013, spending on public cloud IT services (*i.e.*, cloud services

offered to the public rather than to individual organizations) was estimated to be $47.4 billion. Int'l Data Corp. ("IDC"), *IDC Forecasts Worldwide Public IT Cloud Services Spending*, IDC.com (Sept. 3, 2012), http://tiny.cc/ez8kix. This figure is expected to increase to more than $107 billion by 2017, with the market for cloud-computing services growing at a 23.5 percent annual rate in the interim—five times faster than the IT industry as a whole. *Id*.

IDC has also projected that, by 2015, business revenue from IT innovation enabled by cloud computing could reach $1.1 trillion per year. IDC, *White Paper: Cloud Computing's Role in Job Creation* 2 (2012), http://tiny.cc/af9kix. The efficiencies created by cloud computing will result in substantial savings for businesses: between $500 billion and $700 billion annually by 2025, according to the McKinsey Global Institute. McKinsey Global Institute, McKinsey & Company, *Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy* 65 (May 2013), http://tiny.cc/zybqjx. These increased revenues and savings will lead to more jobs. Spending on public and private cloud services will create an estimated 14 million jobs worldwide by 2015, more than half of them at small and midsized businesses. IDC, *Cloud Computing's Role in Job Creation*, at 2–3.

B. Certain Cloud Services May Legitimately Access Other Cloud Services Using a Customer's Access Credentials.

Along with all its benefits, cloud computing also brings with it complexities in terms of users' needs to access multiple cloud services. As more computing services are performed by third-party cloud providers, it becomes increasingly important that businesses and individuals retain at least some control over who may access the information, applications, and other resources that those businesses and individuals have chosen to store in the cloud. This ability to control access may include situations in which a business or individual cloud customer authorizes one cloud provider to access computers owned by another cloud provider on the customer's behalf—often by providing the first provider with the customer's own access credentials for the second provider's service.

The necessity of this limited type of credential sharing is another result of the shift from on-premises computing to cloud computing. In the traditional model of computing, it is commonplace for a user to "authorize" one piece of software to interact with another piece of software on the user's computer in order to accomplish a specific task. For example, a PC owner may install security software developed by one company in order to protect against malicious software that could infect *other* companies' software installed on the PC owner's computer. *See* Meiring de Villiers, *Computer Viruses and Civil Liability: A Conceptual Framework*, 40 Tort Trial & Ins. Prac. L.J. 123, 128 (2004).

In the cloud-computing model—where software and infrastructure are provided as services hosted in third-party data centers—this same process might require a cloud customer to authorize a security cloud provider to deploy its service to protect the customer's files or applications stored on the computers of a different cloud provider. *See, e.g.*, Larry Dignan, *Security Vendors Roll Out AWS Products, Pitch Extra Protection*, ZDNet (Nov. 11, 2014), http://tiny.cc/e53ipx (recently announced third-party security services for customers of Amazon Web Services ("AWS") cloud services). The interaction between these services could require the owner of the files or applications—the cloud customer—to share its cloud-storage access credentials with the security provider, so that the security provider can use these credentials to access the cloud service on the customer's behalf.

Such interactivity among cloud services is becoming increasingly common. One well-known example is Intuit's popular service Mint, available at www.mint.com. By giving Mint access to their online accounts with banks, credit card providers, and other financial institutions, customers can use Mint to better understand their spending habits, create budgets, and track their investments. To enable Mint to access these accounts, Mint's customers provide the service with their access credentials and then authorize Mint to access the accounts on their behalf. *See* Mint.com, *Mint Security FAQ*, http://tiny.cc/8bclix (last visited Nov. 20, 2014). Mint accesses, downloads, and categorizes the information in

these accounts in order to provide financial services to its customers. *Id*. More than ten million users have authorized Mint to access their financial accounts on their behalf, and have shared their access credentials to other financial accounts in order to enable Mint to do so. Mint.com, *How It Works*, http://tiny.cc/udclix (last visited Nov. 20, 2014).

As cloud computing becomes more prevalent, an increasing number of cloud services will require the ability to access the services of other cloud providers on behalf of an authorized user, using that user's legitimate access credentials. *See, e.g.*, Splunk, *Cloud Solutions*, http://tiny.cc/pq4ipx (last visited Nov. 20, 2014) (third-party search services for cloud customers); Alfresco, *Alfresco in the Cloud*, http://tiny.cc/334ipx (last visited Nov. 20, 2014) (third-party content-management services for cloud customers); Manthan, *Technology Partners*, http://tiny.cc/aa5ipx (last visited Nov. 20, 2014) (third-party analytics services for cloud customers).

II. The Court Should Reject a *Per Se* Rule That *All* Third-Party Access Using an Authorized User's Credentials Constitutes Access "Without Authorization" Under the CFAA.

As set out above, a central question in this case is under what circumstances a third party's use of an authorized user's access credentials (such as a user name and password) to access a protected computer, without the express authorization of the computer owner, constitutes access "without authorization" within the meaning of the CFAA.

The CFAA does not define the term "authorization," nor does it specify the mechanisms by which such authorization may be granted, extended, or revoked for purposes of the statute. This Court has held that the term "authorization" in the CFAA should be given its "ordinary, contemporary, common meaning" as defined by the dictionary: "permission or power granted by an authority." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132–33 (9th Cir. 2009) (applying definition in context of employer-employee relationship).

In its orders denying Defendant's Motion to Dismiss Remaining CFAA Counts (Dkt. Nos. 274, 276) and Motion for Acquittal Under Rule 29 (Dkt. No. 436), the district court's holdings could be read to suggest that using another person's credentials to access a protected computer *always* constitutes access "without authorization." ER 163 at 14:7–9 ("If the CFAA were not to apply where an authorized employee gave or even sold his or her password to another unauthorized individual, the CFAA could be rendered toothless."); ER 35–36. The district court's decisions did not appear to take into account the many instances where such access might be both necessary and appropriate, such as in the context of cloud services.[5]

[5] Defendant argued in his motion to dismiss the remaining CFAA counts that his and his co-conspirators' conduct did not violate the CFAA because this Court's earlier *en banc* decision indicated that "if a wife logs into her husband's Facebook

(continued…)

As explained in more detail below, while BSA takes no position on the outcome of this case, BSA urges the Court not to apply a rule derived from the employment context automatically to all instances in which a third party accesses a protected computer using an authorized user's access credentials. Although it is true that a third party's use of an authorized user's credentials to access a protected computer, without the explicit permission of the computer owner, may *frequently* constitute access "without authorization" under the CFAA, a rule that *all* such cases necessarily constitute unauthorized access would be overbroad and could lead to undesirable results.

BSA urges this Court instead to adopt a rule that can accommodate scenarios in which an authorized user may legitimately share her access credentials with a third party to enable that third party to assist her in organizing, securing, or

---

account using his email and password (with his permission), she has violated Facebook's terms of service, but she . . . would not be guilty of a crime under the CFAA." Dkt. No. 276 at 5:24–26; *see United States v. Nosal*, 676 F.3d 854, 861 (9th Cir. 2012) (*en banc*) (discussing Facebook's prohibition against sharing passwords). In rejecting Defendant's argument, the district court did not directly address whether such access by the relative of a Facebook user would constitute access "without authorization" or, if such access *were* deemed authorized, why the decision of Defendant's co-conspirator in this case to "willingly provide[] her access credentials" would not similarly result in authorized access. ER 162 at 13:23–28. Instead, the district court briefly distinguished the Facebook scenario by noting that Facebook's password policy is a "use restriction" and that the type of information accessed by the Facebook user's relative would be the user's "personal account and information" and not "any Facebook trade secrets." *Id.*

otherwise managing the user's online information and resources on another computer, on the user's behalf and for that user's benefit. A contrary rule that imposed *per se* liability under the CFAA for such access using an authorized user's credentials could make it significantly more difficult for customers of cloud services to manage and use data, applications, and other resources stored in the cloud according to their unique needs and circumstances.

Such an approach is consistent with the text of the CFAA, which does not require that all third-party access using an authorized user's credentials must result in liability. On the contrary, the absence of a definition of "authorization" provides courts with breathing room to interpret the statute in a sensible way, including by distinguishing between cases involving third-party access for legitimate ends, on the one hand, and cases where access credentials have been stolen, or are used to perpetrate fraud or theft against the computer owner or authorized user, on the other hand. This approach is also consistent with this Court's previous CFAA decisions, including *Brekka*, and with the approach of lower courts that have considered the meaning of "without authorization" since *Brekka*.

A. To Evaluate Whether Third-Party Access Using an Authorized User's Credentials Is "Without Authorization," Courts Should Take into Account the Circumstances Surrounding Such Access.

Adopting a *per se* rule under which each and every instance of third-party access using an authorized user's credentials constitutes access "without

authorization" could have a harmful effect on cloud services and the businesses and individuals that rely on them. BSA urges the Court to adopt a more pragmatic approach that would require courts to take into account whether the authorized user has a legitimate interest in the data, software, or other resources being accessed as well as whether the authorized user knowingly permitted the third party to act on his or her behalf for a legitimate purpose.

1. Both cloud providers and cloud customers have legitimate interests in controlling access to cloud-hosted data.

As discussed in Section I, an essential characteristic of cloud computing is that IT resources that traditionally were maintained locally by businesses or individuals for their own use are now maintained by a third-party cloud provider for multiple customers. However, despite the fact that a cloud provider now owns and operates many of the IT resources utilized by cloud customers, these customers often create the data that they have chosen to host at the cloud provider's facilities, and may own or license the software applications hosted at those facilities. The result is that *two* parties may have a legitimate interest in access to the data or other materials stored on the cloud service: the cloud provider and the cloud customer.

Consider, for example, a typical example of Infrastructure as a Service ("IaaS"): a business contracts with a cloud provider to host remotely documents and applications that the business previously stored and operated on its own servers, which it maintained on its own premises. Although the cloud provider

likely owns the facilities in which the documents and applications are now maintained—and therefore might have at least limited rights to access those documents and applications—the cloud customer, as the creator of the documents and developer or licensee of the applications themselves, may also have a legitimate claim that it should have at least some control over access to the computers on which those documents and applications are hosted. *See* Orin S. Kerr, *Computer Crime Law* 48 (3d ed. 2013) ("Computer passwords are a bit different from [physical keys], at least in most cases. Usually, there are two parties that have plausible claims to set authorization: the owner/operator of the computer, and the legitimate computer account holder.").

This same set of dual interests may arise in certain Software-as-a-Service ("SaaS") scenarios (such as where an individual cloud customer uses an online email service to write, receive, and store email instead of using a locally hosted email application on her PC or mobile device) and in certain Platform-as-a-Service ("PaaS") scenarios (such as where a business contracts with a cloud provider to host an interactive website that the business previously hosted on its own servers).

In these scenarios, the cloud customer might reasonably expect at least some ability to control access to the data or other resources hosted in the cloud. This might include the ability to share access credentials to such resources so that a third party may access the customer's data—at the customer's direction—in order

to provide additional services (*e.g.*, scanning the customer's remotely stored files and applications for malicious software, or providing advanced search services). *See supra* Section I.B. A *per se* rule that access using an authorized user's credentials is necessarily "without authorization" under the CFAA would discourage the use and development of inventive cloud-based technologies that rely on a cloud customer's ability to grant such access to third-party services.

2. Where a third party accesses a protected computer using an authorized user's credentials, authorization should depend in part on whether the authorized user knowingly shared his or her credential for a legitimate purpose.

The fact that a third party uses an authorized user's valid credentials to obtain access to a protected computer should not, without more, trigger automatic (potentially criminal) liability under the CFAA. Rather, courts should assess whether and to what extent the third party's access was authorized by the authorized user and whether that user shared the credentials for a legitimate purpose.

Not all forms of access using an authorized user's credentials are equal under the CFAA. At one end of the spectrum, accessing a protected computer using access credentials that were obtained by fraud or theft, or to perpetrate fraud or theft against the computer owner or authorized user (such as theft of software or of an online service), is plainly "without authorization" and should result in CFAA liability, assuming all other statutory requirements are met. At the other end of the

spectrum are legitimate cloud services like those described in Section I.B, where the cloud customer knowingly shares her access credentials with a third party so the third party can access the cloud service in order to perform legitimate, lawful tasks at the customer's direction and on that customer's behalf.

Where a third party accesses a computer using an authorized user's credentials at the authorized user's direction and for that user's benefit, in order to engage in a lawful activity, such access should not necessarily be considered without authorization for purposes of the CFAA. For example, for the reasons explained above, an individual reasonably expects to exert a greater degree control over data that she creates or uploads to a cloud platform to which she personally subscribes than she would expect to exert over data owned by her employer and stored on her employer's network (as was at issue in *Brekka* and in this case). The CFAA analysis should be sufficiently flexible to account for the differences between cloud-computing scenarios in which an authorized user grants a third party access to data, applications, or other materials that the user creates, and the employer-network scenario (and similar situations) in which the authorized user enables a third party to access *someone else's* data or material in order to commit fraud or theft.

Accordingly, deciding whether access using an authorized user's credentials constitutes access "without authorization" should require courts to take into

account, for example: (1) whether the authorized user had a legitimate basis for allowing another to access that computer (*e.g.*, because the user created or otherwise has an interest in the data stored on the computer); (2) whether the authorized user in fact permitted the access in question (*e.g.*, by sharing his or her access credentials); (3) whether the access was for the benefit of the owner of the computer or the authorized user; and (4) whether the access was within the scope of authorization granted by the computer owner to the authorized user, such that the access would have been authorized if undertaken by the authorized user.

Under this approach, a third party's access to a computer using stolen access credentials would normally be deemed access "without authorization," as would access for the purpose of defrauding the computer owner or the authorized user (*e.g.*, the cloud customer). On the other hand, where a third party uses an authorized user's credentials to perform services at that user's direction and on the user's behalf, such access may not necessarily be "without authorization"—even if not specifically permitted by the computer owner. This approach would enable courts to avoid criminalizing innocent acts like those in the husband-wife Facebook scenario presented by Defendant in his motion to dismiss (discussed above in footnote 4) and would also help foster the development of important services that rely on access to cloud services using the cloud customer's credentials.

B. The Statutory Language of the CFAA Does Not Require All Third-Party Access Using an Authorized User's Credentials Automatically to Result in Access "Without Authorization."

In addition to encouraging the further development of cloud computing and helping courts draw common-sense distinctions between CFAA violations and innocent conduct, the approach outlined above is fully consistent with the text of the CFAA.

As discussed, the CFAA does not define the term "authorization," nor does it specify the means by which authorization may be granted, extended, or revoked. This Court has held that "authorization" should be given its ordinary meaning: "permission or power granted by an authority." *Brekka*, 581 F.3d at 1133.

Nothing in the text of the CFAA requires that the only "authority" who has the ability to grant such "permission" is the owner of the relevant computer. This leaves open the possibility that a protected computer (or the information stored on it) may be subject to more than one "authority," so that multiple parties—including the computer owner and an authorized user—could each have the ability to grant permission to access the computer.

The CFAA's text also demonstrates that Congress specifically avoided imposing *per se* liability for using another party's credentials to access a protected computer. Section 1030(a)(6) of the statute makes it a crime for anyone to "knowingly and with intent to defraud traffic[] (as defined in section 1029) in any

password or similar information through which a computer may be accessed without authorization." 18 U.S.C. § 1030(a)(6). Under Section 1029 (which deals with fraud and related activity in connection with access devices), to "traffic" means to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." *Id.* § 1029(e)(5).

Section 1030(a)(6)'s narrow scope is notable: the provision proscribes only trafficking in passwords for fraudulent purposes—not receiving them or even using them to access a computer. *See, e.g.*, *State Analysis, Inc. v. Am. Fin. Servs. Ass'n*, 621 F. Supp. 2d 309, 317 (E.D. Va. 2009) (dismissing complaint alleging Section 1030(a)(6) claim where plaintiff had alleged only defendant's receipt and use of passwords). Congress chose not to proscribe *all* uses of another party's credentials to access a protected computer, but rather only those uses that were determined to be "without authorization," a term that the Congress left to the courts to interpret. As discussed below, the interpretations of this Court and lower courts in this Circuit support BSA's position that determining whether access is "without authorization" should require an assessment of the facts and circumstances surrounding the access at issue.

C. Permitting Certain Forms of Third-Party Access Using an Authorized User's Credentials Is Consistent with This Court's Decision in *Brekka*.

This Court's decision in *Brekka* also does not compel a *per se* approach to determining whether third-party access using an authorized user's credentials is "without authorization."

The district court below rejected Defendant's argument that, because a Korn/Ferry employee voluntarily shared her access credentials with the co-conspirators, those co-conspirators could not have acted "without authorization" when they allegedly accessed the Korn/Ferry network. In doing so, the district court relied on this Court's holding in *Brekka* "that it is the actions of the employer who maintains the computer system that determine whether or not a person is acting with authorization." 581 F.3d at 1135.

Read broadly, this passage in *Brekka* could stand for the proposition that the rights of an authorized user of a computer or network are irrelevant to the question of whether access is "without authorization" and that, instead, all that matters is whether the owner of the computer has in some way limited how others may access the computer (such as by using password protection).

However, the better reading of *Brekka* accounts for the fact that that case (like this case) centered on the issue of an *employee's* rights to access her *employer's* computer. *Brekka*'s approach makes sense in the employment context:

there, it is typical for only one party (the employer) to have the right to authorize access to the company's network. Both the network and the data stored on it are usually the employer's property, and the employee (or other network user) typically does not have a property interest in either. Viewed this way, it is reasonable that, in the employment context, only "the actions of the employer who maintains the computer system" would be relevant in determining whether access to a computer is authorized.

In other contexts, particularly those involving cloud-computing services, where the authorized user is actually the computer owner's *customer* and is often compensating that computer owner for such access (either by direct payment or otherwise), there may be more than one entity that has a legitimate need to control access to a computer or network, or to the data or other material hosted on that computer or network. In those scenarios, a more pragmatic approach to determining whether access is authorized—one that also takes into account the legitimate needs and interests of the authorized user—is appropriate. Because *Brekka*'s holding is specific to the employment context, such an approach would not conflict with this Court's holding in that case.

D. Lower Courts in This Circuit Are Already Employing a Similarly Pragmatic Approach to Determining Whether Access Is Authorized.

In decisions following *Brekka*, lower courts have approached the question of whether access to a computer was authorized by considering the facts and circumstances surrounding the access, consistent with the approach proposed here.

For example, in *Multiven, Inc. v. Cisco Systems, Inc.*, 725 F. Supp. 2d 887 (N.D. Cal. 2010), the district court, relying on *Brekka*, granted summary judgment to Cisco on its claim that a former employee violated Sections 1030(a)(4) and 1030(a)(5)(iii) of the CFAA by accessing Cisco's network using a current employee's credentials. Importantly, the court did not hold that the former employee's access was "without authorization" *per se*. Rather, the court considered the facts and circumstances surrounding the access, including whether the current employee had the right to authorize others to access Cisco's network. *See id*. at 892. Noting that it was "undisputed that [the current] employee's giving his login and password to [the former employee] was a violation of Cisco's policies," the court concluded that the current employee's "providing access . . . in this manner did not constitute a valid authorization." *Id*.

Other post-*Brekka* decisions involving whether access to a computer was "without authorization" also have treated the question as a fact-intensive one. *See, e.g.*, *NetApp, Inc. v. Nimble Storage, Inc.*, --- F.Supp.2d ----, 2014 WL 1903639,

at *9 (N.D. Cal. May 12, 2014) (rejecting defendant's contention that access "without authorization" requires circumvention of a technical barrier, and looking instead to other factors surrounding access); *Synopsys, Inc. v. ATopTech, Inc.*, 2013 WL 5770542, at *10 (N.D. Cal. Oct. 24, 2013) (noting that "a breach of a contractual provision may in some cases be enough to allege unauthorized access," but explaining that sufficient facts must be pled to determine whether breach constituted unauthorized access); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 968–70 (N.D. Cal. 2013) (considering plaintiff's statements to defendant regarding access as well as technical restrictions on access in determining complaint sufficiently alleged access "without authorization").

Such nuanced, fact-intensive inquiries as to authorization are both appropriate and necessary given the challenges of applying a decades-old criminal statute like the CFAA to the rapidly evolving technologies of the twenty-first century. As the ways in which people interact with computers—and in which computers interact with one another—continue to evolve, courts should approach the question of authorized access carefully, lest the law end up chilling innovation and investment in some of this century's most promising technologies.

CONCLUSION

For the foregoing reasons, BSA urges this Court to reject a rule that would automatically render a third party's access to a protected computer using an

authorized user's valid access credentials "without authorization" under the CFAA, and instead to adopt an approach that allows for legitimate, beneficial forms of such third-party access, particularly in the context of cloud computing.

December 9, 2014

Respectfully submitted,

COVINGTON & BURLING LLP

By: */s/ Simon J. Frankel*
Simon J. Frankel

Attorneys for *Amicus Curiae*
BSA | The Software Alliance

Of Counsel
Martin Hansen
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001

CERTIFICATION OF COMPLIANCE

I hereby certify that:

1. This brief complies with the type-volume limitation of Federal Rules of Appellate Procedure 29(d) and 32(a)(7)(B) because it contains 6,970 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii).

2. The brief further complies with the requirements of Rule 32(a)(5) and the type-style requirements of Rule 32(a)(6) because it has been prepared in a proportionately spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

December 9, 2014

COVINGTON & BURLING LLP

By: */s/ Simon J. Frankel*
Simon J. Frankel

Attorneys for *Amicus Curiae*
BSA | The Software Alliance

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on December 9, 2014.

Participants in the case are registered CM/ECF users and will be served by the appellate CM/ECF system.

December 9, 2014 COVINGTON & BURLING LLP

By: */s/ Simon J. Frankel*
Simon J. Frankel